UNIVERSIDAD TÉCNICA DEL NORTE

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

REDISEÑO DE LA RED DE DATOS Y OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: MORAN VELASCO JONATHAN MARCELO
DIRECTOR: ING. FABIÁN CUZME

IBARRA, 2016

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto repositorio digital institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad. Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición de la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003146451		
APELLIDOS Y NOMBRES:	Morán Velasco Jonathan Marcelo		
DIRECCIÓN:	Av. Sánchez y Cifuentes 22-38 y Tobías Mena		
EMAIL:	jm010190@hotmail.com		
TELÉFONO FIJO:	2600357	**TELÉFONO MÓVIL:**	0969900388

DATOS DE LA OBRA	
TÍTULO:	REDISEÑO DE LA RED DE DATOS Y OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ.
AUTOR (ES):	Jonathan Marcelo Morán Velasco
FECHA:	19/04/2016
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Fabian Cuzme

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, MORÁN VELASCO JONATHAN MARCELO, con cédula de identidad Nro. 100314645-1, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros

En la ciudad de Ibarra, abril de 2016

EL AUTOR:

Firma

Morán Velasco Jonathan Marcelo

C.I: 100314645-1

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Jonathan Marcelo Morán Velasco**, con cédula de identidad Nro. 100314645-1, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículo 4. 5 y 6, en calidad de autor de la obra o trabajo de grado denominado: **"**REDISEÑO DE LA RED DE DATOS Y OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ.", que ha sido desarrollado para optar por el título de: Ingeniera en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

EL AUTOR:

Morán Velasco Jonathan Marcelo
C.I: 100314645-1

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR

Certifico, que el presente trabajo de "**REDISEÑO DE LA RED DE DATOS Y OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ..**" fue desarrollado en su totalidad por la Sr. Jonathan Marcelo Morán Velasco, bajo mi supervisión.

Firma _____

Ing. Fabián Cuzme
DIRECTOR DE TESIS

AGRADECIMIENTO

Agradezco a Dios, por bendecirme y permitirme alcanzar este sueño tan anhelado.

A la Universidad Técnica del Norte, por darme la oportunidad de estudiar y ser un profesional.

A mi Director de tesis el Ing. Fabián Cuzme por su esfuerzo y dedicación, quien con su experiencia, conocimientos, paciencia y motivación permitió lograr culminar mis estudios con éxito.

Son muchas las personas que han formado parte de mi vida profesional a las que les encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

DEDICATORIA

Esta tesis se la dedico a mi Dios quien supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder la dignidad ni desfallecer en el intento.

Para mis padres por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles y por apoyarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia y coraje para cumplir mis objetivos.

A ti mi amor que te puedo decir, muchas gracias por estos cinco años de conocernos y estar conmigo y en los cuales hemos compartido tantas cosas, hemos pasado tanto que ahora estás conmigo en este día tan importante para mí solo quiero dar te las gracias por todo el apoyo que me has dado para continuar y seguir con mi camino.

JONATHAN

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

RESUMEN

El presente trabajo de titulación consiste en el rediseño de la red de datos y optimización de la seguridad perimetral en el “Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí” (GADMU) este permite mejorar el desempeño mediante la aplicación de un modelo jerárquico basado en el estudio por capas y la microsegmentación a nivel lógico de la red. Se comenzó con la recopilación de la información en base a aspectos relacionados a redes como: medios de transmisión, topologías de red, modelos de referencia, direccionamiento IP y tipo de vulnerabilidades, conjuntamente se obtuvo información sobre infraestructura del edificio principal (GADMU), sobre el cableado horizontal, cableado vertical, cuarto de telecomunicaciones, áreas de trabajo, puesta a tierra con la finalidad de determinar el estado de la red. Luego se planteó la utilización de un modelo jerárquico basado en dos capas: acceso y núcleo colapsado con el cual se estructura la nueva red, cada capa con las configuraciones respectivas para solucionar problemas en aspectos de: dominios de broadcast, fallos de enlace físicos, control de tráfico entre departamentos, logrando mejorar el rendimiento, flexibilidad y facilitando la administración. Para la parte lógica se hizo la microsegmentación se basa en: funciones de cada departamento, recursos que comparten los usuarios y se utilizó VLSM basado en la cantidad de usuarios, con lo cual se pretende mejorar la administración de la red. Para prolongar con la continuidad del servicio de red se utilizó dos equipos para tener redundancia y permite estar disponible en caso de tener fallas el enlace físicos o equipos de red. Para verificar su funcionamiento se realiza las simulaciones respectivas en GNS3 con el cual se pretende validar las configuraciones realizadas demostrando su operatividad. Se realizó un análisis de riesgos y vulnerabilidades mediante la metodología Margerit conjuntamente con la elección de equipo seguridad perimetral comparando JUNIPER y CISCO y determinando la mejor opción para su implementación. Mediante la norma ISO/IEC/IEEE 29148 se determina el sistema operativo para los servidores FTP y PROXY SQUID. Para determinar si el proyecto es factible se realiza un análisis costo/beneficio.

ABSTRACT

This work degree is redesigning the data network and optimization of perimeter security in the "Autonomous Government Decentralized Municipal of San Miguel de Urcuquí" (GADMU). This improves performance by implementing a hierarchical model based on the study by layers and microsegmentación logic level of the network. It started with the collection of information based on aspects related to networks such as streaming media, network topologies, reference models, IP addressing and type of vulnerabilities together information infrastructure of the main building (GADMU) was obtained on the horizontal wiring, vertical wiring, telecommunications room, work areas, grounding in order to determine the status of the network.

Access and core collapsed with which the new network structure, each layer with the respective configurations for troubleshooting issues: broadcast domains, failures physical link control using a hierarchical model based on two layers was then raised traffic between departments, achieving improved performance, flexibility and facilitate administration.

For logic became part microsegmentation is based on: functions of each department, users share resources and VLSM was used based on the number of users, which is intended to improve network management. Two computers for redundancy and allows be available in case of failure the physical link or network equipment used to prolong the continuity of network service.

To verify operation GNS3 the respective simulations with which it is intended to validate the settings made demonstrating its operation is performed.

An analysis of risks and vulnerabilities by Margerit methodology jointly choosing comparing perimeter security equipment JUNIPER and CISCO was made, determining the best option for implementation was performed. By ISO / IEC / IEEE 29148 standard, the operating system for FTP and SQUID PROXY servers is determined. To determine whether the project is feasible a cost / benefit analysis is performed.

CAPÍTULO I

1. ANTECEDENTES

1.1. PROBLEMA

El Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí (GADMU), cuenta con un diseño de red interna básica, deficiente, poco escalable y la cuál no ha sido planificada.

Se han presentado problemas de ciertos funcionarios que acceden a los archivos de departamentos, revisan la información y manipulan documentos importantes; el departamento financiero es el más comprometido debido a su información la cual debería ser confidencial.

En la red de datos del GADMU, se tiene una demora en la solución de problemas, como por ejemplo en la búsqueda de un punto de red dañando; debido al escaso registro de los mismos, ocurrido por la falta de un mapeo físico; provocando así no solo insatisfacción al personal laboral en el GADMU, sino también a la ciudadanía del cantón SAN MIGUEL DE URCUQUÍ, que visita las instalaciones en busca de algún servicio y no está disponible.

Así mismo la falta de un esquema de direccionamiento IP (Protocolo de internet), ha ocasionado que los servicios y recursos de red se encuentren en un mismo rango y cualquier persona que ingrese al servicio de internet tenga acceso a recursos restringido como la impresora, scanner entre otros.

De igual manera el crecimiento de la red ha ocasionado un bajo rendimiento, debido a la infraestructura de switches en cascada que se han venido colocando para solucionar el problema de escalabilidad, esto ha causado una baja

disponibilidad, desperdicio de recurso de ancho de banda, tormentas de broadcast, entre otros.

Otra problemática es la compartición de información; que realiza mediante la red, por lo cual empleados del establecimiento con un conocimiento más amplio en redes, manipulan fácilmente esta información, remplazando la IP de su equipo personal por la IP que deseen hacer daño obtenido un fácil acceso a los recursos, por estos motivos de desorganización de la red es muy fácil que personas tanto internas, como externas realicen manipulaciones indebidas.

Y por último el entretenimiento en redes sociales por parte de los funcionarios públicos en horas laborables provoca un bajo desempeño no adecuado en sus actividades laborables.

Debido a este problema se planteará un modelo adecuado que ayudará a organizar y optimizar la red de datos y la seguridad a la misma, limitando para que el tráfico se mantenga a nivel local y no se acceda a otros lugares, y principalmente reducir problemas de caídas de red.

Por otra parte se realizará un análisis de la situación actual de la red de datos actual, obteniendo información sobre los problemas que afronta la institución.

Para solucionar el inconveniente se realizará un mapeo de la red actual, consiguiendo distinguir a donde va dirigido cada punto de red del establecimiento, conjuntamente se llevará a cabo un direccionamiento VLSM (Longitud Variable de Máscara de Subred) eficiente, para evitar los desperdicios de direcciones IP. La red de datos del GADMU ha ido incrementando por el pasar de los años y ha causado problemas a los usuarios de la misma.

Es primordial reestructurar el diseño para solucionar problemas como: bajo rendimiento de la red, demora en solución de problemas, y lograr fácil acceso a recursos de la red, problemas de escalabilidad por no tener un modelo jerárquico entre otros y optimización de la seguridad perimetral.

1.1. OBJETIVOS

1.1.1. OBJETIVO GENERAL

Mejorar la red de datos y optimizar la seguridad perimetral del Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí, mediante un análisis de los problemas existentes en la red, logrando así mejorar su desempeño y seguridad de la información.

1.1.2. OBJETIVOS ESPECÍFICOS

- Fundamentar teóricamente los temas relacionados al tema propuesto y soluciones existentes para mejor comprensión del tema propuesto.

- Analizar la situación actual de la red de datos y las vulnerabilidades existentes, mediante un análisis físico, para establecer los requerimientos necesarios para el rediseño y optimización de la seguridad de la red.

- Determinar los componentes de red necesarios para elaborar una lista de equipos y marcas que se va a usar en el proyecto.

- Rediseñar la red de datos, mediante la aplicación de un modelo jerárquico para facilidad de diseño y confiabilidad de la red.

- Configurar los servidores FTP (File Transfer Protocol) y PROXY SQUID, mediante el uso de la norma IEEE-STD-830-1998 para seleccionar los requerimientos de software que se van a usar los servidores y de esta manera poder administrar y controlar el flujo de datos que se transmiten.

- Simular la red, mediante el uso de GNS3, para aplicar configuraciones, servidores y poder verificar su funcionamiento.

- Analizar tipos de tecnologías UTM, mediante la investigación de las marcas más actuales en el mercado y los más reconocidos, comparándolos y determinando el mejor de acuerdo a parámetros como: capacidad, costos, entre otros; para optimizar la seguridad perimetral del GADMU.

- Analizar el costo - beneficio que tendrá el proyecto en una implementación futura.

1.2. ALCANCE

Este proyecto consistirá en un rediseño de la red de datos y optimización de la seguridad perimetral para el edificio principal del GADMU, el cual consta de los siguientes departamentos: Planificación Territorial y Desarrollo, Servicios y Obras Públicas, Dirección Administrativa, Dirección Financiera, Comunicación, Auditoría, Fiscalización, Procuraduría, Secretaria General y Concejo Municipal.

El rediseño está conformado principalmente por un modelo jerárquico de red, servidor PROXY SQUID, servidor FTP y optimización de seguridad perimetral usando la tecnología UTM (Unified Thread Management).

Se realizará el levantamiento de información de la situación actual de la red, tomando en cuenta la topología y elementos existentes; logrando así determinar cómo se encuentra la red de datos del edificio principal de la institución mencionada, por lo cual es necesario revisar aspectos como: estructura lógica de la red, la cantidad de usuario que existen, la función que cumple cada departamento, ubicación, estado de los puntos de red, el tipo de amenazas de la red y su origen, vulnerabilidades.

Se va a realizar el dimensionamiento de equipos activos, se calculará el número de usuarios y dispositivos proyectados en la red considerando su crecimiento, con este resultado se obtendrá la cantidad de switches en la capa acceso, además para

calcular la demanda de tráfico actual y futuro se ejecutará un análisis de las diferentes aplicaciones y servicios que puede usar el usuario, esto determinará la velocidad y tipo de puertos en el acceso. Para la conexión hacia la capa de distribución se lo realizará mediante el cálculo de la velocidad de puertos up-link tomando en cuenta parámetros anteriores como número de puertos del switch de acceso y velocidad de puertos.

Y por último en capa núcleo se analizará la cantidad y tipo de puertos, para los enlaces con los equipos de acceso, servidores, interconexión entre switches y se analizará parámetros como la topología y tipos de procesamientos en los equipos a utilizarse en esta capa.

Para el rediseño se usará un modelo jerárquico, su proceso será el siguiente: en la capa acceso se brindará la conexión con el usuario final, por tanto se aplicará VLAN´S para cada uno de los departamentos, se ejecutará el direccionamiento IP mediante el método VLSM, asimismo para prevenir los cambio de direcciones IP en los equipos personales se aplicará el control de acceso mediante MAC(Media Access Control), con esto mejorará la seguridad ya que los paquetes enviarán la información sólo la dirección MAC correspondiente, el tráfico que genere los servidores puede saturar los buffer, por lo cual es necesario habilitar el protocolo de control de agregación de enlace (LAPC) para balancear la carga, esto mejorará el aprovechamiento de ancho de banda.

Para la capa distribución se manejará el enrutamiento inter-vlans, se tomará en cuenta que al intervenir con la capa núcleo es importante que se tenga un enlace redundante en caso de fallo del enlace mediante el protocolo de árbol de expansión (Spanning Tree Protocol) se utilizará PSTV+ para cada VLAN , además se configurará listas de control de acceso, para administrar a las redes internas aplicando reglas como: solo administradores pueden ingresar a un modo privilegiado, solo usuario de la establecimiento tengan acceso a los recursos. Para la capa núcleo se realizará la habilitación del protocolo de árbol de expansión STP, logrando que se active enlace redundante en caso de alguna falla.

Los servidores se lo implementarán en máquinas virtuales en el software Virtualbox debido a que es un software amigable, ligero, gratuito, fácil de instalar.

Se configurará un servidor Proxy que bloqueará mediante IP y dominio; no se bloqueará por tiempo ya le que la empresa necesita conexión continua del servicio de internet. Se bloqueará puertos que faciliten la vulnerabilidad de la empresa, además se bloqueará contenido prohibido y páginas que cause distracción a los usuarios. Además se controlará el acceso al servidor de transferencia de archivos (FTP) hacia todas las máquinas de la institución, consiguiendo que cada departamento acceda a la información independientemente.

Para la selección del sistema operativo de los servidores antes mencionados se realizará un análisis de la norma IEEE-STD-830-1998 (Práctica Recomendada para la Especificación de Requerimientos de Software) esta específica: los requerimientos, funcionalidades y restricciones del sistema operativo a utilizar, por tanto se conseguirá elegir un sistema operativo estable, robusto, con suficientes funcionalidades para satisfacer las necesidades del proyecto.

Se va a diseñar la red en el simulador de redes GNS3 ya que este software permite asociar máquinas virtuales, IOS y simulaciones más reales; con esto se pretende verificar el funcionamiento del diseño propuesto.

Se va a realizar un estudio de la tecnología UTM, determinando marcas en el mercado reconocidas de estos equipos para revisar sus características, costos y determinar la opción más factible que la institución deberá optar.

Para una implementación futura se analizarán los costos que tendrá el proyecto para su desarrollo y se determinarán variables que ayuden a verificar que el proyecto es beneficioso.

1.3. JUSTIFICACIÓN

La realización de este proyecto se va a realizar con la finalidad de contribuir al desarrollo social de la empresa del cantón SAN MIGUEL DE URCUQUÍ, logrando que el beneficiario directo sea el ciudadano, al recibir un servicio mejorado y eficiente por parte de las áreas que están ligadas directamente con ellos, cumpliendo así con la misión y visión de la Universidad Técnica del Norte.

El proyecto del rediseño lógico e implementación de servidores basado en software libre, ayudará al GADMU a una disminución de los tiempos en resolver problemas en caso de fallas, con la ayuda del etiquetamiento y mapeo físico; además se corregirá falencias de seguridad sobre datos almacenados, así se disminuirá las posibilidades de que ocurran daños de información, se optimizará la seguridad perimetral y el ancho de banda según la necesidades de los departamentos, evitando el uso excesivo en páginas no autorizadas por el personal establecimiento; se corregirá problema de inactividad de la red mediante un modelo jerárquico, es decir que un daño en una parte de la red, no ocasione daño a la red completa. Se mejorará el rendimiento, eliminando los tráficos innecesarios en la red, logrando que los empleados y ciudadanía estén satisfecha por el servicio que se ofrece con la prestación de servicios eficientes.

En el proyecto mediante el uso de un diagrama de la red ayudará a solucionar lo más rápido posible, cuando surja un problema de inactividad de la red, además se realizara VLAN´S para que los datos no se crucen entre departamentos, evitando que eliminen la información importante. Además al separar las redes en 3 niveles, la red será más fácil de diseñar, implementar, mantener y escalar la red, la hace más confiable.

La implementación de un servidor PROXY SQUID ayudará a administran los accesos provenientes de internet hacia la red privada, es decir el bloqueo páginas de internet que distraen a los empleados de la institución, permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados. El servidor FTP es un protocolo de transferencia de ficheros entre sistemas conectados a una

red TCP (Protocolo de control de Transmisión) basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar ficheros desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo, con el conocimiento adquirido en la carrera se pondrá solución al problema, afrontando los obstáculos y los inconvenientes que este nos presente, además de adquirir nuevas experiencias y conocimientos que fortalecerán mis habilidades y desempeño laboral.

CAPÍTULO II

2. FUNDAMENTO TEÓRICO

En este capítulo se detalla: conceptos, características, elementos y funcionamiento de temas importantes y netamente vinculados para el desarrollo del proyecto propuesto. Se describe conceptos importantes de seguridad perimetral, cableado estructurado, rediseño de red, servidores, entre otros.

2.1. CONCEPTOS BÁSICOS DE REDES

Es importante comenzar una revisión de términos mínimos para sentar las bases mínimas para desarrollar el proyecto. Entre algunos conceptos importantes se encuentran los siguientes:

2.1.1. QUE ES UNA RED

Stalling (2011) afirma que “Una red de telecomunicaciones es un conjunto de medios técnicos instalados, organizados, operados y administrados con la finalidad de brindar servicios de comunicaciones a distancia”.

Una red es un conjunto de computadoras (dos como mínimo), que se unen a través de medios físicos (hardware) y lógicos (software), para compartir información y recursos, con el fin de llevar a cabo una actividad o labor de forma eficiente y eficaz.

2.1.2. IMPORTANCIA DE LAS REDES DE DATOS

Las redes de datos son importantes, con ellas todo usuario puede transmitir su información; además provee una comunicación fácil, rápida y eficiente. Una de las ventajas de implementar una red es el ahorro de tiempo en el transporte de datos o información entre terminales (computadoras, equipos de red, entre otros). Sin una red simplemente no hay comunicación.

2.1.3. TOPOLOGÍAS DE RED

"Una topología se define como el mapa físico o lógico de una red para intercambiar datos" (Stalling, 2011). Las topologías físicas se basa en la forma de cómo los equipos se encuentran conectados, entre algunos tipos se encuentran: topología tipo bus, topología estrella, topología anillo, entre otras. La topología lógica de una red es la forma en que los equipos se comunican a través del medio, los dos tipos de topología más comunes son: topología broadcast[1], topología por transmisión de tokens[2].

La red de datos actual del GAD Municipal de Urcuquí, trabaja con una red tipo estrella extendida, y para el rediseño de la misma, se mantendrá la topología, por lo que a continuación se detalla una breve descripción de la misma.

2.1.3.1. Estrella Extendida

Santana, & Santos, (2013), hace mención a "La topología en estrella tiene un menor costo de instalación, ademas ofrecen una disponibilidad aceptable siempre que la caída no sea en el nodo central, en cuyo caso la caída sería total."

[1] (TOPORED, 2016). En la topología de broadcast simplemente cada host envía sus datos hacia todos los demás hosts del medio de red.
[2] (TOPORED, 2016). La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir.

Todos los dispositivos (usuario final y red) se encuentran conectados a un punto central. La función de esta topología es replicar los datos a todos los dispositivos conectados a ella; su principal desventaja es la propagación de los dominios de difusión (broadcast). En la Figura 1, se aprecia un ejemplo de la topología estrella extendida.

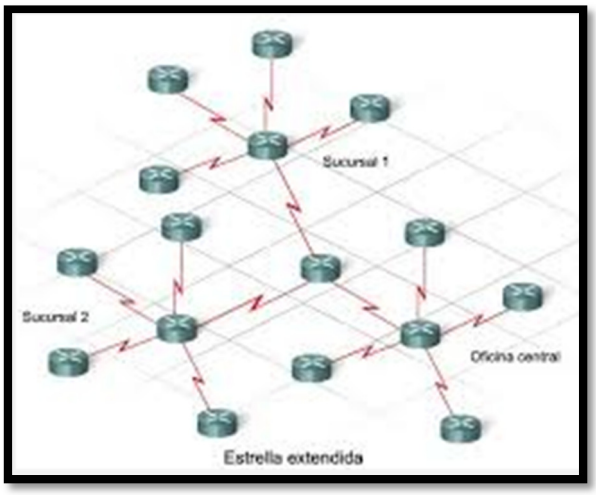

Figura 1. Topología de red estrella extendida

Referencia: http://topologias4conalep.blogspot.com/p/topologia-en-estrella-y-estrella.html

2.1.4. CLASIFICACIÓN DE LAS REDES

Las redes de ordenadores se pueden clasificar según la escala o el grado del alcance de la red, por ejemplo: red personal del área (PAN), red de área local (LAN), red de área metropolitana (MAN) y red de área amplia (WAN).

A continuación se describe brevemente algunas características de las redes LAN, debido a que en proyecto a realizar se basará en este tipo de red.

2.1.4.1. Redes LAN

Las redes LAN, según Stalling, W. (2011) hace referencia a que este tipo de redes permiten la interconexión desde unas pocas hasta miles de computadoras en

la misma área de trabajo como por ejemplo un edificio. Son redes pequeñas con un alcance aproximado de 200m.

2.2. DISPOSITIVOS DE UNA RED DE DATOS

Los dispositivos de red de datos, se clasifican en dos grupos: dispositivos de usuario final y dispositivos de red.

2.2.1. DISPOSITIVO DE USUARIO FINAL

Los dispositivos de usuario final son aquellos que brindan un servicio al usuario como impresoras, computadores, escáner, entre otros. Según Andreu, (2014) estos dispositivos son conocidos como host y permiten imprimir, escanear, enviar correos, obtener información de bases de datos, entre otros; sus capacidades son muy limitadas sino son conectadas con la red.

2.2.2. DISPOSITIVOS DE RED

Andreu, (2014), describe que los dispositivos de red se encargan de transportar datos a los dispositivos de usuario final, cada uno tiene capacidades diferentes, como la administración, control y manejo de la información. Estos dispositivos proveen comunicación entre dispositivos de usuarios finales, como switch, router. A continuación, se describen algunos dispositivos de red.

2.2.2.1. Servidores

“El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona un software; una máquina cuyo propósito es proveer datos de modo

que otras máquinas puedan utilizar esos datos.” (Marin, 2012). En la Figura 2, se puede apreciar algunos servidores.

Figura 2. Servidores de red

Referencia: http://www.inforsys.com.ec/index.php/renta-de-productos/alquiler-de-servidores.html

2.2.2.2. Router

El router es un dispositivo de red, que se encarga de controlar y administrar la conexión de varios segmentos de red. Trabajan a nivel de capa de red, ya que decide la línea de sus datos en base a una IP y su tabla de ruteo. El router también es denominado gateway, ya que se encarga de limitar lo que entra y sale de la red, Gutierrez, (2016) establece: “Éste dispositivo de red tiene la función de asegurar que los mensajes lleguen a su destino en una forma rápida y segura.” En la Figura 3, se puede apreciar un router de la marca Cisco series 881.

Figura 3. Router Cisco series 881

Referencia: http://www.ebay.es/itm/Cisco-cisco887va-m-k9-Antigua-800-887va-m-Ver-15-1-4-M4-de-servicios-integrados-Router-/300970959540

2.2.2.3. Switch

El switch es un dispositivo que permite interconectar redes LAN a nivel de capa enlace, un switch forma un dominio de broadcast y cada uno de sus puertos forman un dominio de colisión, de tal manera que si se administra se puede mejorar el rendimiento y seguridades en la red. En la Figura 4, se puede apreciar un tipo de Switch Cisco 2290 de 24 puertos.

Figura 4. Switch Cisco 2960 – 24 puertos

Referencia: http://www.cisco.com/c/en/us/support/switches/catalyst-2960-24tt-l-switch/model.html

2.2.2.3.1. Tipos de switch

Existe una enorme variedad de switch, con características y prestaciones muy dispares. Estos equipos pueden clasificarse en: switch capa 2 y switch capa 3, entre otros.

A continuación se detallan algunos conceptos, características y principalmente las diferencias entre cada uno de ellos.

- Switch capa 2

Son switches tradicionales o también conocidos como conmutadores, que funcionan como puentes multi-puertos. Su función principal es la de dividir una LAN en varios dominios. Los conmutadores de capa 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes.

- Switch capa 3

Según Benavides, (2013) hace meción “Los switches cumplen funciones tradicionales de la capa 2 e incorporan algunas funciones de routing, como por ejemplo la determinación de un camino basado en informaciones de capa de red y soporte a los protocolos de routing tradicionales (RIP, OSPF, entre otros)”.

Los conmutadores de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.

Permiten la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la LAN, debido a la cantidad excesiva de usuarios.

Como se había mencionado anteriormente, el switch es el encargado de encaminar los datos de un segmento de red a otro. Dentro del estudio de las funcionalidades y características básicas de un switch capa 3, se debe tomar en cuenta las siguientes:

- ACL (Access List Control)

ACL o también conocidas como listas de control de acceso, son básicamente un conjunto de comandos, agrupados por un número o nombre que se utiliza para filtrar el tráfico de entrada o salida de una interfaz.

- VTP (Vlans Trunking Protocol)

VTP o Protocolo del tronco de VLAN, reduce la administración en una red conmutada. Cuando se configura una nueva VLAN en un servidor VTP, la VLAN se

distribuye a través de todos los switches en el dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo propietario de Cisco que está disponible en la mayoría de los productos de la serie Cisco Catalyst. VTP opera de tres maneras diferentes: VTP Server, VTP cliente y VTP transparente.

- HSRP (Hot Standby Router Protocol)

HSRP es un método estándar de Cisco de proveer una alta disponibilidad de la red al proporcionar redundancia de primer salto de hosts IP. Andreu, (2014) menciona que HSRP permite a un conjunto de interfaces del router para trabajar juntos para presentar la apariencia de un único router virtual o puerta de enlace predeterminada a los hosts en una red LAN.

Cuando HSRP está configurado en una red o segmento, se proporciona una dirección virtual de control de acceso al medio (MAC) y una dirección IP que es compartida entre un grupo de routers configurados.

- ETHERCHANNEL

ETHERCHANNEL es una tecnología Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

- VLAN (Virtual Local Area Network)

“Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física” (Benavides, 2013).

Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

2.3. MEDIOS DE TRANSMISIÓN

"El medio de transmisión constituye el canal de transmisión de información entre dos o más terminales. La transmisión se la realiza por medio de una señal electromagnética que se propagan a través del canal. Para la transmisión a veces se usa un canal físico o guiado y otras veces no, es decir no guiado." (NOGUERA & VÁSQUEZ, 2011, pág. 150).

2.3.1. MEDIOS DE TRANSMISIÓN GUIADOS

Los medios guiados son aquellos que necesitan de un medio físico para poder realizar las transmisiones y recepciones de datos, existen algunos medios físicos como: cable coaxial, cable UTP, fibra óptica.

2.3.2. MEDIOS DE TRANSMISIÓN NO GUIADOS

Los medios no guiados son aquellos que no necesitan de un medio físico para realizar las transmisiones de datos, es decir las ondas generadas viajan libremente por el aire.

2.4. MODELOS DE COMUNICACIONES

El modelo de comunicaciones se dividen en dos arquitecturas de redes muy importantes: Modelo OSI y Modelo TCP/IP

2.4.1. MODELO DE REFERENCIA OSI

La ISO (International Standards Organization) propuso un modelo de referencia adaptable a todos los sistemas informáticos, los sistemas que acojan esta arquitectura se llamaran “sistemas abiertos”, estos permiten la comunicación con otros sistemas. En la Figura 5 se muestra como los modelos de referencia OSI se divide en siete capas.

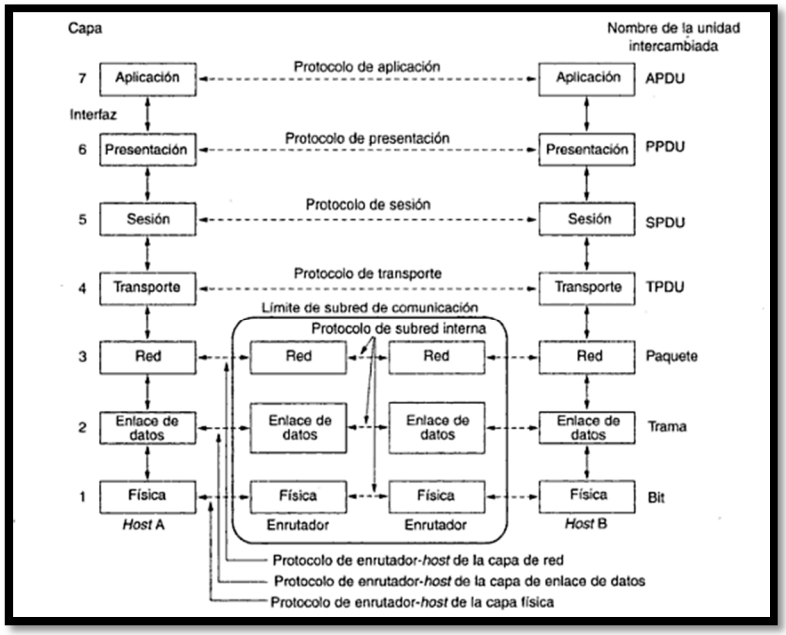

Figura 5. Modelo de Referencia OSI

Referencia: (Tanenbaum, 2011)

A continuación, se detallan las capas del modelo OSI con una breve explicación de cada una de ellas:

2.4.1.1. Capa física

En esta capa, se analiza la transmisión de bits puros, a través del canal de comunicación y verifica que el bit enviado llegue a su destino.

2.4.1.1.1. Características mecánicas, eléctricas, funcionales y de procedimiento

- **Características mecánicas:** definen características físicas del elemento de conexión con la red como: tipo de cable, conectores, número de pines del conector.

- **Características eléctricas:** definen la forma que se representan los bits y su forma de transmisión ejemplo: tensiones, velocidades de transmisión.

- **Características funcionales:** indican la función que cada uno de los circuito de la interfaz física, por ejemplo el pin X es trasmisión y de pin Y es de recepción.

- **Característica de procedimiento**: son pasos a realizarse para la trasmisión de información a través del medio.

2.4.1.1.2. Errores de transmisión

"Todo medio de trasmisión se encuentra expuesto a errores, a este se introducen varios contaminantes de la señal los más comunes son: Distorsión, Interferencia, Ruido, Atenuación, Diafonía" Tanenbaum, (2011).

2.4.1.1.3. Modos de transmisión

La comunicación depende del sentido de la trasmisión los más comunes son los siguientes modos Simplex, Half dúplex y Full dúplex.

2.4.1.2. Capa Enlace

“La función principal de esta capa es convertir los datos que ingresa al medio de transmisión a una línea de código, esto se consigue porque el emisor fragmenta lo datos que ingresan en tramas de datos, si el receptor recibe la trama sin errores, confirma con una trama” (Tanenbaum, 2011, pág. 29).

Es la primera capa lógica, ya que maneja un direccionamiento físico, control, detección de errores, integridad de los datos.

2.4.1.2.1. Direccionamiento MAC

Todo computador forma parte de la red, los cuales poseen una interfaz que le permite transferir datos, esta interfaz es la tarjeta NIC, la cual tiene su dirección MAC, cada computador tiene su dirección de MAC única. Tanenbaum, (2011) hace referencia a que la IEEE tiene los registros de tarjetas de red y les asigna un identificador organizativo único, se conforma de 48 bits es representado en 12 dígitos hexadecimales.

2.4.1.2.2. Entramado

Los datos que se encuentran en la capa enlace son fragmentados y se agrupa en una trama, estos contiene información de control al inicio y al final para evitar errores en la trasmisión.

2.4.1.2.3. Subcapas de la capa enlace

Se divide en dos subcapas: LLC, MAC; en la Tabla 1 se explican se explican características relevantes de las mismas.

Tabla 1. Características de subcapas de la capa enlace

LLC	MAC
Su función principal es brindar un direccionamiento lógico, control de flujo, control de errores.	Responsable en él envió de los paquetes al medio físico.
Proporciona un interfaz común, único entre las capas superiores y la subcapa MAC.	Definidos en la IEEE 802.3, 802.4, 802.5.
Definido por la IEEE 802.2	Utiliza el direccionamiento físico.
	La trama LLC forma parte de la trama MAC.

Nota: LLC (Link Logical Control) y MAC (Media Access Control), son subcapas de la capa enlace, tomadas como referencia de (Willian, 2011).
Referencia: Elaboración propia

2.4.1.2.4. Tecnologías IEEE 802x

Ruiz, (2015), describe ha 802.x como una tecnología IEEE, que especifica formas de acceso al medio, como diferentes formas de transmisión. A continuación se explica la Redes Ethernet/ IEEE 802.3, referenciadas por el autor:

- Originalmente se basa en el acceso múltiple, por escucha de portadora y detección de colisión CSMA/CD. Utilizado en tráfico pesado, o altas velocidades de transmisión.

- En CSMA/CD el canal se está censando hasta que cuando la estación se encuentre libre para transmitir, caso contrario seguirá esperando hasta poder trasmitir.

- Es similar a 802.3 – 10 BASE 5, se conecta al inicio un transeiver (llamado MAU) y al final se encuentra una tarjeta de red.

- Cuando dos estaciones trasmiten al mismo tiempo se produce una colisión, entonces se envía una señal de alerta, para que las demás estaciones dejen de trasmitir.

En la tabla 2 se especifica la clasificación de los tipos medios físicos definidos 802.3 para ser utilizado en tecnologías Ethernet.

Tabla 2. Clasificación de redes Ethernet

VELOCIDAD	METODO DE SEÑALIZACION	MEDIO
10	Base	2
100	Broad	5
1000		-T
10 Gb		-TX

Referencia: Elaboración propia basado en (Arteaga, 2010)

2.4.1.3. Capa red

Esta capa se encarga del enrutar los paquetes, preocupándose que el paquete llegue al destino, además tiene la responsabilidad evitar colisiones y de brindar un servicio sin retardo e inestable.

2.4.1.4. Capa transporte

"La función de esta capa es recibir la información de capas superiores y asegura que la información llegue al otro extremo. Asegura que los datos llegue sin errores hacia el destino y permite el ensamblado y desensamblado de los segmentos de capa sesión hacia capa de red, su comunicación es extremo a extremo" (Tanenbaum, 2011, pág. 40).

2.4.1.5. Capa sesión

Esta capa permite que usuarios de diferentes computadoras establezcan, administren y finalizar sesiones.Ofrece servicios control de dialogo, administración de tokens y sincronización.

2.4.1.6. Capa presentación

En esta capa se define la sintaxis y semántica de la información transmitida, con el fin de comunicar computadoras con diferentes representaciones de datos.

2.4.1.7. Capa aplicación

“Contienen varios protocolos el más utilizado es el protocolo HTTP, su funcionamiento se basa cuando un navegador necesita una página web, este protocolo envía a un servidor el nombre de la página, y este lo devuelve con la información requerida, algunos protocolos utilizados son: correo, transferencia de archivos y noticias” (Tanenbaum, 2011, pág. 41).

2.4.2. MODELOTCP/IP

Este modelo es el más utilizado en la actualidad, maneja la misma lógica del modelo OSI, en la Figura 6 se visualiza las capas de los dos modelo de red.

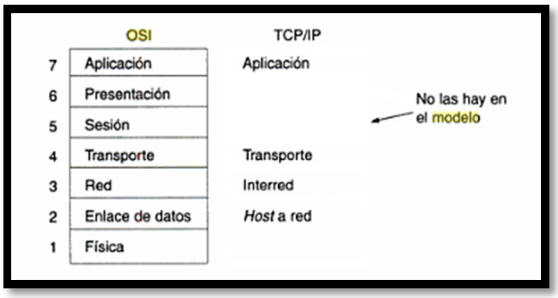

Figura 6. Modelos de referencia

Referencia: (Tanenbaum, 2011)

Este modelo se divide en cuatros capas: Host a red (acceso a la red), Interred (internet), transporte, aplicación. A continuación se detalla cada una de las capas

2.4.2.1. Capa de acceso a la red

"Se encuentra debajo de la capa internet, según en esta capa está conformado por la capa física y capa enlace de datos y abarca todos los aspectos que requiere un paquete IP para realizar un enlace físico" (Quilca, 2011).

2.4.2.2. Capa internet

Esta capa tiene un propósito importante de recibir todos los paquetes que envían los host y verifica que lleguen al destino independientemente de la ruta, se encarga de realizar enrutamiento de paquetes evitando las congestiones. Quilca, (2011) dice que es responsable de procedimientos de conmutación de paquetes y la elección de la mejor ruta, los protocolos utilizados en esta capa son IP, ARP, RARP.

2.4.2.3. Capa transporte

Esta capa permite la comunicación extremo a extremo, se utiliza dos protocolos (TCP y UDP). TCP es un protocolo confiable y orientado a conexión, cuando una máquina envía datos se verifica que estos lleguen sin errores. UDP es un protocolo no confiable y no orientado a conexión, cuando una máquina envía estos no se verifican si llegaron sin errores, utiliza la ley del menor esfuerzo.

2.4.2.4. Capa aplicación

La capa aplicación, maneja varios protocolos TELNET, FTP, SMTP, DNS entre otros, los cuales interactúan con el usuario mediante una computadora.

En la figura 7 se especifica en donde se ocupa cada protocolo y la herramienta para su configuración.

Protocolo	Programa	Ejemplo
SMTP	Correo electrónico	Server Pro
FTP	Transferencia de archivos	Filezilla
Telnet	Cliente/servidor	Telnet
SSH	Navegación	puTTY
SNMP	Gestión	SNMP JManager
TFTP	Transferencia de archivos	TFTPDWIN

Figura 7. Puertos para cada protocolo

Referencia: http://nabilyacobi.blogspot.com/2010/10/protocolos-tcpip-utilizados-en-la-capa.html

2.5. DIRECCIONAMIENTO IP

Andreu, (2014) define a una dirección IP como un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, Tablet, Laptop, Smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. En la Figura 8, se muestra las clases de direcciones IP existentes, los rangos de cada una, y las aplicaciones:

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación
* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.					

Figura 8. Clases de Direcciones IP

Referencia: (Tanenbaum, 2011)

2.6. SEGURIDAD PERIMETRAL

Las redes de comunicación de las empresas al momento de conectarlas a la Internet han sido objeto de ataques de piratas cibernéticos, para acceder a la información o denegar los servicios que se presten dentro de la red.

Aguilera, (2014), menciona que la seguridad de los datos que se cursan dentro, desde y hacia una red informática es la principal preocupación de un administrador de red, es por ello que se deben implementar métodos de seguridad para evitar ataques, intrusos e información que puedan alterar el correcto funcionamiento de la red, para ello está la seguridad perimetral de la red.

2.6.1. DEFINICIÓN DE LA SEGURIDAD PERIMETRAL PARA LA RED DE DATOS

"La seguridad perimetral basa su filosofía en la protección de todo sistema informático de una empresa desde "fuera" es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red". Taboada, Eduardo. (2005).

2.6.2. OBJETIVOS DE LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS

La implementación de un sistema de seguridad perimetral ayuda a la protección de la red contra los ataques internos y externos de la misma, pero para ello se han planteado los siguientes objetivos que debe cumplir este sistema:

- Proporcionar mayor productividad a los usuarios de la red interna, permitiendo acceder y visitar sitios seguros en la Internet y además que se asocien al ambiente laboral y no al de entretenimientos y esparcimiento.

- Proteger los equipos de red y host debido que la mayoría de las amenazas provienen de la Internet, efecto de cómo interactúan los usuarios con la misma.

- Detectar los equipos con presencia de virus y usuarios que están usando programas maliciosos.

- Optimizar el uso de la Internet para el trabajo de los usuarios de la red, administrando su capacidad y velocidad para cada uno de ellos.

- Simplificar la conectividad segura hacia la red desde sucursales vía VPN.

2.6.3. REQUISITOS DE LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS

Según Mora, (2016). “Una técnica de seguridad informática es un mecanismo o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático”, por lo tanto los requisitos que se deben cumplir en un sistema de seguridad perimetral, a más de los que se señalan en la cita, son los siguientes: identificación, autenticación, control de acceso, disponibilidad, confidencialidad, integridad y responsabilidad.

2.6.3.1. Identificación

Se denomina identificación a la verificación al momento en que el usuario se da a conocer al sistema.

2.6.3.2. Autentificación

Se denomina autenticación a la verificación de que el individuo que se ha identificado al sistema, es seguro.

2.6.3.3. Control de Acceso

Se denomina control de acceso a la administración correcta de los usuarios que acceden a los servicios de una red, mientras que a los usuarios seguros se les da el acceso necesario a los usuarios maliciosos se les deniega el acceso.

2.6.3.4. Disponibilidad

Se denomina disponibilidad a que los servicios que se ofrecen dentro de la red, estén operativos el 100% del tiempo, y en caso de fallas tengan una tiempo de recuperación rápida.

2.6.3.5. Confidencialidad

Se denomina confidencialidad a la protección de la información que los usuarios seguros cursan dentro de la red de datos ante usuarios no autorizados.

2.6.3.6. Integridad

Se denomina Integridad a la protección de los datos y transmisiones contra las alteraciones no autorizadas o accidentales que puedan ocurrir dentro de la red.

2.6.3.7. Responsabilidad

Es realizar un seguimiento y almacenamiento de todas las actividades seguras, accidentales y no autorizadas que se den dentro de la red, tanto por los usuarios seguros como usuarios maliciosos.

2.6.4. TIPOS DE VULNERABILIDADES

Las vulnerabilidades, son también denominadas como puntos débiles que pueden afectar u ocasionar riegos en cuanto se refiere a seguridad, entre algunas vulnerabilidades se encuentran: vulnerabilidades físicas, naturales, de hardware y software, medios de almacenamiento, humanas, entre otros.

2.6.4.1. Vulnerabilidad física

Los puntos débiles de orden físico son aquellos presentes en ambientes en los cuales la información se está almacenando o manejando. Como ejemplo de este tipo de vulnerabilidades se tiene:

- Instalaciones inadecuadas del espacio de trabajo.
- Ausencia de recursos para el combate a incendios.
- Disposición desorganizada de cables de energía de res
- Ausencia de identificación de personas.

Estos puntos débiles, al ser explotados por amenazas, afectan directamente los principios básicos de la seguridad de la información, principalmente la disponibilidad.

2.6.4.2. Vulnerabilidades naturales

Los puntos débiles naturales son aquellos relacionados con las condiciones propiamente de la naturaleza y pueden colocar en riesgo la información. Muchas veces, la humedad, el polvo y la contaminación podrán causar daños a los equipos, por eso deben estar protegidos para garantizar su funcionamiento. Entre las amenazas más comunes se puede citar:

- Ambientes sin protección contra incendios

- Locales próximos a ríos propensos a inundaciones
- Infraestructura incapaz de resistir manifestaciones de la naturaleza como terremotos.

2.6.4.3. Vulnerabilidades de hardware

Los posibles defectos de los fabricantes o configuraciones de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos. Entre algunos puntos débiles de hardware se puede mencionar:

- Conservaciones inadecuadas de equipos.
- Ausencia de actualizaciones conforme con las orientaciones de los fabricantes de los programas que se utilizan.

Por lo mismo la seguridad informática busca buscar evaluar algunos factores principales, para no tener estas vulnerabilidades, a continuación se describen algunos:

- Si el hardware utilizado está dimensionado correctamente para sus funciones.
- Si posee áreas de almacenamiento suficientes, procesamiento y velocidad adecuados

2.6.4.4. Vulnerabilidades de software

Los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red. Estas vulnerabilidades podría ser explotadas por diversas amenazas, entre ellas está:

- Configuraciones e instalaciones indebidas de los programas de computadora, que podrán llevar al uso abusivo de los recursos por parte de usuarios mal intencionados.

2.6.4.5. Vulnerabilidad de medios de almacenamiento

Los medios de almacenamiento son soportes físicos o magnéticos donde se puede almacenar información, por ejemplo: CD, discos duros, entre otros. Si estos medios de almacenamiento no se utilizan de manera adecuada, el contenido en los mismos podrá estar vulnerable a una serie de factores que podrían afectar la integridad, disponibilidad y confidencialidad de la información.

2.6.4.6. Vulnerabilidad humana

Este tipo de vulnerabilidad, está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta. Estas debilidades pueden ser intencionales o no. Entre algunos puntos débiles se puede mencionar:

- Falta de capacitación específica para la ejecución de actividades.
- Vandalismo
- Estafas
- Invasiones

2.7. UTM (UNIFIED THREAT MANAGEMENT)

Cameron, Voodberg, Giecco, Berhard & Quinn (2010) afirman que “UTM o Gestión de Amenazas Unificadas es un conjunto de características diseñadas para proporcionar la inspección de capa de aplicación, del tráfico que atraviesa una red. Al igual que en la detección y prevención de intrusiones (IDP por sus siglas en

inglés), los dispositivos de seguridad que admiten características UTM descifran e inspeccionan los protocolos de capa superior para detectar tráfico malicioso o simplemente no reconocido."

Las principales características que debe tener y cumplir el Gestor de Amenazas Unificadas son:

- Cumplir con las funciones de un Firewall
- Filtrar correo, anti spam
- Detección y bloqueo de malware
- Filtrar contenido WEB y URL
- Prevención y Detección de Intrusos, IDS e IPS
- Soporte de VPN y SSL

Gracias a la gran escalabilidad que posee el sistema UTM, el progreso de las tecnologías de seguridad han llevado a los Gestores de Amenazas Unificadas a un nuevo nivel conocido como XTM o Extensible Threat Management que es la nueva generación en gestores de amenazas. Los XTM a más de tener las funciones y características básicas de los UTM desarrollan nuevas aplicabilidades de seguridad, entre las que se puede destacar:

- Implementación de seguridad en mensajería.
- Prevención de pérdida de datos.
- Gestión centralizada mediante interfaces gráficas.
- Autenticación de usuarios de la red automáticamente.
- Monitorización de los eventos de la red.

2.7.1. VENTAJAS

La implementación de un sistema centralizado de seguridad como lo es el UTM, tiene muchas ventajas descritas a continuación:

- **Complejidad reducida:** como UTM es una mescla de todos los productos, esto simplifica la selección de productos, la integración de los productos y el continuo apoyo hacia los mismos.

- **Facilidad de implementación:** los productos de la UTM pueden ser fácilmente instalados y mantenidos. Todos estos productos se pueden acceder a través de sistemas remotos.

- **Flexibilidad:** UTM es flexible, con grandes y centralizados firewalls basados en software.

- **Mínima interacción del operador:** UTM reduce los casos de llamadas de auxilio del sistema y mejora la seguridad. Se utiliza un enfoque de caja negra para limitar el daño relacionado con los dispositivos de red.

CAPÍTULO III

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1. INTRODUCCIÓN

En este capítulo realiza el levantamiento de información de la red en el Gobierno Autónomo Municipal Descentralizado de San Miguel de Urcuquí (GADMU), con sus topologías (lógica y física) y equipos actuales para tener una idea clara del estado actual de la red, para ellos se debe tener consideración en aspectos como: cableado estructurado, estado de equipos red, entre otros.

3.2. ANTECEDENTES

El GADMU, se encuentra en el cantón Urcuquí en la provincia de Imbabura; esta institución actúa como facilitador de los esfuerzos de la comunidad con el objetivo de planificar, ejecutar, generar y distribuir el uso de los servicios que hacen posible la realización de sus aspiraciones sociales.

3.2.1. VISIÓN

La visión del GAD Municipal Urcuquí es, “Tener un cantón democrático, participativo, incluyente, transparente, ecológico, equitativo y solidario, que impulse el desarrollo humano, productivo y agroindustrial mediante asesoría, transferencia de tecnología y gestión para acceder a nuevos mercados. Que facilite y preste servicios públicos de calidad, construido e incluido en el contexto nacional y mundial”, según se describe en el sitio web URCUQUI, (2016).

3.2.2. MISIÓN

La misión del GAD Municipal Urcuquí dice: “Es un organismo autónomo, desconcentrado y descentralizado que impulsa el desarrollo social, étnico, cultural, económico y ético del cantón, que coordina y facilita los esfuerzos y talentos humanos, mediante la planificación, organización, dirección y control de los procesos político administrativos orientados a satisfacer las aspiraciones y necesidades ciudadanas. Ser actores sociales con el cambio del cantón, generando junto al pueblo propuestas, proyectos y programas que mejoren su calidad de vida sobre el respeto y fortalecimiento de la identidad cultural. Promover e incentivar los espacios de participación ciudadana y sus organizaciones de manera positiva, cuidando su ambiente, en procura de satisfacer las necesidades del cantón.” (URCUQUI, 2016).

3.2.3. ORGANIGRAMA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ

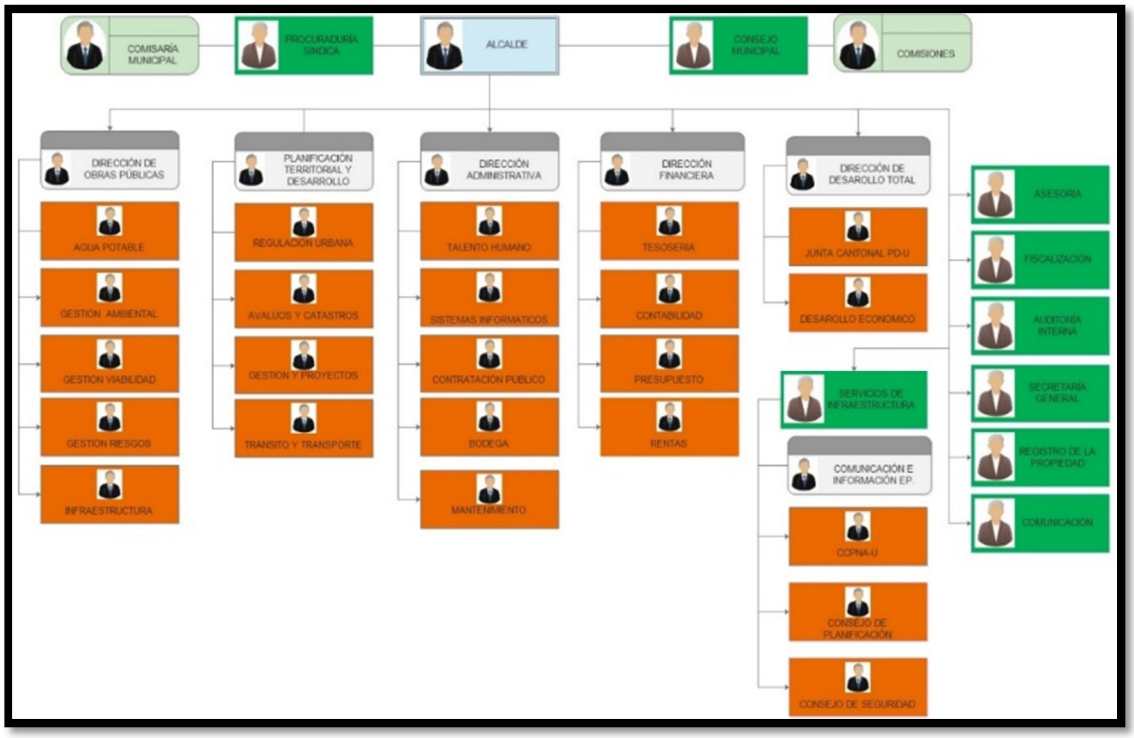

Figura 9. Organigrama actual del GADMU

Referencia: Elaboración propia basado en el organigrama actual del GADMU.

En la figura 9, se indica el organigrama de los departamentos que existen en el GADMU.

3.3. LEVANTAMIENTO DE INFORMACIÓN EN EL EDIFICIO PRINCIPAL DEL GADMU

El GADMU, se encuentra en el centro de la ciudad entre las calles Guzmán y Antonio Ante, al frente del parque central de San Miguel de Urcuquí, ubicado estratégicamente al alcance de todos los pobladores.

Las instalaciones de la institución tienen aproximadamente un uso de 10 años a partir de su construcción. El problema radica con el aumento de la utilización de las TICS (Tecnologías de la Información y Comunicación), esto ha obligado a que la infraestructura de red se adapte a los requerimientos demandando nuevos puntos de red para la prestación del servicio. Por ende es necesario que se realice un estudio que permita identificar el estado actual de la red y sus requerimientos en cuanto a servicios y seguridad de la misma.

En la Figura 10, se visualiza los cables en el suelo sin ninguna protección, junto a estos se encuentran fuentes de energía en funcionamiento, causando una degradación del rendimiento de la red.

Figura 10. Cableado estructurado en el cuarto de telecomunicaciones

Referencia: Fotografía propia

En la Figura 11, se observa dos patch panel de 48 puertos, estos distribuyen el cableado estructurado a los diferentes departamentos del GADMU, esta imagen indica como los cables se encuentran acumulados sin cumplir con la norma ANSI/TIA/EIA-569-A, que indica la forma de estructurar los cables en un cuarto de telecomunicaciones.

Figura 11. Patch panel 48 puertos ubicado en el cuarto de telecomunicaciones

Referencia: Fotografía propia

En la Figura 12, se indica el estado del rack, el cual está ubicado en el cuarto de telecomunicaciones y contiene dos patch paneles, un router cisco 881 y cables de red (Categoría 5e) acumulados en el piso, sin ninguna protección afectando la disponibilidad de la red.

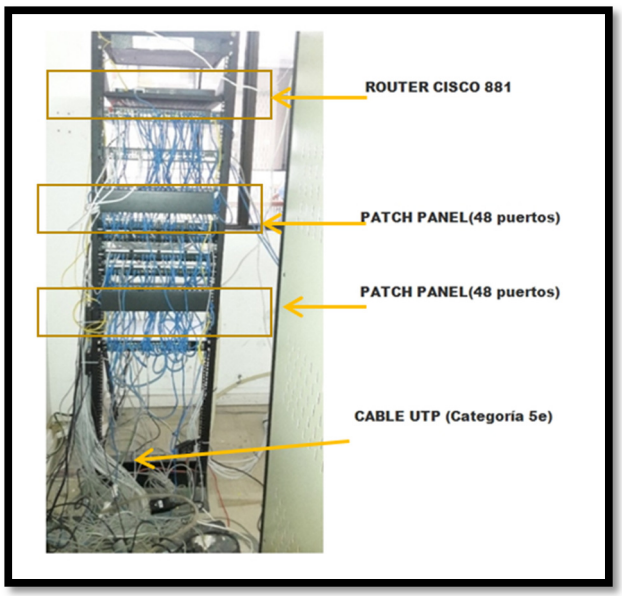

Figura 12. Rack ubicado en el cuarto de equipos vista frontal

Referencia**:** Fotografía propia

En la Figura 13, se observa los cables de red sin cubierta plástica y enredada con los cables de energía, ocasionando la inestabilidad del servicio de red en el departamento de agua potable.

Figura 13. Cableado estructurado en el departamento de agua potable

Referencia: Fotografía propia

En la Tabla 3, se específica el número total de puntos de red de cada piso junto a sus respectivos departamentos.

Tabla 3. Distribución total de puntos de red por cada piso

PLANTAS	DEPARTAMENTOS	PUNTOS DE RED
PRIMERA PLANTA	Recepción Recaudación Rentas Avalúos y catastros Talento humano Obras públicas Fiscalización Agua potable Planificación Auditoria interna Tránsito y transporte Bodega	60

PLANTAS	DEPARTAMENTOS	PUNTOS DE RED
SEGUNDA PLANTA	Secretaría general Sala de sesiones Gestión administrativa Desarrollo social y comunicaciones Financiero Tesorería Contabilidad Sistemas informáticos Salón máximo Procuraduría sindica	33
TERCER PLANTA	Gestión y proyectos	7
	TOTAL	**100**

Referencia: Elaboración propia basada en información del departamento del área de sistemas

En la Tabla 4, se detalla los puntos de red que se encuentran en los departamentos exteriores asociados al GAD Municipal de San Miguel de Urcuquí.

Tabla 4. Detalle de puntos de red de dependencias externas

DEPENDENCIA EXTERNA	PUNTOS DE RED
Plaza de buen vivir	8
Unidad desarrollo social	10
Biblioteca	5
Mantenimiento	2
TOTAL	**25**

Referencia: Elaboración propia basada en información del departamento del área de sistemas

En resumen, el GADMU tiene 125 puntos de red distribuidos entre las dependencias externas e internas.

3.3.1. CABLEADO ESTRUCTURADO

Dentro del levantamiento de información para el cableado estructurado se consideró los siguientes elementos: subsistema horizontal, subsistema vertical, cuarto de equipos, áreas de trabajo, sistema de puesta a tierra.

3.3.1.1. Levantamiento de información del subsistema horizontal

El subsistema horizontal va desde el área de trabajo hasta el armario de telecomunicaciones. En el GADMU se obtuvo la siguiente información:

- La edificación no cuenta con un subsistema horizontal.
- La instalación se realizó mediante la perforación de los pisos para dar el servicio de internet a cada área de trabajo.
- El cableado estructurado en su gran mayoría se encuentra con cable UTP categoría 5e. En los departamentos recaudación, rentas y sistemas informáticos, se encuentra instalado categoría 6.
- No utiliza ductos para guiar el cable de red hacia las respectivas áreas de trabajo.
- No tiene bandejas metálicas para evitar daños en los cables de red.

La norma ANSI/EIA/TIA 568-A (Estándar de Edificios Comerciales para Cableado de Telecomunicaciones), recomienda los parámetros necesarios para un correcto subsistema horizontal **(VER ANEXO A)**.

3.3.1.2. Levantamiento de información del subsistema vertical

La función principal del armario de telecomunicaciones es concentrar las terminaciones de todo tipo de cable horizontal reconocido por el estándar. En el GADMU se obtuvo la siguiente información:

- En la edificación no cuenta con un subsistema vertical.

- El cable es atravesado hacia otros departamentos mediante hoyos taladrados en la pared.

- El subsistema vertical se instaló con cable categoría 5e.
- Los enlaces de backbone no cuentan con ningún tipo de protección a lo largo de su recorrido.

- No se utiliza escalerillas verticales para guiar el cable de red hacia el cuarto de telecomunicaciones.

La norma ANSI/EIA/TIA 569-A (Estándar de Edificios Comerciales para Recorridos y Espacios de Telecomunicaciones), recomienda los parámetros necesarios para un correcto subsistema vertical **(VER ANEXO A)**.

3.3.1.3. Levantamiento de información del cuarto de telecomunicaciones

El cuarto de telecomunicaciones debe ser capaz de albergar equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. En el GADMU se obtuvo la siguiente información:

- Corporación Nacional de Telecomunicaciones provee el servicio de internet, el cual llega mediante fibra óptica al cuarto de telecomunicaciones.

- Cuenta con un rack principal que contiene dos patch panel para albergar los cables de datos, además contiene un ODF (Organizador de fibra óptica) el cual suministra el servicio de internet al router CISCO 881 y router Mikrotik routerboard 750, los cuales está conectado a dos switch cisco SG 200-50.

- Contiene un gabinete donde se alojan dos servidores HP PROLIANT E5649 no operativos, cada equipo con sus respectivos UPS (Uninterruptible power

supply), estos se encuentran bajo llave y es administrado solo por el jefe de área sistemas.

- No posee seguridad para acceso al cuarto de telecomunicaciones, solo es manejado mediante una simple cerradura.

- Posee un equipo de ventilación que se encuentra dañado.

- Cuenta con dos lámparas fluorescentes, no muy adecuadas para el trabajar.
- Contiene una caja para alojar cables electricidad y se encuentra en mal estado.

La norma ANSI/EIA/TIA 569-A (Estándar de Edificios Comerciales para Recorridos y Espacios de Telecomunicaciones), recomienda los parámetros necesarios para un correcto cuarto de telecomunicaciones **(VER ANEXO A)**.

3.3.1.4. Levantamiento de información de las áreas de trabajo

Son los espacios dónde se ubican los escritorios de los usuarios y son lugares habituales para los empleados. En el GADMU se obtuvo la siguiente información:

- En el 40% de las áreas de trabajo, los puntos de red se encuentran en mal estado. Para la instalación de puntos de red en las áreas de trabajo se ocupó la norma ANSI/EIA/TIA 568B y la etiquetación de los mismos se encuentra en la mayoría de las áreas de trabajo, excepto en los nuevos puntos de red que se instalaron recientemente.

- En los departamentos de fiscalización, financiero, obras públicas los puntos de red se encuentran sin flaceplate.

La norma ANSI/TIA/EIA-606 (Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales e incluye estándares para la

rotulación del cableado), recomienda los parámetros necesarios para una correcta instalación en las áreas de trabajo. En el **ANEXO A**, se indica la norma a cumplir para solucionar los problemas con el cableado estructurado de todos los subsistemas del GADMU.

3.3.1.5. Levantamiento de información de la red de internet

La velocidad de transmisión es 12 [Mbps] de subida y 16 [Mbps] de bajada. CNT presta los equipos activos de red como: router cisco 881 y el routerboard 750 que enrutan datos hacia los respectivos departamentos los cuales se conectan a los switch SG 200-50 y estos distribuyen el servicio de internet a los departamentos en funcionamiento en el GADMU.

3.3.1.6. Levantamiento de información del subsistema de puesta a tierra

Cuenta con un sistema puesta a tierra centralizado por una varilla de cobre, que se encuentra ubicada enterrada en los exteriores del edificio del GADMU.

La norma ANSI/EIA/TIA- J-STD-607-A (Requerimientos de puesta a tierra para la infraestructura de telecomunicaciones en edificios comerciales), recomienda los parámetros necesarios para un correcto subsistema de puesta a tierra.

En el **ANEXO A**, se indica dicha norma a considerar para solucionar los problemas identificados en el cableado estructurado del GADMU.

3.3.2. EQUIPOS ACTIVOS

A continuación se presentan los equipos activos que se encuentran en cada piso de las instalaciones, de los cuales algunos se encuentran en uso y otros no.

3.3.2.1. Primer piso

En la tabla 5, se especifican los equipos existentes en el primer piso detallando: su marca, descripción y su estado.

Tabla 5. Equipos primera planta del GADMU

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCIÓN	ESTADO
2	SWITCH	D-LINK DES-1024D	24 puertos 10/100 Mbps	OPERATIVO
1	ROUTER INALÁMBRICO	TP-LINK	2,4 Ghz - 802.11 a/g	OPERATIVO
1	BIOMETRICO	WALDSO		OPERATIVO

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.3.2.2. Segundo piso

En la tabla 6 se especifican los equipos utilizados en el segundo piso detallando: su marca, descripción y el estado de equipo.

Tabla 6. Equipos de la segunda planta del GADMU

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCIÓN	ESTADO
1	SWITCH	D-LINK DES-1024D	24 puertos 10/100 Mbps	OPERATIVO
1	SWITCH	CISCO	SG 200-50	OPERATIVO
1	ROUTER	CISCO	CISCO 881	OPERATIVO
1	TRANCEIVER	HUMANITY	10/100 BASE –TX & 100 BASE FX CONVERTER	OPERATIVO
1	ROUTER	TRENDNET	TK-409	OPERATIVO
1	ROUTER	MIKROTIK	ROUTERBOARD 750	OPERATIVO
1	SWITCH	HP 5130	SERIES SWITCH JG934	NO OPERATIVO

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCIÓN	ESTADO
3	UPS	TRIPP-LITE	APC 1500VA 120 W	NO OPERATIVO
1	UPS	SMART UPS	APC 1500VA 120 W	OPERATIVO
1	ROUTER	D-LINK	2,4 Ghz - 802.11 a/g	OPERATIVO
1	UPS	APC	BACK UPS PRO 1500	OPERATIVO

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

Con el levantamiento de información del segundo piso se obtuvo información sobre los servidores, en la tabla 7 se explica cada equipo con su respectiva marca y su función que cumple en el GAD Municipal de San Miguel de Urcuquí.

Tabla 7. Servidores implementados en el GADMU

CANTIDAD	EQUIPO	SISTEMA OPERATIVO	DESCRIPCIÓN	ESTADO	FUNCIÓN
1	HP	CENTOS 5.5	PROLIANT E5649	NO OPERATIVO	PROXY
1	HP	CENTOS 6.5	PROLIANT ML170	OPERATIVO	CORREO
1	HP	CENTOS 6.5	PROLIANT ML170	OPERATIVO	WEB

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.3.2.3. Tercer piso

En la tabla 8, se especifican los equipos utilizados en el tercer piso detallando: su marca, descripción y el estado de equipo.

Tabla 8. Equipos de la tercera planta del GADMU

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCIÓN	ESTADO
1	SWITCH	D-LINK DES-1024D	24 puertos 10/100 Mbps	OPERATIVO

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.4. ESQUEMA DE TOPOLOGÍA DE RED

El esquema actual de topología de red, se encuentra dividida en dos partes: física y lógica.

3.4.1. TOPOLOGÍA LÓGICA

La topología lógica del GADMU es de tipo bus Ethernet, ya que todos los dispositivos se encuentran conectados por un mismo medio.

En la tabla 9 se explica características lógicas que se obtuvo de la recopilación de información.

Tabla 9. Características lógicas del GADMU

TECNOLOGIA	VELOCIDAD DE TRANSMISION	TIPO DE CABLE	DISTANCIA MAXIMA	TOPOLOGIA
100BaseTX	100 Mbps	Par trenzado(Cat. 5e UTP)	100 M	Estrella-Full Dúplex(Switch)

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.4.2. TOPOLOGÍA FÍSICA

Se basa en una topología de estrella extendida, ya que todos los switch se encuentran conectados a un nodo central.

En la figura 14 se visualiza la topología física actual que se encuentra implementada en el GAD Municipal de San Miguel de Urcuquí.

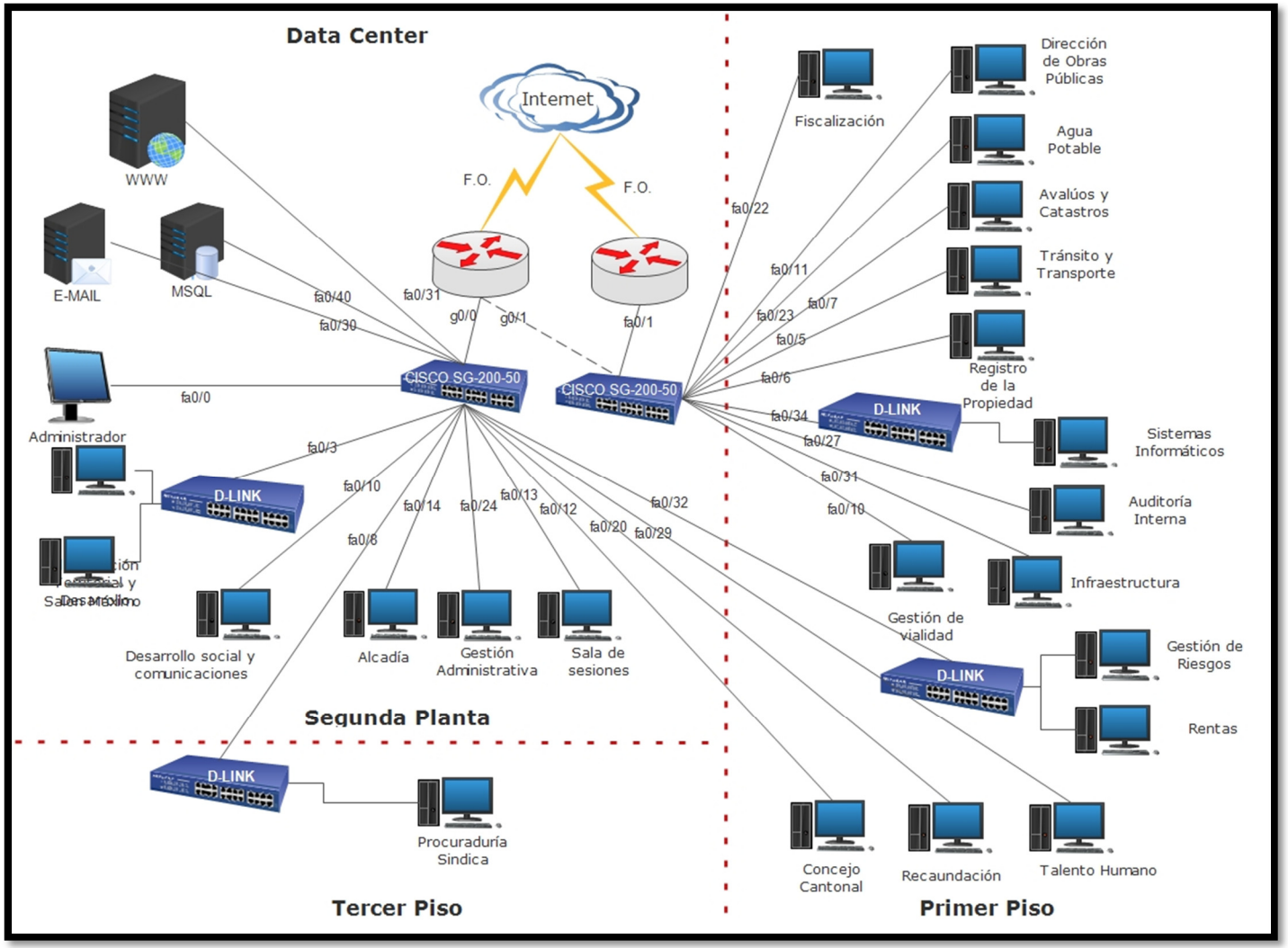

Figura 14. Topología física

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.5. PLANOS DEL EDIFICIO

Dentro del levantamiento de los puntos de red existentes, se elaboró los planos arquitectónicos utilizando la herramienta AUTOCAD. Para lo cual los símbolos a utilizarse que identifican a puntos de red y cableado estructurado. Se detallan en la tabla 10.

Tabla 10. Símbolos utilizados en el cableado estructurado

SIMBOLO	SIGNIFICADO	# DE PUNTOS DE RED
	PUNTOS DE RED	100
	CABLEADO ESTRUCTURADO (Cat. 5e)	

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.5.1. PRIMER PISO

En la figura 15, se muestra el plano del primer piso con su respectiva ubicación de los puntos de red.

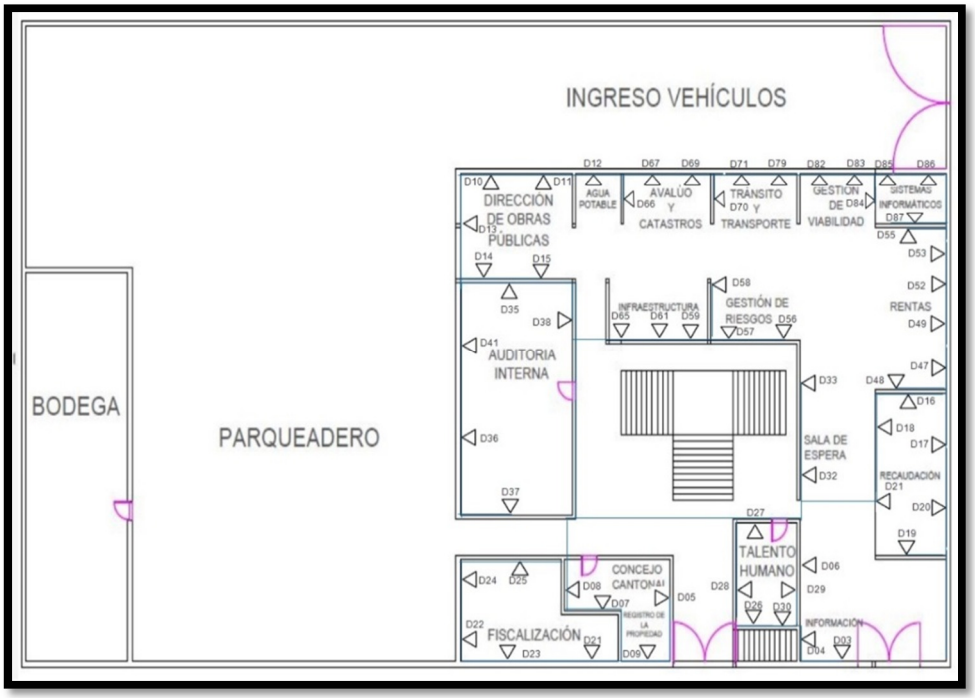

Figura 15. Planos de la planta baja del edificio Principal

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

Adicionalmente, en la tabla 11 se detalla los puntos de red del primer piso.

Tabla 11. Puntos de red en la primera planta del GADMU

	DEPARTAMENTOS	**PUNTOS DE RED**
102	Recaudación	6
103	Rentas	6
104	Avalúos y Catastros	3
105	Talento Humano	5
106	Obras Públicas	5
107	Fiscalización	5
108	Agua Potable	1
109	Consejo Cantonal	3
110	Auditoría Interna	5
111	Tránsito y Transporte	3
112	Registro de la Propiedad	1
113	Agua Potable	1
114	Gestión de Vialidad	3
115	Sistemas Informáticos	3
116	Gestión de Riesgos	3
117	Infraestructura	3
	Información	3
	Sala de espera	5
TOTAL		60

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.5.2. SEGUNDO PISO

En la figura 16, se muestra el plano del primer piso con su respectiva ubicación de los puntos de red.

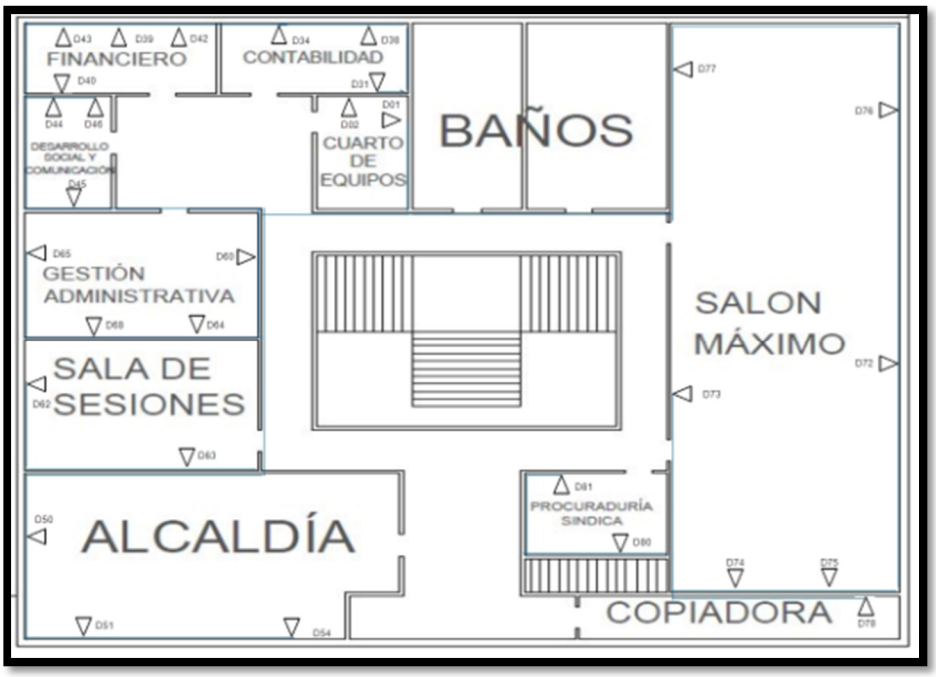

Figura 16. Planos del primer piso del edificio Principal

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

En la tabla 12, se muestran los puntos de red del primer piso que anteriormente se mostraron en el plano de la figura 16.

Tabla 12. Puntos de red de la segunda planta

OFICINA	DEPARTAMENTOS	PUNTOS DE RED
201	Alcaldía	3
202	Copiadora	1
203	Sala de Sesiones	2
204	Gestión Administrativa	3
205	Desarrollo social y Comunicación	3
206	Financiero	4
207	Financiero	4
208	Contabilidad	4
209	Cuarto de Telecomunicaciones	2
210	Salón Máximo	6
211	Procuraduría Sindica	2
	Total	33

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

3.5.3. TERCER PISO

En la figura 17, se muestra el plano del primer piso con su respectiva ubicación de los puntos de red.

Figura 17. Planos del segundo piso del edificio Principal

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

En la tabla 13, se muestran los puntos de red del primer piso que anteriormente se mostraron en el plano de la figura 17.

Tabla 13. *Puntos de red de la tercera planta*

OFICINA	DEPARTAMENTOS	PUNTOS DE RED
301	Desarrollo y Gestión de proyectos	7

Referencia: Elaborado por autor con información obtenida del edificio principal del GADMU

3.6. PARAMETROS A CONSIDERAR EN EL DESEMPEÑO DE LA RED

Para evaluar el desempeño de la red, según Fundamentos en seguridad de la información en redes, (2011) sugiere los siguientes parámetros: escalabilidad, disponibilidad, desempeño, dominio de broadcast, seguridad.

3.6.1. ESCALABILIDAD

Es importante considerar que el equipamiento que se manejará debe contar con características escalables en el tiempo, en el caso de aumentar el número de usuarios y de equipos de cómputo, con lo cual se garantizará un umbral de crecimiento de puertos Ethernet, velocidad de transmisión, entre otros.

3.6.2. DISPONIBILIDAD

En el GAD Municipal de San Miguel de Urcuquí no puede brindar una disponibilidad total a nivel de red debido a que:

La conexión tanto hacia la red de datos como de Internet depende de enlaces externos hacia el GADMU, los cuales no cuentan con canales redundantes, pudiendo ocasionar posibles caídas del servicio al presentarse algún fallo en el enlace.

A nivel de la red interna no se cuenta con enlaces redundantes hacia los principales equipos de conmutación por lo cual de producirse daños o problemas en su conexión la red quedaría parcial o totalmente fuera de servicio.

El equipamiento de red al no contar con un modelo por capas (núcleo y distribución) no cuentan con redundancia, por lo cual de presentarse algún

problema en alguno de ellos se interrumpiría el servicio de red de manera parcial o total.

Además se puede evidenciar que:

- Existe un solo servidor de base de datos que no está configurado en alta disponibilidad, es decir no tiene clúster.

- En el cuarto de telecomunicaciones se encuentran cuatro UPS, logrando asegurar su operatividad por un lazo de tiempo.

3.6.3. DOMINIO DE BROADCAST

En el GADMU los departamentos: sistemas informáticos, gestión de riesgos, rentas, procuraduría sindica, salón máximo utilizan switches en cascada, ocasionan que los switches del cuarto de telecomunicaciones se saturen y colapsen por él envió constante de dominios de broadcast.

3.6.4. SEGURIDAD

Para determinar la seguridad en el GADMU se debe considerar lo siguiente:

- Al no establecer políticas de seguridad los usuarios pueden dañar información importante sin recibir ninguna sanción al respecto.

- Al no existir esquemas de microsegmentación de red y ACLs para restringir el tráfico inter-vlans, este se encuentra abierto para el acceso de los recursos de diferentes departamentos.

- Al no disponer de equipos de seguridad con equipos Firewall UTM, Active director y es complejo brindar protección a la red.

CAPÍTULO IV

4. REDISEÑO LÓGICO DE LA RED DE DATOS

4.1. INTRODUCCIÓN

En este capítulo se elabora el rediseño lógico de la red de datos del GADMU, mediante aspectos importantes como: la proyección del crecimiento de la red, acceso a aplicaciones para cada punto de red, dimensionamiento de equipos de red y la nueva propuesta para las topologías lógicas y física.

Luego se realiza sus configuraciones respectivas basado en el modelo jerárquico y conjuntamente para su comprobación se utiliza la herramienta simuladora de redes GNS3 ya que cumple con funcionalidades similares a switches a elegir.

4.2. ANÁLISIS DE REQUERIMIENTO

Para este análisis es indispensable examinar parámetros como: la proyección del crecimiento de puntos de red, el acceso aplicaciones de manera que este sea funcional. A continuación se explica cada uno de ellos:

4.2.1. ESTUDIO DE LA PROYECCIÓN DEL CRECIMIENTO DE LA RED

Según la información brindada por el departamento de Sistemas, a través del administrador de la red el ingeniero Mario Farinango, en el GADMU no existe un crecimiento de personal, ya que el número de plazas de trabajo es fijo y la mayoría de trabajadores han permanecido fijos al pasar de los años.

Pero el uso de las TIC`S ha demando la instalación de puntos de red sin ninguna planificación, afectado la infraestructura del GADMU. Se estima para el próximo año un incremento aproximado de 148 puntos de red, este crecimiento es para los equipos de red (servidores, computadoras, impresoras, scanner, entre otros).

Mediante la ecuación 1, se determina el crecimiento anual de puntos de red.

$$Tasa\ de\ crecimiento\ anual = \frac{Total\ puntos\ de\ red_n - \ Total\ puntos\ de\ red_{n-1}}{Total\ puntos\ de\ red_n} * 100\%$$

Ecuación 1. Fórmula para la tasa de crecimiento

Referencia: Recuperado de (Vinueza, 2014)

Donde:

n: es el año a elegir:

Para realizar los cálculos de proyección primero se debe especificar el incremento de los puntos de red al pasar de los años; esta información se obtuvo mediante el departamento de sistemas informáticos desde el 2012 hasta la fecha actual. En la tabla 14 se indica esta búsqueda.

Tabla 14. Información de los puntos de red en los últimos 5 años

AÑOS	PUNTOS DE RED
2012	55
2013	75
2014	95
2015	115
2016	125

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

Como ejemplo para determinar el crecimiento anual entre el año 2015 y 2016, se lo realiza mediante la ecuación 1 y la información de la tabla 14 mediante lo siguiente:

$$Tasa\ de\ crecimiento\ anual = \frac{125 - \ 115}{115} * 100 = 8{,}00$$

Ecuación 2.Fórmula para la tasa de crecimiento remplazada con los datos obtenidos en el GADMU

Referencia: Recuperado de (Vinueza, 2014)

Tabla 15. Cálculo de porcentaje del crecimiento anual de puntos de red

AÑOS	TASA DE CRECIMIENTO ANUAL
2012-2013	26,67%
2013-2014	21,05%
2014-2015	17,39%
2015-2016	8,00%
Promedio	18,28%

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

En la tabla 15 se indica el porcentaje de crecimiento anual en los últimos 4 años, dando un promedio de 18,28%(crecimiento anual).Con este resultado se estima que para el próximo año se necesitará un total de 148 puntos de red.

4.2.2. ACCESO A APLICACIONES

En la tabla 16, se visualiza las aplicaciones que se encuentran operativas en el GADMU, entre las que; la aplicación de base de datos (SQL Sever) es la más crítica de acuerdo al administrador de red.

Tabla 16. Aplicaciones funcionales en el GADMU

APLICACIONES	
BASE DE DATOS	SQL Server
APLICACIONES UTILITARIAS	Microsoft Office 2003-2007 Adobe Reader 8 AutoCAD 2007-2009 Sistema de Información Geográfica

APLICACIONES	
APLICACIONES PARA UTILIZACIÓN DE EMPLEADOS	Patentes Catastros Cobros Contabilidad Inventario
SERVICIOS	Internet Correo Impresión en Red Acceso página Web

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

4.3. DIAGRAMA DE BLOQUES

En la figura 18 se indica el proceso para realizar el rediseño de la red de datos, en el cual se indica los pasos a seguir para la elaboración del proyecto.

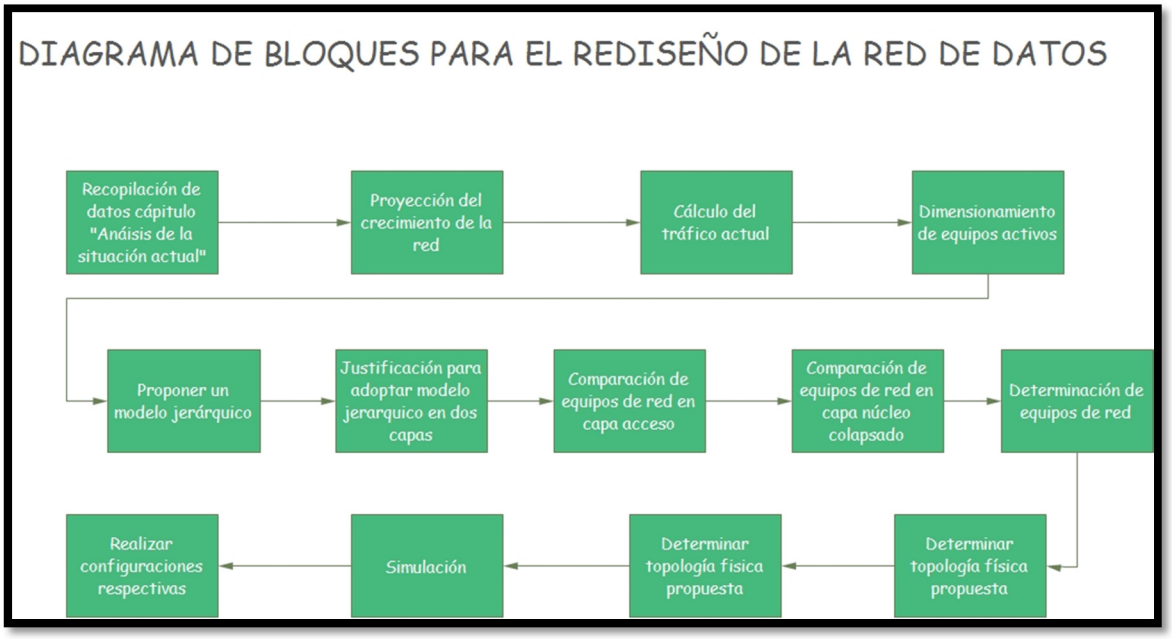

Figura 18. Diagrama de bloques

Referencia: Elaboración propia

4.3.1. CÁLCULO DE TRÁFICO DE SERVICIOS EXTERNOS E INTERNOS BRINDADO POR GADMU

Para el cálculo de tráfico se considera los siguientes servicios que brinda el GADMU: correo electrónico, base de datos, descarga de archivos, páginas web. A continuación se explica el cálculo de cada uno de estos servicios:

4.3.1.1. Tráfico de correo electrónico

El peso estimado de un correo electrónico interno es de 50 KB y si se considera que cada hora se revisa un mail, el cálculo es el siguiente:

$$AB(correo\ interno) = 1\ usuario \times \frac{50\ KB}{mail} \times \frac{1024\ bits}{1KB} \times \frac{2\ mail}{1\ hora} \times \frac{1\ hora}{60\ min} \times \frac{1\ min}{60s}$$

Ecuación 3. Fórmula para cálculo de ancho de banda del correo electrónico interno

Referencia: Recuperado de (Vasco, 2010, pág. 79)

Resultado es el siguiente: $AB(correo\ interno) = 22.44\ bps$

El correo electrónico externo 200 KB y si se considera que cada hora se revisa un mail.

$$AB(correo\ externo) = 1\ usuario \times \frac{200\ KB}{mail} \times \frac{1024\ bits}{1KB} \times \frac{2\ mail}{1\ hora} \times \frac{1\ hora}{60\ min} \times \frac{1\ min}{60s}$$

Ecuación 4. Fórmula para cálculo de ancho de banda del correo electrónico externo

Referencia: Recuperado de (Vannesa, 2012, pág. 80)

El resultado es el siguiente: $AB(correo\ externo) = 113.77\ bps$

4.3.1.2. Tráfico de la base de datos

La base de datos que tiene el GAD Municipal de San Miguel de Urcuquí es utilizada para almacenar y ordenar la información de sus empleados y la ciudadanía en general. Se estima un promedio de 125 computadoras en la institución, cada una en su departamento correspondientes, es decir que si todos usuarios se conectan a la base de datos simultáneamente cada media hora a la base de datos tiene un peso aproximado de 50 KB, el cálculo sería el siguiente:

$$AB = \frac{50\ KB}{usuario} \times \frac{1024\ bits}{1KB} \times \frac{1}{1hora} \times \frac{1\ hora}{3600s}$$

Ecuación 5. Fórmula para cálculo de ancho de banda del acceso a la base de datos interno
Referencia: Recuperado de: https://msdn.microsoft.com/es-es/library/ms175158(v=sql.120).aspx

El resultado es el siguiente: $AB = 14.22\ bps$

4.3.1.3. Tráfico de páginas web

Los usuarios internos utilizarán el servicio de internet, lo mismo que se estima que se accede un promedio 10 páginas por hora y cada página tiene un peso aproximado de 2 MB.

$$AB(web\ interno) = 1\ usuario \times \frac{2048\ KB}{1\ usuario} \times \frac{1024\ bits}{1\ KB} \times \frac{10\ paginas}{1\ hora} \times \frac{1\ hora}{3600\ s}$$

Ecuación 6. Fórmula para cálculo de ancho de banda del acceso a páginas web interno
Referencia: Recuperado (Mirrian, 2013, pág. 46)

El resultado es el siguiente: $AB(web\ interno) = 5{,}825.42\ bps$

Para acceso a la WAN se estima aproximadamente 3 MB.

$$AB(web\ externo) = \frac{3072\ KB}{1\ usuario} \times \frac{1024\ bits}{1\ KB} \times \frac{10\ paginas}{1\ hora} \times \frac{1\ hora}{3600\ s}$$

Ecuación 7. Fórmula para cálculo de ancho de banda del acceso a páginas web externo
Referencia: Recuperado (Mirrian, 2013, pág. 60)

El resultado es el siguiente: $AB(web\ externo) = 8{,}738.13\ kbps$

4.3.1.4. Tráfico de descarga de información de internet

El tamaño promedio de una descarga de internet es de 3MB; para una descarga de 1 MB el tiempo aceptable es 2 minutos. El cálculo será el siguiente:

$$AB = 1\ usuarios \times \frac{3MB}{usuario} \times \frac{1024\ kb}{1KB} \times \frac{1}{6\ min} \times \frac{1\ min}{60s}$$

Ecuación 8. Fórmula para cálculo de ancho de banda de las descargas de información de internet
Referencia: Recuperado (Soraya, pág. 155)

Resolviendo la ecuación (8) quedaría lo siguiente:

$$AB = 1\ usuarios \times \frac{3072\ KB}{usuario} \times \frac{1024\ bits}{1KB} \times \frac{1}{6\ min} \times \frac{1\ min}{60s}$$

El resultado es el siguiente: $AB = 8{,}738.13\ kbps$

En la tabla 17 se detalla los datos obtenidos de los cálculos realizados anteriormente para el tráfico interno por cada usuario en kbps.

Tabla 17. Demanda del tráfico actual

SERVICIOS INTERNOS	CAPACIDAD INDIVIDUAL (KBPS)
Correo Electrónico	0,22
Base de Datos	1,4
Descargas de información de internet	0,05
Acceso a páginas web	0,08
Total	1,75
Total en Mbps	0,001

Referencia: Elaboración propia

En la tabla 18, se detalla los datos obtenidos de los cálculos realizados anteriormente para el tráfico externo por cada usuario.

Tabla 18. Cálculo total de servicios internos

SERVICIOS EXTERNOS	CAPACIDAD INDIVIDUAL (KBPS)
Correo Electrónico	0,11
Acceso a páginas WEB	0,08
Total externo	0,19
Total interno	1,75
Total	1,56
Total en Mbps para cada empleado	0,15

Referencia: Elaboración propia

Por ende se determina que cada usuario necesita 0,15 Mbps y para los 125 usuarios simultáneamente es necesario una capacidad de 19 Mbps.

4.4. DIMENSIONAMIENTO DE EQUIPOS ACTIVOS

El dimensionamiento de equipos activos nos determina la cantidad de equipos de red que se debe utilizar en la capa acceso, mediante el siguiente procedimiento:

4.4.1. PROCEDIMIENTO PARA SWITCHES DE ACCESO

Este procedimiento se determina mediante el cálculo de: información de usuarios existentes, cantidad de usuarios proyectados, velocidad y tipo de puerto de acceso, velocidad de puertos up-link, capacidad de conmutación.

4.4.1.1. Información de usuarios existentes

En la tabla 19, se explica la distribución de los empleados que se encuentran por cada piso.

Tabla 19. Especificación de usuarios por pisos

PISOS	USUARIOS ACTUALES
En el piso 1	60 usuarios
En el piso 2	33 usuarios
En el piso 3	7 usuarios
Dependencias Externas	25 usuarios
TOTAL	125 usuarios

Referencia: Elaboración propia

4.4.1.2. Cantidad de usuarios proyectados

El número de switches de acceso y el número de puertos que requiere cada switch, se determina en función de la cantidad de usuarios y dispositivos proyectados, mediante la siguiente ecuación:

$$\begin{aligned} &Total\ de\ usuarios\ proyectados\ por\ piso \\ &= (Total\ de\ usuarios\ actuales) \\ &+ (10\%\ del\ crecimiento\ para\ usuarios\ cableados) \\ &+ (10\%\ de\ crecimiento\ para\ dispositivos\ de\ red) \end{aligned}$$

Ecuación 9. Fórmula para calcular el total de usuarios proyectados por piso

Referenciado: (Chinchero, 2013)

En la ecuación 9, se remplaza los valores de la tabla 19 y se obtiene los siguientes resultados:

$$Total\ de\ usuarios\ proyectados\ para\ piso\ 1 = (60) + (6) + (6)$$
$$Total\ de\ usuarios\ proyectados\ para\ piso\ 1 = 72\ usuarios$$

$$Total\ de\ usuarios\ proyectados\ piso\ 2 = (33) + (3{,}3) + (3{,}3)$$

$$Total\ de\ usuarios\ proyectados\ para\ piso\ 2 = 39{,}6\ usuarios$$

$$Total\ de\ usuarios\ proyectados\ por\ piso = (7) + (0{,}7) + (0{,}7)$$
$$Total\ de\ usuarios\ proyectados\ para\ piso\ 3 = 8{,}4\ usuarios$$

$$Total\ de\ usuarios\ para\ las\ dependencias = (25) + (2{,}5) + (2{,}5)$$
$$Total\ de\ usuarios\ para\ las\ dependencias = 30\ usuarios$$

En la tabla 20, se resume el total de usuarios proyectados por cada piso del GADMU, considerando que un aumento del 10%.

Tabla 20. Cálculo de usuarios proyectados

PISOS	USUARIOS PROYECTADOS
En el piso 1	72 usuarios
En el piso 2	40 usuarios
En el piso 3	8 usuarios
Dependencias externas	30 usuarios
TOTAL	148 usuarios

Referencia: Elaboración propia

Con la ecuación 10, se determinará cuántos switches de acceso se debe tener cada piso del edificio.

$$Número\ de\ switches\ de\ acceso\ por\ \ piso = \left[\frac{Total\ de\ puertos\ de\ red\ por\ piso}{Número\ de\ puertos\ de\ usuario\ final\ por\ switch}\right]$$

Ecuación 10. Fórmula para calcular el número de switches de acceso

Referenciado: Recuperado (Chinchero, 2013)

Con los datos de la Tabla 20 y en base a la ecuación 10, se determina el número de switches a utilizar por cada piso se considera switches de 48 y 24 puertos, mediante los siguientes cálculos:

$$Número\ de\ switches\ de\ acceso\ por\ \ piso = \left\lceil \frac{Total\ de\ puertos\ de\ red\ por\ piso}{48\ puertos\ de\ usuario\ final\ por\ switch} \right\rceil$$

Referencia: Recuperado (Chinchero, 2013)

$$Número\ de\ switches\ de\ acceso\ para\ el\ piso\ 1 = \frac{72}{48}$$

$$Número\ de\ switches\ de\ acceso\ para\ el\ \ piso\ 1 = \ 2$$

$$Número\ de\ switches\ de\ acceso\ para\ el\ piso\ 2 = \frac{40}{48}$$

$$Número\ de\ switches\ de\ acceso\ para\ el\ \ piso\ 2 = \ 1$$

$$Número\ de\ switches\ de\ acceso\ para\ el\ piso\ 3 = \frac{8}{24}$$

$$Número\ de\ switches\ de\ acceso\ para\ \ el\ piso\ 3 = \ 1$$

$$Número\ de\ switches\ para\ dependenicas\ externas = \frac{30}{48}$$

$$Número\ de\ switches\ para\ dependenicas\ externas = \ 1$$

En la tabla 21, se indica un resumen de los resultados calculados anteriormente.

Tabla 21. Especificación de equipos por cada piso

Pisos	Usuarios proyectados
En el piso 1	2 SWITCH (48 puertos)
En el piso 2	1 SWITCH (48 puertos)
En el piso 3	1 SWITCH (24 puertos)
Dependencias externas	1 SWITCH (48 puertos)

Referencia: Elaboración propia

En el GADMU se necesita 5 switches en la capa acceso (4 switches con 48 puertos y 1 switch con 24 puertos), es importante considerar la adquisición de 1 switch (48 puertos) por motivos de contingencia.

4.4.1.3. Velocidad y tipo de puerto de acceso

La velocidad y tipo de puerto para usuarios finales, se determina mediante el tráfico actual y futuro generado por cada usuario existente.

Con el análisis sobre cálculos de tráfico de servicios (externos e internos) dado en la tabla 17 y 18, se determina que el tráfico actual que es generado por un usuario es de 19 Mbps entre aplicaciones dentro y fuera de la institución. Para evitar posibles encolamientos y saturación debe tener como mínimo el doble de la capacidad calculada (38 Mbps), al no existir equipos a 38 Mbps se puede estandarización sus utilizaciones a 100 Mbps para las necesidades actuales y futuras.

4.4.1.4. Velocidad de los puertos up-link

Para el cálculo de la velocidad de transmisión de puertos up-link, se considera las mejores prácticas recomendadas por el fabricante Cisco.

(Cisco, 2011), describe: que las mejores prácticas de diseño para los switches de acceso se basan en los niveles de sobresuscripción de los equipos, que es la cantidad de puertos de usuario final, los cuales pueden trasmitir de manera simultánea a través de un enlace de backbone o up-link. Los niveles de sobresuscripción considerados son:

- " De 1:1 a 20:1 para redes con niveles de tráfico bajo
- De 10:1 a 20:1 para redes con niveles de tráfico medio bajo (aplicaciones típicas)
- De 4:1 a 12:1 redes empresariales con niveles de tráfico medio-alto (aplicaciones típicas y especiales, alto ancho de banda)
- De 5:1 a 10:1 redes empresariales con tráfico de servidores virtuales.
- De 1.1 a 4:1 redes de Data Centers con un nivel de tráfico alto con aplicaciones especiales con alto requerimiento de ancho de banda." (Cisco, 2011).

Para el GADMU se considera como una red con un nivel de tráfico medio-alto, relación de sobresuscripción debería estar en el rango 10:1 a 20:1, para lo cual se determina mediante la ecuación 11.

$$10 \leq \frac{\sharp\ total\ de\ puertos\ de\ usuario\ del\ sw\ acceso * velocidad\ de\ los\ puertos}{Velocidad\ del\ puerto\ up-link\ de\ enlaces\ con\ el\ Backbone} \leq 20$$

Ecuación 11. Fórmula para determinar velocidad de puertos up-link
Referencia: Recuperado de (Chinchero, 2013)

Remplazando datos en la ecuación anterior determinamos lo siguiente:

$$10 \leq \frac{48\ puertos * 200\ Mbps_{full\ dulplex}}{Velocidad\ del\ puerto\ up-link\ de\ enlaces\ con\ el\ Backbone} \leq 20$$

$$10 \leq \frac{9{,}6\ Gbps}{Velocidad\ del\ puerto\ up-link\ de\ enlaces\ con\ el\ Backbone} \leq 20$$

$$\frac{9{,}6\ Gbps}{20} \leq Velocidad\ del\ puerto\ up-link\ de\ enlaces\ con\ el\ Backbone \leq \frac{9{,}6\ Gbps}{10}$$

$$0{,}4\ Gbps \leq Velocidad\ del\ puerto\ up-link\ de\ enlaces\ con\ el\ Backbone \leq 0{,}9\ Gbps$$

El rango calculado va entre (0,4 Gbps y 0,9 Gbps) al no existir estas velocidades para puertos up-link se puede estandarización sus utilizaciones velocidades de 1 Gbps para las necesidades actuales y futuras.

4.4.1.5. Capacidad de conmutación

La capacidad de conmutación y el parámetro conocido como “back-plane” definen el ancho de banda máximo que soporta un “switch”, esto dependerá del procesador, del número de tramas que sea capaz de procesar. Para los switches de acceso, se calcula considerando la transmisión simultánea full dúplex, mediante ecuación 12.

$$Capacidad\ de\ conmutacion\ de\ switches\ de\ acceso$$
$$= ((Número\ de\ puertos\ de\ usuario\ final)$$
$$* (Velocidad\ de\ puertos\ de\ usuario\ final) + (Número\ de\ puertos\ de\ up-link)$$
$$* (Velocidad\ de\ puertos\ up-link)) * 2$$

Ecuación 12. Fórmula para determinar capacidad de conmutación en equipos de acceso
Referencia: Recuperado de (Chinchero, 2013)

Remplazando valores en ecuación (12), obtenemos el siguiente resultado:

$$Capacidad\ de\ conmutacion\ de\ switches\ de\ acceso$$
$$= \big((48\ puertos) * (100\ Mbps) + (2) * (1\ Gbps)\big) * 2 = 13{,}6\ Gbps$$

En la tabla 22 se encuentra los requerimientos básicos para adoptar en el proyecto propuesto en la capa acceso.

Tabla 22. Requerimientos para capa acceso

REQUERIMIENTOS	VALORES
Switches de 48 puertos	4
Switches de 24 puertos	1
Switches por motivos de contingencia	1
Velocidad hacia las estaciones de trabajo	100 Mbps
Velocidad de puertos up-link hacia las capa núcleo	1 Gbps
Capacidad de conmutación	13,6 Gbps

Referencia: Elaboración propia

4.5. REDISEÑO DE LA RED DE DATOS

En este ítem se explica el rediseño de la red de datos para el GAD Municipal de San Miguel de Urcuquí, el cual se divide en dos partes: física y lógica; para la parte física se plantea un modelo en dos capas (núcleo colapsado y acceso), los cuales serán esquematizados indicando la función que realiza cada capa; y para la parte lógica se plantea un esquema de creación de vlans con sus direccionamientos respectivos para cada una de ellas.

Para determinar el tipo equipo de red a utilizarse, se realiza un análisis de cálculo del tráfico actual con el cual se determina el ancho de banda que necesita cada empleado de la institución el cual es [0,15 Mbps]. Con estos cálculos se realiza un dimensionamiento para la capa acceso, con ello se determina el número de switches que se necesita cada capa acceso, en la tabla 22 requerimientos mínimos (se detalla un resumen que debe cumplir cada switch de acceso para ser utilizado). Una vez analizado todos estos parámetros se procede a elegir los equipos de red a utilizarse, realizando un cuadro en donde se comparan marcas que ofrecen los equipamientos de red.

Finalmente, se simula el diseño en el programa GNS3 con la finalidad de verificar el funcionamiento.

4.5.1. JUSTIFICACIÓN PARA ADOPTAR MODELO EN DOS CAPAS

(Domíguez Limaico & Gordillo Pasquel, 2006) menciona que: EL modelo jerarquico para una red de datos basado en las mejores practicas dadas por CISCO Systems, especifica que los equipos que conforman la sección de “backbone” o “Core”, deben tener la capacidad de conmutación (backplane) suficiente capaz de soportar los requerimientos de la red, además debe proporcionar opciones de redundancia. Para la capa de distribución, se debe controlar y monitorear el tráfico de la red, además se recomienda implementar seguridad y autenticación de usuarios registrados; que dependiendo del tamaño de la red, se la puede integrar junto con la sección de backbone en un solo equipo. Dando lugar a una arquitectura de core colapsado.

Por lo expuesto anteriormente, para el diseño propuesto se escoge la arquitectura de core colapsado, toda vez que; el número de empleados que tiene el GAD Municipal de San Miguel de Urcuquí es pequeño (125 usuarios). Ademas se debe considerar que en la institución cuenta con un presupuesto limitado para el área tecnologica, por lo que este modelo se adapta perfectamente a las necesidades del GADMU.

“Actualmente existen switches de gran capacidad los cuales integran interfaces Ethernet, FastEthernet, 1 Gigabit Ethernet para UTP y fibra óptica, y 10 Gigabit Ethernet para fibra óptica, los mismos que logran conmutación a gran velocidad.” (Domíguez Limaico & Gordillo Pasquel, 2006). Para el proyecto se necesitará switches Fastethernet (100 Mbps), este análisis se encuentra en este mismo capítulo en el ítem (4.3) dimensionamiento para switches de capa acceso. Y un resumen de los parámetros que se necesitan la capa acceso se indica en la tabla 22.

(Domíguez Limaico & Gordillo Pasquel, 2006), hace mención: “En la actualidad existen switches que manejan capa 2, capa 3 y hasta capa 4 (capa transporte) denominados switches multicapa. Con este tipo de equipos se puede implementar seguridades tales como restricción de direcciones MAC, direcciones IP’s y puertos lógicos de capa transporte, a manera de un cortafuegos14 (firewall). Por lo tanto en el presente diseño se utilizará en cada nodo este tipo de dispositivos.” Para el rediseño se utilizarán switches de capa 2 y capa 3.

En la figura 19, se indica una topología física propuesta en la cual se divide en dos capas (acceso y núcleo colapsado), se puede apreciar que en la capa de núcleo colapsado se encuentran dos equipos de red, un equipo principal y un secundario (redundancia), se recomienda utilizar en la institución un equipo redundante en caso de que el equipo principal falle, el otro equipo entra en funcionamiento y la red se mantenga operativa.

Además se observa que los switches de acceso se conectan hacia los switches de núcleo colapsado, mediante interfaces de uplink a 1 Gigabit por lo cual estos equipos necesitarán: 2 puertos uplink a 1 Gigabit para cada uno de estos para aplicaciones futuras.

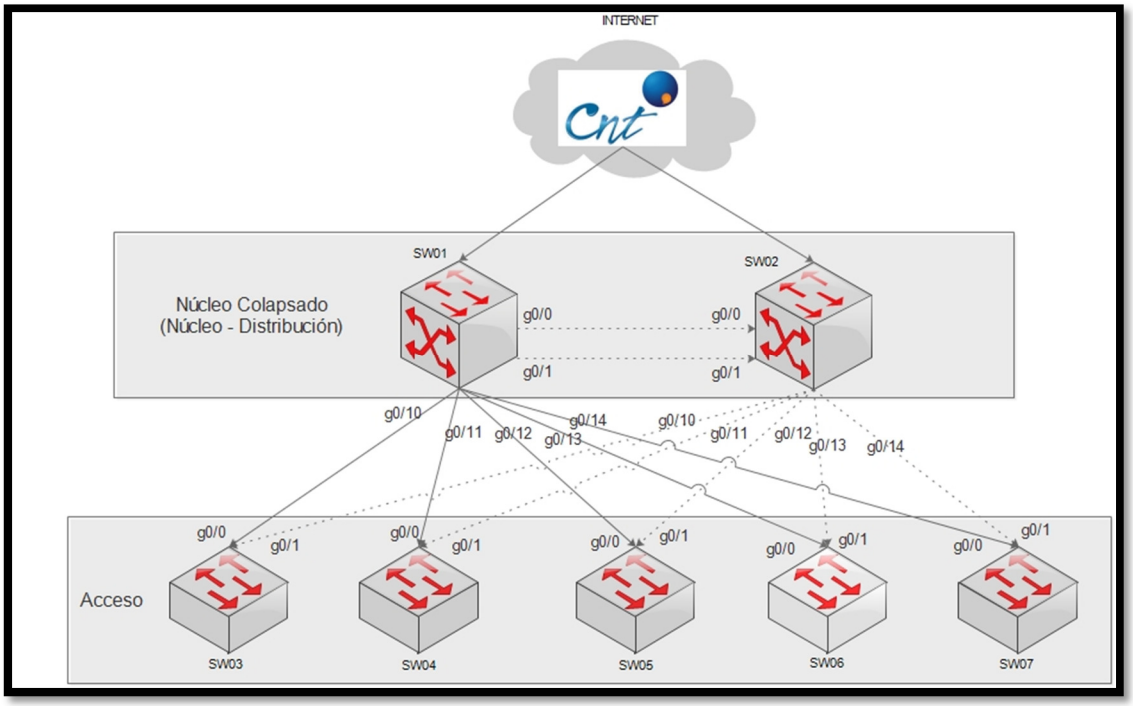

Figura 19. Modelo de red propuesto

Referencia: Elaboración propia

Para las configuraciones de capa en resumen se realiza lo siguiente:

Para la capa acceso se separan los dominios de broadcast mediante VLANs, las que se utilizan para la conexión lógica de capa 2 entre switches. Así mismo para obtener caminos redundantes entre switches de esta capa, se utiliza el protocolo rapid - spanning tree, empleado en cada VLAN.

Para la capa 3 se manejan direcciones lógicas y es posible separar dominios de broadcast de capa 2 mediante el enrutamiento entre vlans. Los protocolos a configurase en esta capa, son HSRP (Hot Standby Router Protocol), VTP (VLAN Trunking Protocol), Listas de control de acceso, entre otros.

Continuación, se explica detalladamente las configuraciones para las capas de: núcleo colapsado y acceso; en los cuales se explica que protocolo se utilizarán para mejorar el desempeño de la red.

4.5.2. CONFIGURACIONES EN CAPA NÚCLEO COLAPSADO

Para la capa núcleo colapsado se realiza la configuración para crear la VLANs, estas se agruparon según la funciones de los departamentos en el GAD Municipal de Urcuquí, conjuntamente a estas se configuró el enrutamiento entre VLANs que se utiliza para la transportación de información de dichas Vlans.

Se configura el protocolo VTP (VLAN Trunking Protocol) en modo servidor con lo cual se evitará la creación de VLAN en los switches de acceso en modo manual, evitando problemas con fallos de escritura al momento de crear una Vlans.

Es muy importante tener en cuenta aspectos de fallos (equipos), por lo cual se habilitará HSRP, su funcionamiento básico es: cuando un switch se pone en modo activo y otro en espera, si el switch activo falla el que se encuentra en espera desempeña las funciones de éste.

Se configurará listas de acceso con las cuales se impedirá y aceptará principalmente la comunicación entre departamentos agrupado por Vlans mediante reglas, por ejemplo se permitirá la comunicación entre departamento financiero y departamento administrativo, estas reglas fueron escogidas por el departamento de sistemas.

Los puertos conectado hacia los switches de capa acceso, se configura en modo troncal para el transporte de muchas Vlans por un solo enlace.

En la figura 20, se observa como deberá ir conectados los switches en la capa núcleo colapsado. Los cuales deben ir conectados entre sí mediante enlaces de up-link de 1 Gbps.

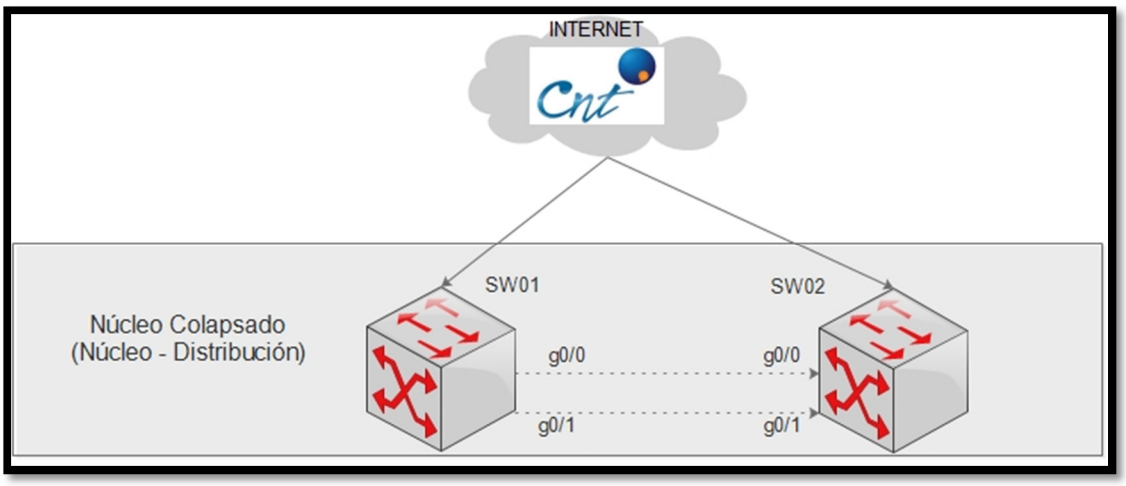

Figura 20. Modelo jerárquico - Núcleo colapsado
Referencia: Elaboración propia

4.5.2.1. Recomendaciones de diseño para capa núcleo colapsado

Se recomienda en esta capa núcleo-distribución tener otro equipos de respaldo, ya que en caso de falló este se pondrá en modo activo y evitará que la institución se quede sin el servicio.

Además es importante que también se cuente redundancia para el backbone en el cuarto de telecomunicaciones, asegurando la continuidad del servicio de internet.

Se recomienda la instalación de los enlaces (up-link) y (servidores) mediante fibra óptica a 1Gbps.

4.5.3. CONFIGURACIONES EN CAPA ACCESO

En la capa acceso es indispensable configurar la autenticación mediante MAC para cada computadora que existentes en el edificio principal del GAD Municipal de Urcuquí, esto evitará el acceso a los recursos (impresora, internet, base de datos, correo institucional). Se realiza la configuración de VTP (VLAN Trunking Protocol) en modo cliente para evitar configurar las Vlans en forma manual.

Los puertos conectado hacia los usuarios finales, se configurará en modo acceso para el transporte tráfico de cada usuario conectado a esa VLAN.

Se configura el protocolo rapid-spanning tree esto permite recuperar la conectividad después de una interrupción, esto proporciona una rápida convergencia si el enlace falla.

En la figura 21, se observa cómo deben estructurarse los switches en capa acceso brindando conexión a todos los departamentos existentes.

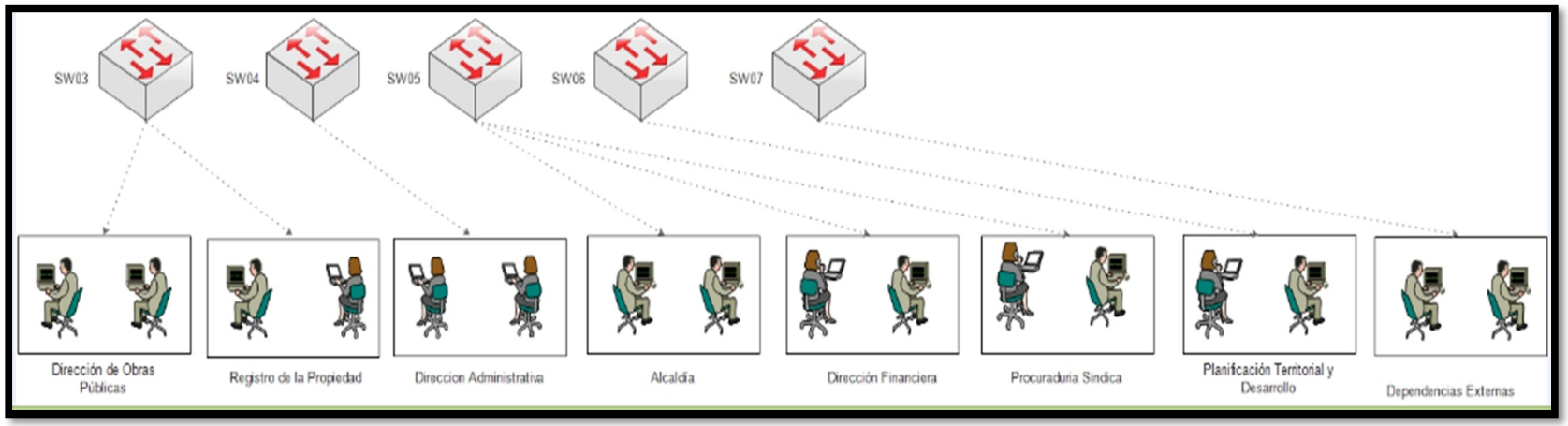

Figura 21. Modelo jerárquico para capa acceso

Referencia**:** Elaboración propia

4.5.3.1. Para aplicaciones futuras se debe considerar los siguientes aspectos

- QoS.- La red debe tener prioridades en el tráfico sea voz, datos o video mediante QoS, el switch de esta capa debe admitir este parámetro.

- POE: Una herramienta muy indispensable para energizar equipos mediante el cable Ethernet, el switch Catalys 2960 admite él envió de información y energía mediante POE.

4.5.3.2. Recomendaciones de diseño para capa acceso

Para asegurar que los usuarios del GADMU no utilicen direcciones IP ajenas sin previa autorización y utilice recursos que no les corresponde, se limitará el uso de la red a un determinado usuario, este verificará la dirección MAC de la computadora personal si este parámetro no coincide no puede acceder al servicio de red.

4.5.4. PROPUESTA DEL MODELO DE RED PROPUESTO LÓGICO

Para la parte lógica se realiza la microsegmentación basado en VLANs, conjuntamente se realiza el cálculo de direccionamiento IP mediante VLSM, su cálculo se basa en número de usuarios que tiene cada VLANs. A continuación se explica el procedimiento para la parte lógica.

4.5.4.1. Segmentación de la red

La segmentación basada en VLANs es una solución que principalmente brinda: seguridad, limita los dominios de broadcast, además ayuda a la gestión y administración, obteniendo la infraestructura lógica ordenada.

En la figura 23, se observa las VLANs con diferentes imágenes los cuales se encuentran situados en diferentes pisos; se propone la creación un total de 14 Vlans. En el **ANEXO D**, se indica las distribución de direcciones IP que se encuentran asignadas cada empleado base primordial para el cálculo de direccionamiento a utilizarse.

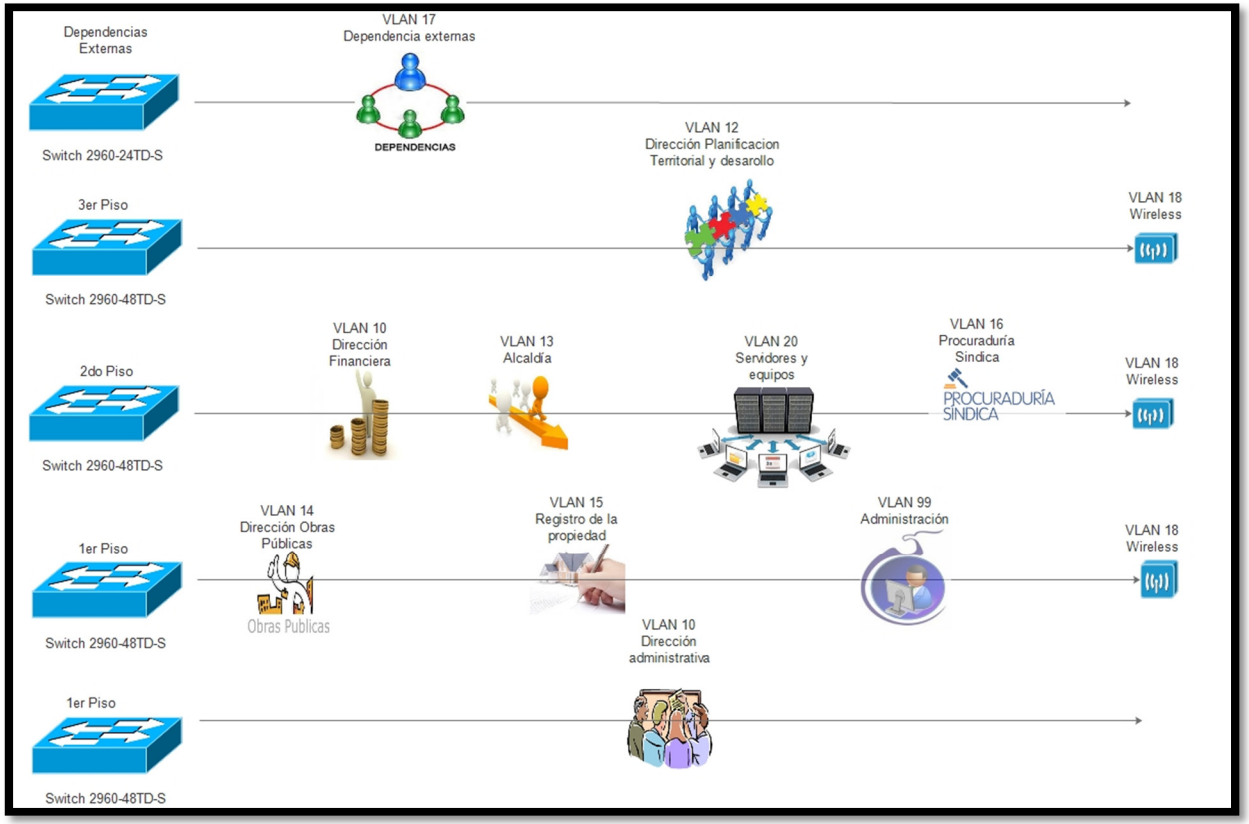

Figura 22. Distribución de VLAN en el GADMU

Referencia: Elaboración propia

Mediante la creación de VLANs se tiene un esquema lógico en forma ordenada, con una gran ventaja de brindar mayor control al administrador ya que se encuentran asignadas localmente, la agrupación de departamentos se basa en la tabla 27.

Tabla 23. *Agrupación de los departamentos*

VLAN	AGRUPACIÓN DE DEPARTAMENTOS	DEPARTAMENTOS
10	Dirección Administrativa	Talento Humano Sistemas Informáticos Bodega Contratación Pública Mantenimiento
11	Dirección Financiera	Presupuesto Contabilidad Tesorería Rentas
12	Planificación territorial y desarrollo	Regulación Urbana Avalúos y Catastros Gestión y proyectos Tránsito y Transporte
13	Alcaldía	Comunicación Secretaria General Asesoría Fiscalización Auditoria Interna Alcaldía Consejo Municipal
14	Dirección de Obras publicas	Agua Potable Infraestructura Gestión de Riesgos Gestión Ambiental
15	Registro de la Propiedad	
16	Procuraduría Sindica	Comisaria Municipal

VLAN	AGRUPACIÓN DE DEPARTAMENTOS	DEPARTAMENTOS
17	Dependencias externas	Plaza del Buen Vivir
		Unidad de Desarrollo Social
		Biblioteca
		Mantenimiento

Referencia: Elaboración propia

En la tabla 28, se indican la VLANs complementarias que se propone crear en el GADMU para administración y monitoreo.

Tabla 24. Vlans complementarias en GADMU

VLAN	USO
18	Wireless
19	Servidores y Equipos
20	Área de sistemas
99	Administración
22	Voz
23	Video Vigilancia

Referencia: Elaboración propia

4.5.4.2. Direccionamiento IP

Para la asignación de direcciones IP se consideró los grupos de VLANs con mayor cantidad de usuarios y también el de menores usuarios, en nuestro caso el grupo (Dependencias externas) tiene mayor afluencia de usuarios y grupo de Procuraduría Sindica con menor afluencia de usuarios. Con los siguientes datos recolectados se describe en las siguientes subredes:

- Una subred de 24 host para ser asignado a la VLAN de dirección administrativa.
- Una subred 24 host para ser asignados a la VLAN dirección financiera.
- Una subred 24 host para ser asignados a la VLAN planificación territorial y desarrollo.
- Una subred 18 host para ser asignados a la VLAN Alcaldía.

- Una subred 18 host para ser asignados a la VLAN dirección de obras públicas.
- Una subred 11 host para ser asignados a la VLAN registro de la propiedad.
- Una subred 7 host para ser asignados a la VLAN Procuraduría Síndica.
- Una subred de 29 host para ser asignado a la VLAN de dirección Dependencias externas.
- Una subred 240 host para ser asignados a la VLAN Wireless.
- Una subred 40 host para ser asignados a la VLAN Servidores.
- Una subred 20 host para ser asignados a la VLAN Área de sistemas.
- Una subred 10 host para ser asignados a la VLAN Administración.

Para aplicaciones futuras: Una subred 150 host para ser asignados a la VLAN Voz, una subred 50 host para ser asignados a la VLAN Video vigilancia.

En la tabla 29, se indica cómo queda el prefijo según la cantidad de usuarios que tiene cada departamento.

Tabla 25. Cálculo para subneteo

USUARIOS	**CALCULO DE HOST**			**PREFIJO (172.16.0.0/24)**		
240	8 Bits	2^8=256	Máximo 254 host	8-8=0	24+0=24	/24
150	8 Bits	2^8=256	Máximo 254 host	8-8=0	24+0=24	/24
50	6 Bits	2^6=64	Máximo 62 host	8-6=2	24+2=26	/26
40	6 Bits	2^6=64	Máximo 62 host	8-6=2	24+2=26	/26
29	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
24	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
24	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
24	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
20	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
18	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
18	5 Bits	2^5=32	Máximo 30 host	8-5=3	24+3=27	/27
11	4 Bits	2^4=16	Máximo 14 host	8-4=4	24+4=28	/28
10	4 Bits	2^4=16	Máximo 14 host	8-4=4	24+4=28	/28

Referencia: Elaboración propia

En la tabla 30, se especifica el direccionamiento basado en VLANs, junto con su respectiva mascara de red, puerta de enlace y ubicación, con la IP 172.16.0.0/24 se propone las siguientes redes:

Tabla 26. *Direccionamiento basado en VLAN´S*

VLAN	DEPARTAMENTO	ACRÓNIMO	# PUNTOS DE RED	MÁSCARA RED	DIRECCIÓN DE RED	1ERA IP UTILIZABLE	ÚLTIMA IP UTILIZABLE	BROADCAST	LOCALIZACIÓN
18	Wireless	WIRELESS	240	/24	172.16.0.0	172.16.0.1	172.16.0.254	172.16.0.255	P1,P2,P3
23	Voz	VOZ	150	/24	172.16.1.0	172.16.1.1	172.16.1.254	172.16.1.255	P1,P2,P3
24	Video vigilancia	VIDEOVIG	50	/26	172.16.2.0	172.16.2.1	172.16.2.62	172.16.1.63	P1,P2,P3
19	Servidores y Equipos	SRVEQU	40	/26	172.16.2.64	172.16.2.65	172.16.2.126	172.16.2.127	Cuarto de equipos
17	Dependencia externas	DEPEXT	29	/27	172.16.2.128	172.16.2.129	172.16.2.158	172.16.2.159	EXTERIORES
10	Dirección administrativa	DIRADMIN	24	/27	172.16.2.160	172.16.2.161	172.16.2.190	192.16.2.191	P1
11	Dirección Financiera	DIRFINAN	24	/27	172.16.2.192	172.16.2.193	172.16.2.222	172.16.2.223	P2
12	Planificación Territorial y desarrollo	PLANDES	24	/27	172.16.2.224	172.16.2.225	172.16.2.254	172.16.2.255	P3
20	Área de sistemas	ARSIST	20	/27	172.16.3.0	172.16.3.1	172.16.3.30	172.16.3.31	P1
13	Alcaldía	DEPALCD	18	/27	172.16.3.32	172.16.3.33	172.16.3.62	172.16.3.63	P1,P2,P3

VLAN	DEPARTAMENTO	ACRÓNIMO	# PUNTOS DE RED	MÁSCARA RED	DIRECCIÓN DE RED	1ERA IP UTILIZABLE	ÚLTIMA IP UTILIZABLE	BROADCAST	LOCALIZACIÓN
14	Dirección Obras Públicas	DIROBPUB	18	/27	172.16.3.64	172.16.3.65	172.16.3.94	172.16.3.95	P1
15	Registro de la propiedad	REGPRO	11	/28	172.16.3.96	172.16.3.97	172.16.3.110	172.16.3.111	P1
16	Procuraduría Sindica	PROSIN	10	/28	172.16.3.112	172.16.3.113	172.16.3.126	172.16.3.127	P1

Referencia: Elaboración propia

Se debe considerar que para la VLAN 99 (Administración) se considera una IP clases C: 192.168.0.0/24 para las configuraciones respectivas. Dentro de la distribución se diferencia las siguientes VLAN ´S, a continuación se explica la función de la cada una de estas:

- VLAN de Servidores y equipos: Es una subred para la distribución de direcciones IP para la granja de servidores del GADMU y el equipamiento activo.
- VLAN de Administración: Utilizado por los administradores de red, los usuarios que se encuentren en esta red sin excepción pueden tener acceso al equipamiento activo.
- VLAN Wireless: Utilizada para la red Wireless de la institución, para brindar conexión de internet, ubicada en cada piso.

En el **ANEXO E**, se indica el nuevo direccionamiento IP basado en cada VLAN, especificando la dirección IP antigua, cargo, responsable, ubicación.

4.5.4.3. Lista de control de acceso

Utilizada principalmente para permitir y denegar el acceso tráfico a la red entre Vlans del GAD Municipal de San Miguel de Urcuquí.

4.5.4.3.1. Lista de control de acceso estándar

Estas listas de control se implementan en el switch de núcleo colapsado para limitar el tráfico, estas fueron dadas por el departamento de sistemas para mejorar el tráfico entre las Vlans. Las reglas son las siguientes:

- El usuario con la IP 172.16.3.34 (Alcalde) tendrá acceso a las Vlans de: Dirección administrativa, Dirección Financiera, Planificación territorial y desarrollo, Dirección de Obras públicas, Registro de la Propiedad, Procuraduría Sindica, Dependencias externas.
- Los usuarios con la red 172.16.2.160 (Dirección administrativa) tendrá acceso a los recursos VLAN de dirección Financiera.
- Los usuarios con la red 172.16.2.192 (Dirección financiera) tendrá acceso a los recursos VLAN de Dirección Administrativa.
- El usuario con la IP 172.16.3.2 (Área de Sistemas) tendrá acceso todos los recursos de la red.

4.6. ELECCIÓN DE LOS EQUIPOS DE RED

En la tabla 22 se presenta los parámetros para capa acceso son: número de puertos (48 – 24 puertos), velocidades hacia las áreas de trabajo (100 Mbps), velocidades de puertos up-link (1Gbps), capacidad de conmutación (13,6 Gbps).

Otro punto importante es la cantidad de puertos y tipos de interfaces que deben tener los equipos de conmutación para capa núcleo colapsado. Hay que considerar

una capacidad de crecimiento a futuro y a la vez integrar en un solo equipo (distribución y núcleo), por lo que es recomendable una cantidad de al menos 24 puertos GigabitEthernet 1 [Gbps] y 4 interfaces 10 Gigabit Ethernet para fibra óptica, de las cuales 2 son utilizadas para tener conexión redundante entre nodos de acuerdo al diagrama de la figura 23. Los switches de capa acceso y capa núcleo deben trabajar con los siguientes protocolos.

- IEEE 802.3x para recepción y transmisión simultáneos (full dúplex).

- IEEE 802.3u para conexión de los equipos finales mediante tarjetas 10/100 Mbps a través de cable UTP CAT6.

- IEEE 802.3ab para conexión de los equipos finales mediante tarjetas 10/100/1000 Mbps a través de cable UTP CAT6 y el estándar.

- IEEE 802.3z para la conexión de los enlaces de fibra óptica a 1 Gbps.

- IEEE 802.1q permite tener múltiples redes compartiendo el mismo espacio físico, mediante esta alternativa se generan segmentos de red lógicos en el GADMU este protocolo permite crear Vlans.

- Es necesario garantizar la redundancia de la red, que los enlaces tengan disponibilidad por lo cual se establece utilizar protocolos tales como IEEE 802.1d y 802.1w.

- Para aplicaciones futuras el switch principal debe brindar calidad de servicio y etiquetar el trafico diferenciándolo si son datos o es voz. Para lo cual se necesita tener el protocolo IEEE 802.1p, y diferenciar el tráfico generado por las Vlans.

- Tanto los switches de acceso como los de núcleo deben proveer el servicio dinámico de asignación de hosts.

- A nivel de seguridad se requiere que los puertos de los switches soporten el protocolo IEEE 802.1x para autenticación y que mediante listas de acceso se brinde permisos a los usuarios, las listas de acceso deberán ser estándares y extendidas.

- Inclusive la administración del equipo debe proveer seguridad mediante el protocolo SSH, acceso remoto con el protocolo Telnet, y que soporte el protocolo de administración SNMP en sus versiones actuales. Y los equipos de conmutación deben soportar administración tanto por interfaz gráfica como por línea de comando.

Para resumir los requisitos mínimos para capa acceso y capa núcleo se describen en las siguientes tablas 23 y 24:

Tabla 27. Características mínimas para elección de equipos en capa acceso

REQUERIMIENTOS MÍNIMOS	**CARACTERISTICAS**
Capacidad de conmutación	13,6 Gbps
Protocolo de gestión	SNMP 1, SNMP2, Telnet, HTTP,TFTP,SSH
Puertos	48 puertos (RJ-45) Ethernet 10/100/1000. 2 puertos SFP a 10 Gbps y 2 puertos SFP a 1 Gbps.
Puertos	24 puertos (RJ-45) Ethernet 10/100/1000. 2 puertos SFP a 10 Gbps y 2 puertos SFP a 1 Gbps.
Velocidad de puertos up-link	1 Gbps
Cumplimiento de normas	IEEE 802.3ab, IEEE 802.3x (control de flujo) IEEE 802.3u (Fast Ethernet) IEEE 802.1Q (VLAN) IEEE 802.1p (CoS) IEEE 802.3ad (LACP) IEEE 802.1x (Seguridad) IEEE 802.1w (RSTP)

Referencia: Elaboración Propia

Tabla 28. Características mínimas para elección de equipos en capa núcleo

REQUERIMIENTOS MÍNIMOS	CARACTERISTICAS
Protocolo de gestión	SNMP 1, SNMP2, Telnet, HTTP,TFTP,SSH
Puertos	24 puertos (RJ-45) Ethernet 10/100/1000. 1 puerto USB tipo A. 1 puerto por consola - mini USB tipo B. 1 puerto 10Base-T / 100Base-TX - RJ-45 - RS-232 gestión del dispositivos.
Cumplimiento de normas	IEEE 802.3ab IEEE 802.3af IEEE 802.3at IEEE 802.1D (STP) IEEE 802.1p (CoS) IEEE 802.1Q (VLAN) IEEE802.1s (MSTP) IEEE 802.1w (RSTP) IEEE 802.1X (Seguridad) IEEE 802.3ad (LACP) IEEE 802.3ae (10G Ethernet) IEEE 802.3i (10BASE-T) IEEE 802.3u (Fast Ethernet) IEEE 802.3x (control de flujo) IEEE 802.3z (Gigabit Ethernet)
Funciones	Conmutación en capa 2 y 3

Referencia: Elaboración Propia

4.6.1. DETERMINACIÓN DEL EQUIPO EN CAPA ACCESO

Para determinar los equipos en capa acceso se consideró las características mínimas dada en las tablas 23 y 24, con ello se realizó la comparación entre 2 marcas (CISCO, 3COM) desarrollado en la tabla 25. Con la recolección de estos datos se logrará determinar el equipo que se adapte al proyecto propuesto, además se tomará en cuenta el valor económico de los equipos a escoger, ya que es muy limitado el recurso monetario en el GAD Municipal de Urcuquí.

Tabla 29. Comparación entre equipos de red para capa acceso

CARACTERÍSTICAS	**Switch WS-C2960 - (48 puertos)** **WS-C2960 - (24 puertos)**	**Switch 5500G-EI (48 puertos)** **5500G-EI (24 puertos)**
		
Marca	CISCO SYSTEMS	3COM
Memoria FLASH	64 Mb	32 Mb
Memoria DRAM	256 Mb	256 Mb
Capacidad de conmutación	Switch 48 puertos(176 Gbps) Switch 24 puertos(108 Gbps)	Switch 48 puertos(176 Gbps) Switch 24 puertos(108 Gbps)
Método de autenticación	SSH, Radius	SSH, Radius
IPV6	SI	SI
Voltaje de alimentación	CA 120/230 V (50/60 Hz)	CA 120/230 V (50/60 Hz)
Protocolo de gestión remota	SNMP 1, SNMP2, Telnet, HTTP,TFTP,SSH	SNMP 1, SNMP2, Telnet, HTTP,TFTP,SSH
Puertos	48 puertos (RJ-45) Ethernet 10/100/1000. 2 puertos SFP+ a 10 Gbps y 2 puertos SFP a 1 Gbps.	48 puertos (RJ-45) Ethernet 10/100/1000. 4 puertos SFP a 1 Gbps
	24 puertos (RJ-45) Ethernet 10/100/1000. 2 puertos SFP+ a 10 Gbps y 2 puertos SFP a 1 Gbps.	24 puertos (RJ-45) Ethernet 10/100/1000. 4 puertos SFP a 1 Gbps
Cumplimiento de normas	IEEE 802.3 IEEE 802.3 ab (Gigabit Ethernet sobre cable UTP) IEEE 802.3 ad (LACP) IEEE 802.3ah (Ethernte última milla) IEEE 802.3 u (Fast Ethernet) IEEE 802.3 x (control de flujo)	IEEE 802.3 IEEE 802.3 ab (Gigabit Ethernet sobre cable UTP) IEEE 802.3 ad (LACP) IEEE 802.3ah (Ethernte última milla) IEEE 802.3 u (Fast Ethernet) IEEE 802.3 x (control de flujo)

	IEEE 802.3 z (Gigabit Ethernet sobre fibra óptica) IEEE 802.1ab (LLDP) IEEE 802.1D (STP) IEEE 802.1Q (VLAN) IEEE 802.1p (CoS) IEEE 802.1w (RSTP) IEEE 802.1x (Seguridad) IEEE 802.1s (MSTP)	IEEE 802.3 z (Gigabit Ethernet sobre fibra óptica) IEEE 802.1ab (LLDP) IEEE 802.1D (STP) IEEE 802.1Q (VLAN) IEEE 802.1p (CoS) IEEE 802.1w (RSTP) IEEE 802.1x (Seguridad) IEEE 802.1s (MSTP)
Direcciones MAC	8000	16000
Conmutación capa 2	SI	SI
Conmutación capa 3	SI	SI
POE	SI	SI
Algoritmo de cifrado	SSL	SSL
Precio	$ 2278	$ 2461

Referencia: Elaboración propia

De acuerdo a las características de los equipos presentados en la tabla 25, se observa que los dos fabricantes(Cisco y 3Com) cumplen con los requerimientos que necesita la red propuesta en cuanto a capacidad de conmutación, normas IEEE; pero se escoge el switch CATALYST WS-C2960 (24 y 48 puertos) del fabricante CISCO SYSTEMS, porque ofrece mejores características en lo referente al número de puertos up-link (brinda 2 puertos a 10 Gbps), los cuales ayudarán en caso de crecer el tráfico en la institución en futuras aplicaciones.

En el **ANEXO B** se encuentra el datasheet del equipo CISCO CATALYST 2960-X, especificando todas las características escogidas.

4.6.2. DETERMINACIÓN DE EQUIPO EN CAPA NÚCLEO

Para determinar los equipos en capa núcleo se consideró las características mínimas dada en la tabla 24, con ello se realizó la comparación entre 2 marcas (CISCO, 3COM) desarrollado en la tabla 26.

Tabla 30. Comparación entre equipos de red para capa acceso

CARACTERÍSTICAS	SWITCH WS-C3750X-24-PS	SWITCH 3COM SERIE 7700
		
Memoria FLASH	128 Mb	128 Mb
Memoria DRAM	256 Mb	256 Mb
Capacidad de conmutación	240 Gbps	160 Gbps
Método de autenticación	Kerberos, Secure Shell (SSH), RADIUS	Kerberos, Secure Shell (SSH), RADIUS
IPV6	SI	SI
Voltaje de alimentación	CA 120/230 V (50/60 Hz)	CA 120/230 V (50/60 Hz)
Protocolo de gestión remota	CLI modo de configuración (interfaz de línea de comandos). Configuración mediante el puerto de consola (consola de control). Configuración local / remoto a través de Telnet La configuración remota a través de módem de acceso telefónico. La configuración del sistema con SNMP v1, 2, y 3 estadísticas completas RMON (Remote Monitoring) grupos de estadísticas, historial, alarmas y eventos Estadísticas de ACL / QoS. Estadísticas de la interfaz IP. Registro del sistema syslog.	CLI modo de configuración (interfaz de línea de comandos). Configuración mediante el puerto de consola (consola de control). Configuración local / remoto a través de Telnet La configuración remota a través de módem de acceso telefónico. La configuración del sistema con SNMP v1, 2, y 3 estadísticas completas RMON (Remote Monitoring) grupos de estadísticas, historial, alarmas y eventos Estadísticas de ACL / QoS. Estadísticas de la interfaz IP. Registro del sistema syslog.
Puertos	24 x 10Base-T / 100Base-TX / 1000Base-T - RJ-45 - PoE	24 x 10Base-T / 100Base-TX / 1000Base-T.

Cumplimiento de normas	IEEE 802.3ab IEEE 802.3af IEEE 802.3at IEEE 802.1D (STP) IEEE 802.1p (CoS) IEEE 802.1Q (VLAN) IEEE802.1s (MSTP) IEEE 802.1w (RSTP) IEEE 802.1X (Seguridad) IEEE 802.3ad (LACP) IEEE 802.3ae (10G Ethernet) IEEE 802.3i (10BASE-T) IEEE 802.3u (Fast Ethernet) IEEE 802.3x (control de flujo) IEEE 802.3z (Gigabit Ethernet)	IEEE 802.3ab IEEE 802.3af IEEE 802.3at IEEE 802.1D (STP) IEEE 802.1p (CoS) IEEE 802.1Q (VLAN) IEEE802.1s (MSTP) IEEE 802.1w (RSTP) IEEE 802.1X (Seguridad) IEEE 802.3ad (LACP) IEEE 802.3ae (10G Ethernet) IEEE 802.3i (10BASE-T) IEEE 802.3u (Fast Ethernet) IEEE 802.3x (control de flujo) IEEE 802.3z (Gigabit Ethernet)
Número máximo de pilas	8	8
Precio	$ 3024,00	$ 6750,00

Referencia: Elaboración propia

De acuerdo a las características de los equipos presentados en la tabla 26, se observa que los dos fabricantes cumplen con los requerimientos que necesita la red diseñada en: normas IEEE, puertos utilizados, protocolos de gestión, entre otros; pero se escoge el switch WS-C3750X-24-PS del fabricante CISCO System, ya que ofrece un mejor características en la capacidad de conmutación (240 Gbps), en comparación al equipo del fabricante 3Com.

Entre sus características más destacadas de este equipo es: manejo de puertos Gigabit Ethernet, presenta funciones de conmutación capa 2 y capa 3, manejo de VLAN, HSRP, ACL, agregado de enlace y mediante la tecnología Cisco StackWise se puede crear arquitecturas de conmutación unificadas que permite el apilamiento de estos para un futuro crecimiento a nivel de puntos de red.

En el **ANEXO C** se encuentra el datasheet del equipo CISCO CATALYST 3750-X, especificando todas las características.

En la figura 23, se muestra la topología a realizarse en la cual cuenta con dos equipos (SWITCH WS-C3750X-24-PS) para la parte núcleo colapsado, estos se encuentran establecidos con dos enlaces redundantes gigabitEthernet. Para la parte de capa de acceso tenemos 5 switches (SWITCH CISCO CATALYST WS-C2960) donde están creadas diferentes VLANs estos también cuentan con enlaces redundantes también a una velocidad de gigabitethernet, con los cual procura tener un red operativa en caso de falló de equipos o enlaces.

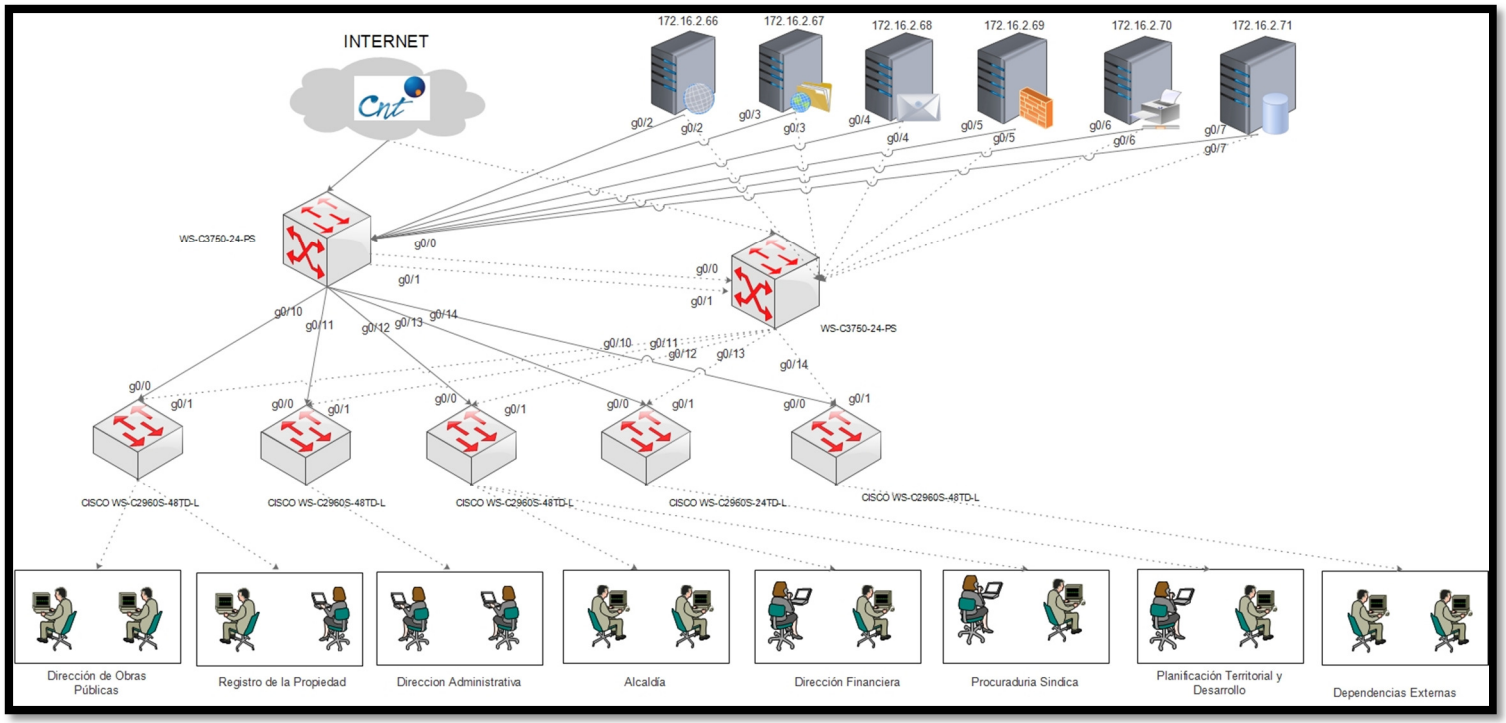

Figura 23. Topología física propuesta

Referencia: Elaboración propia

4.7. SIMULACIONES Y CONFIGURACIONES

Una vez desarrollado el rediseño de la red de datos es necesario validar el modelo propuesto, se utilizará el programa GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutar simulaciones en él, además es un emulador de routers Cisco dando soporte a plataformas 1700, 2600, 3600, 3700 y 7200, para probar el funcionamiento del proyecto se utilizaron los routers 2961 y 7200 (como switches de capa 3), enseguida se explica la utilización de estos dos equipos de red.

Para capa acceso se escogió la IOS del router 2691 ya que en este equipo se puede configurar: seguridad a nivel de puerto, VLANs, configuración listas de control acceso (ACL), soporta rapid-spanning tree; en cambio para capa núcleo colapsado se escogió la IOS del router 7200 ya que soporta HSRP (Hot Standby Router Protocol), VTP (VLAN Trunking Protocol), creación de VLAN, configuración de enrutamiento estático, dinámico, enrutamiento entre VLANs, configuración de ACL.

Dado que los equipos brindan las características mencionadas anteriormente y son adaptables al tema propuesto se procederá a realizar las configuraciones para demostrar el funcionamiento.

En el **ANEXO F** se explica las configuraciones básicas y las configuraciones basadas en cada capa (acceso y núcleo colapsado) que se realizaron. Entre las configuraciones básicas son la configuración de: contraseñas de acceso, direcciones IP para cada VLAN, SSH (Secure SHell), banner de bienvenida. Y en cambio para las configuraciones basadas en capas se realizó en la capa núcleo colapsado la configuración de las respectivas Vlans, puerto en modo acceso y modo troncal, redundancia (HSRP), listas de control de acceso (ACLs), VTP (modo servidor). Y en capa acceso en cambio se configuró la autenticación mediante MAC, VTP (modo cliente), VCP (enlaces redundantes).

En la figura 24, se indica la topología en funcionamiento cuenta con dos switch para núcleo colapsado con sus respectivos enlaces redundantes, además se observa las VLAN cada una estas configurada con su respectiva dirección IP y se en una máquina virtual(Ubuntu). En el **ANEXO G,** se indica todas las configuraciones que se realizó en cada swicth de la topología.

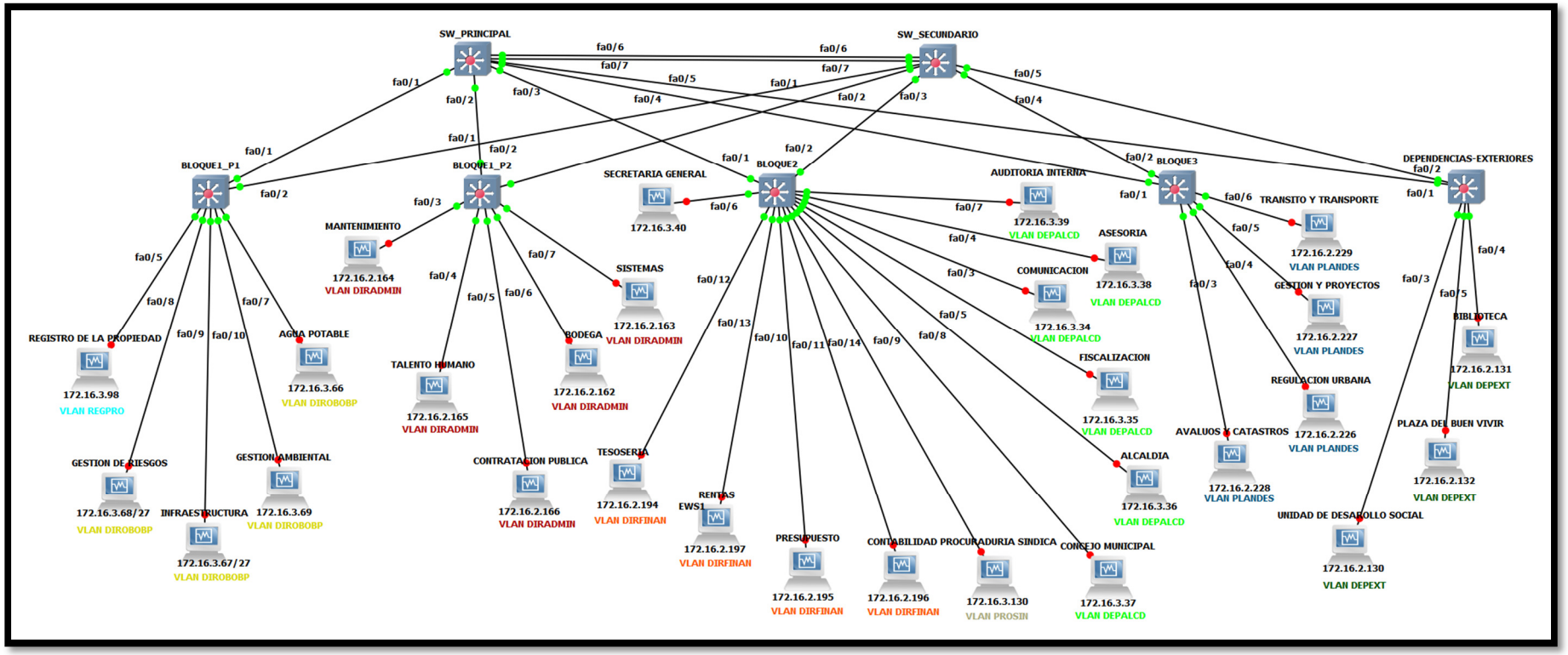

Figura 24. Topología física simulada en GNS3

Referencia: Elaboración propia

4.8. RESUMEN GENERAL DEL REDISEÑO

Para un funcionamiento del rediseño de la red es importante que el cableado estructurado se encuentre en óptimas condiciones, en el GAD Municipal de San Miguel de Urcuquí no cuenta con ninguna norma por ende en el **ANEXO A**, se muestra algunas consideraciones para solucionar los problemas identificados en el cableado estructurado del GADMU.

Mediante cálculos realizados en este capítulo se determinó que se necesitan 4 switches de acceso de 48 puertos y un switch 24 puertos, estos deben tener velocidades hacia las áreas de trabajo de 100 Mbps y velocidades de up-link de 1 Gbps, con una capacidad de conmutación de 13,6 Gbps y para la parte de núcleo se necesita dos switches con 24 puertos FastEthernet a 1Gbps con 8 puertos up-link a 1 Gbps para conexión con equipos de capa acceso, con una capacidad de conmutación de 160 Gbps.

Los equipos seleccionados para cada capa son switches Cisco Catalyst WS-C2960 y WS-C3750X-24-PS que se adaptan al rediseño propuesto en las tablas 25 y 26 se especifican las características más relevantes y además en el **ANEXO B** y **ANEXO C,** se indican los datasheet de cada uno de estos equipos.

Con la finalidad de verificar el funcionamiento del rediseño se utilizó el programa GNS3, en el cual se configuró todos los protocolos mencionados anteriormente, en el **ANEXO F** se indica la configuración de las dos capas del modelo jerárquico.

CAPÍTULO V

5. OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL

5.1. INTRODUCCIÓN

En este capítulo se adoptará la metodología MARGERIT para determinar un análisis de riesgos, con ello se pretende distinguir las vulnerabilidades en el GAD Municipal de Urcuquí; conjuntamente se realizará una comparación entre dos propuestas con las marcas (JUNIPER y CISCO) y se escogerá un equipo para la seguridad perimetral, logrando proteger activos de red e información importante.

Luego para la elección del sistema operativo a utilizarse en los servidores (FTP y PROXY SQUID) se utiliza la norma ISO/IEC/IEEE 29148:2011.

5.2. DISEÑO DE LA SEGURIDAD PERIMETRAL

Con la metodología MAGERIT se realizará un análisis de riesgos de la seguridad de la red de la Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí, dicho análisis permitirá identificar amenazas que afecten a la vulnerabilidad de la información y al final poder proponer un equipo para optimizar la seguridad perimetral.

De esta manera los administradores de la red podrán identificar fácilmente las amenazas y poder tomar decisiones más acertadas al momento de que algunas amenazas.

5.2.1. JUSTIFICACIÓN DE LA METODOLOGÍA MAGERIT

En la figura 25 se observan las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de la información son: MAGERIT, OCTAVE, CRAMM, IRAM, para determinar cuál es la metodología que genere confianza en la mitigación de riesgos se ha realizado la siguiente tabla comparativa.

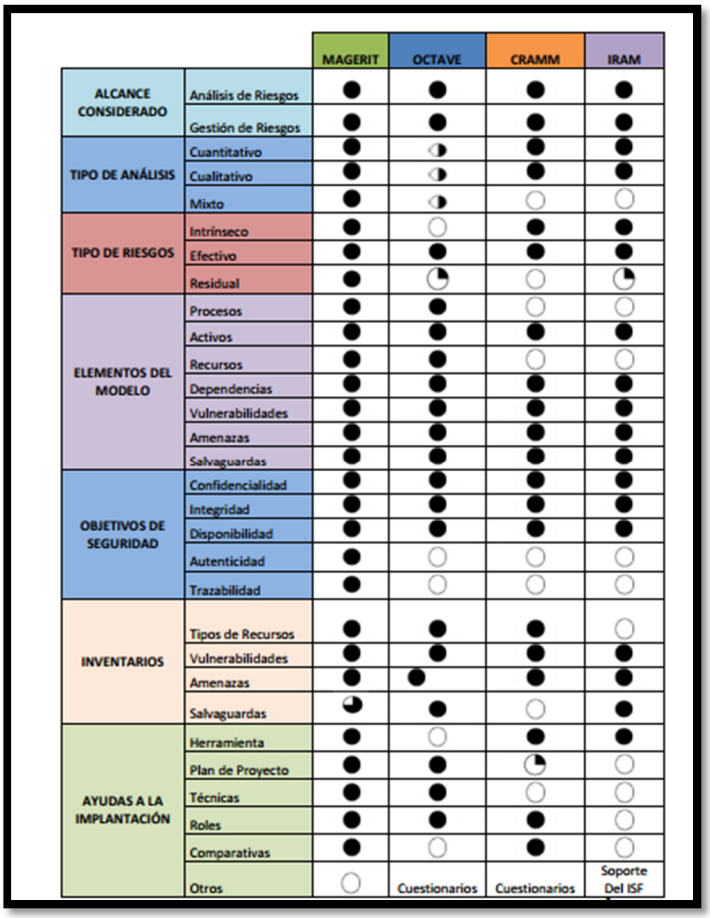

Figura 25. Comparación de metodologías

Referencia: Basado de (Álvarez, 2014)

De la tabla comparativa anteriormente desarrollada se puede concluir que MAGERIT, es una metodología completa porque tiene procesos, actividades.

Una parte fundamental dentro de la gestión de la seguridad de la información, es conocer y controlar los riesgos a los cuales está expuesta la información del GAD

Municipal de Urcuquí. Precisamente MAGERIT se basa en analizar el impacto que puede tener para la institución, buscando identificar las amenazas que pueden llegar a afectar la institución y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas. Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para una empresa.

5.2.2. ELABORACIÓN DEL ANALASIS DE RIESGO DEL GADMU

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento, para el proceso de análisis de riesgos se realizará los siguientes pasos como se indica en la siguiente figura.

TAREAS DELANÁLISIS DE RIESGOS
Paso 1. Caracterización de los activos
1.1 Identificación de los activos
1.2 Dependencias entre activos
1.3 Valoración de los activos
Paso 2. Caracterización de las Amenazas
2.1 Identificación de las amenazas
2.2 Valoración de las amenazas
Paso 3. Caracterización de las salvaguardas
3.1 Identificación de las salvaguardas pertinentes
3.2 Valoración de las salvaguardas.
Paso 4. Estimación del estado de riesgo
4.1 Estimación del impacto
4.2 Estimación del riesgo

Figura 26. Tabla para análisis de riesgos

Referencia: Basado en (Álvarez, 2014)

En la figura 26 se indica los pasos 4 pasos que se va a cumplir para determinar los riesgos y vulnerabilidades.

5.2.2.1. Identificación y clasificación de activos de la red

La identificación de activos es importante ya que permite plasmar con precisión el alcance del proyecto, permite valorar los activos con exactitud e identificando y valorando las amenazas a las que están expuestos dichos activos. Se realizó la respectiva recolección de información de los activos.

La descripción de toda la información recolectada ya se la ha mencionado anteriormente en el capítulo 3 “Análisis de la situación actual”, a través de las tablas 5, 7, 8.

Como resultado de las anteriores entrevistas realizadas a los administradores de la infraestructura del GAD Municipal de Urcuquí, se ha identificado el siguiente conjunto de activos de red LAN:

5.2.2.1.1. Datos/ Información

Los datos son la parte principal que permite a una organización prestar sus servicios. La información es un activo impreciso que será almacenado en equipos. Dentro del GADMU se han identificado que es necesario proteger la información de ciudadanos almacenada en la base de datos

5.2.2.1.2. Equipos informáticos (hardware)

Son medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la institución, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Dentro de este tipo de activos de red que posee el GADMU, tenemos los siguientes:

- ✓ Servidores de correo
- ✓ Servidor de base de datos

5.2.2.1.3. Instalaciones

Entre los lugares donde se hospedan los sistemas de información y comunicaciones. En el GADMU cuenta con un cuarto de telecomunicaciones.

5.2.2.1.4. Personal

En este tipo de activos aparecen las personas relacionadas con los sistemas de comunicaciones. Además este tipo de activos (Personal) no se identifican dependencias. En el área del GADMU se han podido identificar que son los Administradores de Redes

5.2.2.2. Valoración de los activos

Se puede concluir que los activos con mayor valor muy alto para la organización en la dimensión de seguridad disponibilidad en forma descendente son los siguientes:

- Cuarto de telecomunicaciones
- Servidor de Base de datos
- Servidor de correo

5.2.2.3. Identificación de amenazas

Luego de la identificación de los activos se deben de identificar las amenazas que pueden afectar a cada activo, por lo que una amenaza puede desencadenar muchas más.

5.2.2.4. Valoración de las amenazas

En la valoración de amenazas, se estima la frecuencia y degradación de las que se vio necesario realizarla de forma manual para una mayor comprensión. Entonces una vez identificada la amenaza hay que estimar cuan vulnerable es el equipo activo, en dos sentidos: la degradación y la frecuencia.

En la figura 28, se indica la degradación que mide el daño causado por un incidente en el supuesto de que ocurriera. Se caracteriza con una fracción del valor del activo.

NIVELES	DEGRADACIÓN
0% - 25 %	Poco (P)
26% - 50%	Medio(M)
51% - 75%	Alto(A)
76% - 100%	Muy Alto(MA)

Figura 27. Indicativo para la degradación

Referencia: Basado en (Álvarez, 2014)

Para aquellos activos que reciben una calificación de impacto y/o riesgo muy alto deben ser objeto de atención inmediata y los que reciban una calificación de riesgo alto, deben ser objeto de planificación inmediata de salvaguardas. A continuación se muestra la escala que se tomara en consideración.

En la figura 29, se indica la valorización de la frecuencia es cada cuanto se materializa la amenaza, se modela como una tasa anual de ocurrencia, siendo valores típicos.

PERIODICIDAD	FRECUENCIA
360	A diario
12	Mensualmente
4	Cuatro veces al año
2	Dos veces al año
1	Una vez al año
1/12	Cada varios año

Figura 28. Valorización de la frecuencia

Referencia: Basado en (Álvarez, 2014)

En la siguiente tabla 31 se indica la frecuencia y degradación de los equipos activos.

Tabla 31. Valorización de amenazas en el GADMU

	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
Instalaciones	Cuarto de telecomunicaciones	Fuego Daños por agua Desastres naturales Desastres industriales Contaminación mecánica Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Errores del administrador Errores de mantenimiento actualización de programas Perdida de equipos Alteración de secuencia Acceso no autorizado Uso no previsto Manipulación de los equipos Emanaciones electromagnéticas Manipulación de Programas	2	75%
Person	Administradores de red	Indisponibilidad del personal Deficiencias en la organización Fugas de información Extorsión	12	75 %

al		Ingeniería social		
Equipamiento	Servidores	Fuego Daños por agua Desastres naturales Desastres industriales Contaminación mecánica Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Errores del administrador Errores de mantenimiento actualización de programas Perdida de equipos Alteración de secuencia Acceso no autorizado Uso no previsto Manipulación de los equipos Divulgación de información Manipulación de programas	2	25 %
Datos	Información de ciudadanos almacenada en la base de datos	Errores del administrador Alteración accidental de la información Destrucción de información Fuga de información Suplantación de identidad del usuario Abuso de privilegios de acceso Acceso no autorizado Modificación deliberada de la información Destrucción de información Divulgación de información	12	75

Referencia: Elaboración propia basado en (Álvarez, 2014)

En la tabla anterior se puede observar que los activos que mayor porcentaje de degradación y mayor frecuencia de que las amenazas es la información de ciudadanos almacenada en la base de datos y lo primero que los atacantes atacan es esta información.

5.2.2.5. Identificación de Salvaguardas

Una vez identificado las amenazas, se identificara los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos ofrecen (Disponibilidad, Integridad, Confidencialidad, Autenticidad). Las salvaguardas entran en el cálculo del riesgo de dos formas:

5.2.2.5.1. Reduciendo la frecuencia de las amenazas

Llamadas salvaguardas preventivas. Una salvaguarda preventiva ideal mitiga completamente la amenaza.

5.2.2.5.2. Limitando el daño causado

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance.

Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

Las salvaguardas se caracterizan, principalmente, por su eficacia frente al riesgo que pretenden conjurar.

En la tabla 32, se observa las diferentes salvaguardas que tienen los activos de red identificados anteriormente, con sus respectivas dimensiones de seguridad que estos ofrecen.

Tabla 32. Salvaguardas para activos de red

	ACTIVOS	**SALVAGUARDAS**
Instalaciones	Cuarto de telecomunicaciones	Control de los accesos físicos Aseguramiento de la disponibilidad Alarmas Ventilación Extintores Ups
Personal	Administradores de red	Formación y concienciación. Aseguramiento de la disponibilidad.
Equipamiento	Servidores	Claves. Protección del equipo dentro de la organización. Se aplica perfiles de seguridad. Autenticación del canal. Protección de la integridad de los datos intercambiados.
Datos	Información de ciudadanos almacenada en la base de datos	Protección de la información

Referencia: Elaboración propia basada en (Álvarez, 2014)

5.2.2.6. Estimación del impacto

En este paso permite conocer el alcance del daño producido, como resultado de la materialización de las amenazas sobre los activos.

Tabla 33. Impactos de parámetros

PARAMETRO	CONCEPTO	DIMENSIÓN	CAUSAS
Disponibilidad	La disponibilidad es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requiera a la información y a sus activos asociados.	**Alto**	Probablemente cause una interrupción sería de las actividades propias de la organización con un impacto significativo. Administración y gestión: probablemente impediría la operación efectiva de la organización. Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general. Intereses comerciales o económicos: de alto interés para la competencia, causa de graves pérdidas económicas. Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación. Información personal: probablemente afecte gravemente a un grupo de individuos. Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
Integridad	Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.	**Alto**	Impida la investigación de delitos graves o facilite su comisión. Administración y gestión: probablemente impedirá la operación efectiva de la organización. Intereses comerciales o económicos: causa de graves pérdidas económicas. Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación.

			Información personal: probablemente afecte gravemente a un grupo de individuos.
Confidencialidad	Es el aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.	**Medio**	Probablemente sea causa una cierta publicidad negativa: por afectar negativamente a las relaciones con otras organizaciones, por afectar negativamente a las relaciones con el público. Intereses comerciales o económicos: de cierto interés para la competencia, de cierto valor comercial. Información personal: probablemente quebrante leyes o regulaciones.
Autenticidad	Es el aseguramiento de la identidad u origen.	**Alto**	Administración y gestión: probablemente impedirá la operación efectiva de la organización. Intereses comerciales o económicos: causa de graves pérdidas económicas. Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación. Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal. Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

Referencia: Elaboración propia basada en (Álvarez, 2014)

5.2.3. ESTUDIO DE LA TEGNOLOGIA UTM

Hoy en día las amenazas son cada más peligrosas y complejas, por ende para implementar un sistema de seguridad es necesario varios sistemas de control de diferentes servicios que se encuentra en la red, proxy, firewall, antivirus, anti-spam.

La solución es centralizar los servicios y una excelente opción es la gestión de amenazas unificada. Los fabricantes para la seguridad perimetral cada vez sacan características nuevas, los fabricantes más comunes son: Juniper Networks, Astaro, SonicWall, Watchguard, Netgear, Crossbeam entre otras, para este caso se analizará la solución CISCO y JUNIPER ya que se poseen masivas características que se adaptan al proyecto.

5.2.4. COMPARACIÓN DE TEGNOLOGÍAS UTM

Para la elección del equipo UTM, se verificara la mejor opción para la institución según los costos y a las necesidades, las opciones presentas son JUNIPER y CISCO:

JUNIPER presenta una propuesta de acorde a la necesidad de empresas medianas y grandes aportando con lo último en tecnología de seguridad.

CISCO presenta con una alternativa en la confiabilidad en la red, pero ha implementado alternativas de seguridad en sus equipos, así que este proveedor no presentar una propuesta acorde a las necesidades de la empresa.

5.2.4.1. Elección del equipo para la seguridad perimetral

El dispositivo a escoger para proveer seguridad en el GADMU, el cual debe satisfacer la necesidad mínima de la institución a continuación se indicas cuales son:

5.2.4.2. Especificaciones técnicas

Para la elección es necesario cumplir con estas características mínimas para la el equipo firewall (cortafuegos), estas se determinaron mediante la relación con las

características de los servidores existentes en el GAD Municipal de San Miguel de Urcuquí las cuales son las siguientes:

1. Memoria RAM mínimo de 1024 MB.
2. Interfaces al menos seis con capacidad de 10 /100 / 1000 Mbps.
3. Capacidad de manejo de ancho de banda por interfaces.
4. Conexiones simultáneas al menos 400.000 sesiones.
5. Capacidad de servicio para 150 usuarios.
6. Disco duro al menos de 20 GB.
7. Soporte para Vlans (802.1Q) en sus interfaces.
8. Incluya capacitación al menos a dos personas.
9. Garantía del equipo al menos dos años.
10. Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc.)
11. Soporte autenticación mediante certificados 802.1X.
12. Interfaz para administración y configuración vía web, telnet y/o CLI.
13. Actualización automática de servicios de seguridad: IDS / IPS, Anti Spam, Antivirus (mínimo cada hora) y Lista de URLs.
14. Costo anual de las subscripciones a los servicios de seguridad.
15. Soporte técnico mensual.

5.2.4.3. Especificaciones funcionales

Se elige dos equipos JUNIPER (Network SCG 550 M) y CISCO (ASA 5550), se realiza la comparación entre estos determinando las necesidades mínimas como: características básicas, FIREWALL, VPN, IDS/IPS, antivirus, entre otros.

En la tabla 34, se explica las características mínimas que ofrece el equipo Juniper (Network SCG 550 M).

Tabla 34. Propuesta Juniper

JUNIPER	**Juniper Networks SSG 550M**
Características Requeridas	Características Ofrecidas
CARACTERÍSTICAS GENERALES	
Memoria RAM Mínimo 1024 MB	1024 MB
Interfaces al menos 6	Ethernet de 10/100/1000 Mbps 4 puertos 10/100/1000 Mbps
Manejo de ancho de banda por interfaces	Si
Conexiones simultáneas al menos 256.000	256.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	80 GB
Soporte para VLAN´S en sus interfaces	Virtualización, 150 VLAN´S
Autenticación certificados X.509v3 (PKI, IKE)	VeriSing, Entrust, Microsoft, RSA Keon, Baltimore, DoD PKI
Interfaz para administración: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	EAL4, EAL4+, ICSA (Firewall y VPN)
Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	VPN, SSH, HTTPS
Características y Servicios de Seguridad	
FIREWALL	
Rendimiento Firewall al menos de 1 Gbps	1 Gbps
Capacidad de Stateful Inspection	Si
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación a nivel de usuario basada LDAP, RADIUS, Active Directory y Novell Directory	LDAP, RADIUS, RSA SecurID
Capacidad para bloquear tráfico P2P, IM	Si
VPN	
Rendimiento VPN al menos 100 Mbps	500 Mbps
Capacidad para creación de VPN al menos 15 300	300
Soporte encriptación DES, 3DES, AES-128, AES-256	3DES, AES-256

Soporte VPN para autenticación SHA-1, MD5	SHA-1, MD-5
Soporte para encapsulamiento IPSec, SSL	L2TP, IPSec
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix.	
IDS / IPS	
Rendimiento IDS / IPS al menos 500 Mbps	No especifica
ANTIVIRUS	
Rendimiento del antivirus al menos 100 Mbps	No especifica
Filtrado web	Si
Anti Spam	Si
Reportes y Logs	Si

Referencia: Elaboración propia

En la tabla 35 se indica la propuesta de Cisco (ASA 5550)

Tabla 35. Propuesta Cisco

CISCO	**CISCO ASA 5550**
Características Requeridas	Características Ofrecidas
CARACTERÍSTICAS GENERALES	
Memoria RAM Mínimo 1024 MB	4096 MB
Interfaces al menos 6	8 Interfaces Ethernet 10/100/1000 Mbps 4 SPF Fiber 1 10/100 Mbps
Manejo de ancho de banda por interfaces	Si
Conexiones simultáneas al menos 256.000	650.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	No especifica
Soporte para Vlans en sus interfaces	250 Vlans
Autenticación certificados X.509v3 (PKI, IKE)	Certificados X.509, soporte CRL, (Certificate Revocation List)
ADMINISTRACIÓN	
Interfaz para administración: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	No especifica

Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	No especifica
Características y Servicios de Seguridad	
FIREWALL	
Throughput Firewall al menos de 1 Gbps	1,2 Gbps
Capacidad de Stateful Inspection	Si
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación a nivel de usuario basada LDAP, RADIUS, Active Directory y Novell Directory	AAA
Capacidad para bloquear tráfico P2P, IM	
VPN	
Throughput VPN al menos 100 Mbps	425 Mbps
Capacidad para creación de VPN al menos 15 300	No especifica
Soporte encriptación DES, 3DES, AES-128, AES-256	3DES, AES
Soporte VPN para autenticación SHA-1, MD5	No especifica
Soporte para encapsulamiento IPSec, SSL	PPTP, IPSec, SSL
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix	
Dispositivos CISCO Adicionales	CISCO IPS 4255 / CISCO ASA 5520
IDS / IPS	
Rendimiento IDS / IPS al menos 500 Mbps	500 Mbps
ANTIVIRUS	
Rendimiento del antivirus al menos 100 Mbps	450 Mbps
Filtrado web	Si
AntiSpam	Si
Reportes y Logs	Si

Referencia: Elaboración propia

5.2.5. ANÁLISIS DEL COSTO DEL SISTEMA DEL SEGURIDAD PERIMETRAL

El equipo SSG-500G fue la opción que se considera para la propuesta JUNIPER, y el equipo ASA5550 fue considerada para la propuesta CISCO, a continuación se realizar las tablas especificado que equipo cumple con las necesidades de la empresa. A continuación se presenta los costos monetarios de hardware, software y servicio suscripción (Licencias) y adicionales (instalación, configuración y capacitación) de las dos propuestas, para comparar precios para la selección de los equipos adecuado acorde a las necesidades tanto lógicas como monetarias.

5.2.5.1. Costo de la propuesta Juniper

En la tabla 36, se especifica el costo monetario de la propuesta cisco para el equipo (SSG550M).

Tabla 36. Costos para la propuesta Juniper

CANTIDAD	ELEMENTO	COSTO
	Hardware	
1	SSG 550M	10.500
	TOTAL	10.500
	Software	
1	Incluido en el dispositivo UTM (JUNOS)	0
	SERVICIOS Y SOPORTE (POR 12 MESES)	
	Protección	
SSG 550M	Anti-Virus Juniper-Kaspersky, NS-K-AVS-SSG550	3.150
	Anti-Spam, NS-SPAM-ISG1000	5.000
	Web Filtering, NS-WF-SSG550	2.300
	Deep Inspection, NS-DI-SSG550	1.050
	Soporte	
	J-Care Support Services, SVC-COR-SSG550M	750
	TOTAL	**12.250**
	ADICIONALES	
	Instalación y Configuración	950

	Capacitación 3 días	2.050
	TOTAL	**3.000**
	COSTO TOTAL DE LA SOLUCIÓN	**27.750**

Referencia: Elaboración propia

5.2.5.2. Costo de la propuesta cisco

En la tabla 37 se especifica el costo monetario de la propuesta cisco para el equipo (ASA 5550).

Tabla 37. Costos de la propuesta Cisco

CANTIDAD	ELEMENTO	COSTO
	HARDWARE	
1	CISCO ASA 5550 (ASA5550-BUN-K9)	12.00
	TOTAL	**12.00**
1	CISCO IPS 4255 (IPS-4255-K9)	15.00
	TOTAL	**15.00**
1	CISCO IPS 4255 (ASA5520-CSC20-K9)	10.00
	TOTAL	**10.00**
	SOFTWARE	
1	CISCO OS: Incluido en el dispositivo Hardware	0
	SERVICIOS Y SOPORTE (POR 12 MESES)	
Cisco IPS 4255	CON-SNTE-IPS-4255 Smartnet 8x5x4	3.000
Cisco ASA 5520 (Inspector de Contenidos)	ASA 5500 CSC SSM20 Plus Lie, Spam/URL/Phish	1.800
	CON-SNTE-AS2C20K9 Smartnet 8x5x4	1.500
	TOTAL	**6.300**
	ADICIONALES	
	Instalación y Configuración	1.400
	Capacitación 98 días (5 personas)	2.250
	TOTAL	**3.650**
	COSTO TOTAL DE LA SOLUCIÓN	**46.950**

Referencia: Elaboración propia

5.2.6. ESQUEMA PROPUESTO PARA LA SEGURIDAD PERIMETRAL

Con el análisis de riesgo y con la elección de equipos por la tecnología UTM se determina un equipo como Firewall (cortafuego) para el GAD Municipal de San Miguel de Urcuquí, el cual permitirá solucionar los problemas para las vulnerabilidades mediante la metodología MARGERIT analizada anteriormente. En la figura 30 se observa un esquema propuesto para la seguridad perimetral, el cual utiliza un equipo Juniper Networks SSG 550M con un equipo firewall (cortafuego) para restringir el tráfico que ingresa y sale.

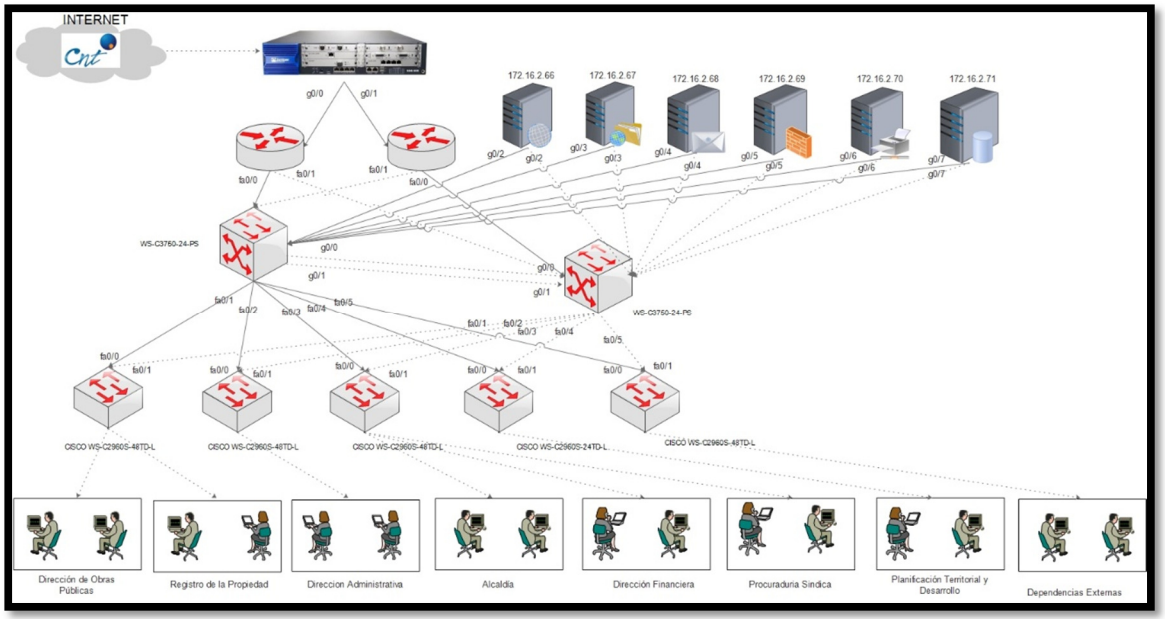

Figura 29. Esquema propuesto para la seguridad perimetral

Referencia: Elaboración propia

5.3. ELECCIÓN DEL SISTEMA OPERATIVO

Para la elección del sistema operativo se utilizó la norma ISO/IEC/IEEE 29148, a continuación se describe un resumen especificado los requisitos a seguir y valorización entre los diferentes sistemas operativos.

En el **ANEXO K**, se presenta el análisis de la norma ISO/IEC/IEEE 29148:2011(sistemas e ingeniería de software - ciclos de vida procesos - ingeniería de requisitos en el cual se indica los pasos a seguir para elección del sistema operativo.

5.3.1. REQUISITOS PARA EL SISTEMA OPERATIVO

En la tabla 38, se presentarán los requisitos más importantes que debe tener el sistema operativo.

Tabla 38. Requisitos para selección del sistema operativo

REQUISITOS	CRITERIOS	OBSERVACIONES
REQ01	Software Libre	El sistema operativo debe ser libre (con licencia GLP es decir usar el programa sin limitaciones).
REQ02	Estabilidad	El software no debe estar en desarrollo, debe ser una versión estable y estar disponible en la actualidad.
REQ03	Seguridad	Garantizar la seguridad al acceso.
REQ04	Velocidad del sistema de arranque	El arranque debe ser lo más rápido posible para mantener una comunicación eficiente.
REQ05	Velocidad de respuesta del sistema	La respuesta ante la transferencia de archivos y envió de paquetes debe ser lo más rápida posible.
REQ06	Documentación	Gran variedad de información, soporte y mantenimiento, además debe facilitar el aprendizaje y conocimiento.
REQ07	Repositorio de paquetes	Disponer de masiva variedad de paquetes para el funcionamiento correcto del sistema operativo.
REQ08	Configuración	Facilidades para configurar los administradores de red basada en consola.

REQ09	Compatibilidad	EL sistema operativo tendrá la facilidad de instalarse en la mayor variedad de arquitecturas presentes actualmente.
REQ10	Requisitos de Hardware	Fáciles de adquirir y en su mayoría de repuestos económicos.

Referencia: Elaboración propia basado en la norma ISO/IEC/IEEE 29148

5.3.2. ESTABLECIMIENTO DE VALORIZACIÓN PARA LOS REQUERIMIENTOS.

Mediante la tabla 39, se valoriza los requerimientos para la selección del sistema operativo base, se realiza la valoración perteneciente de los requerimientos:

Tabla 39. Valorización de requisitos

Requisitos	Valorización
REQ01: Software libre	0 No posee licencia libre 1 Posee licencia con costo 2 Posee licencia gratuita
REQ02: Estabilidad	0 Sistema operativo no estable 1 Sistema operativo estable
REQ03: Seguridad.	0 No tiene seguridad 1 Tiene seguridad completa
REQ04: Velocidad del sistema de arranque	0 Poca rapidez en el arranque 1 Su rapidez es moderada 2 Tiene mayor rapidez
REQ05: Velocidad de respuesta	0 Respuesta lenta 1 Respuesta moderada 2 Respuesta rápida
REQ06. Documentación	0 Poca 1 Media 2 Alta
REQ07. Repositorio de paquetes	0 Poca 1 Media 2 Alta
REQ08: Configuración	0 No posee una interfaz grafica 1 Posee una interfaz grafica 2 Configuración mediante consola
REQ09: Arquitecturas Soportadas	0 Soporta pocas arquitecturas 1 Soporta varias arquitecturas

REQ10: Requisitos de hardware	0 No opera en equipos de baja capacidad 1 Opera en equipos de baja capacidad

Referencia: Elaboración propia

En la tabla 40, se indica la valorización de cada uno de los sistemas operativos a elegirse (Centos, Ubuntu, Debian) esta se realizó conjuntamente con la información de la tabla 39.

Tabla 40. Cálculo de requisitos para selección del sistema operativo

	CENTOS	**UBUNTU**	**DEBIAN**
REQ01	2	1	2
REQ02	2	1	2
REQ03	2	1	2
REQ04	2	1	1
REQ05	2	1	2
REQ06	2	2	1
REQ07	2	2	1
REQ08	2	1	1
REQ09	1	1	0
REQ10	1	0	0
TOTAL	18	11	12

Referencia: Elaborado por autor basado en la norma ISO/IEC/IEEE 29148

Luego de analizar los requerimientos se determinó que la mejor opción es el sistema operativo Centos, ya que tiene la mayor valorización en los requerimientos analizados en la tabla 40. Con el cuál se realizará la implementación de los servidores FTP y PROXY SQUID. En el **ANEXO H,** se indica el proceso a seguir para la instalación de Centos.

En el **ANEXO I,** se presenta la elaboración del servidor FTP el cual ayudará para almacenar información importante, para lo cual cada empleado del edificio tendrá acceso mediante un usuario y contraseña establecido por el departamento de sistemas.

En el **ANEXO J,** se presenta la elaboración del servidor PROXY SQUID el cual limitará el acceso a páginas no autorizadas las cuales son definidas por el departamento de sistemas.

CAPITULO VI

6. ANÁLSIS COSTO-BENEFICIO

En este capítulo se da a conocer todos los costos que se utilizaran para el rediseño de la red de datos y optimización de seguridad perimetral para una futura implementación para la red de datos.

6.1. COSTOS DE LOS EQUIPOS Y MATERIALES NECESARIOS

Los costos referenciales en caso de que se desee implementar, se han tomado de páginas como: mercado libre[3], empresas proveedoras de equipos de redes[4], empresas de los mismos fabricantes[5], entre otros.

6.1.1. COSTO DE EQUIPOS PARA EL REDISEÑO DE LA RED INTERNA DEL GAD

En la tabla 41, se muestran los equipos que existen en la Institución y se reusarán para beneficio del rediseño.

Tabla 41. Equipos de reúso para el Sistema

EQUIPO	CANT.	VALOR UNIT.	VALOR TOTAL
SERVIDOR PROLIANT E5649	1	2.730	2.730
SERVIDOR PROLIANT ML170	1	1.880	1.880
TOTAL			4.610

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

[3] http://www.mercadolibre.com.ec/
[4] http://www.router-switch.com/ws-c4510r-e-p-517.html
[5] http://www.dlinkla.com/

En la tabla 42, se detallan los costos de los equipos que deberán ser comprados por la institución, para el rediseño de la red interna.

Tabla 42. Costo de Equipos para el rediseño de la der del GAD

EQUIPO	CANT.	VALOR UNIT.	VALOR TOTAL
Switch (CISCO WS-C2960S-48TD-L[6])	4	2.278	9.112
Switch (CISCO WS-C2960S-24TD-L[7])	1	1.629	1.629
Switch (CISCO WS-C3750X-24-PS[8])	2	3.024	6.048
TOTAL			16.789

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

COSTO DE EQUIPOS PARA SEGURIDAD PERIMETRAL

En la tabla 43, se detallan los costos de equipos para seguridad perimetral que deberán ser comprados por la institución si se desea la implementación.

Tabla 43. Costo de equipos para seguridad perimetral

EQUIPO	CANT.	VALOR UNIT.	VALOR TOTAL
SSG 550M[9]	1	10.500	10.500
Anti-Virus Juniper-Kaspersky, NS-K-AVS-SSG550	1	3.150	3.150
Anti-Spam, NS-SPAM-ISG1000	1	5.000	5.000
Web Filtering, NS-WF-SSG550	1	2.300	2.300
Deep Inspection, NS-DI-SSG550	1	1.000	1.000
J-Care Support Services, SVC-COR-SSG550M	1	750	750
TOTAL			22.700

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

[6] http://www.router-switch.com/ws-c2960s-48td-l-p-1510.html
[7] http://www.router-switch.com/ws-c2960s-24td-l-p-1511.html
[8] http://www.router-switch.com/ws-c3750x-24p-s-p-1536.html
[9] http://www.amazon.com/Juniper-550M-Firewall-NEBS Compliant/dp/B007Q1Y8JU/ref=sr_1_3?s=pc&ie=UTF8&qid=1453352847&sr=1-3&keywords=SSG+550M

COSTO DE MATERIAL DE RED

En la tabla 44, se detallan los costos de materiales de red que deberán ser comprados por la institución, para la red inalámbrica interna.

Tabla 44.Costo de materiales de red

DESCRIPCIÓN	CANT.	VALOR UNIT.	VALOR TOTAL
Cable UTP Cat 6A(305m)[10]	2 rollo	350,00	700,00
Conector RJ-45[11]	1 caja	8,50	8,50
Canaletas plásticas 32x12[12]	10	2,10	21,60
TOTAL			730,1

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

COSTO DE MATERIAL ELÉCTRICO

En la tabla 45, se detallan los costos de materiales eléctricos que deberán ser comprados por la institución.

Tabla 45.Costo de material eléctrico

DESCRIPCIÓN	CANT.	VALOR UNIT.	VALOR TOTAL
Tomas eléctricas[13]	30	0,20	6,00
Cable eléctrico 12AWG[14]	2 rollos 100mts c/u	40,00	80,00
TOTAL			86,00

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración Propia

COSTO DE MANO DE OBRA

En la tabla 46, se detallan los costos de mano de obra que deberán ser contratados por la institución, para las instalaciones de los equipos para seguridad

[10] http://www.tuugo.ec/Companies/jr-electric-supply-cia/1260007531#!
[11] http://www.tuugo.ec/Companies/jr-electric-supply-cia/1260007531#!
[12] http://www.tuugo.ec/Companies/jr-electric-supply-cia/1260007531#!
[13] http://www.tuugo.ec/Companies/jr-electric-supply-cia/1260007531#!
[14] http://www.tuugo.ec/Companies/jr-electric-supply-cia/1260007531#!

perimetral, parte de cableado estructurada correspondiente a rediseño de red y configuración de equipos de red. El número de personas necesarias para el trabajo es de 2 personas.

Tabla 46.Costo de mano de Obra

DESCRIPCIÓN	# PERSONAS	COSTO/DÍA	#DIAS	TOTAL
Mano de obra calificada[15]	2	250	4	$ 1000

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración Propia

6.2. DETERMINACIÓN DE COSTO TOTAL DEL REDISEÑO DE LA RED DE DATOS Y OPTIMIZACION DE LA SEGURIDAD PERIMETRAL

En la tabla 47, se observa que la sumatoria de gastos para la parte del rediseño de la red y la seguridad perimetral

Tabla 47.Costos totales del rediseño de la red y seguridad perimetral

DESCRIPCIÓN	COSTO
Costo de equipos para rediseño de la red interna	16.789,00
Costo de equipos para seguridad perimetral	22.700,00
Costo de material de red	817,71
Costo de material eléctrico	96,32
Costo mano de obra	1.000,00
SUBTOTAL	40.722,49
IVA 12%	4.886,69
TOTAL	45.609,18

Referencia: Elaboración Propia

[15] (TELMAT, s.f.) que presta los servicios de técnicos calificados hace mención que la mano de obra calificada de un técnico con respecto a video-vigilancia tiene un valor aproximado de 40 dólares el día.

6.2.1. DETERMINACIÓN DEL BENEFICIO

En el GAD Municipal de San Miguel de Urcuquí actualmente trabajan 125 empleados, distribuidos entre el edificio principal y las dependencias externas. El pago mensual que desembolsa la institución es de 156.748,75 dólares, en el **ANEXO L,** se muestra una tabla con los valores detallados de salarios de cada empleado.

Para determinar el salario promedio de cada trabajador, se aplica la ecuación 13.

$$Valor\ a\ pagar\ mensualmente\ a\ cada\ empleado = \frac{Sueldo\ desembolsado\ mensualmente}{Número\ total\ de\ empleados}$$

Ecuación 13. Cálculo del sueldo promedio

Referencia: Elaboración Propia

$$Valor\ a\ pagar\ mensualmente\ a\ cada\ empleado = \frac{156.748{,}75\ dólares}{125\ empleados}$$

$$Valor\ a\ pagar\ mensualmente\ a\ cada\ empleado = \$\ 1.253{,}99$$

En la tabla 47, se detalla el valor a pagar de cada empleado de forma: mensual, diaria, por hora y por minuto, para objeto de cálculo.

Tabla 48. Valores monetario que recibe cada empleado

DESCRIPCIÓN	VALOR
Valor a pagar mensualmente a cada empleado	1.253,99 dólares
Valor a pagar diariamente a cada empleado	41,79 dólares
Valor a pagar por hora para cada empleado	5,22 dólares
Valor a pagar por minuto para cada empleado	0,08 ctvs.

Referencia: Elaboración Propia

Los empleados de dicha institución, trabajan 8 horas diarias establecidas por la ley. Sin embargo; debido a problemas en la red actual no se trabaja de manera continua, lo cual provoca distracciones de los funcionarios y genera pérdidas a la institución. Se realizó una encuesta a 25 personas escogidos alzar, para determinar un promedio de tiempo en la que la red no está disponible, obteniendo como resultados un promedio del 5%. En el **ANEXO M,** se muestra la encuesta y su tabulación.

Mediante la ecuación 14, se determina el tiempo (horas) sin servicio en el GAD Municipal de San Miguel de Urcuquí.

$$5\%\_en\_horas = (8\ horas)x\ 0{,}05 = 0{,}4\ horas$$

Ecuación 14. Determinación del tiempo sin servicio por horas

Referencia: Elaboración Propia

Conjuntamente con la ecuación anterior se determina el cálculo de pérdida del servicio en minutos, especificado en la ecuación 15.

$$5\%\_en\_minutos = \ 0{,}4\ x\ (60\ minutos) = 24 minutos$$

Ecuación 15. Determinación del tiempo sin servicio por minutos

Referencia: Elaboración Propia

Con estos valores podemos concluir que el 5% de indisponibilidad del servicio de red corresponde a 24 minutos al día, en la ecuación 16, se multiplica este tiempo por el valor promedio que gana cada trabajador por minuto, arrojando un valor de 2,08 dólares.

$$Beneficio\ por\ cada\ empleado = \ 24\ minutos\ x\ 0{,}08\ ctvs = 2{,}08\ dólares$$

Ecuación 16. Beneficio total por día

Referencia: Elaboración Propia

En la ecuación 16, se determina el beneficio total diario, que el GADMU ahorraría si la red estuviera en buen estado.

$$Beneficio_{total_{diario}} = 2{,}08\ dólares\ x\ 125\ empleados = 261{,}25\ dólares$$

En la tabla 49, se describe el beneficio por diario, semanal, mensual y anual.

Tabla 49. Resumen del cálculo de beneficio

DESCRIPCIÓN	BENEFICIO
Valor del beneficio total por día	261,25 dólares
Valor del beneficio total por semana	1.828,75 dólares
Valor del beneficio total por mes	7.837,43 dólares
Valor del beneficio total por año	94.050,00 dólares

Referencia: Elaboración Propia

6.2.2. CALCULO COSTO/BENEFICIO

Luego del análisis de los gastos y beneficios que genera el proyecto, aplicamos la ecuación 17, para determinar el beneficio/costo, para lo cual se usa los siguientes parámetros:

- Si B/C es mayor que 1 se acepta el proyecto
- Si B/C es igual a 1 el proyecto es indiferente
- Si B/C es menor que 1 se rechaza el proyecto

$$\frac{B}{C} = \frac{\Sigma\ \text{Beneficios}}{\Sigma\ \text{Costos}}$$

Ecuación 17. Cálculo del Beneficio/Costo

Fuente: (Buettrich, 2014)

$$\frac{B}{C} = \frac{94.050{,}00}{45.609{,}18} = \mathbf{2.06}$$

Al aplicar la ecuación el valor es de 2,06; por lo que se determina que el proyecto es aceptable.

6.2.3. PERIODO DE DEVENGACIÓN

La tabla 50, se aplica para determinar en qué mes se recupera la inversión, sin embargo para tener un período de tiempo más exacto se aplica la ecuación 18.

Tabla 50. *Periodo de devengación*

MES	BENEFICIO / MES	BENEFICIO ACUMULADOS
		- 45.609
1	7.837,44	7.837
2	7.837,44	15.675
3	7.837,44	23.512
4	7.837,44	31.350
5	7.837,44	39.187
6	7.837,44	47.025

Nota: el valor de 45,609 es el costo total especificado en la tabla 46 y el valor de 7.837,44 es el cálculo del beneficio por mes especificado en la tabla 48

Referencia: Elaboración propia

$$\text{Período \_devengación} = mes\ de\ devengación + \left(\frac{Costo\ total - \Sigma\ de\ 6\ meses}{Beneficio\ Mensual}\right)$$

Ecuación 18: Período de recuperación de la inversión

Fuente: (Monteros, 2015)

$$\text{Período \_devengación} = 6\ meses + \left(\frac{45.609 - 47.025}{7.837,44}\right)$$

$$\text{Período \_devengación} = 6\ meses + (0{,}18\ x\ 30 dìas)$$

$$\text{Período \_devengación} = 6\ meses + 5\ dìas$$

Estos cálculos nos muestran que se tendrá un período de devengación de la inversión de 6 meses y 5 días.

6.3. BENEFICIARIOS DEL PROYECTO

Los beneficiarios directos son todos aquellos que hacen uso del sistema directo o indirectamente, a continuación se detallan cada uno de ellos.

6.3.1. DIRECTOS

Los beneficiarios directos son todos los 125 usuarios que se encuentran en el edificio central del Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí distribuidos en empleados, trabajadores y personal a contrato.

6.3.2. INDIRECTOS

Los beneficiarios indirectos son todas aquellas personas que hacen uso de los servicios que presta el GAD San Miguel de Urcuquí, ya que con la implementación del proyecto propuesto se beneficiarán al realizar sus trámites (servicios que brinda la el GADMU a la ciudadanía) sin inconvenientes, esto incurre en ahorro de gastos de movilización y pérdida de tiempo en movilización desde sus hogares hacia la municipalidad.

CAPITULO VII

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Mediante la utilización de libros, artículos y tesis afines al tema, se estableció criterios esenciales para la elaboración de la fundamentación teórica de los componentes involucrado en la investigación.

- Como resultado del levantamiento de información de la situación actual de la red, se determinó que el estado físico de la red no cumple con ninguna norma de cableado estructurado; ocasionando inconformidad para los empleados y esto va en concordancia con el estado lógico de la red; la misma que no se encuentra configurada adecuadamente ya que los equipos no son administrables y se encuentran difundiendo dominios de broadcast ocasionando la saturación del éstos, afectando el rendimiento de la red.

- Mediante el cálculo del tráfico interno y externo que se genera cada usuario, y conjuntamente con el análisis del dimensionamiento de equipos activos se determinó los equipos de red a utilizarse y se escogió la marca Cisco porque brinda una solución adaptable al proyecto y con la ventaja en los ahorro monetarios para GAD Municipal de San Miguel de Urcuquí, además estos equipos son excelentes para en ámbitos de producción, y ofrece una gama amplia de productos con precios accesible para la empresa, con beneficio en los siguientes aspectos confiabilidad, escalabilidad y fiabilidad.

- Para el rediseño de la red de datos del GADMU se implementa un modelo jerárquico basado en capas que mejorará características de disponibilidad, escalabilidad y flexibilidad; de esta manera se puede optimizar el

rendimiento de la de red, a nivel de enlaces físicos y equipamiento activo, asegurando la continuidad del servicio.

- El servidor FTP permite mejorar el acceso a los archivos de los empleados, y con el servidor PROXY SQUID se limitará el acceso a páginas de entretenimiento no autorizadas por el GADMU, ayudando a mejorar el desempeño de los empleados y reduciendo el tráfico innecesario en la red.

- Para seleccionar los requerimientos del software que tendrá los servidores FTP y Proxy SQUID, se propuso un análisis con la norma IEEE-STD-830-1998 pero en el desarrollo se concluyó que esta no está vigente, por ende se utilizó la norma ISO/IEC/IEEE 29148; la misma que brinda una solución para elección adecuada del sistema operativo eligiendo características esenciales como robustez, estabilidad, con la que se determinó que Centos 6.3 (32 bits) modo texto, es la opción más factible para la implementación de los servidores.

- Para simular la red se propuso GNS3 la versión 1.3.0, debido a que cumplen características similares a los equipos elegidos con los switches 2960 y 3560.

- Mediante el análisis de riesgos mediante la metodología MARGERIT y conjuntamente con la tecnología UTM, se determinó que la mejor opción para la implementación de la seguridad perimetral es Juniper, ya que en comparación con otras marcas, tiene un precio económico al alcance de la empresa; mejorando la protección de la información personal, prevención de intrusos, control de acceso del usuario, seguridad, administración e ingreso a las aplicaciones de forma seguras.

- El proyecto es rentable según los cálculos del costo/beneficio, recuperando así la inversión en un periodo de 6 meses y 5 días

6.2. RECOMENDACIONES

- Se recomienda que el personal a cargo de la red de datos del GADMU, continuamente se encuentre el en proceso de capacitación y aprendizaje, lo cual ayudaría a solucionar problemas de forma rápida.

- Se debe llevar una bitácora donde conste todos los eventos que se presentan en la red y los incidentes con las acciones que se realizaron para de esta manera si el personal cambia, el nuevo responsable de red, pueda entender el estado de actual de la misma y sea más sencilla su administración.

- Se propone implementar políticas de seguridad en la institución que permita establecer niveles de seguridad, orientadas a la parte de la organización, tecnológica y de usuarios, de manera que regule y controle el uso y acceso a la red.

- Se aconseja restringir el acceso mediante el uso de biométricos e incluir cámaras para registrar lo eventos maliciosos que puede ocurrir en este.

- Se sugiere cambiar las contraseñas periódicamente, estas deben contener letras mayúscula, minúsculas, números y caracteres especiales para mayor seguridad.

- Es indispensable tener un backup de las configuraciones realizadas en los equipos, ya que en caso de la una configuración mal realizada se puede restaurar el sistema sin afectarlo.

- Se recomienda la utilización de herramienta de monitoreo, para determinar los incidentes o eventos que suscitan en la red.

- Se debe tomar en cuenta que ningún equipo brinda seguridad completa, por lo cual se debe adquirir equipos de seguridad adicionales para tener más confiabilidad en el sistema.

BIBLIOGRAFÍA

Aguilera, P. (s.f.). *Seguridad Informatica.* Editex.

Alulema, D. (14 de Junio de 2010). *Estudio y diseño de un sistema de seguridad perimetral utilizando tecnologia UTM.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/618/1/CD-1580%282008-06-30-03-34-00%29.pdf.

Andrade, L. (17 de Septiembre de 2012). *Categorias del cable UTP.* Obtenido de http://es.scribd.com/doc/5443708/Categorias-de-Cable-UTP#scribd.

Andreu, J. (2014). *Redes Locales.* México: Editex.

Arciniega, L. (11 de Enero de 2010). *Cable coaxial.* Obtenido de http://docente.ucol.mx/al003306/Teleprocesos2/cable%20coaxial.html.

Arias, G. (11 de Marzo de 2012). *Diseño de una red de voz y datos para una industria agricola utilizando la plataforma CISCO.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/5455/1/T1895.pdf-

Arteaga, F. (14 de Agosto de 2010). *Modelo OSI y TCP.* Obtenido de https://books.google.com.ec/books?id=WWD-4oF9hjEC&pg=PA37&dq=modelo+osi&hl=es&sa=X&ei=HwWSVZ6BNoXQtQX0qoPADQ&ved=0CCIQ6AEwAQ#v=onepage&q=modelo%20osi&f=false

Atelín, F. (2011). *Transmisión asincrónica y sincrónica.* El Salvador: ENI.

Ayala, C. (2012 de Septiembre de 02). *VLSM (MASCARAS DE SUBRED DE LONGITUD VARIABLE)*. Obtenido de http://southworks.com/blog/2008/09/02/vlsm-mascaras-de-subred-de-longitud-variable/.

Benavides, A. (16 de Agosto de 2013). *ETHERNET 10BASE-F.* Obtenido de http://www.textoscientificos.com/redes/ethernet/10base-f.

Bernal, L. (17 de Octubre de 2013). *Medios de Transmisión.* Obtenido de http://es.slideshare.net/JacquelineMuozAnacona/medios-de-transmision-jacqueline-muñoz.

Boquera, M. C. (2012). *Servicios avanzados de telecomunicaciones .* Madrid.

Candela, S., García, R., Quesada, A., Santana, F., & Santos, J. M. (2013). *FUNDAMENTOS DE SISTEMAS OPERATIVO.* España: Librotex.

Casas, D. (2013 de Octubre de 22). *Subnetting, subredes y máscaras de red*. Obtenido de http://informaticacoslada.com/subnetting-subredes-mascaras-de-red/.

Castro, A. (2012). *Señales ,Analógicas y Digitáles.* Barcelona: Reverté. Obtenido de https://books.google.com.ec/books?id=W5qfR_axiGsC&pg=PA54&dq=se%C3%B1ales+analogicas+y+digitales&hl=es&sa=X&ei=HxmGVevTHJLBgwTJ0oCABQ&ved=0CBsQ6AEwAA#v=onepage&q=se%C3%B1ales%20analogicas%20y%20digitales&f=false.

Cesamar, O. (12 de Septiembre de 2011). *Niveles de acceso.* Obtenido de https://iproot.wordpress.com/2013/04/01/ios-comandos/.

Dirección IP Clase A, B, C, D y E. (12 de Febrero de 2012). Obtenido de https://ricardoral.files.wordpress.com/2012/02/subneteo.pdf.

Dominios de Colisión y Difusión. (26 de Febreo de 2011). Obtenido de https://telematika2.wordpress.com/2011/02/26/dominios-de-colision-y-difusion/.

Dordoigne, J. (2013). *Estructura de una direccion IPV4.* Argentina: Edinor.

Ecured. (2016 de Marzo de 21). *Medios guiados y no Guiados*. Obtenido de http://www.ecured.cu/Medios_Guiados_y_no_Guiados.

España, M. (2011). *Imágenes de direccionamiento IP.* Madrid: Diaz de Santos.

Especificación de Requisitos según el estándar. (13 de Mayo de 2011). Obtenido de http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf.

Fernandez, S. (s.f.). *Cuánto hay que separar los cables*. Obtenido de http://marismas-emtt.blogspot.com/2010/09/cuanto-hay-que-separar-los-cables.html.

Fundamentos en seguridad de la información en redes. (11 de Marzo de 2011). Obtenido de http://dspace.ucbscz.edu.bo/dspace/bitstream/123456789/1009/1/4466.pdf.

Gallegos, J. C. (2011). *Instalación y mantenimiento de redes para trasmision de datos.* Editoria Editex.

Garometta, O. (19 de Octubre de 2010). *Seguridad en el acceso a dispositivos Cisco.* Obtenido de http://librosnetworking.blogspot.com/2008/10/seguridad-en-el-acceso-dispositivos.html.

Gobierno Urcuquí, A. D. (s.f.). *Gobierno Autónomo Descentralizado de San Miguel de Urcuquí*. Obtenido de http://www.municipiourcuqui.gob.ec/munurcuqui/.

Guillén, C. (18 de Marzo de 2012). *Modos Simplex Half-Duplex y Full-Duplex.* Obtenido de http://www.eveliux.com/mx/Modos-Simplex-Half-Duplex-y-Full-Duplex.html.

Guitiérrez, M. (19 de Febrero de 2010). *Características y Específicaciones: 10BASE5, 10BASE2, 10BASET.* Obtenido de

https://marcogutierrez.wordpress.com/2009/08/31/caracteriisticas-especificaciones-10base5-10base2-10baset/.

Gutierrez, A. (09 de Marzo de 2016). *Qué es la dirección IP y diferencia entre IPv4 e IPv6*. Obtenido de http://windowsespanol.about.com/od/RedesYDispositivos/f/Que-Es-Ip-Ipv4-Ipv6.html.

Heredia, A. (11 de Agosto de 2012). *Comunicación y Redes-CABLES UTP - STP.* Obtenido de http://comunicacionyredesinfo.blogspot.com/2012/08/cables-utp-stp.html.

Lechtaler, Ricardo, & Fusario. (2010). *Teleinformática para ingenieros en sistemas de información.* España: EDITORIAL REVERTÉ.

LINEAMIENTOS PARA LA ELABORACIÓN DE PROYECTOS DE CABLEADO ESTRUCTURADOS. (s.f.). Obtenido de http://www.dnic.unal.edu.co/docts/LINEAMIENTOS%20PARA%20PROYECTOS%20DE%20CABLEADO.pdf.

LINEAMIENTOS PARA LA ELABORACIÓN DE PROYECTOS DE CABLEADO ESTRUCTURADOS EN LA. (s.f.). Obtenido de http://www.dnic.unal.edu.co/docts/LINEAMIENTOS%20PARA%20PROYECTOS%20DE%20CABLEADO.pdf.

Llagua, A. (9 de Diciembre de 2012). *Dirección IP Clase A, B, C, D y E.* Obtenido de http://alejollagua.blogspot.com/2012/12/direccion-ip-clase-b-c-d-y-e.html

Manual para aplicar la norma TIA/EIA para cableado estructurado. (s.f.). Obtenido de http://dgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Manual%20para%20aplicar%20la%20norma%20TIA.EIA%20para%20Cableado%20Estructurado.pdf.

Marin, Y. (2012 de Enero de 2012). *Direccionamiento Mac.* Obtenido de http://7422agos.wikispaces.com/5.1.1+Direccionamiento+Mac.

Maya, E. (12 de Mayo de 2014). *Red inalámbrica de sensosres a travéz de 6OWPAN para una agricultira de precisición en Ibarra.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/7897/9.56.000617.pdf?sequence=4.

Meneses, L. (29 de Enero de 2013). *Aspectos Generales de seguridad en informática.* Obtenido de http://repositorio.utc.edu.ec/bitstream/27000/536/1/T-UTC-1052(1).pdf.

Mifsud, E. (s.f.). *Introducción a la seguridad informática - Vulnerabilidades de un sistema informático*. Obtenido de http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3.

Modelos de seguridad. (s.f.). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ModelosSeg.php.

NOGUERA, J., & VÁSQUEZ, A. (2011). *Diseño eimplementación de un circuito cerrado de televisión con cámaras IP inalámbricas y monitoreo remoto, notificaciones de eventualidades mediante el uso de un servidor para la grabación de video bajo la plataforma Linux usando zonemider para el labora.* Quito.

Normas sobre cableado estructurado. (12 de Enero de 2011). Obtenido de http://unitel-tc.com/normas-sobre-cableado-estructurado/.

Palomeque, Y. (s.f.). *Mantenimiento preventivo y correctivo* . Obtenido de http://evanyyineth.blogspot.com/.

Quilca, P. (13 de Marzo de 2011). *Modelo de referencia TCP/IP-Administración de redes.* Obtenido de https://docs.fajardo.inter.edu/Acad/atorres/CSIR2121/Shared%20Documents/El%20modelo%20de%20referencia%20TCP_IP.pdf.

Redes de LAN. (28 de Septiembre de 2010). Obtenido de http://pantheanet.blogspot.com/2012/01/tema-1-diseno-de-lan.html.

Rios, J. (12 de Octubre de 2012). *Importancia de Seguridad en Redes.* Obtenido de http://es.slideshare.net/Cibernauta1991/importancia-seguridadredes.

Romero, A. (s.f.). *Configuración de listas de acceso* . Obtenido de http://virtualbook.weebly.com/uploads/2/9/6/2/2962741/ac__list.pdf.

Róvira, J. (24 de Junio de 2010). *Fundamentos de Óptica.* Obtenido de https://books.google.com.ec/books?id=C3MlCEpvxLAC&pg=PA37&dq=que+es+el+espectro+electromagnetico&hl=es&sa=X&ei=WTBmVYiJM5X-sASZhoCICA&ved=0CBsQ6AEwAA#v=onepage&q=que%20es%20el%20espectro%20electromagnetico&f=false.

Ruiz, J. (19 de Marzo de 2015). *CSMA/CD.* Obtenido de http://docente.ucol.mx/al970310/public_html/CSMA.html.

Solano, J. (14 de Septiembre de 2010). *Modelo OSI.* Obtenido de http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml22/documentos/index2.html.

Solano, J. (s.f.). *El modelo OSI* . Obtenido de http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml22/index.html.

Staky. (s.f.). *Cisco Networking Academy Program*. Obtenido de http://www.uhu.es/diego.lopez/REDES0708/CCNA-1-2.pdf.

Stalling, W. (2011). *Fundamentos de seguridad en redes aplicaciones y estándares.* España: Pearson.

Tanenbaum, A. (2011). *Redes de computadoras.* México: Pearson.

Tipos de servidores. (2015). Obtenido de http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179.

TOPORED. (03 de Abril de 2016). Obtenido de http://topored.wikifoundry.com/page/Broadcast+y+Transmision+de+Tokens.

Vasco, M. (12 de Octubre de 2010). *Dimensionamiento de una central telefónica IP utilizando estandares abiertos y software libre para la empresa conectividad global.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/2497/1/CD-3199.pdf.

Vásquez, M. (18 de Julio de 2012). *Ancho de banda Importancia del ancho de banda.* Obtenido de http://www.alfinal.com/Temas/bandaancha.php.

Villalba, S. (2011). *Diseño de un esquema de seguridad para la intranet y extranet del CONESUP*. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/562/1/CD-1073.pdf.

Vinueza, A. (s.f.). *Calculo del porcentaje del crecimiento anual*. Obtenido de http://es.calcuworld.com/calcular-porcentaje-de-crecimiento-con-excel/.

Willian. (2011). *Redes.* Argentina.

ACRÓNIMOS

GBPS: GIGABIT PER SECONDS (Gigabit por segundo)

MBPS: MEGABIT PER SECONDS (Megabit por segundo)

STP: SHIELDED TWISTED PAIR (Par trenzado blindado)

UTP: UNSHIELDED TWISTED PAIR (Par trenzado sin blindaje)

OSI: OPEN SYSTEM INTERCONECCION (Interconexión de Sistemas Abiertos)

TCP/IP: TRANSMISSION CONTROL PROTOCOL (Protocolo de control de transmisión) / INTERNET PROTOCOL (Protocolo de internet)

ISO: INTERNATIONAL STANDARDS ORGANIZATION (Organización Internacional de Estándares)

NIC: NETWORK INTERFACE CARD (Tarjeta de interfaz de red)

MAC: MEDIA ACESS CONTROL (Control de acceso al medio)

LLC: LINK LOGICAL CONTROL (Control de enlace lógico)

CSMA/CD: CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (Acceso Múltiple por Detección de Portadora con Detección de Colisiones

HTTP: HYPERTEXT TRANSFER PROTOCOL (Protocolo de transferencia de hipertexto)

ARP: ADDRESS RESOLUTION PROTOCOL (Protocolo de Resolución de Direcciones)

RARP: REVERSE ADDRESS RESOLUTION PROTOCOL (Protocolo de Resolución de Dirección Inversa)

TCP: TRANSMISSION CONTROL PROTOCOL (Protocolo del Control de Transmisión)

UDP: USER DATAGRAM PROTOCOL (Protocolo de Datagrama de Usuario)

TELNET: TELECOMUNICACIÓN NETWORK (Red de Telecomunicaciones)

FTP: FILE TRANSFER PROTOCOL (Protocolo de Transferencia de Archivos*)*

SMTP: SIMPLE MAIL TRANSFER PROTOCOL (Protocolo Simple de Transferencia de Correo)

DNS: DOMAIN NAME SYSTEM (Sistema de nombres de dominios)

NAT: NETWORK ADDRESS TRANSLATION (Traducción de direcciones de red)

VLSM: VARIABLE LENGTH SUBNET MASK (Máscara de subred de longitud variable)

OSPF: OPEN SHORTEST PATH FIRST (Primero el Camino Libre más Corto)

EIGRP: ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (Protocolo de Enrutamiento de Gateway Interior Mejorado)

RIPV2: ROUTING INFORMATION PROTOCOL VERSION 2 (Protocolo de Información de Enrutamiento)

WIFI: WIRELESS FIDELITY (Fidelidad Inalámbrica)

MAN: METROPOLITAN ÁREA NETWORK (Redes de área metropolitana)

WAN: WIDE ÁREA NETWORK (Redes de área amplia)

VLAN`S: VIRTUAL LOCAL AREA NETWORK (Red de área local virtual)

ACL: ACCESS CONTROL LIST (Lista de control de acceso)

QOS: QUALITY OF SERVICE (Calidad de servicio)

ODF: OPTICAL DISTIBUTION FRAME (Distribuidor de Fibra Óptica)

UPS: UNINTERRUPTIBLE POWER SUPPLY (Sistema de potencia ininterrumpida)

ANSI: AMERICAN NATIONAL STANDARDS INSTITUTE (Instituto nacional estadounidenses de estándares)

EIA: ELECTRONICS INDUSTRY ASSOCIATION (Asociación de industrias electrónicas)

TIA: TELECOMMUNICATIONS INDUSTRY ASSOCIATION (Asociación de la industria de telecomunicaciones)

HSRP: HOT STANDBY ROUTING PROTOCOL (Protocolo de enrutamiento de espera caliente)

LACP: LINK AGGREGATION CONTRL PROTOCOL (Protocolo de control de agregación de enlaces)

GLP: General Public License (Licencia publica general)

ANEXOS

ANEXO A

INCUMPLIMIENTO DE NORMAS Y ESTÁNDARES DE CABLEADO ESTRUCTURADO

Basados en las normas y estándares de cableado estructurado, durante el levantamiento de información se detectó el incumplimiento de algunas de ellas. Las más importantes se enumeran a continuación:

SUBSISTEMA HORIZONTAL

La norma ANSI/EIA/TIA 568-A (Estándar de Edificios Comerciales para Cableado de Telecomunicaciones) establece lo siguiente:

- No deben existir empalmes a lo largo del subsistema horizontal, sin embargo debido al mal dimensionamiento de los cables se ha colocado jacks flotantes y patch cords para reflejarse en el patch panel.

- Todas las conexiones realizadas hacia el área de trabajo deben ser correctamente protegidas, además las mismas no deben causar inconvenientes o problemas para los usuarios, pero algunas de las conexiones nuevas no tienen las debidas canalizaciones ni ductos necesarios como se detalló anteriormente.

- Se debe tener un máximo de llenura en los conduit instalados del 40%, sin embargo se permite hasta un máximo de llenura del 60% cuando se han debido realizar adiciones no planeadas luego de la instalación inicial, no obstante, los conduit instalados en el edificio no permiten adición en los mismos y algunos de los cables de red instados no cuentan con ningún tipo de protección, por lo cual para las nuevas conexiones que se realicen y las

que se deban modificar, es necesario tener en cuenta la aplicación de la norma.

La norma ANSI/TIA/EIA-606 (Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales e incluye estándares para la rotulación del cableado):

Indica el uso de etiquetas que aseguren su clara identificación y lectura de los puntos de red y de todas las conexiones realizadas, sin embargo durante el levantamiento de información se encontraron 50 puntos de red sin la debida etiquetación, así también algunos de los puntos de red que si bien cuentan con una etiqueta, éstas no son las más adecuadas debido a que su lectura puede ser confundida o en muchos casos ilegible, al no haberse utilizado los materiales adecuados.

SUBSISTEMA VERTICAL

Se debe regirse a la norma ANSI/EIA/TIA 569-A (Estándar de Edificios Comerciales para Recorridos y Espacios de Telecomunicaciones) establece lo siguiente:

- Se debe usar conduit para proteger la fibra óptica o cable UTP utilizado como cableado de backbone, sin embargo el cableado vertical del edificio no cuenta con protección física alguna.

- Es necesario contar con diversos puntos de entrada para proveer el servicio de telecomunicaciones, asegurando la no interrupción del servicio por falla en la ruta. Al momento no se cuenta con redundancia del backbone principal por lo cual de existir una falla del canal, la red quedaría parcial o totalmente fuera de servicio.

CUARTOS DE TELECOMUNICACIONES

Se debe regirse a la norma ANSI/EIA/TIA 569-A (Estándar de Edificios Comerciales para Recorridos y Espacios de Telecomunicaciones) establece lo siguiente:

- Los cables de telecomunicaciones deben estar separados físicamente de los conductores de energía eléctrica.
- Si dichos conductores pasan por la misma canaleta o bandeja deben estar separados por barreras entre el cableado lógico y eléctrico.
- Dentro de las cajas de distribución o compartimentos de tomas, debe haber separación física total entre los cableados.
- No debe haber tubería de agua pasando por (sobre o alrededor) el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso.
- Como retardante del fuego se recomienda cubrir un mínimo de una de las paredes con plywood de 19mm, de preferencia sin vacíos, con 2.4m de alto y bien fijado a la pared.
- Se deben instalar luces y señales de emergencia, emplazadas de manera que no se obstaculice la salida de emergencia. La señalización usada en los cuartos de telecomunicaciones debe ser desarrollada en base a un plan de seguridad del edificio.
- Los pisos, paredes y techo deben ser tratados con productos especiales para eliminar el polvo, así también el suelo debe tener propiedades antiestáticas.
- Se recomienda que un mínimo de una de las paredes del cuarto de equipos deben estar cubiertas con plywood de 19mm, de preferencia sin vacíos, a una altura de 2.4m y bien fijado a la pared, su uso actúa como un retardante ante la presencia de fuego.
- Las puertas deben ser de mínimo 0.9 metros de ancho y dos metros de altura, y con facilidad de remoción.

- Es necesario realizar un estudio de la carga permitida por el piso, de manera que la concentración de equipos no exceda el límite de carga por metro cuadrado.
- La temperatura y humedad debe ser controlada proveyendo una continua operación entre los rangos de 18ºC a 24ºC con 30% a 55% de humedad relativa. Estas medidas deben ser realizadas a 1,5 m del suelo.
- Se debe contar con diversos puntos de entrada para el servicio de telecomunicaciones, asegurando la no interrupción del mismo por falla en la ruta del enlace, permitiendo la continuidad de servicio y las necesidades existentes. Adicionalmente se deben escoger vías alternas para su instalación.

Para reducir el acoplamiento de ruido producido por cables eléctricos, fuentes de frecuencia de radio, motores y generadores de energía eléctrica, se deben considerar las siguientes precauciones:

- Uso de protectores contra irrupción en las instalaciones eléctricas para limitar la propagación de descargas.
- Uso de canaletas o conductos metálicos, totalmente cerrados y puestos a tierra, o uso de cableado instalado próximo a superficies metálicas puestas a tierra.

PUESTA A TIERRA

Se debe regirse a la norma ANSI/EIA/TIA- J-STD-607-A (Requerimientos de puesta a tierra para la infraestructura de telecomunicaciones en edificios comerciales).

- El gabinete deberá disponer de una toma de tierra, conectada a la tierra general de la instalación eléctrica, para efectuar las conexiones de todo equipamiento.

- Los cables de tierra de seguridad serán puestos a tierra en el subsuelo se debe instalar una puesta de tierra para uso exclusivo de la red eléctrica, además se deberá instalar una varilla de cobre tipo Coperweld para obtener una puesta a tierra menor a 0.5 ohm.

- Todas las salidas eléctricas para computadoras deben ser polarizadas y llevadas a una tierra común, todos los equipos de comunicaciones y computadoras deben de estar conectados a fuentes de poder interrumpibles (UPS) para evitar pérdidas de información.

- Todos los componentes metálicos tanto de la estructura como del mismo cableado deben ser debidamente llevados a tierra para evitar descargas por acumulación de estática.

ANEXO B

CISCO CATALYST 2960-X

The Cisco® Catalyst® 2960-S and 2960 Switches de la serie son el líder Capa 2 borde, proporcionando una mayor facilidad de uso, las operaciones comerciales de alta seguridad, mejora de la sostenibilidad, y una experiencia de red sin fronteras. El Catalyst 2960-S Series Switches incluyen interruptor FlexStack nueva capacidad de apilamiento con 1 y 10 Gigabit de conectividad y Power over Ethernet Plus (PoE +) con los conmutadores Cisco Catalyst de la serie 2960 ofrecen conectividad Fast Ethernet y capacidades de acceso PoE. El Cisco Catalyst 2960-S y la Serie 2960 son conmutadores de configuración fija de acceso diseñados para la empresa, medianas y grandes redes de sucursales para proporcionar un menor coste total de propiedad. El Cisco Catalyst 2960-S se muestra en la Figura 1, y el Cisco Catalyst 2960 Series Switches se muestra en la Figura 2. ¿Qué hay de nuevo para el Cisco Catalyst 2960-S Series Switches LAN con el software Base:

- 10 y 1 Gigabit Ethernet flexibilidad enlace ascendente con Small Form-Factor Plus Pluggable (SFP +), proporcionando la continuidad del negocio y la rápida transición a 10 Gigabit Ethernet
- 24 o 48 puertos de Gigabit Ethernet Conectividad de escritorio
- Cisco FlexStack módulo de apilamiento de 20 Gbps de rendimiento, lo que permite la facilidad de uso con una sola configuración y actualización del conmutador simplificado
- PoE + con hasta 30 W por puerto que le permite soportar las últimas PoE + dispositivos capaces
  • Opciones de suministro de energía, con fuentes de alimentación de 740W o 370W fijos para PoE + conmutadores están disponibles
- USB de almacenamiento para copias de seguridad de archivos, distribución y operaciones simplificadas
- Una amplia gama de funciones de software para proporcionar facilidad de operación, operaciones de negocios de alta seguridad, la sostenibilidad, y una experiencia de red sin fronteras
- Garantía de hardware limitada de por vida, incluyendo siguiente día hábil reemplazo con un servicio de 90 días y el apoyo
- El Cisco Catalyst 2960 Series Switches LAN con el software de Base ofrecen lo siguiente:
- doble propósito para enlaces ascendentes Gigabit Ethernet de enlace ascendente flexibilidad, lo que permite el uso de cualquiera de un enlace ascendente de cobre o fibra, cada doble propósito tiene un puerto de enlace ascendente Ethernet 10/100/1000 y un puerto SFP Gigabit Ethernet basado en puerto, con un puerto activo en una vez
- 24 o 48 puertos de conectividad Fast Ethernet de sobremesa
- PoE configuraciones con un máximo de 15,4 W por puerto 187

- Una amplia gama de funciones de software para proporcionar facilidad de operación, operaciones de negocios de alta seguridad, la sostenibilidad, y una experiencia de red sin fronteras
- Garantía de hardware limitada de por vida

Figura 1. Cisco Catalyst 2960-S Series Switches

Figura 2. Cisco Catalyst 2960 Series Switches Configuraciones del switch

Tabla 1 se muestra la información de configuración de los switches de la serie Catalyst 2960 con software básico LAN. Tabla 1. Las configuraciones de los switches de la serie Cisco Catalyst 2960 con software LAN Base.

Cisco Catalyst 2960 Switch Model	Descripción	Uplinks
Cisco Catalyst 2960-24TT-L	24 Ethernet 10/100 ports	2 Ethernet 10/100/1000 ports
Cisco Catalyst 2960-48TT-L	48 Ethernet 10/100 ports	2 Ethernet 10/100/1000 ports

Tablas 2, 3, 4 y 5 proporcionan características de hardware, especificaciones eléctricas, apoyo a la gestión y las normas e información de seguridad y cumplimiento para el Cisco Catalyst 2960-S y 2960 Series Switches LAN con software básico.

Tabla 2. Cisco Catalyst 2960-S y 2960 Series Switches LAN con el rendimiento de la base del interruptor de software y la información de escalabilidad.

Rendimiento y Escalabilidad para todos los modelos del Switchs		
	Catalyst 2960-S	**Catalyst 2960**
Forwarding bandwidth	88 Gbps	16 Gbps 32 Gbps (2960G)
Switching bandwidth*	176 Gbps	32Gbps 32 Gbps (2960G)
Flash memory	64 MB	32 MB

Memory DRAM	128 MB	64 MB	
Max VLANs	255	255	
VLAN IDs	4000	4000	
Maximum transmission unit (MTU)	9198 bytes	Up to 9000 bytes	
Jumbo frames	9216 bytes	9018 bytes (2960G only)	
Forwarding Rate: 64-Byte Packet Cisco Catalyst 2960			
Cisco Catalyst 2960-24TT-L	6.5 mpps		
Cisco Catalyst 2960-48TT-L	10.1 mpps		
Resource: Cisco Catalyst 2960-S and 2960	Default	QoS	Dual
Unicast MAC addresses	8000	8000	8000
IPv4 IGMP groups	255	255	255
IPv4 MAC QoS access control entries (ACEs)	128	384	0
IPv4 MAC security ACEs	384	128	256

Tabla 3. Dimensiones, peso, acústicas, MTBF y ambientales rango

Dimensions (H x W x D)				
Cisco Catalyst 2960	Inches		Centimeters	
Cisco Catalyst 2960-24TT-L	1.73 x 17.7 x 9.52		4.4 x 45 x 23.6	
Cisco Catalyst 2960-24TC-L				
Cisco Catalyst 2960-24LT-L				
Cisco Catalyst 2960	Pounds		Kilograms	
Cisco Catalyst 2960-24TT-L	8		3.6	
Environmental Ranges				
	Cisco Catalyst 2960-S		**Cisco Catalyst 2960**	
	Fahrenheit	Centigrade	Fahrenheit	Centigrade
Operating	0° to	-5° to 45°C	23° to	-5° to 45°C

temperature up to 5000 ft (1500 m)	113ºF		113ºF	
Operating temperature up to 10,000 ft (3000 m)	23º to 104ºF	-5º to 40ºC	23º to 104ºF	-5º to 40ºC
Short-term exception at sea level	23º to 31ºF	-5º to 55ºC	23º to 31ºF	-5º to 55ºC
Short-term exception up to 5000 feet (1500 m)*	23º to 122ºF	-5º to 50ºC	23º to 122ºF	-5º to 50ºC
Short-term exception up to 10,000 feet (3000 m)*	23º to 113ºF	-5º to 45ºC	23º to 113ºF	-5º to 45ºC
Short-term exception up to 13,000 feet (4000 m)*	23º to 104ºF	-5º to +40ºC	23º to 104ºF	-5º to 40ºC
Storage temperature up to 15,000 feet (4573 m)	-13º to 158ºF	-25º to 70ºC	-13º to 158ºF	-25º to 70ºC
	Feet	Meters		
Operating altitude	Up to 10,000	Up to 3000	Up to 10,000	Up to 3000
Storage altitude	Up to 13,000	Up to 4000	Up to 13,000	Up to 4000

Operating relative humidity	10% to 95% noncondensing	10% to 95% noncondensing
Storage relative humidity	10% to 95% noncondensing	10% to 95% noncondensing

Acoustic Noise
Measured per ISO 7779 and declared per ISO 9296.
Bystander positions operating mode at 25°C ambient.
Mean time between failures (MTBF)

Cisco Catalyst 2960-S		**Cisco Catalyst 2960**	
Model	MTBF in hours	Model	MTBF in hours

Tabla 4. Tensión y potencia la información

AC/DC input voltage and current			
Cisco Catalyst 2960	Voltage (Autoranging)	Current	Frequency
Cisco Catalyst 2960-24TT-L and Catalyst 2960-24TC-L and Catalyst 2960-48TT-L and Catalyst 2960-48TC-L		1.3 to 0.8 A	
Power Rating			
Cisco Catalyst 2960-S		Cisco Catalyst 2960	
Model	Power Rating	Model	Power Rating
Cisco Catalyst 2960S-24PD-L	0.46 kVA	Cisco Catalyst 2960-24TT-L	0.05 kVA
Cisco Catalyst 2960S-48TD-L	0.09 kVA	Cisco Catalyst 2960-48TT-L	0.075 kVA
DC input voltages (RPS input)			
Cisco Catalyst 2960			
Cisco Catalyst 2960-24TT-L	12V at 5 A	5 A	
PoE and PoE+			

Tabla 5. Especificaciones Técnicas para switches de la serie Cisco Catalyst 2960 con software LAN Base.

Description	C2960 Specifications				
Models	C2960-48TT-L	C2960-24TT-L	C2960G-48TC-L	C2960G-24TC-L	C2960-24T-L
100 Percent Throughput					
Measured Power Consumption	42W	28W	123W	72W	22W

5 Percent Throughput					
Measured Power Consumption	38W	26W	114W	65W	21W
5 Percent Throughput (with 50 Percent PoE Loads)					
Measured Power Consumption	-	-	-	-	-
100 Percent Throughput (with Maximum Possible PoE Loads)					
Measured Power Consumption	-	-	-	-	-

Tabla 6. Información de pedido para switches de la serie Cisco Catalyst 2960 con software LAN Base.

Part Numbers	Description
WS-C2960-24TT-L	• 24 Ethernet 10/100 ports and 2 10/100/1000 TX uplinks • 1 RU fixed-configuration • LAN Base image
WS-C2960-48TT-L	• 48 Ethernet 10/100 ports and 2 10/100/1000 TX uplinks • 1 RU fixed-configuration • LAN Base image

ANEXO C

CISCO CATALYST 3750-X

El Cisco Catalyst 3750-X El Cisco ® catalizador ® 3750-X Series Switches son una línea de clase empresarial de conmutadores apilables e independientes, respectivamente. Estos conmutadores proporcionan alta disponibilidad, la escalabilidad, la seguridad, la eficiencia energética y facilidad de uso con características innovadoras, tales como Cisco StackPower (disponible sólo en el Catalyst 3750-X), IEEE 802.3at Poder sobre Ethernet Plus (PoE +) configuraciones, módulos de red opcionales, fuentes de alimentación redundantes y Media Access Control características de seguridad (MACsec). El Cisco Catalyst 3750-X Series con StackWise ® Plus tecnología proporciona escalabilidad, facilidad de manejo y protección de la inversión para las necesidades empresariales en evolución. El Cisco Catalyst 3750-X y 3560-X mejoran la productividad al permitir aplicaciones tales como telefonía IP, inalámbricas y de vídeo para una experiencia de red sin fronteras.

Cisco Catalyst 3750-X Series características principales:

- 24 y 48 puertos 10/100/1000 PoE + y no PoE modelos, y 12 y 24 modelos de GE SFP puertos.
- Cuatro módulos de red opcionales de enlace ascendente con GE o puertos 10GE • Primero en la industria PoE + con 30W de potencia en todos los puertos en una unidad de rack (RU) factor de forma.
- Dos fuentes de alimentaciones modulares redundantes y ventiladores.
- Media Access Control de Seguridad (MACsec) cifrado basado en hardware.
- Flexible NetFlow y switch-to-switch de cifrado de hardware con el módulo de servicio.
- Open Shortest Path First (OSPF) para el acceso a la imagen de enrutado IP Base.
- IPv4 e IPv6 routing, multicast routing, avanzada de la calidad de servicio (QoS), y características de seguridad de hardware.
- Mayor garantía limitada de por vida (LLW) con el siguiente día laborable (NBD) avanzar reemplazo de hardware y 90 días de acceso a Cisco Technical Assistance Center (TAC) el apoyo.
- Mejora de Cisco EnergyWise para la optimización de los costos operativos mediante la medición de consumo de energía real de los dispositivos PoE, informar y reducir el consumo de energía a través de la red.
- USB tipo A y tipo B puertos, para el almacenamiento y la consola, respectivamente, y un out-ofband puerto de gestión Ethernet.
- Además de las características anteriores, el Cisco Catalyst 3750-X cambia también ofrecemos:

- Cisco StackPower ™ tecnología: Una característica innovadora y primera en la industria para compartir el poder entre los miembros de la pila.
- Cisco StackWise Plus tecnología para la facilidad de uso y flexibilidad con 64 Gbps de rendimiento.
- Protección de la inversión con la compatibilidad hacia atrás con todos los otros modelos de switches de la serie Cisco Catalyst 3750.

Configuraciones del switch

Todos los modelos de interruptor pueden ser configurados con cuatro módulos de red opcionales. El + PoE y no PoE modelos de switches están disponibles con la LAN Base, Base IP y servicios IP conjunto de características. Los modelos GE SFP interruptor están disponibles con base IP o IP Services conjunto de características. Switches apilables

La figura 1 muestra el Cisco Catalyst 3750-X Series Switches
La Tabla 1 muestra el Cisco Catalyst 3750-X Series configuraciones.
Tabla 1. Cisco Catalyst 3750-X Series Configuraciones

Feature Set	Modelos	Total de puertos Ethernet 10/100/1000	Predeterminado AC Power Supply	Potencia disponible PoE	StackPower
LAN Base	WS-C3750X-24T-L	24	350W	-	Si en la versión de software 15.0 (2) SE y más tarde (cables StackPower vende por separado)
	WS-C3750X-48T-L	48			
	WS-C3750X-24P-L	24 PoE +	715W	435W	
	WS-C3750X-48P-L	48 PoE +			
	WS-C3750X-48PF-L	48 PoE +	1100W	800W	
IP Base	WS-C3750X-24T-S	24	350W	-	Sí
	WS-C3750X-48T-S	48			
	WS-C3750X-24P-S	24 PoE +	715W	435W	
	WS-C3750X-48P-S	48 PoE +			
	WS-C3750X-48PF-S	48 PoE +	1100W	800W	
	WS-C3750X-12S-S	12 GE SFP	350W +	-	
	WS-C3750X-24S-S	24 GE SFP	350W	-	
Servicios IP	WS-C3750X-12S-E	12 GE SFP	350W	-	
	WS-C3750X-24S-E	24 GE SFP		-	
	WS-C3750X-24T-E	24		-	
	WS-C3750X-48T-E	48			
	WS-C3750X-24P-E	24	715W	435W	
	WS-C3750X-48P-E	48			
	WS-C3750X-48PF-E	48	1100W	800W	

Cisco Catalyst 3750-X Series Software Además de Base IP y servicios IP conjuntos de características, el Cisco Catalyst 3750-X vienen con un nuevo conjunto de funciones LAN Base.
La función de tres sets disponibles con todos los switches Cisco Catalyst 3750-X y 3560-X Series Switches son:

- LAN Base: Mejora de Servicios Inteligentes
- Base IP: servicios de línea de base para empresas
- Servicios IP: Servicios para empresas

La Base de LAN conjunto de características mejoradas ofrece servicios inteligentes que incluyen amplias funciones de nivel 2, con un máximo de 255 VLANs. El conjunto de funciones IP Base ofrece servicios de línea de base de la empresa, además de todas las funciones de base inalámbrica, con VLAN 1K.
Base IP también incluye el apoyo para el acceso enrutado, MACsec, y el nuevo módulo de Servicio de Cisco.
Los servicios IP conjunto de características ofrece servicios completos que incluyen empresas de nivel 3 avanzado características como Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Protocol Independent Multicast (PIM), y IPv6 enrutamiento como OSPFv3 y EIGRPv6.
Todas cuentan con soporte avanzado software establece la seguridad, QoS y características de manejo.
El Cisco Catalyst 3750-X Series Switches LAN con el conjunto de características de base sólo se puede acumular con otros switches Cisco Catalyst 3750-X Series Switches LAN Base.
Una pila mixta de conmutador LAN Base con base IP o características de servicio que figuran IP no es compatible.
Los clientes pueden actualizar de forma transparente la función de software ubicado en el Cisco Catalyst 3750-X y 3560-X Series Switches Cisco IOS a través de ® La activación del software. Activación del software autoriza y permite que los conjuntos de funciones de Cisco IOS Software.
Un archivo especial que figura en el interruptor, llamado archivo de licencia, es examinado por el software Cisco IOS cuando el interruptor está encendido. Con base en el tipo de licencia, el software Cisco IOS activa el conjunto de características apropiadas. Tipos de licencia se puede cambiar o actualizar, activar un conjunto de características diferentes

Cisco Catalyst 3750-X Series Switches Habilitar Experiencia Cisco Borderless Network

Borderless Networks de Cisco, una arquitectura, ofrecer la experiencia nueva área de trabajo, la conexión de cualquier persona, en cualquier lugar, con cualquier dispositivo, a cualquier recurso de forma segura, fiable y transparente.

Arquitectura Borderless Networks de Cisco aborda primario de TI y los retos empresariales para ayudar a crear una experiencia verdaderamente sin fronteras llevando interacción más estrecha con el empleado y el cliente.
Experiencia sin bordes sólo es posible con los elementos de red inteligente diseñado y diseñada para satisfacer las necesidades de un espacio de trabajo global.
Cisco Network Access es un componente principal de esta arquitectura, que permite a varios servicios de red sin fronteras, como la movilidad, la seguridad, MediaNet, EnergyWise, y la facilidad de las operaciones para aumentar la productividad y la eficiencia operativa.
Cuando el acceso de red inteligente, que conoce la identidad del usuario, así como cuando el usuario está en la red. Se sabe que se conecta a la red, para aprovisionar automáticamente a la red para QoS y la entrega.
Llega a ser consciente de los servicios para optimizar la experiencia del usuario. Sólo con la red de acceso inteligente, su empresa puede ir sin bordes de forma segura y transparente. Su empresa puede ahorrar energía, simplificar las operaciones con eficiencia empresarial mejor, y tienen un costo total de propiedad optimizado.
Acceso Cisco Borderless Network para la solución se centra en las áreas principales siguientes:

- Sostenibilidad
- Facilidad de operaciones
- Seguridad de Fronteras
- Experiencia sin fronteras

Sostenibilidad

Cisco Catalyst soluciones de conmutación permitir prácticas más ecológicas a través de la eficiencia energética mensurable, servicios integrados, y las innovaciones continuas como Cisco EnergyWise, una solución para toda la empresa que controla y conserva la energía con políticas personalizadas. Juntos, la tecnología Cisco EnergyWise y Cisco Catalyst cambia reducir gases de efecto invernadero (GEI) y aumentar el ahorro en costos de energía y el comportamiento empresarial sostenible.
Características de sostenibilidad en el Cisco Catalyst 3750-X y 3560-X Series Switches incluir los conjuntos de características siguientes:

- La tecnología Cisco EnergyWise
- Eficiente operación del interruptor
- Gestión inteligente de energía

Cisco EnergyWise Tecnología

Cisco EnergyWise es una innovadora arquitectura, sumado a los conmutadores de configuración fija, la promoción de la sostenibilidad de toda la compañía por reducir el consumo de energía a través de una infraestructura corporativa completa y que afecta a más del 50 por ciento de las emisiones globales de gases de efecto invernadero creados por la construcción de infraestructura en todo el mundo, un efecto mucho mayor que el 2 por ciento generado por la industria de TI.
Cisco EnergyWise permite a las empresas medir el consumo de energía de la infraestructura de red y los dispositivos conectados a la red y gestionar el consumo de energía con políticas específicas, lo que reduce el consumo de energía para realizar un mayor ahorro de costos, afectando potencialmente a cualquier dispositivo alimentado.
EnergyWise abarca una gran inteligencia basada en la red enfoque para comunicar mensajes que medida y control de la energía entre los dispositivos de red y los puntos finales. La red detecta los dispositivos Cisco EnergyWise manejables, vigila su consumo de energía, y actúa con base en las reglas de negocio para reducir el consumo de energía.
EnergyWise utiliza un único sistema de nombres de dominio para consultar y resumir información de grandes conjuntos de dispositivos, por lo que es más simple que las tradicionales capacidades de gestión de red.
Interfaces de Cisco EnergyWise de gestión permiten a las instalaciones y aplicaciones de gestión de red para comunicarse con los criterios de valoración y de los demás que utilizan la red como un tejido unificador. La interfaz de administración utiliza el estándar SNMP o TCP para integrar Cisco y otros sistemas de gestión.

Inteligente de la energía a través de Ethernet Gestión

El Cisco Catalyst 3750-X y 3560-X modelos de la serie PoE compatible con los teléfonos IP de Cisco y Cisco Aironet puntos de acceso WLAN proporcionan hasta 30 W de potencia por puerto, así como cualquier IEEE 802.3af dispositivo final.

Cisco Discovery Protocol versión 2 permite que el Cisco Catalyst 3750-X y 3560-X Series Switches para negociar un ajuste de potencia más granular cuando se conecta a un dispositivo de Cisco potencia, como teléfonos IP o puntos de acceso que lo establecido por la clasificación de IEEE.
Por puerto consumo de energía comando permite a los clientes especificar el ajuste de la potencia máxima en un puerto individual.
Por puerto PoE de detección mide el poder real está dibujando, permitiendo un control más inteligente de los dispositivos alimentados.
La MIB PoE proporciona visibilidad proactiva en el uso de energía y permite a los clientes establecer diferentes umbrales de nivel de potencia. Facilidad de Operaciones El Cisco Catalyst 3750-X y 3560-X ayudan a reducir los costos operativos a través de:

- Cisco Catalyst inteligente de Operaciones
- Fácil de usar características de implementación y control
- Avanzadas herramientas de gestión de redes inteligentes

Cisco Catalyst inteligente de Operaciones

Cisco Catalyst inteligente de Operaciones es un conjunto completo de capacidades que simplifican el despliegue LAN, configuración y solución de problemas.

Además de la adaptación, siempre en tecnologías como StackWise y StackPower, Cisco Catalyst Operaciones inteligentes permiten Zero Touch Installation y el reemplazo de interruptores, actualización rápida, así como la facilidad de solución de problemas con costo operativo reducido.

Cisco Catalyst inteligente de Operaciones es un conjunto de características que incluye Smart Install, Smartports automóviles, configuración inteligente y solución de problemas inteligente para mejorar la excelencia operativa.

Cisco Smart Install es un tapón transparente y jugar la tecnología para configurar la imagen de Cisco IOS Software y cambiar la configuración sin intervención del usuario. Smart Install utiliza la asignación dinámica de direcciones IP y la asistencia de otros switches para facilitar la instalación proporcionando enchufe de red transparente y el juego.

Auto Smartports de Cisco permiten una configuración automática, los dispositivos se conectan al puerto del switch, permitiendo la detección automática y plug and play del dispositivo en la red.

Cisco Configuration inteligente proporciona un único punto de gestión para un grupo de switches y además añade la capacidad de archivo y los archivos de copia de seguridad de configuración en un servidor de archivos o un interruptor que permite el reemplazo sin fisuras cero teclas táctiles.

Solución de problemas Cisco Smart es una amplia gama de depuración de comandos de diagnóstico y los controles del sistema de salud en el interruptor, incluyendo genéricos Diagnóstico en línea (GOLD) y el registro de fallo a bordo (OBFL).

Fácil de usar Características de implementación y control

Gerente Embedded Event (EEM) es una función potente y flexible que proporciona en tiempo real la detección de eventos de red y la automatización a bordo. Usando EEM, los clientes pueden adaptar el comportamiento de sus dispositivos de red para alinearse con las necesidades de sus negocios. Esta función requiere set IP operación base.

IP de nivel de servicio (SLA) permiten a los clientes asegurar nuevas aplicaciones críticas de negocio de propiedad intelectual, así como servicios de IP que utilizan datos, voz y video, en una red IP. Esta función requiere la función de Servicios IP establecida.

Dynamic Host Configuration Protocol (DHCP) de configuración automática de varios switches mediante un servidor de arranque facilita la instalación del interruptor.

Automático QoS (AutoQoS) simplifica la configuración de QoS en la voz sobre IP (VoIP) mediante la emisión de interfaz y los comandos de Global Switch para detectar teléfonos IP de Cisco, clasificar el tráfico y ayudar a activar la configuración de salida de la cola.

Apilamiento maestro gestión de la configuración y la tecnología Cisco StackWise ayuda a asegurar que todos los interruptores se actualizan automáticamente cuando el interruptor maestro recibe una nueva versión de software. Comprobación automática de la versión de software y la actualización de asegurar que todos los miembros de la pila tengan la misma versión de software.

Autonegotiation en todos los puertos selecciona automáticamente half o full-duplex modo de transmisión para optimizar el ancho de banda. • Protocolo de enlace troncal dinámico (DTP) facilita la configuración de enlace troncal dinámico en todos los puertos del switch.

Port Aggregation (Protocolo PAgP) automatiza la creación de Cisco Fast EtherChannel ® grupos o grupos Gigabit EtherChannel para vincular a otro switch, router o servidor.

Link Aggregation Control Protocol (LACP) permite la creación de canalización Ethernet con equipos que se ajusten a IEEE 802.3ad. Esta función es similar a la tecnología de Cisco EtherChannel y PAgP.

Automático medios de comunicación dependientes de la interfaz de cruce (MDIX) ajusta automáticamente la transmisión y recepción de pares si un tipo de cable incorrecto (cruzado o directo-) está instalado.

Protocolo de detección unidireccional Link (UDLD) y UDLD agresivo permiten enlaces unidireccionales causados por la incorrecta fibra óptica cableados o fallas de puerto para ser detectado y desactivado en interfaces de fibra óptica.

El cambio de base de datos Manager (SDM) plantillas de acceso, enrutamiento, y el despliegue VLAN permiten al administrador maximizar fácilmente la asignación de memoria a las características ideales en función de los requisitos específicos de implementación.

Local Proxy Address Resolution Protocol (ARP) trabaja en conjunto con Private VLAN Edge para reducir al mínimo las emisiones y maximizar el ancho de banda disponible.

VLAN1 minimización permite VLAN1 estar deshabilitado en cualquier individuo tronco VLAN.

Multicast inteligente, con tecnología Cisco StackWise Plus, permite que el Cisco Catalyst 3750-X Series para ofrecer una mayor eficiencia y soporte para flujos de datos de más de multidifusión, como el vídeo, poniendo cada paquete de datos en el backplane sólo una vez.

Internet Group Management Protocol (IGMP) Snooping para IPv4 e IPv6 MLD Snooping v1 y v2 proporcionará al Cliente rápido se une y deja de secuencias de multidifusión y los límites de ancho de banda intensivo de tráfico de vídeo sólo a los solicitantes.

Multicast registro de VLAN (MVR) envía continuamente secuencias de multidifusión en una VLAN de multidifusión mientras que el aislamiento de las corrientes de VLANs suscriptores de ancho de banda y razones de seguridad.

Por puerto de la difusión, multidifusión y unidifusión control de tormentas impide estaciones defectuosas fin de disminuir el rendimiento general del sistema. **VLAN de voz** simplifica las

instalaciones de telefonía, manteniendo el tráfico de voz en una VLAN separada para facilitar la administración y solución de problemas.

Cisco VLAN Trunking Protocolo (VTP) soporta VLAN dinámicas y configuración dinámica del tronco en todos los switches.

Interruptor remoto puerto Analyzer (RSPAN) permite a los administradores controlar de forma remota los puertos de una red de Capa 2 del interruptor desde cualquier otro interruptor en la misma red.

Para mejorar la gestión del tráfico, monitoreo y análisis, el Embedded Remote Monitoring (RMON) agente de software es compatible con cuatro grupos RMON (historial, estadísticas, alarmas y eventos).

Capa 2 traceroute facilita la solución de problemas mediante la identificación de la ruta física que sigue un paquete desde el origen al destino.

Trivial File Transfer Protocol (TFTP) reduce el costo de administración de actualizaciones de software mediante la descarga desde una ubicación centralizada.

Network Timing Protocol (NTP) proporciona una indicación de la hora exacta y consistente para todos los conmutadores de intranet. Advanced Intelligent Network Management Tools.

El Cisco Catalyst 3750-X y 3560-X Series Switches ofrecen tanto una CLI superior para la configuración detallada y software Cisco Network Assistant, una herramienta basada en PC para la configuración rápida basada en plantillas predefinidas. Además, CiscoWorks LAN Management Solution (LMS) es compatible con el Cisco Catalyst 3750-X y 3560-X Series Switches para la gestión de toda la red.

Cisco Network Assistant

Una aplicación de red basado en PC de gestión diseñado para pequeñas y medianas empresas (SMB) redes de hasta 250 usuarios, Cisco Network Assistant ofrece gestión de red centralizada y capacidades de configuración. Cisco Network Assistant utiliza la tecnología Cisco Smartports para simplificar tanto el despliegue inicial y el mantenimiento continuo.

Esta aplicación también cuenta con una interfaz gráfica de usuario intuitiva donde los usuarios pueden solicitar los servicios comunes a través de conmutadores de Cisco, routers y puntos de acceso, tales como:

- Gestión de la configuración
- Asesoramiento Solución de problemas
- Informes de inventario • Notificación de eventos
- Red de configuración de seguridad
- Contraseña de sincronización
- Arrastrar y soltar Cisco IOS actualizaciones de software
- Tecnología inalámbrica segura

CiscoWorks LAN Management Solution

CiscoWorks LAN Management Solution (LMS) es un ciclo de vida completo de la red solución de gestión. Ofrece una amplia biblioteca de funciones fáciles de usar características para automatizar el manejo inicial y el día a día de su infraestructura de red de Cisco.
CiscoWorks LMS únicamente utiliza el hardware de Cisco y software de la plataforma conocimiento y experiencia operacional en un potente conjunto de flujo de trabajo basada en la configuración, supervisión, solución de problemas, elaboración de informes y herramientas administrativas. Incluye:

- Apoyo a las nuevas plataformas de hardware de Cisco el día en que el envío
- Apoyo a las nuevas tecnologías y servicios de despliegue inicial de la administración del día a día y de gestión, como EnergyWise, Identidad, Cisco Auto Smartports, Cisco Smart Install, y mucho más.
- Herramientas de gestión de configuración construido a partir de la experiencia de Cisco y Cisco Validated Recomendaciones de diseño • Monitoreo y solución de problemas de capacidad que incorpora las mejores prácticas de Cisco de hardware y características de diagnóstico.
- La automatización en la gestión de inventarios de hardware, las vulnerabilidades de seguridad (PSIRTS) y plataforma final de su vida útil y el apoyo ciclos.

Seguridad sin bordes

El Cisco Catalyst 3750-X y 3560-X Series Switches proporcionan superiores de nivel 2 las capacidades de defensa de amenazas para mitigar los ataques man-in-the-middle (como MAC, IP y ARP spoofing). TrustSec, un elemento primordial de la Arquitectura de Seguridad sin fronteras, ayuda a los clientes empresariales a asegurar sus redes, datos y recursos de la política basada en el control de acceso, la identidad y la creación de redes de rol consciente, integridad penetrante y confidencialidad.
La seguridad sin bordes está activada de los conjuntos de características siguientes en el Cisco Catalyst 3750-X y 3560-X Series Switches:

- Amenaza defensa
- Cisco TrustSec
- Otras características de seguridad avanzadas

Amenaza de Defensa

Funciones de seguridad integradas de Cisco es una solución líder en la industria disponible en switches Cisco Catalyst que protege proactivamente su infraestructura de red crítica.

La entrega de gran alcance, fácil de utilizar herramientas para prevenir eficazmente los más comunes y potencialmente perjudiciales de Capa 2 amenazas de seguridad, funciones de seguridad integradas de Cisco proporciona seguridad robusta a través de la red.

Cisco Integrated características de seguridad incluyen protección portuaria, snooping DHCP, Dynamic ARP Inspection y guardia IP de origen.

Puerto de seguridad asegura el acceso a un acceso o puerto de enlace troncal basada en la dirección MAC. Se limita el número de direcciones MAC aprendidas negar dirección MAC de inundación.

DHCP Snooping evita que usuarios malintencionados suplantación de un servidor DHCP y el envío de direcciones falsas.

Esta función es utilizada por otras funciones de seguridad principales para prevenir una serie de otros ataques, como el envenenamiento ARP.

Dynamic ARP Inspection (DAI) ayuda a garantizar la integridad del usuario al evitar que usuarios malintencionados explotación de la naturaleza insegura del protocolo ARP.

IP Source Guard impide que un usuario malintencionado spoofing o hacerse cargo de la dirección IP de otro usuario mediante la creación de una tabla de enlace entre el cliente IP y la dirección MAC, el puerto y VLAN.

Cisco TrustSec

TrustSec protege el acceso a la red, hace cumplir las políticas de seguridad, y ofrece soluciones de seguridad basadas estándar tales como 802.1X que permite una colaboración segura y cumplimiento de políticas.

Capacidades de liderazgo de Cisco TrustSec reflejar el pensamiento, las innovaciones y el compromiso con el éxito del cliente. Estas nuevas capacidades incluyen:

IEEE 802.1AE MACsec norma previa con 802.1X-REV Gestión de claves: industria fija con interruptores primera norma previa 802.1X-Rev gestión de claves.

Disponible en Cisco Catalyst 3750-X y 3560-X Series Switches, MACsec ofrece Layer 2, velocidad de línea de datos Ethernet confidencialidad e integridad en el host frente a los puertos, la protección contra los ataques manin-the-middle (curiosear, manipulación y reproducción).

FIPS 140-2 validados para dispositivos utilizados en entornos gubernamentales y sensibles para los niveles extremadamente altos de seguridad de datos.

Autenticación flexible que soporta múltiples mecanismos de autenticación, incluyendo 802.1X, MAC Authentication Bypass y autenticación web utiliza una configuración única y coherente.

Modo abierto que crea un entorno fácil de usar para las operaciones de 802.1X.

La integración de la tecnología de dispositivos de perfiles y el acceso para invitados manejo con conmutación de Cisco para mejorar significativamente la seguridad y reducir los problemas de implementación y operativos.

Cambiar radio de llamadas de autorización y descargable para amplias capacidades de administración de políticas.

Suplicante 802.1X con la red de transporte perimetral de acceso (NEAT) permite ampliar el acceso seguro donde switches compactos en las salas de conferencias tienen el mismo nivel de seguridad que los interruptores en el armario de cableado bloqueado.

Otras características de seguridad avanzada Otras características de seguridad avanzada incluyen pero no se limitan a:

VLAN privadas restringen el tráfico entre hosts en un segmento común mediante la segregación de tráfico en la capa 2, convirtiendo un segmento de difusión en un segmento multiaccesslike no es de difusión.

Private VLAN Edge proporciona seguridad y aislamiento entre los puertos de switch, que ayuda a asegurar que los usuarios no pueden espiar el tráfico de otros usuarios.

Unicast Reverse Path Forwarding (RPF) característica ayuda a mitigar los problemas causados por la introducción de direcciones de origen malformados o forjado (falsificado) IP en una red de paquetes IP descartar que carecen de una dirección IP de origen verificable.

Autenticación Multidominio permite que un teléfono IP y una PC para autenticar en el mismo puerto del switch al mismo tiempo, la puesta en voz apropiada y la VLAN de datos.

VLAN ACL de seguridad de Cisco en todas las VLAN evitar que los flujos de datos no autorizadas de ser puente entre las VLAN.

Cisco estándar y extendida ACL IP del router de seguridad definir las políticas de seguridad en las interfaces enrutadas para el plano de control y tráfico de datos plano. ACL IPv6 pueden aplicarse para filtrar el tráfico IPv6.

Puerto ACL basadas en Capa 2 interfaces permiten las políticas de seguridad que se aplicarán en los puertos de conmutación individuales.

Secure Shell (SSH) Protocolo, Kerberos y Simple Network Management Protocol versión 3 (SNMPv3) proporcionan seguridad de red mediante el cifrado de tráfico del administrador durante las sesiones Telnet y SNMP.

Protocolo SSH, Kerberos y la versión criptográfica de SNMPv3 requieren una imagen criptográfico software especial debido a las restricciones de exportación de Estados Unidos.

Soporte de datos bidireccional en el Analizador Switched Port (SPAN) puerto permite intrusiones Cisco Detection System (IDS) para tomar medidas cuando detectan a un intruso.

TACACS + y RADIUS facilita el control centralizado del switch y restringe a los usuarios no autorizados puedan alterar la configuración.

Notificación de direcciones MAC permite a los administradores a ser notificado de los usuarios agregan o se quitan de la red.

Seguridad multinivel en el acceso a la consola evita que usuarios no autorizados puedan alterar la configuración del switch.

Puente unidad de datos de protocolo (BPDU) Guardia apaga Spanning Tree PortFast interfaces habilitadas cuando se reciben las BPDU para evitar bucles accidentales topología.

Spanning Tree Root Guard (STRG) evita que los dispositivos de borde no en el control del administrador de red se conviertan en Spanning Tree Protocol nodos raíz.

IGMP filtrado proporciona autenticación mediante el filtrado de multidifusión no suscriptores y limita el número de secuencias de multidifusión simultáneas disponibles por puerto.

Asignación de VLAN dinámica con el apoyo a través de la implementación de pertenencia a la VLAN capacidad de cliente del servidor de políticas para proporcionar flexibilidad en la asignación de puertos a las VLAN. VLAN dinámica facilita la asignación rápida de direcciones IP.

Experiencia sin fronteras Borderless Network permite la movilidad empresarial y grado negocios servicios de video. Industria de la red unificada primero (alámbrico e inalámbrico) servicios de localización habilitar el seguimiento de activos móviles y los usuarios de dichos activos, tanto para dispositivos cableados e inalámbricos.

La experiencia sin fronteras verdadero está habilitado de los conjuntos de características siguientes en el Cisco Catalyst 3750-X y 3560-X Series Switches:

- Alta disponibilidad
- Alto rendimiento de enrutamiento IP
- Excelente calidad de servicio
- Ubicación conciencia y la movilidad

Alta disponibilidad

El Cisco Catalyst 3750-X Series incrementa la disponibilidad para switches apilables. Cada conmutador puede funcionar tanto como controlador maestro y como la transferencia de procesador. Cada conmutador de la pila puede servir como un maestro, creando un 1: esquema de la disponibilidad de N para el control de la red.

En el improbable caso de un fallo de unidad, todas las demás unidades siguen reenviar el tráfico y mantener la operación. Otras características de alta disponibilidad incluyen, pero no están limitados a:

- Cruce-Stack EtherChannel ofrece la posibilidad de configurar la tecnología de Cisco EtherChannel a través de los diferentes miembros de la pila para obtener una alta elasticidad.
- Flexlink proporciona redundancia de enlace con el tiempo de convergencia inferior a 100 ms.
- IEEE 802.1s / w Rapid Spanning Tree Protocol (RSTP) y Multiple Spanning Tree Protocol (MSTP) proporcionan una rápida convergencia spanning-tree independiente de los

temporizadores spanning-tree y también ofrecen el beneficio de equilibrio de carga de Capa 2 y procesamiento distribuido. Unidades apiladas se comportan como un único nodo del árbol de expansión.

- Per-VLAN Rapid Spanning Tree (PVRST +) permite una rápida spanning-tree re-convergencia en cada VLAN spanning-tree base, sin necesidad de la implementación de instancias de spanning tree.
- Cisco Hot Standby Router Protocolo (HSRP) es compatible para crear redundante a prueba de fallos de enrutamiento topologías.
- Switch-puerto recuperación automática intentará automáticamente volver a activar un enlace que está inhabilitado debido a un error de red.

High-Performance Routing IP

Cisco Express Forwarding hardware arquitectura de enrutamiento IP ofrece muy alto rendimiento de enrutamiento en el Cisco Catalyst 3750-X y 3560-X Series Switches.

- Enrutamiento estático (16 rutas) con juego de LAN operación base.
- IP unicast protocolos de enrutamiento (estático, Routing Information Protocol Version 1 [RIPv1], y RIPv2, RIPng, talón de EIGRP) son compatibles con las pequeñas aplicaciones de red de enrutamiento IP con el conjunto de características de Base.
- Advanced IP unicast protocolos de enrutamiento (OSPF, EIGRP, BGPv4 e IS ISv4-) son compatibles con el equilibrio de carga y la construcción de redes de área local escalable. IPv6 182 routing (OSPFv3, EIGRPv6) se apoya en hardware para un rendimiento máximo. OSPF para el acceso enrutado se incluye en la imagen de base IP. El conjunto de servicios IP función es necesaria para la plena OSPF, EIGRP, BGPv4 e IS ISv4.
- Igualdad de costo de enrutamiento de capa 3 facilita el balanceo de carga y redundancia a través de la pila.
- Enrutamiento basado en políticas (PBR) permite un control superior al facilitar la redirección de flujo independientemente del protocolo de enrutamiento configurado. El conjunto de servicios IP función es necesaria.
- Hot Standby Routing Protocol (HSRP) proporciona balanceo de carga y failover dinámico para los enlaces enrutados, hasta 32 enlaces HSRP apoyadas por unidad o pila.
- Protocol Independent Multicast (PIM) para el enrutamiento IP multicast es compatible, incluyendo el modo PIM disperso (PIM-SM), PIM modo denso (PIM-DM), PIM modo denso y disperso-Source Specific Multicast (SSM). El conjunto de servicios IP función es necesaria.
- Virtual de enrutamiento y reenvío (VRF)-Lite permite a un proveedor de servicios para apoyar a dos o más redes privadas virtuales, con la superposición de direcciones IP. Servicios IP set característica es necesaria.

Calidad de servicio superior

El Cisco Catalyst 3750-X y la Serie 3560-X ofrece una velocidad GbE con servicios inteligentes que mantener todo fluye sin problemas, incluso a 10 veces la velocidad normal de la red.
Líderes en el sector de mecanismos para el marcado, la clasificación y programación ofrecen un rendimiento superior para datos, voz y vídeo de tráfico, todo ello a velocidad de cable.
A continuación se presentan algunas de las características de QoS compatibles con el Cisco Catalyst 3750-X y 3560-X Series Switches:

- Cross-stack QoS permite que se configure a través de toda la pila (disponible sólo en el Catalyst 3750-X).
- 802.1p clase de servicio (CoS) y el punto de código de servicios diferenciados (DSCP) clasificación de campo se proporcionan, usando marcado y reclasificación en función de cada paquete por direcciones de origen y destino IP, la dirección MAC o de Capa 4 TCP / UDP número de puerto.
- Cisco plano de control y de datos plano ACL de QoS en todos los puertos ayudar a asegurar el marcado adecuado en función de cada paquete.
- Ocho colas de salida por puerto Ayuda permitir una gestión diferenciada de los distintos tipos de tráfico a través de la pila. Cuatro colas son configurables por el usuario, y cuatro están reservados para uso del sistema.
- Shaped Round Robin (SRR) programación ayuda a garantizar la priorización diferencial de los flujos de paquetes de forma inteligente el mantenimiento de las colas de entrada y las colas de salida.
- Caída de la cola ponderada (DMP) proporciona evitar la congestión en las colas de entrada y salida antes de una interrupción ocurre.
- Colas de prioridad estricta ayuda a asegurar que los paquetes de mayor prioridad son atendidos por delante de cualquier otro tráfico.
- La tasa de Cisco información comprometida (CIR) proporciona el ancho de banda en incrementos tan bajos como 8 kbps.
- Velocidad límite se proporcionan en función de la fuente y la dirección IP de destino, origen y dirección de destino MAC, nivel 4 TCP / UDP, o cualquier combinación de estos campos, usando QoS ACL (ACL IP o ACL MAC), mapas de clase, y los mapas políticos.
- Hasta 64 policers agregados o individuales están disponibles por Fast Ethernet o un puerto GbE.

Conocimiento de ubicación y movilidad

Con el fin de proporcionar la entrega de una experiencia de red mejor en su clase para los usuarios finales, es fundamental para el acceso a la red para ser conscientes ubicación.

Una amplia variedad de dispositivos pueden aparecer en la red, tanto por cable (switches, routers, teléfonos IP, PCs, puntos de acceso, controladores de video reproductores de medios digitales, etc) e inalámbricas (dispositivos móviles, etiquetas inalámbricas, pícaros, etc).

En muchas industrias, la localización de los activos es principalmente un proceso manual y requiere mucho tiempo y propenso a errores.

La imposibilidad de localizar los activos en tiempo real y para ayudar a asegurar su disponibilidad cuando y donde se necesitan plazos de reacción y eficiencia.

Los servicios de localización contestar preguntas críticas de negocio sobre los dos activos móviles y los usuarios de esos activos con independencia de que dichos activos se conecta mediante cable o inalámbrica, y por lo tanto mejoran directamente la rentabilidad de la organización. Servicios de ubicación de red también mejorar la seguridad y acelerar la solución de problemas del cliente mediante la localización de un activo, usuario o dispositivo en la red.

- Visibilidad de red y de control proporcionan visibilidad centralizada de dispositivos alámbricos e inalámbricos de la red y su ubicación.
- Ubicación de solución de problemas con ayuda de cliente permite el seguimiento de los clientes cableados o inalámbricos para la resolución rápida del problema.
- El seguimiento de activos y proporcionar una mayor seguridad inventario centralizado de los dispositivos con cable e inalámbricas y gestión de activos de los procesos de negocio mejorados.
- Cisco Mobility Service Engine (MSE) Open API proporciona un API abierto (basado en el acceso a objetos del Protocolo simple de [SOAP] y el protocolo XML) para cualquier aplicación de negocios que necesita los datos de localización.
- La política basada en la localización permite un mayor control y visibilidad. Con EnergyWise, las políticas de energía se puede configurar (para reducir la potencia o apagar la energía de un puerto) basado en la ubicación.
- Cisco Emergency Responder (CER) mejora de llamada de emergencia desde Cisco Unified CallManager. Esto ayuda a asegurar que Cisco Unified CallManager envía llamadas de emergencia al correspondiente punto de respuesta de seguridad pública (PSAP) para la ubicación de la persona que llama.

Cisco Catalyst 3750-X y 3560-X Series Especificaciones

Cambie Performance

La Tabla 2 muestra Cisco Catalyst 3750-X y 3560-X Series Switches especificaciones de rendimiento.

Tabla 2. Cisco Catalyst 3750-X y 3560-X Especificaciones de rendimiento

Los números de rendimiento para todos los modelos de interruptor	
Tejido de conmutación	160 Gbps
DRAM	256 MB (512 MB para 3750X y 3750X-12S 24S-)
Flash	64 MB (128 MB para 3750X y 3750X-12S 24S-)
VLANs totales	1005
ID de VLAN	4K
Total conmutada Interfaces virtuales (SVI)	1K
Jumbo Frame	9216 Byte
Total de puertos enrutados por 3750-X Stack	468
Tasa de reenvío de los modelos de interruptor (con dos enlaces ascendentes 10GbE)	
	Tasa de reenvío
3750X-24T **3750X-24P**	65,5 Mpps
3750X-48T **3750X-48P** **3750X-48PF**	101,2 Mpps
3750X-12S	35,7 Mpps
3750X-24S	65,5 Mpps
3560X-24T **3560X-24P**	65,5 Mpps
3560X-48T **3560X-48P** **3560X-48PF**	101,2 Mpps

Números de escalabilidad

MAC, enrutamiento, seguridad, y los números de QoS de escalabilidad dependen de la plantilla del tipo usado en el interruptor. Enrutamiento de plantilla no es compatible con el conjunto de funciones LAN Base.

La tabla 3 muestra Cisco Catalyst 3750-X y 3560-X Series Switch números de escalabilidad.

Tabla 3. Cisco Catalyst 3750-X y 3560-X Números de Serie de conmutadores escalabilidad

Acceso	Defecto	Enrutamiento	VLAN	
Unicast direcciones MAC	4K	6K	3K	12K
Grupos multicast IGMP y rutas	1K	1K	1K	1K
Rutas unicast	6K	8K	11K	0
Hosts conectados directamente	4K	6K	3K	0
Rutas indirectas	2K	2K	8K	0
Basadas en políticas de enrutamiento ACE	0.5K	0	0.5K	0
QoS ACE clasificación	0.5K	0.5K	0.5K	0.5K
ACE Seguridad	2K	1K	1K	1K
VLANs	1K	1K	1K	1K

ANEXO D

TABLA DE DISTRIBUCIÓN DE PUNTOS DE RED EN EL GADMU

En la siguiente tabla se encuentra la distribución actual del direcciones IP, especificando el departamento, lugar, a quien pertenece y si se encuentra etiquetado.

	Dirección	172.16.1.0				
	Máscara	255.255.0.0				
	Gateway	172.16.1.1				
	DIRECCIÓN IP	DEPENDENCIA	CARGO - USUARIO	OBSERVACIONES	LUGAR	FACEPLATE
1	172.16.1.2	Sistemas	Servidor Linux Centos 5.5		Segunda	
2	172.16.1.3	Sistemas	Servidor Linux Centos 6.5		Segunda	
3	172.16.1.4	Sistemas	Servidor Windows Server 2008		Segunda	
4	172.16.1.6	Sistemas	Mario Farinango		Segunda	
5	172.16.1.7	Alcaldía	Router 639 Alcaldía		Segunda	
6	172.16.1.9	Avalúos y Catastros	Mirian Calderón		Primera	D03
7	172.16.1.11	Sistemas	Router 672 Sistemas		Segunda	
8	172.16.1.33	Auditoría Interna	Lenin Ubidia		Primera	
9	172.16.1.34	Procuraduría	Deysy Játiva		Segunda	D30
10	172.16.1.35	Procuraduría	Mario Carrera		Segunda	D29
11	172.16.1.45	Comisaría	Amilcar Cruz			
12	172.16.1.50	Sistemas	Impresora HP Unidad de Sistemas		Segunda	

13	172.16.1.55	Registro de la Propiedad	Cristina Flores			
14	172.16.1.56	Registro de la Propiedad	Estrella Benavides			
15	172.16.1.57	Registro de la Propiedad	Carmen Andrango			
16	172.16.1.58	Registro de la Propiedad	Cristina Flores			
17	172.16.1.65	Planificación	Sandra Vaca		Primera	D26
18	172.16.1.66	Planificación	Julio Caicedo		Primera	
19	172.16.1.67	Avalúos y Catastros	Marco Andrade		Tercera	
20	172.16.1.68	Avalúos y Catastros	Raúl Manrique		Segunda	
21	172.16.1.69	Avalúos y Catastros	Edgar Iles		Primera	D04
22	172.16.1.70	Planificación	Vinicio Ortiz		Primera	
23	172.16.1.71	Planificación	Pilar Quito		Primera	
24	172.16.1.72	Participación Ciudadana	Sonia Valles		Primera	
25	172.16.1.73	Avalúos y Catastros	Orlando Echeverría		Primera	
26	172.16.1.82	Secretaría	Andrés Enríquez		Segunda	D52
27	172.16.1.83	Secretaría	Rosario Chuma		Segunda	D51
28	172.16.1.84	Información	Fernanda Recalde		Primera	D19
29	172.16.1.86	Secretaría	Escolta del Alcalde		Segunda	D50
30	172.16.1.98	Dirección Administrativa	Iván Segarra		Segunda	
31	172.16.1.99	Recursos Humanos	Carlos Chicaiza		Primera	D01
32	172.16.1.100	Dirección Administrativa	Francisco Álvarez		Exterior	
33	172.16.1.102	Obras Públicas	Impresora HP obras públicas		Primera	
34	172.16.1.103	Administrativo	Patricia Rea		Segunda	D28
35	172.16.1.105	Bodega	Marcela Michelena		Primera	
36	172.16.1.106	Compras Públicas	Anita Montenegro		Segunda	D45

37	172.16.1.108	Biblioteca	Cecilia Echeverría			
38	172.16.1.109	Dirección Administrativa	Impresora HP Compras Públicas		Segunda	
39	172.16.1.110	Bodega	Carlos Tamayo		Primera	D69
40	172.16.1.114	Contabilidad	Magdalena Recalde		Segunda	D34
41	172.16.1.115	Tesorería	Marisol Gallegos		Segunda	
42	172.16.1.117	Contabilidad	Iván Gallegos		Segunda	D38
43	172.16.1.118	Recaudaciones	Milton Lara		Primera	D05
44	172.16.1.119	Recaudaciones	Fausto Caranqui		Primera	D20
45	172.16.1.120	Contabilidad	Edwin Oña		Segunda	D35
46	172.16.1.121	Recaudaciones	Efrén Carrillo		Primera	D06
47	172.16.1.122	Contabilidad	Magdalena Gordillo		Segunda	D31
48	172.16.1.123	Agua Potable	Aura Félix		Primera	D13
49	172.16.1.124	Tesorería	Patricio Dueñas		Segunda	
50	172.16.1.126	Financiero	Cesar Pinto		Segunda	D43
51	172.16.1.130	Obras Públicas	Gerardo Bustos		Primera	D11
52	172.16.1.131	Fiscalización	Oscar Acosta		Primera	D07
53	172.16.1.132	O. P. Topografía	Homero Hurtado		Primera	D09
54	172.16.1.133	Agua Potable	Marco Bolaños		Primera	D14
55	172.16.1.134	Agua Potable	Oscar Yacelga		Primera	
56	172.16.1.135	Fiscalización	Sofía Pazmiño		Primera	
57	172.16.1.136	O. P. Infraestructura	Patricio Escobar		Primera	D08
58	172.16.1.137	Financiero	Lupita Gordón		Segunda	D42
59	172.16.1.138	Obras Públicas	Rosana Varela		Primera	
60	172.16.1.139	Agua Potable	Ramiro Martínez		Primera	D12

61	172.16.1.145	Planificación	Israel Estévez		Primera	D27
62	172.16.1.146	Obras Públicas	Edvio Enríquez		Primera	
63	172.16.1.148	Comunicación	Lorena Piñán		Segunda	
64	172.16.1.149	Planificación	William Chuquín		Tercera	
65	172.16.1.162	Comunicación	Luis Aceldo		Segunda	
66	172.16.1.164	Comunicación	Luis Aceldo		Segunda	
67	172.16.1.165	Comunicación	Anita Yalama		Segunda	D64
68	172.16.1.166	Participación Ciudadana	Wendy Ruiz		Tercera	
69	172.16.1.168	Planificación	Digitadora Actualización		Tercera	
70	172.16.1.184	Sala de Sesiones	Concejales		Segunda	D76
71	172.16.1.189	Patronato Municipal	Router Patronato		Exterior	
72	172.16.1.191	Biblioteca	Cecilia Echeverría			
73	172.16.1.192	Biblioteca	Cecilia Echeverría			
74	172.16.1.193	Biblioteca	Cecilia Echeverría			
75	172.16.1.196	Biblioteca	Cecilia Echeverría			
76	172.16.1.202	Policía Urcuquí	Router UPC Urcuquí		Exterior	
77	172.16.1.242	Catastros	Gonzalo Torres		Tercera	D62
78	172.16.1.253	Compras Públicas	Anita Montenegro		Segunda	D46

ANEXO E

El nuevo direccionamiento propuesto se especifica en las siguientes tablas:

VLAN 10: DIRECCIÓN ADMINISTRATIVA		**IP:172.16.2.161 – 172.16.2.190**		**MASK: 255.255.255.224**		
GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.6	172.16.2.161	Sistemas Informáticos	Mario Farinango	Primer Piso	
2	172.16.1.50	172.16.2.162	Sistemas Informáticos	Mario Farinango	Primer Piso	
3	172.16.1.11	172.16.2.163	Sistemas Informáticos	Mario Farinango	Primer Piso	
4	172.16.1.5	172.16.2.164	Sistemas Informáticos	Mario Farinango	Primer Piso	
5	172.16.1.109	172.16.2.165	Sistemas Informáticos	Impresora	Primer Piso	
6	172.16.1.103	172.16.2.166	Contratación Publica	Patricia Rea	Segundo Piso	D28
7	172.16.1.89	172.16.2.167	Contratación Publica	Iván Segarra	Segundo Piso	
8	172.16.1.193	172.16.2.168	Contratación Pública	Libre	Primer Piso	D69
9	172.16.1.105	172.16.2.169	Bodega	Marcelo Michelena	Primer Piso	D01
10	172.16.1.110	172.16.2.170	Bodega	Carlos Tamayo	Primer Piso	
11	172.16.1.99	172.16.2.171	Talento Humano	Carlos Chiza	Primer Piso	
12	172.16.1.72	172.16.2.172	Talento Humano	Diego Andrade	Primer Piso	
13	172.16.1.166	172.16.2.173	Talento Humano	Diego Andrade	Primer Piso	
14	172.16.1.191	172.16.2.174	Mantenimiento	Libre	Primer Piso	

15	172.16.1.192	172.16.2.175	Mantenimiento	Libre	Primer Piso	

VLAN 11: DIRECCIÓN FINANCIERA	**IP:172.16.2.193 – 172.16.2.222**	**MASK: 255.255.255.224**				
GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.126	172.16.2.193	Presupuesto	Cesar Pinto	Segundo Piso	D43
2	172.16.1.137	172.16.2.194	Presupuesto	Lupita Gordon	Segundo Piso	D42
3	172.16.1.124	172.16.2.195	Tesorería	Patricia Dueñas	Segundo Piso	
4	172.16.1.115	172.16.2.196	Tesorería	Marisol Gallegos	Segundo Piso	
5	172.16.1.114	172.16.2.197	Contabilidad	Magdalena Recalde	Segundo Piso	D34
6	172.16.1.117	172.16.2.198	Contabilidad	Iván Gallegos	Segundo Piso	D38
7	172.16.1.122	172.16.2.199	Contabilidad	Magdalena Gordillo	Segundo Piso	D31
8	172.16.1.120	172.16.2.200	Contabilidad	Edwin Oña	Segundo Piso	D35
9	172.16.1.121	172.16.2.201	Rentas	Libre	Primer Piso	
10	172.16.1.84	172.16.2.202	Información	Fernanda Recalde	Primer Piso	D19

VLAN 12: PLANIFICACIÓN TERRITORIAL Y DESARROLLO	**IP:172.16.2.225 – 172.16.2.254**	**MASK: 255.255.255.224**				
GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.9	172.16.2.225	Avalúos y Catastros	Mirian Calderón	Primer Piso	D03

2	172.16.1.67	172.16.2.226	Avalúos y Catastros	Marco Andrade	Tercer Piso	
3	172.16.1.68	172.16.2.227	Avalúos y Catastros	Raúl Manrique	Segundo Piso	
4	172.16.1.69	172.16.2.228	Avalúos y Catastros	Edgar Iles	Primer Piso	D04
5	172.16.1.73	172.16.2.229	Avalúos y Catastros	Orlando Echeverría	Primer Piso	
6	172.16.1.242	172.16.2.230	Avalúos y Catastros	Gonzalo Torres	Tercer Piso	D62
7	172.16.1.65	172.16.2.231	Regulación Urbana	Sandra Vaca	Primer Piso	D26
8	172.16.1.66	172.16.2.232	Regulación Urbana	Julio Caicedo	Primer Piso	
9	172.16.1.70	172.16.2.233	Regulación Urbana	Vinicio Ortiz	Primer Piso	
10	172.16.1.71	172.16.2.234	Tránsito y Transporte	Pilar Quito	Primer Piso	
11	172.16.1.145	172.16.2.235	Tránsito y Transporte	Israel Estévez	Primer Piso	D27
12	172.16.1.149	172.16.2.236	Tránsito y Transporte	Willian Chuquín	Tercer Piso	
13	172.16.1.168	172.16.2.237	Gestión Proyectos	Digitadora	Segundo Piso	
14	172,16.1.106	172.16.2.238	Compras Públicas	Anita Montenegro	Segundo Piso	
15	172.16.1253	172.16.2.239	Anita Montenegro	Anita Montenegro	Segundo Piso	

VLAN 13: ALCALDÍA	**IP:172.16.3.33 – 172.16.3.62**	**MASK: 255.255.255.224**

GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.148	172.16.3.33	Comunicación	Lorena Piñan	Segundo Piso	
2	172.16.1.162	172.16.3.34	Comunicación	Luis Alcedo	Segundo Piso	
3	172.16.1.164	172.16.3.35	Comunicación	Luis Alcedo	Segundo Piso	
4	172.16.1.165	172.16.3.36	Comunicación	Anita Yalama	Segundo Piso	D64

5	172.16.1.100	172.16.3.37	Comunicación	Libre	Segundo Piso	
6	172.16.1.82	172.16.3.38	Secretaría General	Andrés Enríquez	Segundo Piso	D52
7	172.16.1.83	172.16.3.39	Secretaría General	Rosario Chuma	Segundo Piso	D51
8	172.16.1.86	172.16.3.40	Secretaría General	Escolta del Alcalde	Segundo Piso	D50
9	172.16.1.189	172.16.3.41	Secretaría General	Libre	Segundo Piso	
10	172.16.1.202	172.16.3.42	Asesoría	Libre	Segundo Piso	
11	172.16.1.7	172.16.3.43	Alcalde	Victor Cruz	Segundo Piso	
12	172.16.1.131	172.16.3.44	Fiscalización	Oscar Acosta	Primer Piso	D07
13	172.16.1.135	172.16.3.45	Fiscalización	Sofía Pazmiño	Primer Piso	
14	172.16.1.108	172.16.3.46	Fiscalización	Libre	Primer Piso	
15	172.16.1.33	172.16.3.47	Auditoría Interna	Lenin Ubidia	Primer Piso	
16	172.16.1.196	172.16.3.48	Auditoria Interna	Libre	Primer Piso	
17	172.16.1.184	172.16.3.49	Sala de Reuniones	Consejales	Segundo Piso	D76

VLAN 14: DIRECCIÓN OBRAS PÚBLICAS	**IP:172.16.3.65 – 172.16.1.94**	**MASK: 255.255.255.224**

GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.123	172.16.3.65	Agua Potable	Aura Felix	Primer Piso	D13
2	172.16.1.133	172.16.3.66	Agua Potable	Marco Bolaños	Primer Piso	D14
3	172.16.1.134	172.16.3.67	Agua Potable	Oscar Yacelga	Primer Piso	
4	172.16.1.139	172.16.3.68	Agua Potable	Ramiro Martínez	Primer Piso	D12
5	172.16.1.132	172.16.3.69	Infraestructura	Homero Hurtado	Primer Piso	D09

6	172.16.1.136	172.16.3.70	Infraestructura	Patricio Escobar	Primer Piso	D08
7	172.16.1.30	172.16.3.71	Gestión de Riesgos	Gerardo Bustos	Primer Piso	D11
8	172.16.1.138	172.16.3.72	Gestión Ambiental	Rosana Varela	Primer Piso	
9	172.16.1.146	172.16.3.73	Gestión Viabilidad	Edvio Enrinquez	Primer Piso	
10	172.16.1.102	172.16.3.74	Gestión Viabilidad	Impresora	Primer Piso	

VLAN 15: REGISTRO DE LA PROPIEDAD	**IP:172.16.3.97– 172.16.1.110**	**MASK: 255.255.255.240**

GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.55	172.16.3.97	Registro de la Propiedad	Cristina Flores	Primer Piso	
2	172.16.1.58	172.16.3.98	Registro de la Propiedad	Cristina Flores	Primer Piso	
3	172.16.1.56	172.16.3.99	Registro de la Propiedad	Estrella Benavidez	Primer Piso	
4	172.16.1.57	172.16.3.100	Registro de la Propiedad	Carmen Anrango	Primer Piso	

VLAN 16: PROCURADURÍA SINDICA	**IP:172.16.3.129 – 172.16.1.142**	**MASK: 255.255.255.240**

GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.34	172.16.3.101	Procuraduría Sindica	Daysi Játiva	Primer Piso	D30

2	172.16.1.35	172.16.3.102	Procuraduría Sindica	Mario Carrera	Primer Piso	D29
3	172.16.1.45	172.16.3.103	Comisiones	Amílcar Cruz	Segundo Piso	
4	172.16.1.118	172.16.3.104	Recaudaciones	Milton Lara	Primer Piso	D05
5	172.16.1.119	172.16.3.104	Recaudaciones	Fausto Caranquí	Primer Piso	D20
6	172.16.1.121	172.16.3.105	Recaudaciones	Efrén Carrillo	Primer Piso	D06

VLAN 17 : DEPENDENCIAS EXTERNAS	**IP:172.16.2.129 – 172.16.2.158**	**MASK: 255.255.255.224**

GRUPO	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**CARGO-USUARIO**	**RESPONSABLE**	**UBICACIÓN**	**TOMA**
1	172.16.1.72	172.16.2.129	Unidad de desarrollo social	Sonia Valles		
2	172.16.1.108	172.16.2.130	Biblioteca	Cecilia Chávez		
3	172.16.1.109	172.16.2.131	Biblioteca	Cecilia Chávez		
4	172.16.1.110	172.16.2.133	Biblioteca	Cecilia Chávez		
5	172.16.1.111	172.16.2.133	Biblioteca	Cecilia Chávez		
6	172.16.1.112	172.16.2.134	Biblioteca	Cecilia Chávez		
7	172.16.1.166	172.16.2.135	Plaza del Buen Vivir	Wendy Ruiz		
8	172.16.1.167	172.16.2.136	Plaza del Buen Vivir	Wendy Ruiz		
9	172.16.1.168	172.16.2.137	Plaza del Buen Vivir	Wendy Ruiz		
10	172.16.1.169	172.16.2.138	Plaza del Buen Vivir	Wendy Ruiz		

ANEXO F

CONFIGURACIONES EN GSN3

Primordialmente se debe realizar las configuraciones básicas para cada uno de los equipos activos existentes en la topología física, ya que con estas configuraciones se puede asegurar una fácil administración.

La simulación del modelo propuesto para la red de datos de la Institución fue desarrollada utilizando un simulador del mercado el cual permite demostrar la funcionalidad del modelo en independencia de la tecnología de equipamiento utilizado, cumpliendo los objetivos enfocados en brindar seguridad, disponibilidad, flexibilidad y escalabilidad. El software utilizado para la simulación es GNS3 versión 1.3.0.

Dentro de la capa de distribución su objetivo está enfocado en asegurar la continuidad del servicio; en cambio la capa acceso está enfocada en brindar conexión hacia usuario final teniendo en cuenta criterios de segmentación a nivel lógico, además de control el tráfico generado dentro de las diferentes vlans y aplicar seguridad en el acceso hacia el equipamiento activo.

El modelo diseñado está basado en una topología del tipo jerárquica que permite tener una infraestructura de red flexible que se adapte a los cambios de una forma fácil y ágil sin tener que modificar el modelo aplicado, adicionalmente su estructura facilita el aislamiento de fallas dado que se permite aislar segmentos específicos sin dejar de brindar el servicio al resto de la red, además al contar con control en el tráfico inter-vlans impide que tráfico no deseado se propague por la red.

CONFIGURACIONES BÁSICAS

Configuración de contraseñas de acceso: El modo exec privilegiado permite el ingreso y modificación de la información que tiene el equipo de red, por ende debe ir con su debida contraseña. Para proteger el acceso al equipamiento activo

se debe configurar la contraseña para el acceso de consola y el acceso por telnet. La configuración se lo realiza mediante las siguientes líneas.

- Line console
- Password contraseña
- Login

Una vez realizado las configuraciones de contraseña de acceso, al ingresar al equipo nos pide una contraseña como en muestra la figura 30.

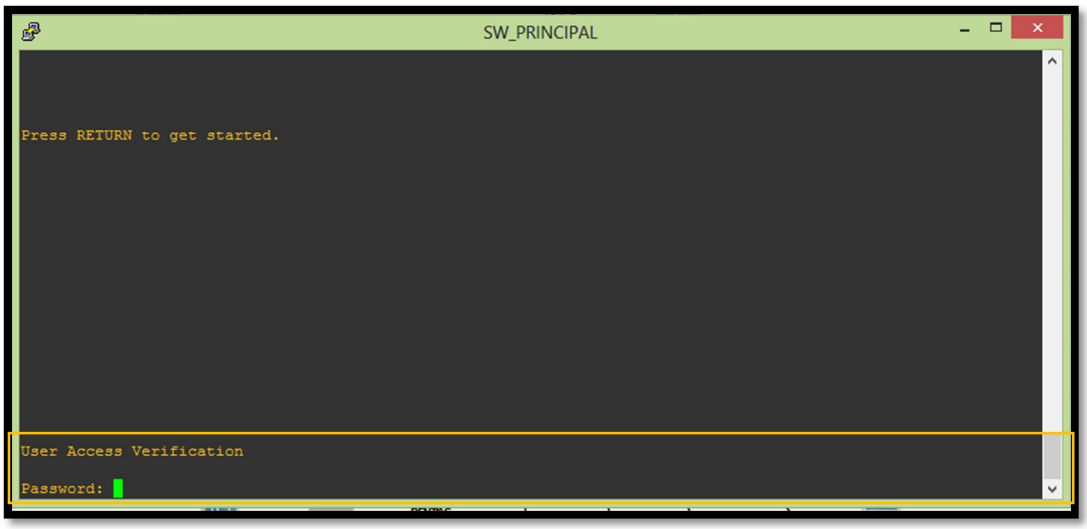

Figura 30. Acceso al equipo mediante línea de consola

Referencia: Elaboración propia

Para crea la contraseña en modo exec privilegiado, se lo realiza mediante el siguiente comando:

- Enable secret password {contraseña}

Con la cual restringe el acceso al equipo de red y permite resguardar la información que se encuentra configurado en estos.

Es importante que las contraseñas se almacenen cifrada se observa en la siguiente figura 31:

Figura 31. Contraseña de exec privilegiado cifrada

Referencia: Elaboración propia

En la figura 32, se encuentra las configuraciones realizadas acceso mediante contraseñas de acceso y acceso mediante terminal virtual.

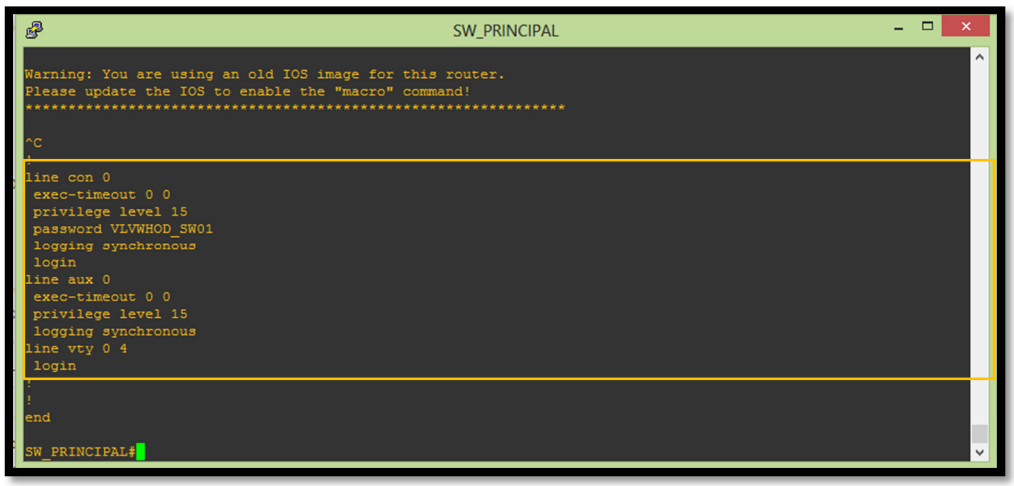

Figura 32. Vista de contraseñas de acceso

Referencia: Elaboración propia

En caso de ingreso al equipo de red no se podrán utilizar por ende es importante cifrar estas contraseñas mediante el siguiente comando: Service password-encryption

Una vez ejecutado el comando las contraseñas se almacenan cifradas como indica a continuación en la figura 33:

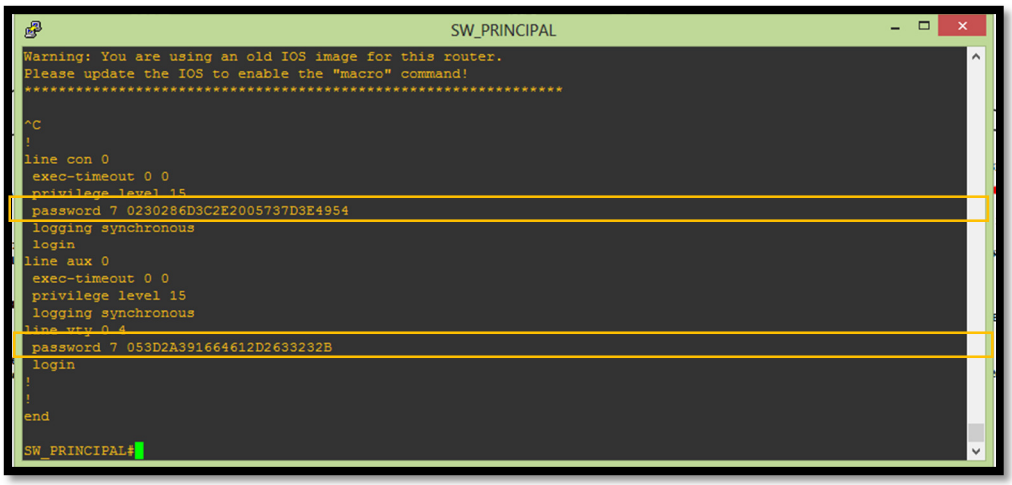

Figura 33. Vista de contraseñas de acceso cifradas

Referencia: Elaboración propia

Configuración de la dirección IP en los equipos: La configuración de los equipos es indispensable para identificar algún daño en el equipo utilizado y poder solucionarlo de manera oportuna, por motivos de seguridad se debe configurar una VLAN de administración con la cual se pueda acceder remotamente, mediante la VLAN 99 con la dirección IP: 172.16.3.145 255.255.255.240. Para su configuración se puede seguir los siguientes comandos:

- Ingreso de la interfaz de administración
- Agregar la IP de administración del equipo

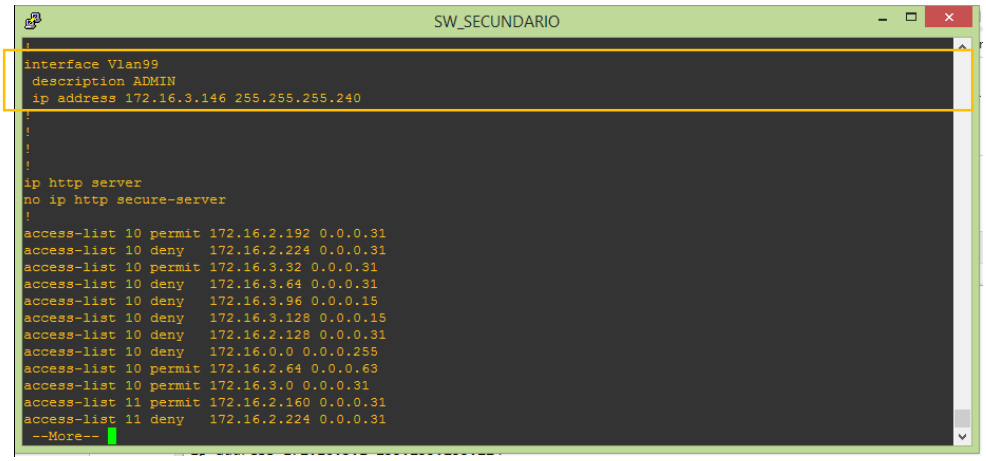

Figura 34. Configuración IP de administración

Referencia: Elaboración propia

En la figura 34, se indica la configuración de dirección IP en el switch principal el cual puede conectarse remotamente vía telnet, para su acceso es mediante la contraseña de las líneas de terminal vty.

Configuración nombre del equipo: Mediante esta configuración facilita la administración del personal su configuración se realiza mediante la siguiente línea de comando:

- Hostname nombre_equipo

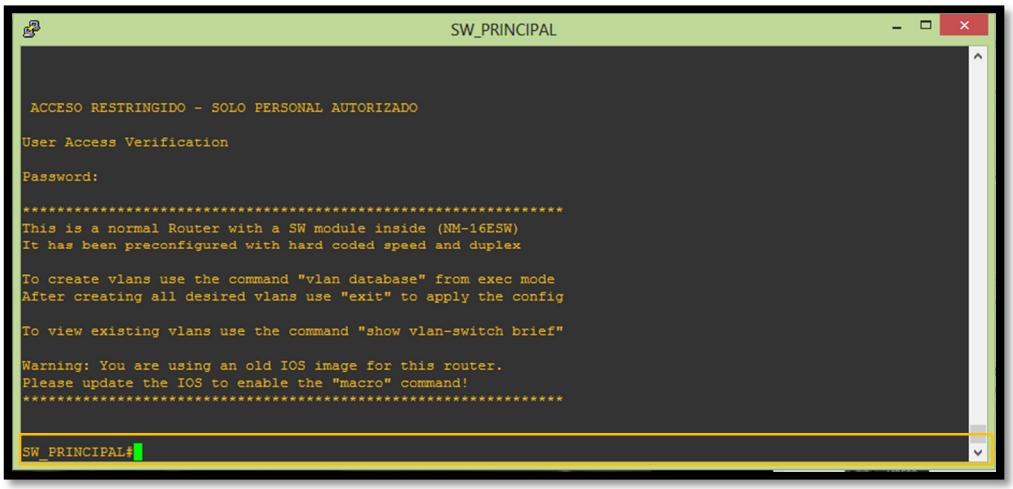

Figura 35.Visualización del nombre del equipo
Referencia: Elaboración propia

Configuración de acceso ssh: Antes de la configuración de acceso ssh es necesario que tenga configurado el nombre del equipo y definido el nombre de dominio, el cual sirve como base para la generación de la clave RSA.

- Configuración del nombre del dominio ip domain-name gadmu.com
- Generación de las claves RSA - crypto key generate rsa

Mediante los siguientes pasos se configura el acceso ssh:

1. Especificar el número de bits a utilizarse. Por defecto se encuentra establecido en 512
2. Definición del tiempo de time out de ssh
3. Define el reintentos validos permitidos
4. Definición de la versión ssh
5. Definición de usuario y contraseña para el acceso ssh.
6. Habilitar ssh para terminal virtual
7. Máximo de intentos para modo exc privilegiado
8. Aplicar el acceso ssh
9. Definir el método de logeo

Mediante el acceso a modo configuración los pasos a configurase son utilizarse es la siguiente:

1. 512
2. ip ssh time-out 20
3. ip ssh authentication-retries 4
4. ip ssh version 2
5. username root privilege 15 password VLVWHOD_SSH
6. line vty 0 4
7. exec-timeout 3
8. transport input ssh 2
9. login local

Figura 36. Configuración SSH

Referencia: Elaboración propia

En la figura 36, se indica que está funcionando ssh mediante el comando show ip ssh

Configuración de banner de bienvenida: Mediante el siguiente comando se realiza la configuración del banner.

- Banner motd & mensaje_de_bievenida &

Figura 37. Visualización del Banner de Bienvenida

Referencia: Elaboración propia

CONFIGURACIÓN BASADA EN CAPAS

Al finalizar las configuraciones básicas, en cada uno de los equipos que corresponden al modelo propuesto, se realiza las configuraciones correspondientes a cada capa.

CAPA NÚCLEO COLAPSADO

Esta capa maneja el tráfico interno hacia el nivel de acceso, por lo cual se debe realizar configuraciones sobre disponibilidad del servicio, listas de acceso entre otras.

Configuración de VLAN: Las vlans se utilizarán para la segmentación del tráfico y dominios de broadcast a nivel de acceso. En la tabla 27 y 28 se especifica las vlans correspondientes a cada departamento, para la configuración se debe realizar los siguientes pasos:

- Creación de una VLAN con id valido
- Agregar una descripción para la VLAN
- Especificar un nombre único para especificar la VLAN

Los 2 últimos pasos no son obligatorios, pero colaboran a una ordenada administración, en la figura 38 se indica las vlans creadas.

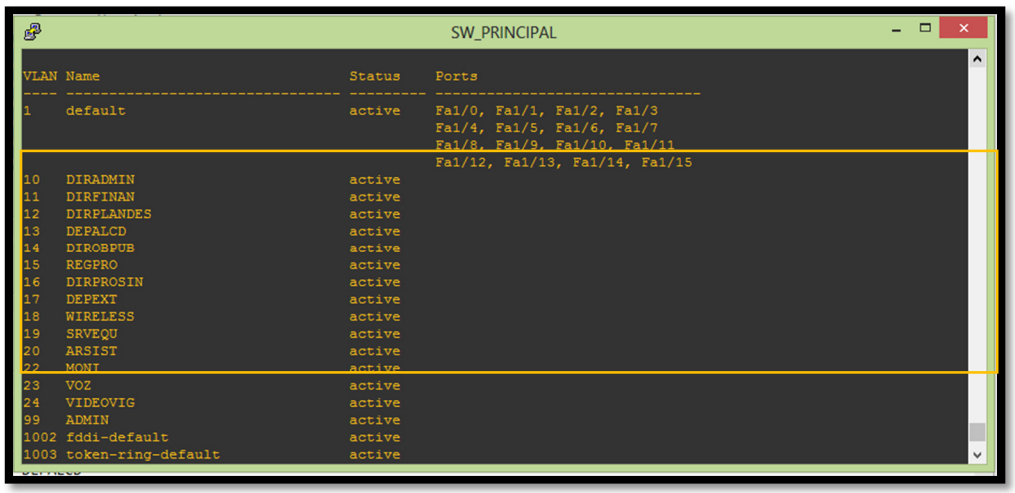

Figura 38. Creación vlan - Capa núcleo colapsado

Referencia: Elaboración propia

Los equipos de esta capa deberán manejar el enrutamiento inter-vlans es indispensable que se asigne una direccionamiento IP de las VLAN utilizadas a nivel de acceso.

En la figura 39 se indica asigna las direcciones IP respectivas a cada Vlan, este direccionamiento se especifica en la Tabla 30 en el capítulo del rediseño de la red.

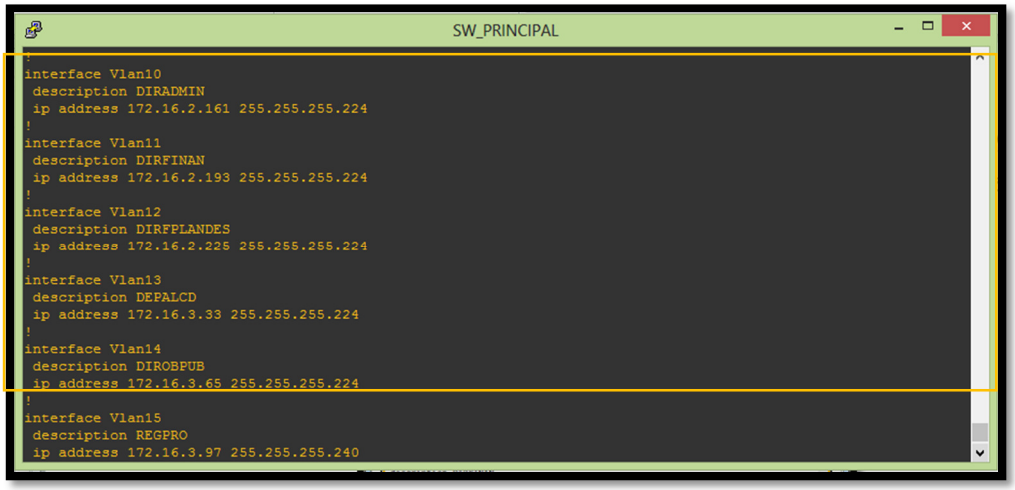

Figura 39. Asignación de IP a VLAN correspondientes

Referencia: Elaboración propia

En función del nivel se manejará el tipo de puerto a utilizarse, se operará dos puertos tipo access y tipo trunk

Configuración puertos de acceso: Este modo se utiliza para la conexión con los servidores se utiliza este tipo de puerto, además para conexión con los bloques de cada piso. Su configuración es la siguiente:

- Ingreso a la interfaz del puerto deseado
- Designar el puerto en modo acceso
- Establecer la vlan a la cual pertenece el puerto

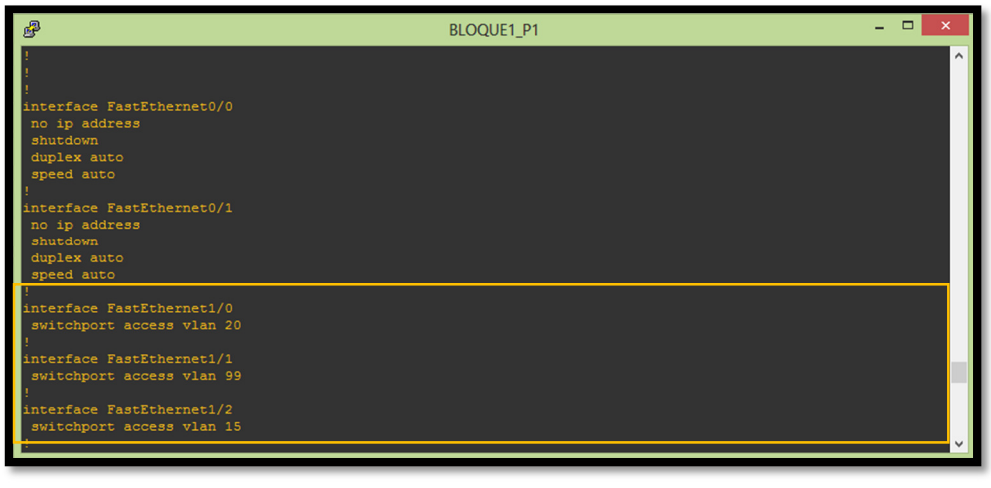

Figura 40. Configuración a nivel de acceso

Referencia: Elaboración propia

Es indispensable que se agregue un puerto, para que facilite la gestión y administración del equipamiento activo.

Configuración de puertos trunk: Con este puerto se comunicarán múltiples vlans existente en la capa de acceso, mediante los siguientes pasos se configura los puertos en modo trunk:

- Configurar la interfaz de la vlan con la dirección IP
- Configurar el puerto de conexión tipo trunk
- Asignación de las vlan que van a pasar por el puerto trunk

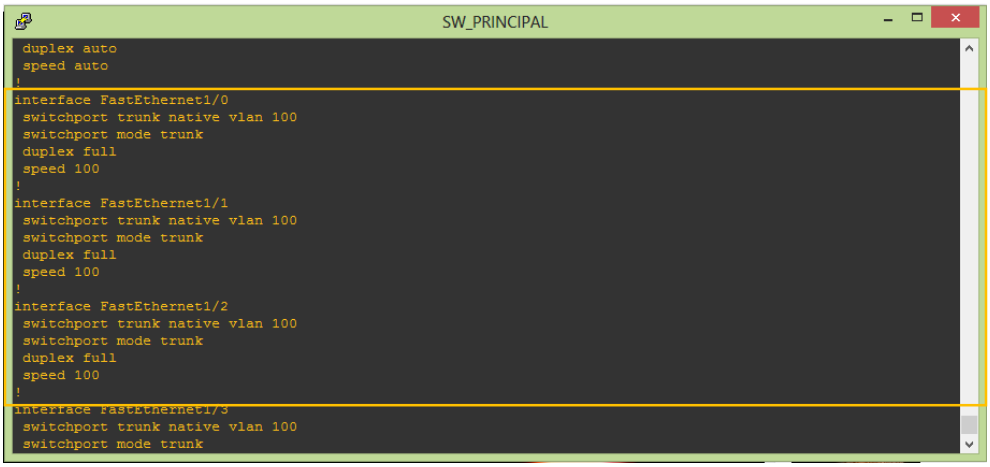

Figura 41. Configuración de puertos trunk

Referencia: Elaboración propia

Configuración de protocolo troncal de VLAN (VTP): Cuando configure una VLAN nueva en un servidor VTP, se distribuye la VLAN por todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. El VTP es un protocolo patentado de Cisco disponible en la mayoría de los productos de la serie Catalyst de Cisco. Para su configuración se debe seguir los siguientes pasos:

- Crear vtp en modo servidor
- Crear una dominio
- Crear una contraseña de acceso

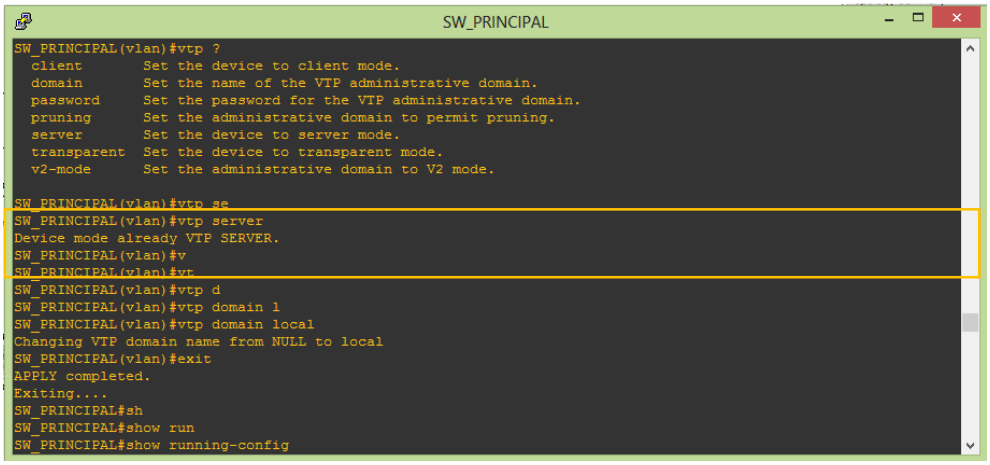

Figura 42.Creación VTP en switch principal

Referencia: Elaboración propia

Habilitación de alta disponibilidad: Al brindan conexión a la capa acceso es importante que se brinda alta disponibilidad asegurando la conexión; al ocurrir un daño podría perderse la comunicación interna para la configuración se debe seguir los siguientes pasos:

- Ingreso a la interface de la vlan
- Configuración de la dirección IP a la interfaz física
- Configuración de IP virtual.
- Configuración prioridades en HSRP.

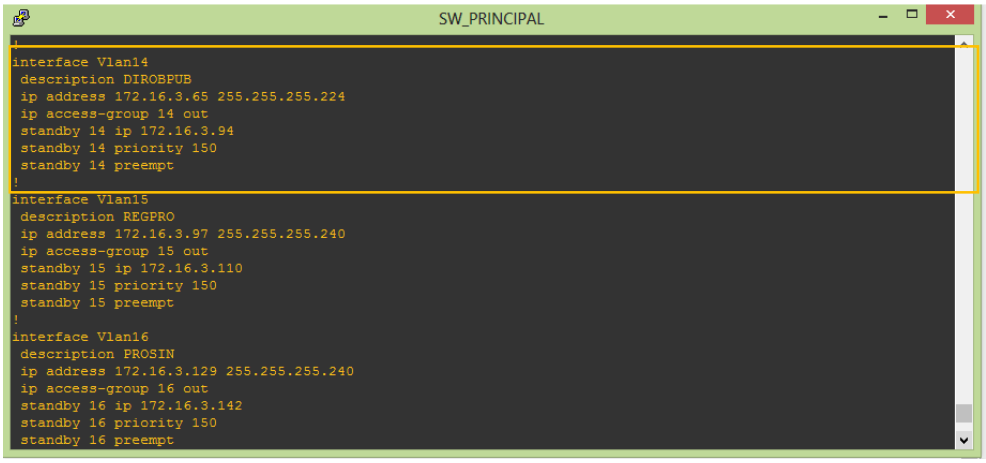

Figura 43. Configuración de alta disponibilidad

Referencia: Elaboración propia

Configuración de listas de control de acceso: Es importante tener un control para el acceso del equipamiento activo, se debe configurar las siguientes líneas para mejorar el rendimiento de la red.

- El usuario con la IP 172.16.3.34 tendrá acceso a las Vlans de: Dirección administrativa, Dirección Financiera, Planificación territorial y desarrollo, Dirección de Obras públicas, Registro de la Propiedad, Procuraduría Sindica, Dependencias externas.
- El usuario con la IP 172.16.2.162 tendrá acceso a los recursos VLAN de dirección Financiera.
- El usuario con la IP 172.16.2.194 tendrá acceso a los recursos VLAN de Dirección Administrativa.
- El usuario con la IP 172.16.3.2 tendrá acceso todos los recursos de la red.
- El usuario con la IP 172.16.3.146 tendrá acceso a todos los recursos de la red.

Estas líneas de control de acceso son formuladas por el grupo en el área de sistemas, con estas se puede permiten y denegar la comunicación entre departamentos. La configuración se realiza mediante los siguientes pasos:

- Definir la vlan para el control de acceso al equipamiento activo
- Aplicar la ACLs creada dentro de la interfaz terminal virtual

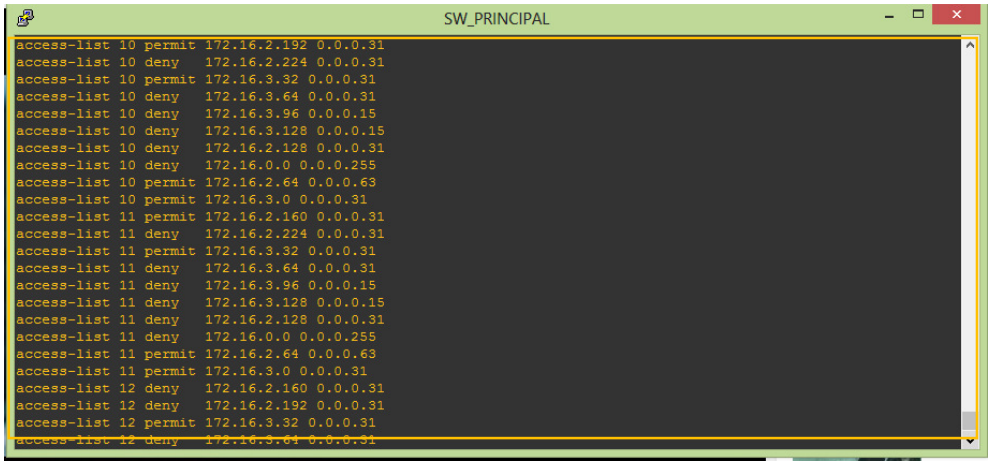

Figura 44. Configuración de lista de control de acceso

Referencia: Elaboración propia

En la figura 45 se asocia las listas de acceso a cada interfaz de cada vlan creada, se puede configurar en dos formas (in, out) según el tráfico de cada lista de acceso.

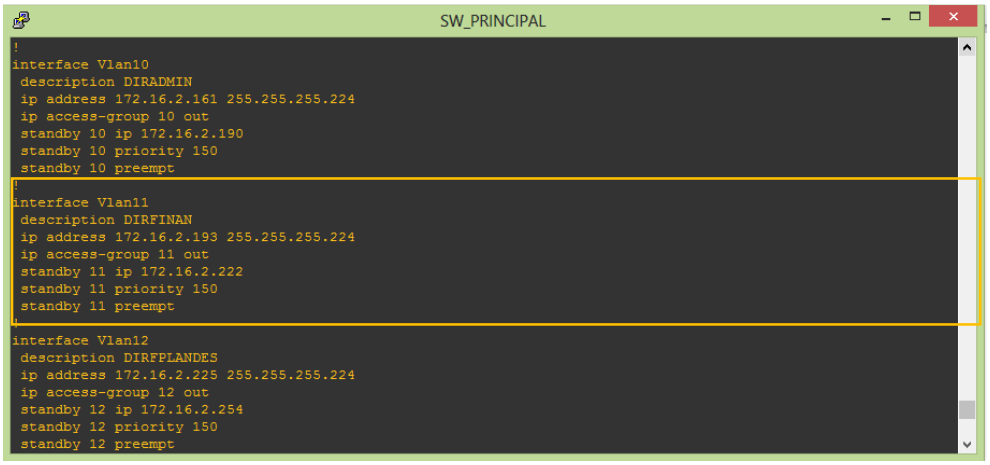

Figura 45.Configuración de lista de control de acceso en cada Vlans

Referencia: Elaboración propia

Configuración de agregación de enlaces: Esta configuración permite balancear la carga tanto de entrada como de salida, brindando la estabilidad a la conexión, en función de la carga manejada se debe considerara la habilitación en los equipos a utilizarse.

Para su implementación los puertos deben contener las mismas configuraciones básicas, así mismo pertenecer a la misma unidad, para su configuración se debe seguir los siguientes pasos:

- Especifique las interfaces que componen al grupo Etherchannel.
- Crear la interfaz de canal de puertos.
- Asociar al canal creado.

En la figura 46, se indica la habilitación de etherchannel en el switch principal de la topología propuesta.

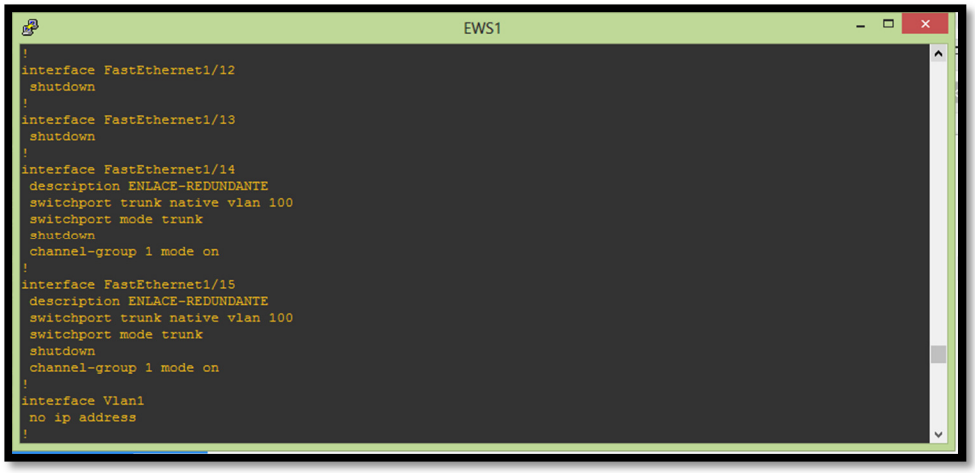

Figura 46. Configuración de EtherChannel

Referencia: Elaboración propia

CAPA ACCESO

Esta capa brinda la conexión al usuario final, por ende se debe tomar seguridades a nivel de puerto, con lo cual brinde mayor seguridad y permita mejorar el rendimiento y reducir los dominios de broadcast.

Configuración de protocolo troncal para Vlans (VTP): Cuando configure una VLAN nueva en un servidor VTP, se distribuye la VLAN por todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. El VTP es un protocolo patentado de Cisco disponible en la mayoría de los productos de la serie Catalyst de Cisco. Para su configuración se debe seguir los siguientes pasos:

- Crear vtp en modo cliente
- Crear una dominio
- Crear una contraseña de acceso

Figura 47. Configuración VTP capa acceso en el BLOQUE 2
Referencia: Elaboración propia

Configuración de puertos de acceso: Una vez declarado las vlans necesarias a nivel de acceso, se debe configurar los puertos hacia nivel de usuario basándose en el anexo B “Direccionamiento IP basado en VLAN”, donde se especifica el nuevo direccionamiento propuesto basando en VLAN´S.

Conjuntamente se configura las estaciones de trabajo con la finalidad de habilitar el acceso del usuario en la red. El procedimiento se realiza de dos maneras especificadas a continuación: Dentro de la vlan indicada.

- Definir la vlan - determinada por el ID
- Definir el puerto de conexión

Dentro de la interfaz deseada.

- Definir el puerto de conexión
- Definir el tipo de conexión del puerto
- Declarar la vlan correspondiente

Figura 48. Configuración tipo acceso BLOQUE 2

Referencia: Elaboración propia

Configuración de puertos trunk: El manejo de diferentes vlans se maneja por cada bloque, es necesario que los puertos que configuren tipo trunk, identificando claramente los puertos utilizados como conexión hacia los equipos de distribución, para la configuración de puertos en tipo trunk:

- Ingresar la interfaz a configurarse
- Definir el tipo de conexión de puerto
- Declarar las vlan permitidas a pasar por la interfaz

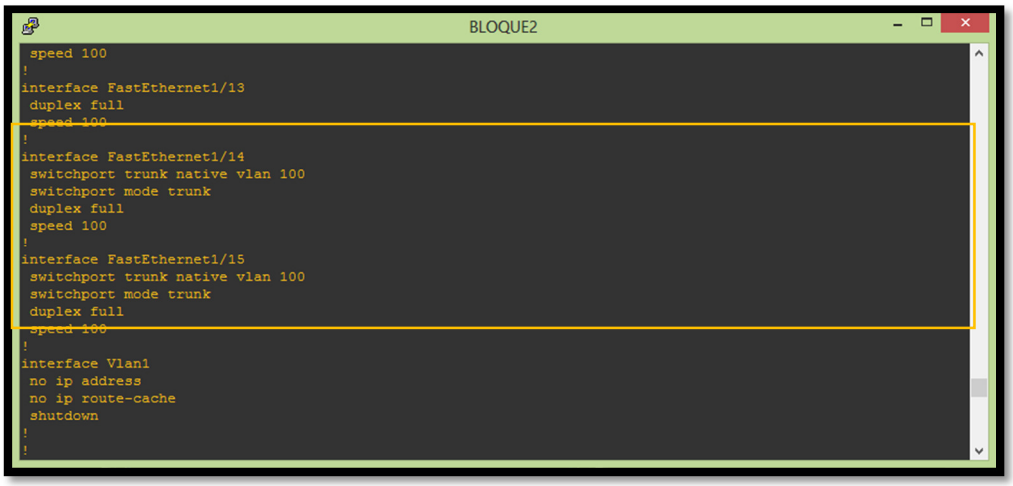

Figura 49. Configuración de puerto tipo trunk BLOQUE 2

Referencia: Elaboración propia

Se considera el siguiente parámetro (Control de acceso mediante MAC): El objetivo principal es impedir el cambio de dirección IP en los equipos de GADMU sin autorización, además evitar que equipos que ingresar a la institución y no sean los empleados tengan acceso a los recursos, por ende se ha considerado configurar lista de control de acceso basada en la dirección MAC de los equipos del GADMU, una vez que se encuentre configurado el puerto con su MAC, específicamente envía el paquete solo cuando hay coincidencia, con lo cual se mejora la seguridad y la administración de la red.

- Ingreso a la interfaz de configuración
- Asignar el control de acceso basado en la dirección MAC del usuario

Figura 50. Configuración de listas de acceso BLOQUE 2

Referencia: Elaboración propia

Luego de realizar todas las configuraciones respectivas para una de las capas de modelo de acuerdo a los criterios basadas en el capítulo 3, la red se encuentra totalmente operativa, además se tiene criterios sobre seguridad, flexibilidad.

Conjuntamente se ha limitado los dominios de broadcast en función de todo el análisis realizado anteriormente, dado que el modelo jerárquico es basado en capas facilita el mantenimiento y ayuda a una ordena administración, gestión a los encargados de la administración de la red, es recomendable la utilización de una herramienta de monitoreo.

ANEXO G

CONFIGURACIONES BASADO EN CAPAS

CONFIGURACIONES DE SW PRINCIPAL

```
SW_PRINCIPAL#show running-config
Building configuration...

Current configuration: 9622 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname SW_PRINCIPAL
enable secret 5 $1$mERr$/0rj7qQ.UfBi8p5rKOdpk.
ip routing
ip ssh authentication-retries 2
ip ssh time-out 30
no ip domain-lookup
ip domain-name gadmu.local
spanning-tree mode pvst
spanning-tree vlan 1 priority 24576
interface Port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/2
```

```
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/5
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/6
description ENLACE-REDUNDANTE
channel-group 1 mode active
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/7
description ENLACE-REDUNDANTE
channel-group 1 mode active
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

```
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
```

```
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
description DIRADMIN
ip address 172.16.2.161 255.255.255.224
ip access-group 10 out
standby version 2
standby 10 ip 172.16.2.190
standby 10 priority 150
standby 10 preempt
!
interface Vlan11
description DIRFINAN
```

```
ip address 172.16.2.193 255.255.255.224
ip access-group 11 out
standby version 2
standby 11 ip 172.16.2.222
standby 11 priority 150
standby 11 preempt
!
interface Vlan12
description DIRFPLANDES
ip address 172.16.2.225 255.255.255.224
ip access-group 12 out
standby version 2
standby 12 ip 172.16.2.254
standby 12 priority 150
standby 12 preempt
!
interface Vlan13
description DEPALCD
ip address 172.16.3.33 255.255.255.224
ip access-group 13 out
standby version 2
standby 13 ip 172.16.3.62
standby 13 priority 150
standby 13 preempt
!
interface Vlan14
description DIROBPUB
ip address 172.16.3.65 255.255.255.224
ip access-group 14 out
standby version 2
standby 14 ip 172.16.3.94
standby 14 priority 150
standby 14 preempt
```

```
!
interface Vlan15
description REGPRO
ip address 172.16.3.97 255.255.255.240
ip access-group 15 out
standby version 2
standby 15 ip 172.16.3.110
standby 15 priority 150
standby 15 preempt
!
interface Vlan16
description PROSIN
ip address 172.16.3.129 255.255.255.240
ip access-group 16 out
standby version 2
standby 16 ip 172.16.3.142
standby 16 priority 150
standby 16 preempt
!
interface Vlan17
description DEPEXT
ip address 172.16.2.129 255.255.255.224
ip access-group 17 out
standby version 2
standby 17 ip 172.16.2.158
standby 17 priority 150
standby 17 preempt
!
interface Vlan18
description WIRELESS
ip address 172.16.0.1 255.255.255.0
ip access-group 18 out
standby version 2
```

```
standby 18 ip 172.16.0.254
standby 18 priority 150
standby 18 preempt
!
interface Vlan19
description SRVEQU
ip address 172.16.2.65 255.255.255.192
ip access-group 19 out
standby version 2
standby 19 ip 172.16.2.126
standby 19 priority 150
standby 19 preempt
!
interface Vlan20
description ARSIST
ip address 172.16.3.1 255.255.255.224
ip access-group 20 out
standby version 2
standby 20 ip 172.16.3.30
standby 20 priority 150
standby 20 preempt
!
interface Vlan23
description VOZ
ip address 172.16.1.1 255.255.255.0
!
interface Vlan24
description VIDEOVIG
ip address 172.16.2.1 255.255.255.192
!
interface Vlan99
description ADMIN
ip address 172.16.3.113 255.255.255.240
```

```
!
ip classless
!
ip flow-export version 9
!
!
access-list 10 permit 172.16.2.192 0.0.0.31
access-list 10 deny 172.16.2.224 0.0.0.31
access-list 10 permit 172.16.3.32 0.0.0.31
access-list 10 deny 172.16.3.64 0.0.0.31
access-list 10 deny 172.16.3.96 0.0.0.15
access-list 10 deny 172.16.3.128 0.0.0.15
access-list 10 deny 172.16.2.128 0.0.0.31
access-list 10 deny 172.16.0.0 0.0.0.255
access-list 10 permit 172.16.2.64 0.0.0.63
access-list 10 permit 172.16.3.0 0.0.0.31
access-list 11 permit 172.16.2.160 0.0.0.31
access-list 11 deny 172.16.2.224 0.0.0.31
access-list 11 permit 172.16.3.32 0.0.0.31
access-list 11 deny 172.16.3.64 0.0.0.31
access-list 11 deny 172.16.3.96 0.0.0.15
access-list 11 deny 172.16.3.128 0.0.0.15
access-list 11 deny 172.16.2.128 0.0.0.31
access-list 11 deny 172.16.0.0 0.0.0.255
access-list 11 permit 172.16.2.64 0.0.0.63
access-list 11 permit 172.16.3.0 0.0.0.31
access-list 12 deny 172.16.2.160 0.0.0.31
access-list 12 deny 172.16.2.192 0.0.0.31
access-list 12 permit 172.16.3.32 0.0.0.31
access-list 12 deny 172.16.3.64 0.0.0.31
access-list 12 deny 172.16.3.96 0.0.0.15
access-list 12 deny 172.16.3.128 0.0.0.15
access-list 12 deny 172.16.2.128 0.0.0.31
```

```
access-list 12 deny 172.16.0.0 0.0.0.255
access-list 12 permit 172.16.2.64 0.0.0.63
access-list 12 permit 172.16.3.0 0.0.0.31
access-list 13 permit 172.16.2.160 0.0.0.31
access-list 13 permit 172.16.2.192 0.0.0.31
access-list 13 permit 172.16.2.224 0.0.0.31
access-list 13 permit 172.16.3.64 0.0.0.31
access-list 13 permit 172.16.3.96 0.0.0.15
access-list 13 permit 172.16.3.128 0.0.0.15
access-list 13 permit 172.16.2.128 0.0.0.31
access-list 13 permit 172.16.0.0 0.0.0.255
access-list 13 permit 172.16.2.64 0.0.0.63
access-list 13 permit 172.16.3.0 0.0.0.31
access-list 14 deny 172.16.2.160 0.0.0.31
access-list 14 deny 172.16.2.192 0.0.0.31
access-list 14 deny 172.16.2.224 0.0.0.31
access-list 14 permit 172.16.3.32 0.0.0.31
access-list 14 deny 172.16.3.96 0.0.0.15
access-list 14 deny 172.16.3.128 0.0.0.15
access-list 14 deny 172.16.2.128 0.0.0.31
access-list 14 deny 172.16.0.0 0.0.0.255
access-list 14 permit 172.16.2.64 0.0.0.63
access-list 14 permit 172.16.3.0 0.0.0.31
access-list 15 deny 172.16.2.160 0.0.0.31
access-list 15 deny 172.16.2.192 0.0.0.31
access-list 15 deny 172.16.2.224 0.0.0.31
access-list 15 permit 172.16.3.32 0.0.0.31
access-list 15 deny 172.16.3.64 0.0.0.31
access-list 15 deny 172.16.3.128 0.0.0.15
access-list 15 deny 172.16.2.128 0.0.0.31
access-list 15 deny 172.16.0.0 0.0.0.255
access-list 15 permit 172.16.2.64 0.0.0.63
access-list 15 permit 172.16.3.0 0.0.0.31
```

```
access-list 16 deny 172.16.2.160 0.0.0.31
access-list 16 deny 172.16.2.192 0.0.0.31
access-list 16 deny 172.16.2.224 0.0.0.31
access-list 16 permit 172.16.3.32 0.0.0.31
access-list 16 deny 172.16.3.64 0.0.0.31
access-list 16 deny 172.16.3.96 0.0.0.15
access-list 16 deny 172.16.2.128 0.0.0.31
access-list 16 deny 172.16.0.0 0.0.0.255
access-list 16 permit 172.16.2.64 0.0.0.63
access-list 16 permit 172.16.3.0 0.0.0.31
access-list 17 deny 172.16.2.160 0.0.0.31
access-list 17 deny 172.16.2.192 0.0.0.31
access-list 17 deny 172.16.2.224 0.0.0.31
access-list 17 permit 172.16.3.32 0.0.0.31
access-list 17 deny 172.16.3.64 0.0.0.31
access-list 17 deny 172.16.3.96 0.0.0.15
access-list 17 deny 172.16.3.128 0.0.0.15
access-list 17 deny 172.16.0.0 0.0.0.255
access-list 17 permit 172.16.2.64 0.0.0.63
access-list 17 permit 172.16.3.0 0.0.0.31
access-list 18 deny 172.16.2.160 0.0.0.31
access-list 18 deny 172.16.2.192 0.0.0.31
access-list 18 deny 172.16.2.224 0.0.0.31
access-list 18 permit 172.16.3.32 0.0.0.31
access-list 18 deny 172.16.3.64 0.0.0.31
access-list 18 deny 172.16.3.96 0.0.0.15
access-list 18 deny 172.16.3.128 0.0.0.15
access-list 18 deny 172.16.2.128 0.0.0.31
access-list 18 permit 172.16.2.64 0.0.0.63
access-list 18 permit 172.16.3.0 0.0.0.31
access-list 19 permit 172.16.2.160 0.0.0.31
access-list 19 permit 172.16.2.192 0.0.0.31
access-list 19 permit 172.16.2.224 0.0.0.31
```

```
access-list 19 permit 172.16.3.32 0.0.0.31
access-list 19 permit 172.16.3.64 0.0.0.31
access-list 19 permit 172.16.3.96 0.0.0.15
access-list 19 permit 172.16.3.128 0.0.0.15
access-list 19 permit 172.16.2.128 0.0.0.31
access-list 19 permit 172.16.0.0 0.0.0.255
access-list 19 permit 172.16.3.0 0.0.0.31
access-list 20 permit 172.16.2.160 0.0.0.31
access-list 20 permit 172.16.2.192 0.0.0.31
access-list 20 permit 172.16.2.224 0.0.0.31
access-list 20 permit 172.16.3.32 0.0.0.31
access-list 20 permit 172.16.3.64 0.0.0.31
access-list 20 permit 172.16.3.96 0.0.0.15
access-list 20 permit 172.16.3.128 0.0.0.15
access-list 20 permit 172.16.2.128 0.0.0.31
access-list 20 permit 172.16.0.0 0.0.0.255
access-list 20 permit 172.16.2.64 0.0.0.63
line con 0
password 7 081760783E312A332D383B547B
login
!
line aux 0
!
line vty 0 4
password 7 081760783E312A332D3D383D
login
end
```

CONIGURACIONES DE SW SECUNDARIO

```
SW_SECUNDARIO#show running-config
Building configuration...
```

```
Current configuration : 9302 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname SW_SECUNDARIO
enable secret 5 $1$mERr$PFMWQfSSfdtCTWT0nnvHZ.
ip routing
username root password 7 081760783E312A332D383F2C
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 30
ip domain-name gadmu.local
spanning-tree mode pvst
spanning-tree vlan 1 priority 28672
!
interface Port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
```

```
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/5
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/6
description ENLACE-REDUNDANTE
channel-group 1 mode passive
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/7
description ENLACE-REDUNDANTE
channel-group 1 mode passive
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
```

```
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
```

```
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
description DIRADMIN
ip address 172.16.2.161 255.255.255.224
ip access-group 10 out
standby version 2
standby 10 ip 172.16.2.190
!
interface Vlan11
description DIRFINAN
ip address 172.16.2.193 255.255.255.224
ip access-group 11 out
standby version 2
standby 11 ip 172.16.2.222
!
interface Vlan12
description DIRFPLANDES
```

```
ip address 172.16.2.225 255.255.255.224
ip access-group 12 out
standby version 2
standby 12 ip 172.16.2.254
!
interface Vlan13
description DEPALCD
ip address 172.16.3.33 255.255.255.224
ip access-group 13 out
standby version 2
standby 13 ip 172.16.3.62
!
interface Vlan14
description DIROBPUB
ip address 172.16.3.65 255.255.255.224
ip access-group 14 out
standby version 2
standby 14 ip 172.16.3.94
!
interface Vlan15
description REGPRO
ip address 172.16.3.97 255.255.255.240
ip access-group 15 out
standby version 2
standby 15 ip 172.16.3.110
!
interface Vlan16
description PROSIN
ip address 172.16.3.129 255.255.255.240
ip access-group 16 out
standby version 2
standby 16 ip 172.16.3.142
!
```

```
interface Vlan17
description DEPEXT
ip address 172.16.2.129 255.255.255.224
ip access-group 17 out
standby version 2
standby 17 ip 172.16.2.158
!
interface Vlan17
description DEPEXT
ip address 172.16.2.129 255.255.255.224
ip access-group 17 out
standby version 2
standby 17 ip 172.16.2.158
!
interface Vlan18
description WIRELESS
ip address 172.16.0.1 255.255.255.0
ip access-group 18 out
standby version 2
standby 18 ip 172.16.0.254
!
interface Vlan19
description SRVEQU
ip address 172.16.2.65 255.255.255.192
ip access-group 19 out
standby version 2
standby 19 ip 172.16.2.126
!
interface Vlan20
description ARSIST
ip address 172.16.3.1 255.255.255.224
ip access-group 20 out
standby version 2
```

```
standby 20 ip 172.16.3.30
!
interface Vlan23
description VOZ
ip address 172.16.1.1 255.255.255.0
!
interface Vlan24
description VIDEOVIG
ip address 172.16.2.1 255.255.255.192
!
interface Vlan99
description ADMIN
ip address 172.16.3.113 255.255.255.240
!
ip classless
!
ip flow-export version 9
!
!
access-list 10 deny 172.16.2.224 0.0.0.31
access-list 10 deny 172.16.3.32 0.0.0.31
access-list 10 deny 172.16.3.64 0.0.0.31
access-list 10 deny 172.16.3.96 0.0.0.15
access-list 10 deny 172.16.3.128 0.0.0.15
access-list 10 deny 172.16.2.128 0.0.0.31
access-list 10 deny 172.16.0.0 0.0.0.255
access-list 10 permit 172.16.3.0 0.0.0.31
access-list 10 permit 172.16.2.192 0.0.0.31
access-list 10 permit 172.16.3.32 0.0.0.31
access-list 10 permit 172.16.2.64 0.0.0.63
access-list 11 permit 172.16.2.160 0.0.0.31
access-list 11 deny 172.16.2.224 0.0.0.31
access-list 11 permit 172.16.3.32 0.0.0.31
```

```
access-list 11 deny 172.16.3.64 0.0.0.31
access-list 11 deny 172.16.3.96 0.0.0.15
access-list 11 deny 172.16.3.128 0.0.0.15
access-list 11 deny 172.16.2.128 0.0.0.31
access-list 11 deny 172.16.0.0 0.0.0.255
access-list 11 permit 172.16.2.64 0.0.0.63
access-list 11 permit 172.16.3.0 0.0.0.31
access-list 12 deny 172.16.2.160 0.0.0.31
access-list 12 deny 172.16.2.192 0.0.0.31
access-list 12 permit 172.16.3.32 0.0.0.31
access-list 12 deny 172.16.3.64 0.0.0.31
access-list 12 deny 172.16.3.96 0.0.0.15
access-list 12 deny 172.16.3.128 0.0.0.15
access-list 12 deny 172.16.2.128 0.0.0.31
access-list 12 deny 172.16.0.0 0.0.0.255
access-list 12 permit 172.16.2.64 0.0.0.63
access-list 12 permit 172.16.3.0 0.0.0.31
access-list 13 permit 172.16.2.160 0.0.0.31
access-list 13 permit 172.16.2.192 0.0.0.31
access-list 13 permit 172.16.2.224 0.0.0.31
access-list 13 permit 172.16.3.64 0.0.0.31
access-list 13 permit 172.16.3.96 0.0.0.15
access-list 13 permit 172.16.3.128 0.0.0.15
access-list 13 permit 172.16.2.128 0.0.0.31
access-list 13 permit 172.16.0.0 0.0.0.255
access-list 13 permit 172.16.2.64 0.0.0.63
access-list 13 permit 172.16.3.0 0.0.0.31
access-list 14 deny 172.16.2.160 0.0.0.31
access-list 14 deny 172.16.2.192 0.0.0.31
access-list 14 deny 172.16.2.224 0.0.0.31
access-list 14 permit 172.16.3.32 0.0.0.31
access-list 14 deny 172.16.3.96 0.0.0.15
access-list 14 deny 172.16.3.128 0.0.0.15
```

```
access-list 14 deny 172.16.2.128 0.0.0.31
access-list 14 deny 172.16.0.0 0.0.0.255
access-list 14 permit 172.16.2.64 0.0.0.63
access-list 14 permit 172.16.3.0 0.0.0.31
access-list 15 deny 172.16.2.160 0.0.0.31
access-list 15 deny 172.16.2.192 0.0.0.31
access-list 15 deny 172.16.2.224 0.0.0.31
access-list 15 permit 172.16.3.32 0.0.0.31
access-list 15 deny 172.16.3.64 0.0.0.31
access-list 15 deny 172.16.3.128 0.0.0.15
access-list 15 deny 172.16.2.128 0.0.0.31
access-list 15 deny 172.16.0.0 0.0.0.255
access-list 15 permit 172.16.2.64 0.0.0.63
access-list 15 permit 172.16.3.0 0.0.0.31
access-list 16 deny 172.16.2.160 0.0.0.31
access-list 16 deny 172.16.2.192 0.0.0.31
access-list 16 deny 172.16.2.224 0.0.0.31
access-list 16 permit 172.16.3.32 0.0.0.31
access-list 16 deny 172.16.3.64 0.0.0.31
access-list 16 deny 172.16.3.96 0.0.0.15
access-list 16 deny 172.16.2.128 0.0.0.31
access-list 16 deny 172.16.0.0 0.0.0.255
access-list 16 permit 172.16.2.64 0.0.0.63
access-list 16 permit 172.16.3.0 0.0.0.31
access-list 17 deny 172.16.2.160 0.0.0.31
access-list 17 deny 172.16.2.192 0.0.0.31
access-list 17 deny 172.16.2.224 0.0.0.31
access-list 17 permit 172.16.3.32 0.0.0.31
access-list 17 deny 172.16.3.64 0.0.0.31
access-list 17 deny 172.16.3.96 0.0.0.15
access-list 17 deny 172.16.3.128 0.0.0.15
access-list 17 deny 172.16.0.0 0.0.0.255
access-list 17 permit 172.16.2.64 0.0.0.63
```

```
access-list 17 permit 172.16.3.0 0.0.0.31
access-list 18 deny 172.16.2.160 0.0.0.31
access-list 18 deny 172.16.2.192 0.0.0.31
access-list 18 deny 172.16.2.224 0.0.0.31
access-list 18 permit 172.16.3.32 0.0.0.31
access-list 18 deny 172.16.3.64 0.0.0.31
access-list 18 deny 172.16.3.96 0.0.0.15
access-list 18 deny 172.16.3.128 0.0.0.15
access-list 18 deny 172.16.2.128 0.0.0.31
access-list 18 permit 172.16.2.64 0.0.0.63
access-list 18 permit 172.16.3.0 0.0.0.31
access-list 19 permit 172.16.2.160 0.0.0.31
access-list 19 permit 172.16.2.192 0.0.0.31
access-list 19 permit 172.16.2.224 0.0.0.31
access-list 19 permit 172.16.3.32 0.0.0.31
access-list 19 permit 172.16.3.64 0.0.0.31
access-list 19 permit 172.16.3.96 0.0.0.15
access-list 19 permit 172.16.3.128 0.0.0.15
access-list 19 permit 172.16.2.128 0.0.0.31
access-list 19 permit 172.16.0.0 0.0.0.255
access-list 19 permit 172.16.3.0 0.0.0.31
access-list 20 permit 172.16.2.160 0.0.0.31
access-list 20 permit 172.16.2.192 0.0.0.31
access-list 20 permit 172.16.2.224 0.0.0.31
access-list 20 permit 172.16.3.32 0.0.0.31
access-list 20 permit 172.16.3.64 0.0.0.31
access-list 20 permit 172.16.3.96 0.0.0.15
access-list 20 permit 172.16.3.128 0.0.0.15
access-list 20 permit 172.16.2.128 0.0.0.31
access-list 20 permit 172.16.0.0 0.0.0.255
access-list 20 permit 172.16.2.64 0.0.0.63
!
banner motd ^C ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO ^C
```

line con 0
password 7 081760783E312A332D383B5478
login
!
line aux 0
!
line vty 0 4
exec-timeout 3 0
password 7 081760783E312A332D383B547A79
login
transport input ssh
!
end

BLOQUE 1

BLOQUE_1#show running-config
Building configuration...

Current configuration : 2559 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname BLOQUE_1
!
enable secret 5 1mERr$6DXK9lYZE4AWJRqkez0ox0
!
ip ssh version 2
ip ssh authentication-retries 2

```
ip ssh time-out 30
no ip domain-lookup
ip domain-name gadmu.local
!
username root privilege 1 password 7 081760783E312A332D383F2C
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
!
interface FastEthernet0/5
switchport access vlan 15
switchport mode access
mac-address-table static 000D.BD5E.7861 interface FastEthernet0/5 vlan 15
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
switchport access vlan 14
switchport mode access
```

```
mac-address-table static 00E0.F9DB.3246 interface FastEthernet0/7 vlan 14
!
interface FastEthernet0/8
switchport access vlan 14
switchport mode access
mac-address-table static 0090.2B90.0C76 interface FastEthernet0/8 vlan 14
!
interface FastEthernet0/9
switchport access vlan 14
switchport mode access
mac-address-table static 0006.2A40.C462 interface FastEthernet0/9 vlan 14
!
interface FastEthernet0/10
switchport access vlan 14
switchport mode access
mac-address-table static 000A.41D2.8D65 interface FastEthernet0/10 vlan 14
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
```

```
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
description ADMIN
ip address 172.16.3.147 255.255.255.240
```

```
!
banner motd ^C ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO ^C
!
!
!
line con 0
password 7 081760783E312A332D2920547B
login
!
line vty 0 4
exec-timeout 3 0
password 7 081760783E312A332D3D383D
login local
transport input ssh
line vty 5 15
login
!
!
end
```

BLOQUE 1_P1

```
BLOQUE_1_P1#show running-config
Building configuration...

Current configuration : 2342 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
```

```
hostname BLOQUE_1_P1
!
enable secret 5 $1$mERr$6DXK9lYZE4AWJRqkez0ox0
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 30
no ip domain-lookup
ip domain-name gadmu.local
!
username root privilege 1 password 7 081760783E312A332D383F2C
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
mac-address-table static 0001.64CE.9540 interface FastEthernet0/3 vlan 10
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
```

```
mac-address-table static 0060.5C48.60EB interface FastEthernet0/4 vlan 10
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
mac-address-table static 0001.C93D.385E interface FastEthernet0/5 vlan 10
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
mac-address-table static 0001.4208.4C0C interface FastEthernet0/6 vlan 10
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
mac-address-table static 0001.6473.08B6 interface FastEthernet0/7 vlan 10
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
```

```
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
```

```
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
no ip address
!
banner motd ^C ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO ^C
!
!
!
line con 0
password 7 081760783E312A332D2920547B
login
!
line vty 0 4
exec-timeout 3 0
password 7 081760783E312A332D3D383D
login local
transport input ssh
line vty 5 15
login
!
!
end
```

BLOQUE 2

```
BLOQUE_2#show running-config
Building configuration...
```

```
Current configuration : 3333 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname BLOQUE_2
!
enable secret 5 $1$mERr$tHbhoE3w5eZDLemJcpZ1W0
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 30
no ip domain-lookup
ip domain-name gadmu.local
!
username root privilege 1 password 7 081760783E312A332D383F2C
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport mode trunk
!
```

```
interface FastEthernet0/3
switchport access vlan 13
switchport mode access
mac-address-table static 0002.4A9D.49C0 interface FastEthernet0/3 vlan 13
!
interface FastEthernet0/4
switchport access vlan 13
switchport mode access
mac-address-table static  0030.A3A2.26CC interface FastEthernet0/4 vlan 13
!
interface FastEthernet0/5
switchport access vlan 13
switchport mode access
mac-address-table static  00D0.FF21.413B interface FastEthernet0/5 vlan 13
!
interface FastEthernet0/6
switchport access vlan 13
switchport mode access
mac-address-table static 0060.3E0C.2D84 interface FastEthernet0/6 vlan 13
!
interface FastEthernet0/7
switchport access vlan 13
switchport mode access
mac-address-table static 00D0.BAED.6098 interface FastEthernet0/7 vlan 13
!
interface FastEthernet0/8
switchport access vlan 13
switchport mode access
mac-address-table static 0060.3EA2.008A interface FastEthernet0/8 vlan 13
!
interface FastEthernet0/9
switchport access vlan 13
switchport mode access
```

```
mac-address-table static 0003.E4C6.8D94 interface FastEthernet0/9 vlan 13
!
interface FastEthernet0/10
switchport access vlan 11
switchport mode access
mac-address-table static 00E0.F73E.97AE interface FastEthernet0/10 vlan 11
!
interface FastEthernet0/11
switchport access vlan 11
switchport mode access
mac-address-table static 000B.BE58.8E58 interface FastEthernet0/11 vlan 11
!
interface FastEthernet0/12
switchport access vlan 11
switchport mode access
mac-address-table static 0030.A3BE.287E interface FastEthernet0/12 vlan 11
!
interface FastEthernet0/13
switchport access vlan 11
switchport mode access
mac-address-table static 0003.E4E1.8E8B interface FastEthernet0/13 vlan 11
!
interface FastEthernet0/14
switchport access vlan 18
switchport mode access
mac-address-table static 0004.9A4D.858E interface FastEthernet0/14 vlan 11
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
```

```
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO ^C
!
!
!
line con 0
```

password 7 081760783E312A332D29205478
login
!
line vty 0 4
exec-timeout 3 0
password 7 081760783E312A332D3D383D
login
transport input ssh
line vty 5 15
login
!
!
end

BLOQUE 3

BLOQUE_3#show running-config
Building configuration...

Current configuration : 2205 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname BLOQUE_3
!
enable secret 5 1mERr$kErOssh2U5.pkMhqlTSeg0
!
!
!
ip ssh version 2

```
ip ssh authentication-retries 2
ip ssh time-out 30
no ip domain-lookup
ip domain-name gadmu.local
!
username root privilege 1 password 7 081760783E312A332D383F2C
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 12
switchport mode access
mac-address-table static 000B.BE86.3194 interface FastEthernet0/3 vlan 12
!
interface FastEthernet0/4
switchport access vlan 12
switchport mode access
mac-address-table static 0090.2114.EB6C interface FastEthernet0/4 vlan 12
!
interface FastEthernet0/5
switchport access vlan 12
switchport mode access
mac-address-table static 0001.433A.E019 interface FastEthernet0/5 vlan 12
!
```

```
interface FastEthernet0/6
switchport access vlan 12
switchport mode access
mac-address-table static 00D0.FF34.3BC7 interface FastEthernet0/6 vlan 12
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
```

```
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO ^C
!
!
```

```
!
line con 0
password 7 081760783E312A332D29205479
login
!
line vty 0 4
exec-timeout 3 0
password 7 081760783E312A332D3D383D
login
transport input ssh
line vty 5 15
login
!
!
end
```

BLOQUE EXTERIORES

```
BLOQUE_EX#show running-config
Building configuration...

Current configuration : 2071 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname BLOQUE_EX
!
enable secret 5 $1$mERr$rXtgZbRkQKvAlJOmdArmy/
!
```

```
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 30
no ip domain-lookup
ip domain-name gadmu.local
!
username root privilege 1 password 7 081760783E312A332D383F2C
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 17
switchport mode access
mac-address-table static 000B.BE53.DAC7 interface FastEthernet0/3 vlan 17
!
interface FastEthernet0/4
switchport access vlan 17
switchport mode access
mac-address-table static 0003.E439.E268 interface FastEthernet0/4 vlan 17
!
interface FastEthernet0/5
switchport access vlan 17
```

```
switchport mode access
mac-address-table static 0002.4A0C.E726 interface FastEthernet0/5 vlan 17
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
```

```
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
```

```
shutdown
!
banner motd ^C ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO ^C
!
!
!
line con 0
password 7 081760783E312A332D29202112
login
!
line vty 0 4
exec-timeout 3 0
password 7 081760783E312A332D3D383D
login
transport input ssh
line vty 5 15
login
!
!
end
```

ANEXO H

INSTALACIÓN DE CENTOS 6.3 (MODO TEXTO)

Para la instalación del sistema operativo Centos, se va a realizar en una máquina virtual VM VirtualBox 4.3.6.

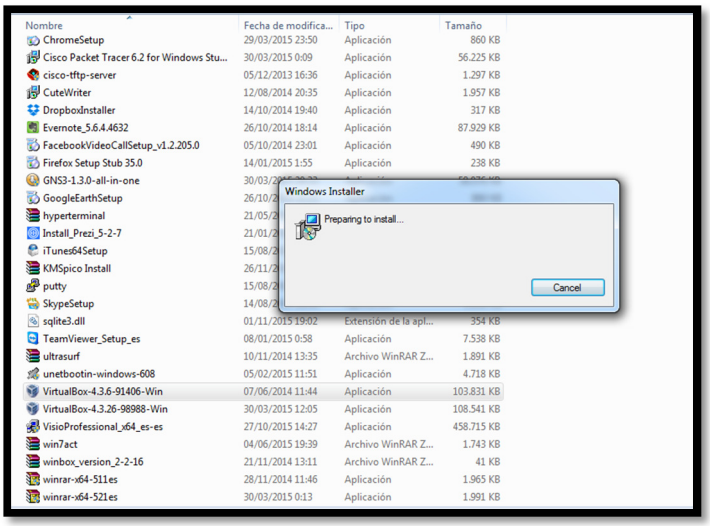

Figura 51. Búsqueda de archivo

Referencia: Elaboración propia

Al iniciar el proceso aparece la pantalla de bienvenida de instalación y se da clic en siguiente

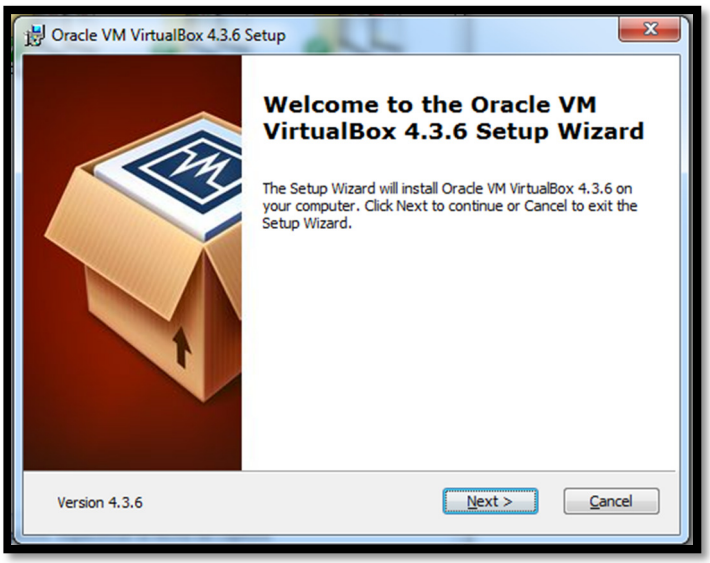

Figura 52.Pantalla de Bienvenida de VM VirtualBox 4.3.6

Referencia: Elaboración propia

En la siguiente figura se instalará algunas aplicaciones para la máquina virtual.

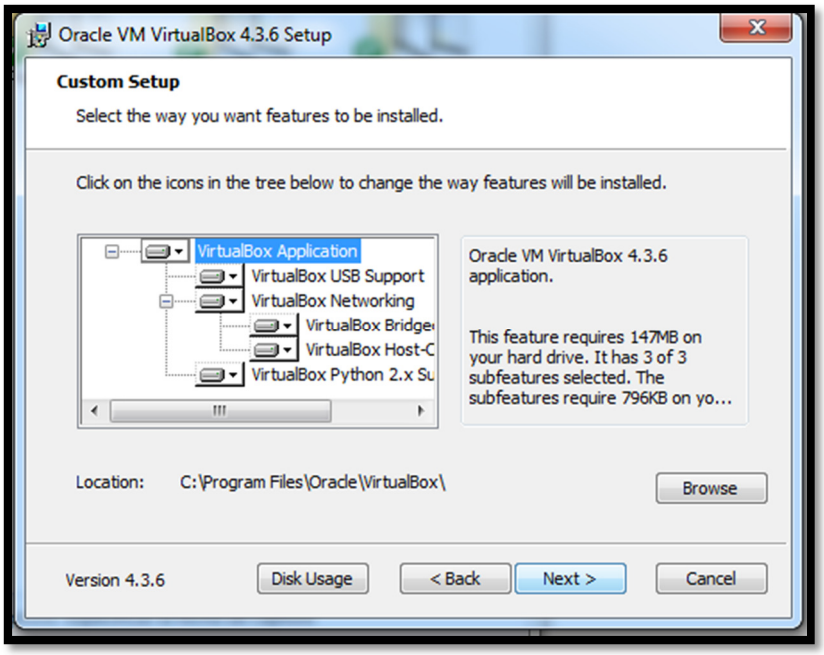

Figura 53. Aplicaciones en VirtualBox

Referencia: Elaboración propia

En la siguiente pantalla se crean los accesos directos para este software.

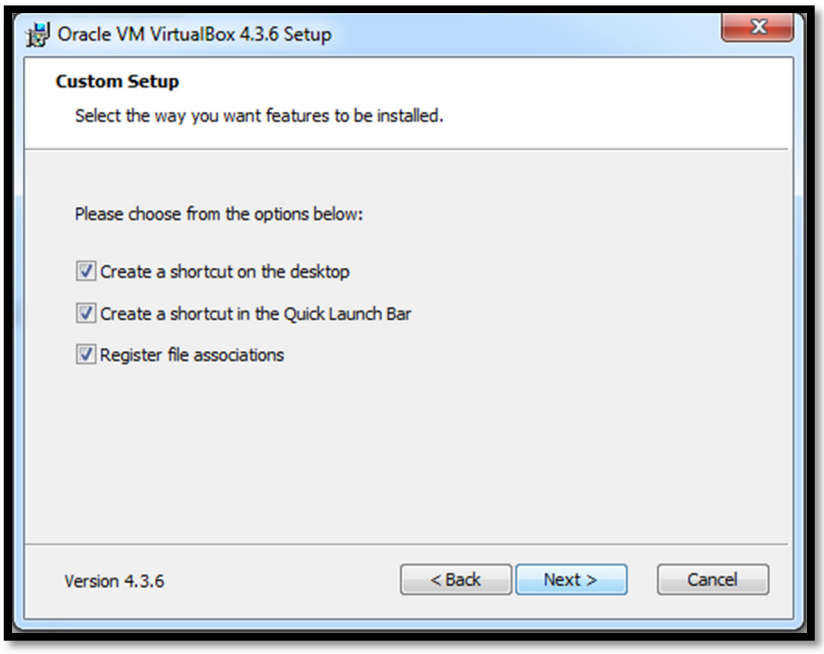

Figura 54. Selección de accesos directos

Referencia: Elaboración propia

En la siguiente pantalla se muestra la instalación de las interfaces de red.

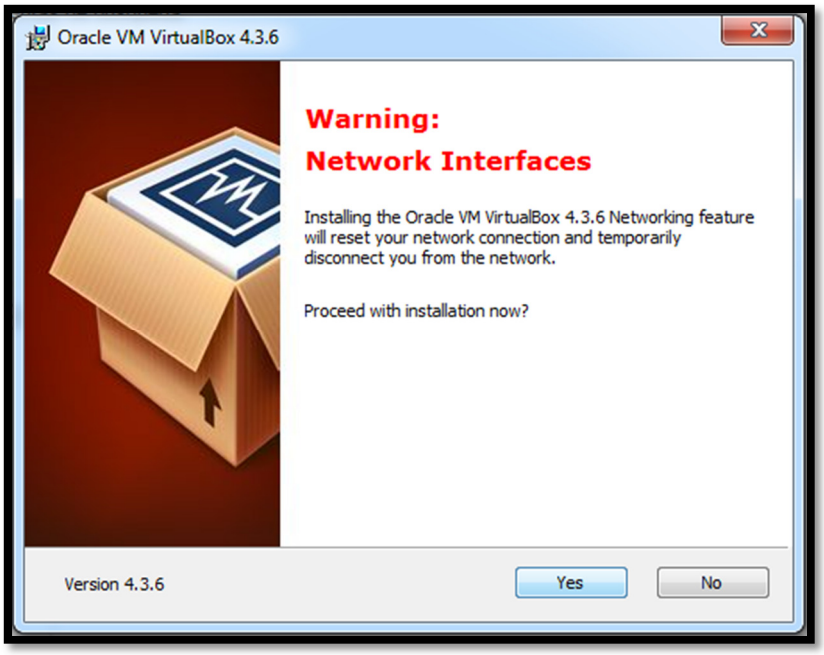

Figura 55. Instalación de interfaces de red

Referencia: Elaboración propia

Una vez configurada la máquina virtual, se espera que termine la máquina virtual.

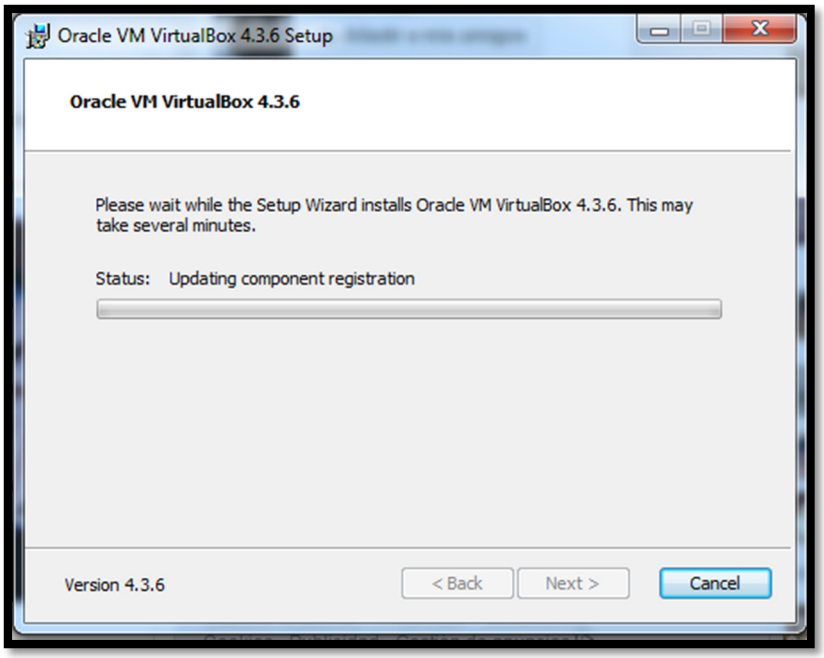

Figura 56. Proceso de Instalación

Referencia: Elaboración propia

Para finalizar, se selecciona el check si se desea correr el programa.

Figura 57. Pantalla de finalización de Instalación

Referencia: Elaboración propia

Una vez Instalado el software, se procede a realizar las configuraciones de la máquina virtual.

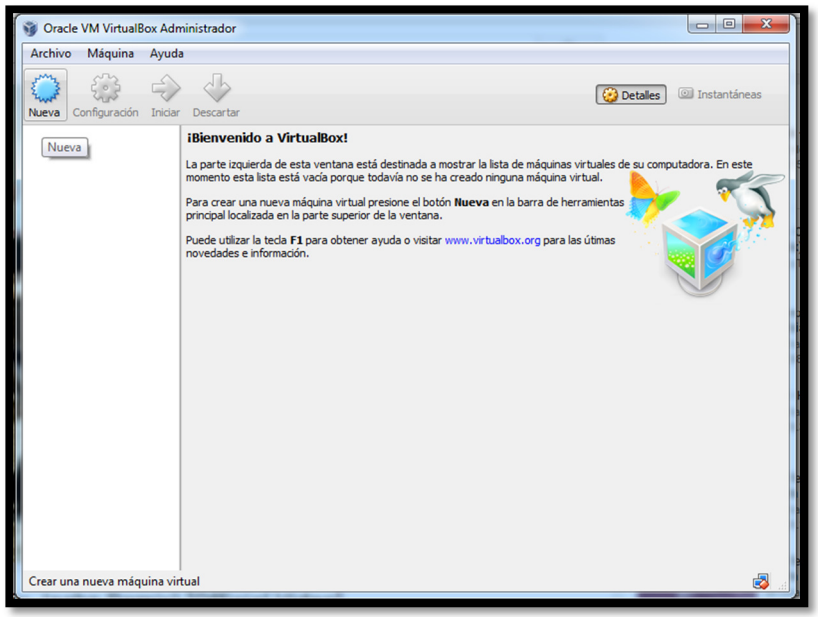

Figura 58. Configuraciones de pantalla principal

Referencia: Elaboración propia

Se selecciona, el nombre de la máquina virtual, el tipo de sistema operativo y la versión.

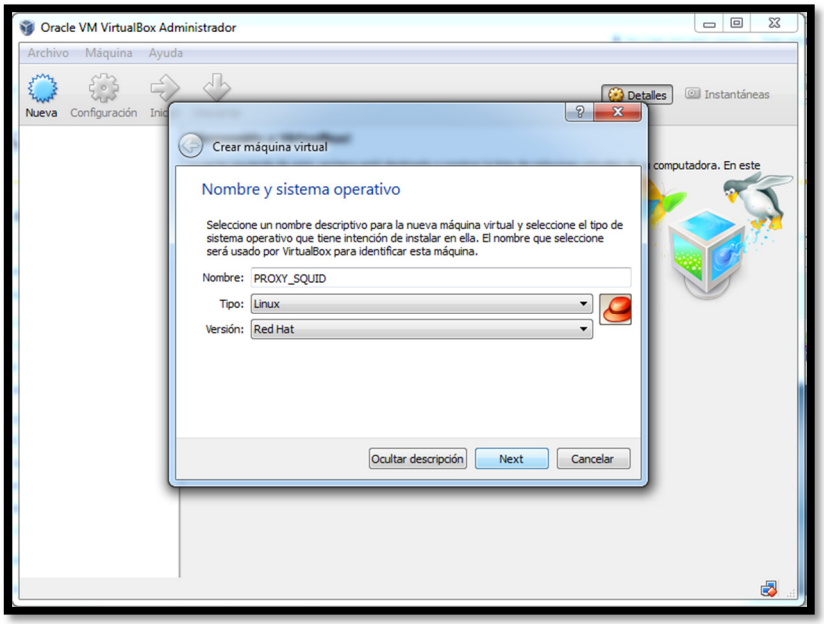

Figura 59. Ubicación de nombre de máquina virtual

Referencia: Elaboración propia

Se determina el tamaño de memoria, que tendrá el sistema operativo.

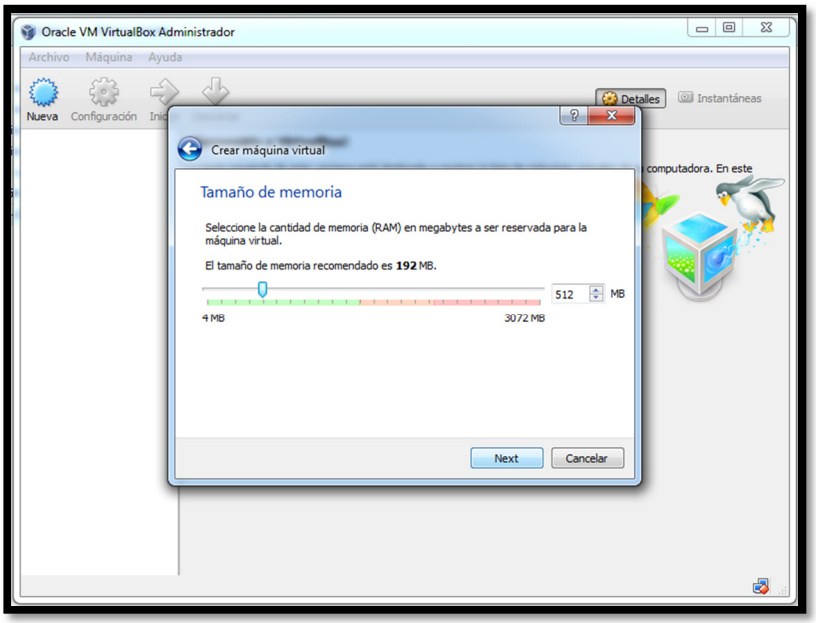

Figura 60. Tamaño de memoria

Referencia: Elaboración propia

Una vez determinado el espacio de memoria, se determina si se agregará un nuevo disco duro vacío.

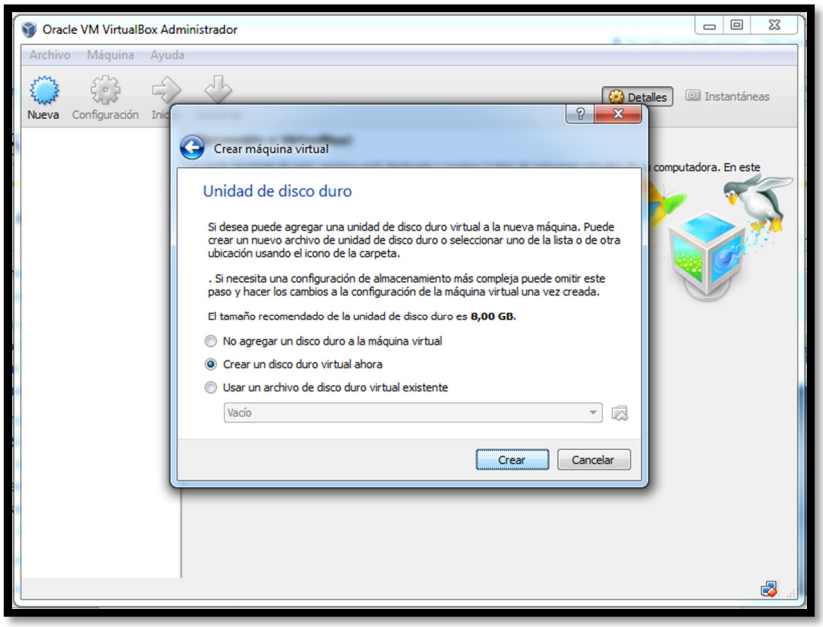

Figura 61. Espacio de memoria

Referencia: Elaboración propia

Luego se elige el tipo de archivo de unidad de disco duro.

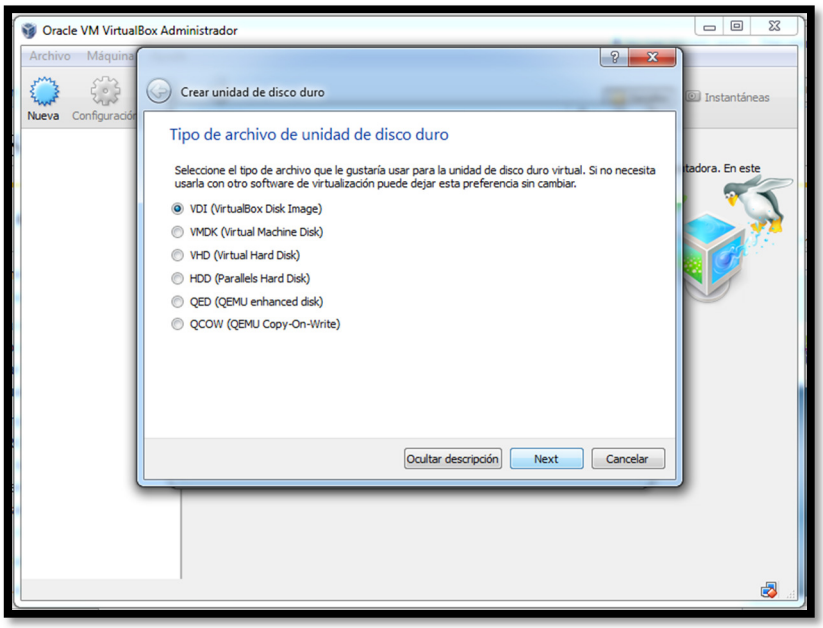

Figura 62. Selección de archivo de disco duro

Referencia: Elaboración propia

Además de estas configuraciones, es importante determinar el tipo de almacenamiento en la unidad de disco duro que tendrá el sistema operativo.

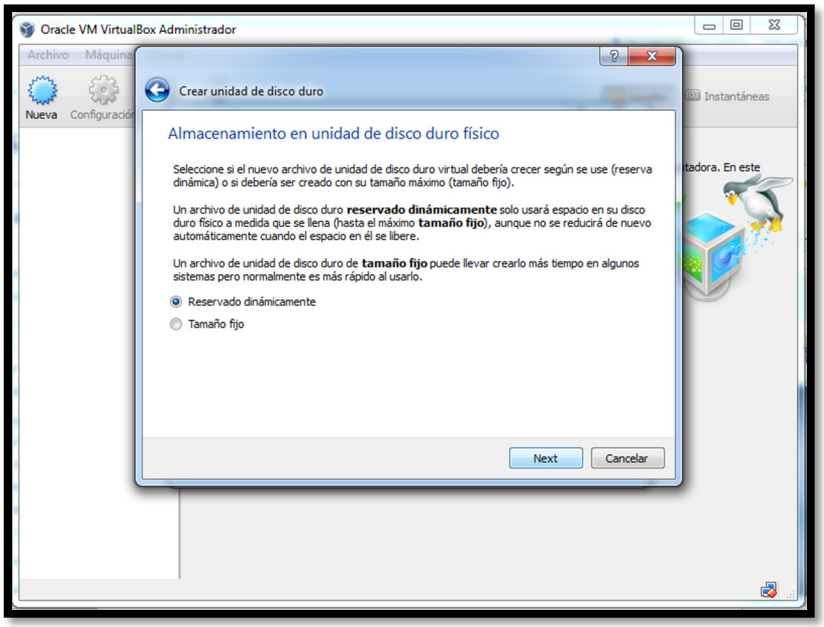

Figura 63. Configuraciones básicas

Referencia: Elaboración propia

Luego se selecciona la ubicación del archivo y tamaño.

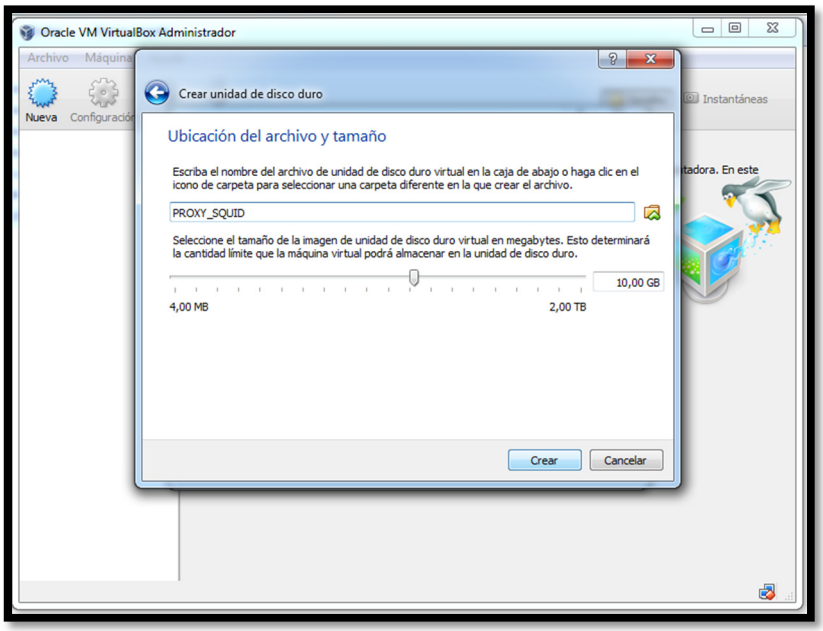

Figura 64. Ubicación de archivo y tamaño

Referencia: Elaboración propia

Una vez terminadas todas las configuraciones, en la siguiente pantalla, se muestran las configuraciones.

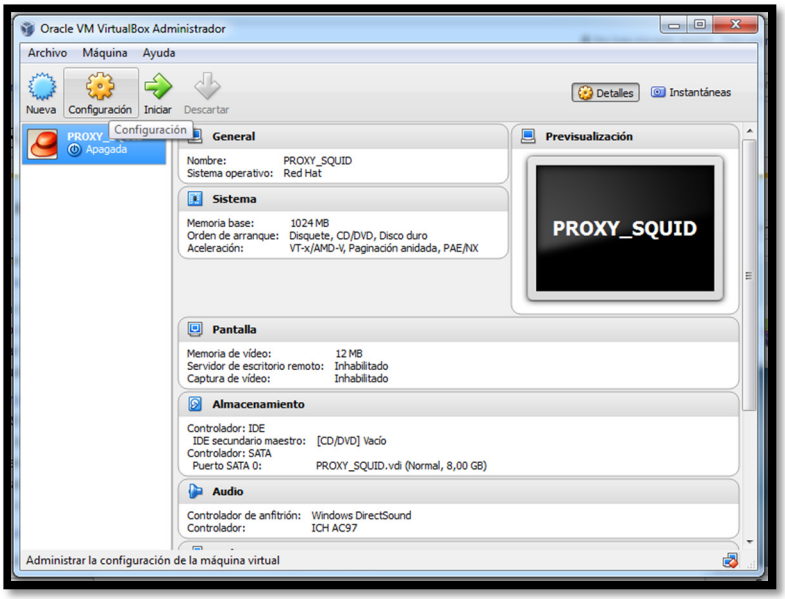

Figura 65. Configuraciones básicas de VM VirtualBox

Referencia: Elaboración propia

Si falto algún tipo de configuración, en esta pantalla se puede visualizar e ir modificando cada ítem mostrado.

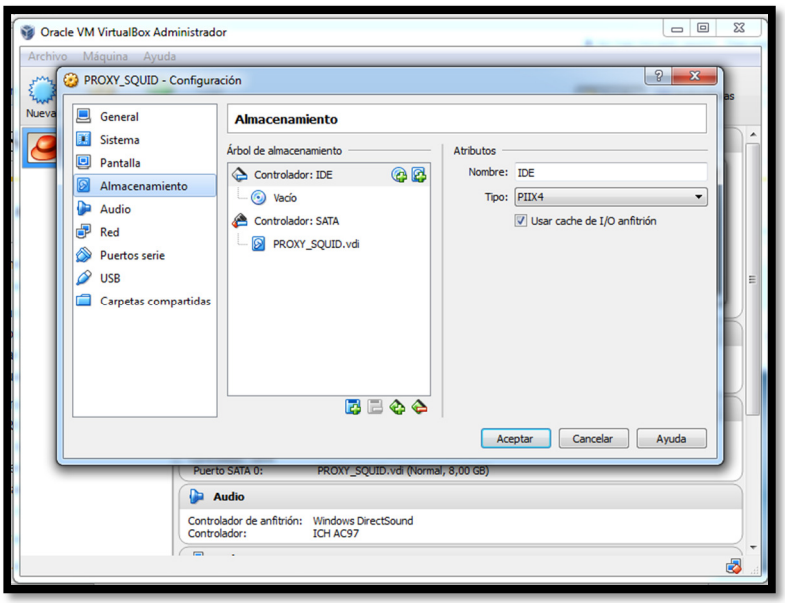

Figura 66. Configuraciones básicas de VM VirtualBox

Referencia: Elaboración propia

Una vez, realizadas todas las configuraciones, se selecciona el sistema operativo.

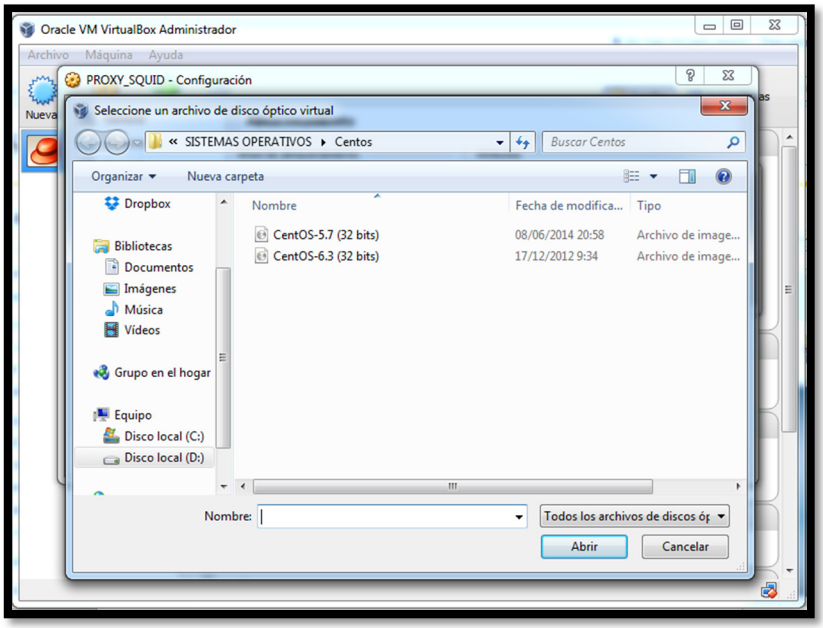

Figura 67. Selección del sistema operativo

Referencia: Elaboración propia

Al correr el sistema operativo Centos, de da clic en instalar.

Figura 68. Pantalla de bienvenida de instalación Centos

Referencia: Elaboración propia

En al siguiente pantalla se elige si se desea instalar o realizar un test de verificación.

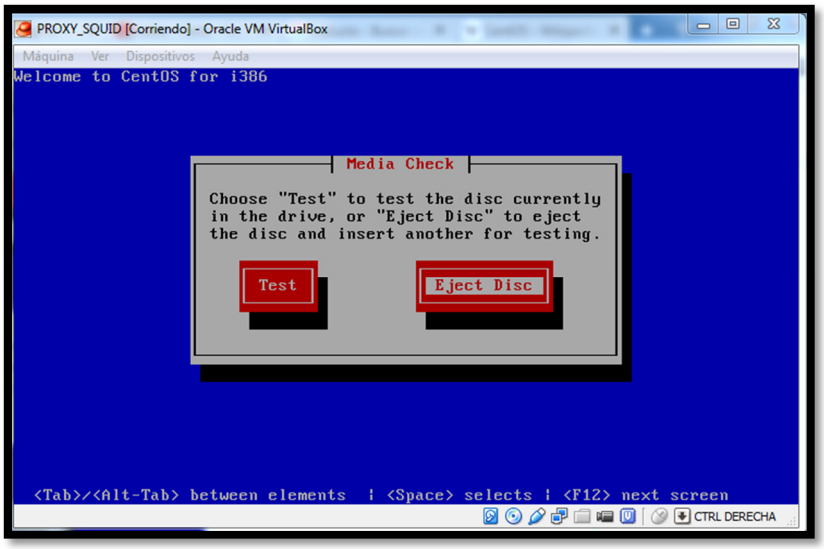

Figura 69. Bienvenida de Centos

Referencia: Elaboración propia

Luego se elige se está seguro si desea continuar y damos clic en OK.

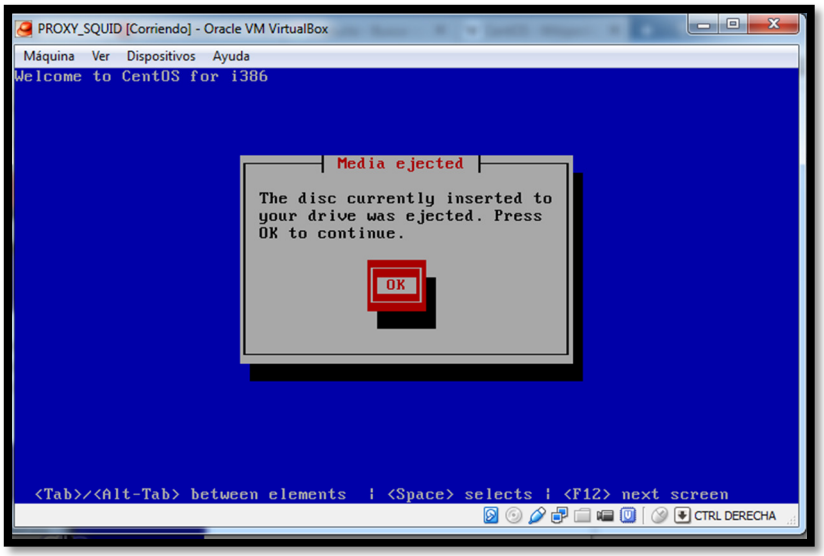

Figura 70. Pantalla de verificación de instalación

Referencia: Elaboración propia

En al siguiente pantalla se selecciona el tipo de teclado, idioma.

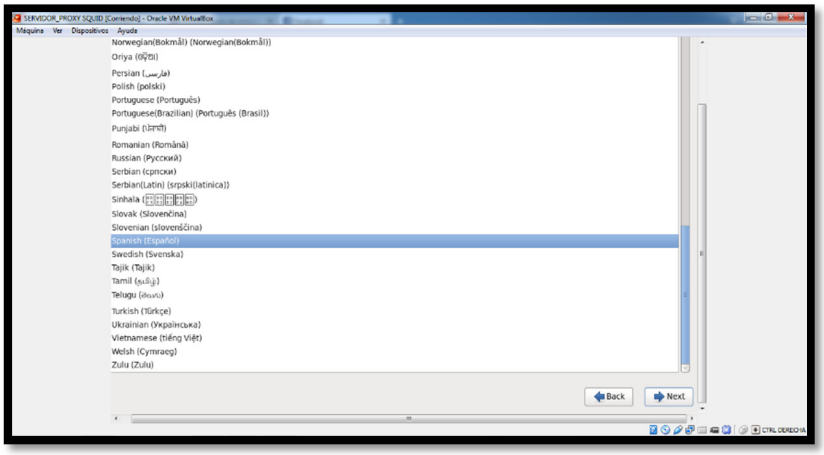

Figura 71. Selección de Teclado

Referencia: Elaboración propia

Se proporciona el tipo de nombre de la máquina virtual.

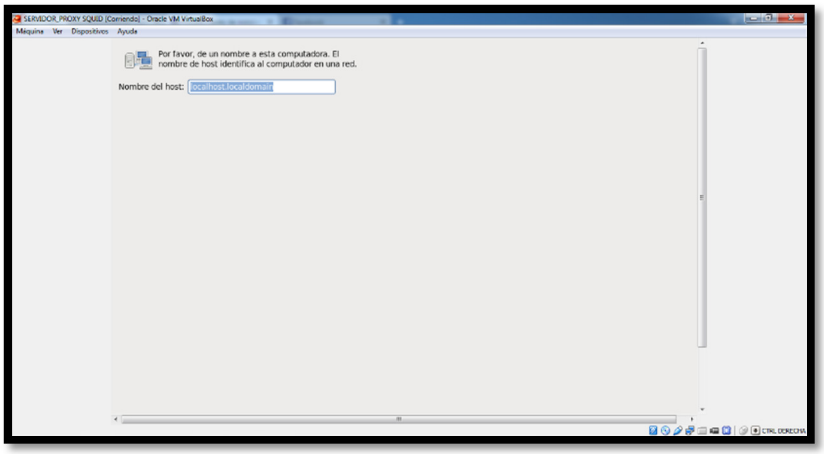

Figura 72. Nombre del Sistema Operativo

Referencia: Elaboración propia

Se selecciona la ubicación.

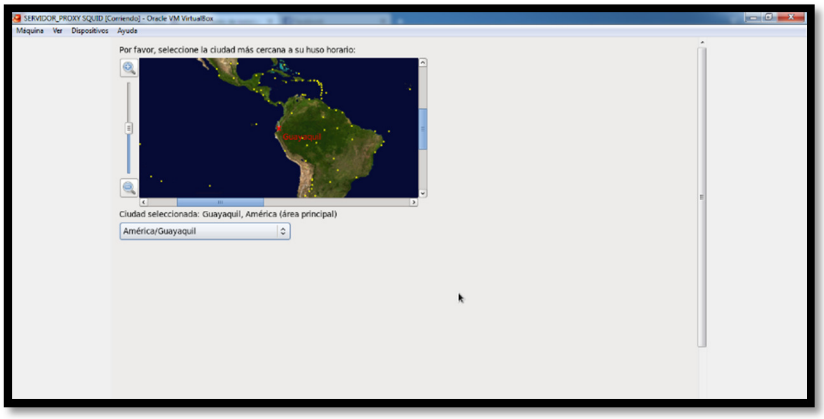

Figura 73. Selección del país

Referencia: Elaboración propia

Y la instalación de máquina virtual y sistema operativo se finaliza correctamente.

ANEXO I

ELABORACIÓN DEL SERVIDOR FTP

Comenzamos con la instalación de CENTOS 6.3 (32 bits), en el ANEXO C "Instalación de CENTOS 6.3" se especifica los pasos a seguir en la instalación.

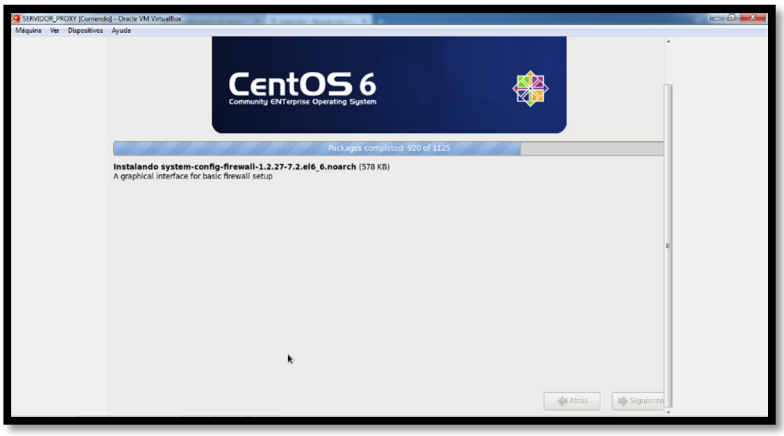

Figura 74. Plataforma Centos 6.3
Referencia: Elaboración propia

Instalamos el paquete vsftpd para la configuración de nuestro servidor FTP, con el siguiente comando yum install vsftpd.

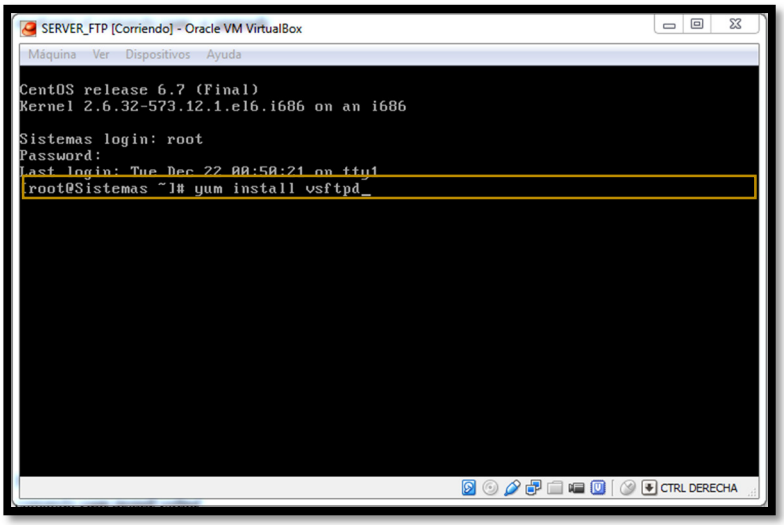

Figura 75. Comando de instalación de paquete vsftpd
Referencia: Elaboración propia

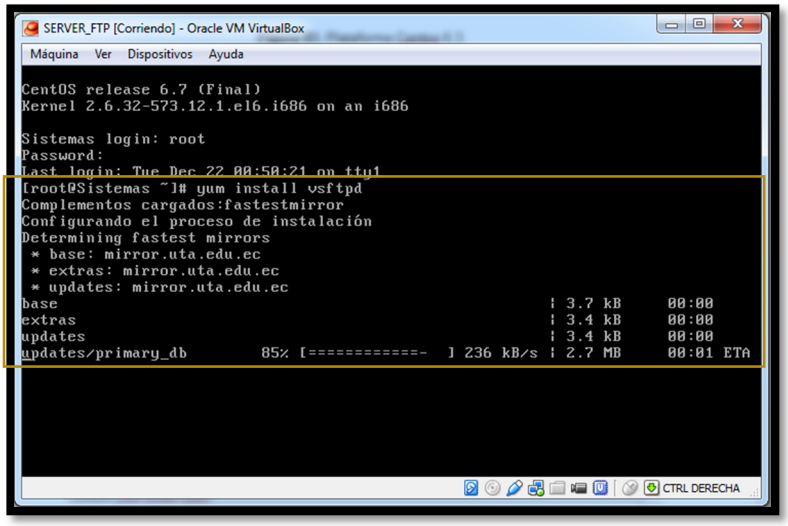

Figura 76. Instalación de paquetes vsftpd

Referencia: Elaboración propia

Ahora editamos la dirección IP del host escribiendo en el terminal el siguiente comando: gedit /etc/host, con ello aparecerá el siguiente script de configuración:

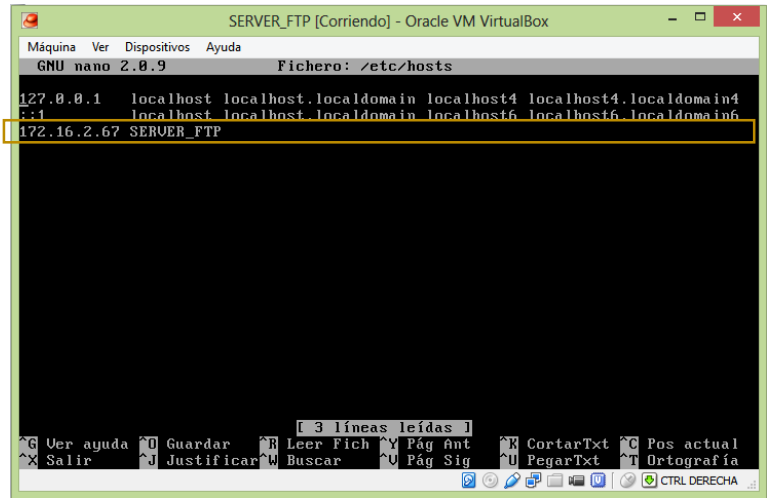

Figura 77. Modificación del fichero hosts

Referencia: Elaboración propia

En este script se escribirá la dirección 172.16.2.68 la misma que estará vinculada a SERVER_FTP.servidorftp.com SERVER_FTP, que es el dominio y nombre del host. Guardamos y Cerramos.

Ahora se configurará la dirección IP, mascara de red y Gateway, para lo cual se escribe en el terminal el siguiente comando: gedit /etc/sysconfig/network-scripts/ifcfg-eth0.

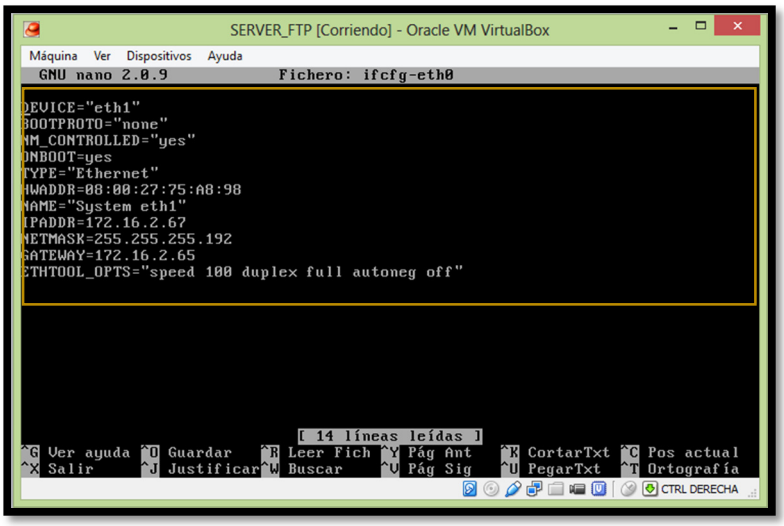

Figura 78. Modificación del fichero network
Referencia: Elaboración propia

Luego de ejecutar el comando antes mencionado, saldrá el siguiente script para editar:

- Dirección IP = 172.16.2.67
- Mascara de red = 255.255.255.192
- Gateway = 172.16.2.65

Una vez añadidos estos parámetros, guardamos y cerramos.

Ahora se procede a la configuración del fichero resolv.conf para configurar la dirección IP del servidor FTP, tras escribir el siguiente comando en el terminal: gedit /etc/resolv.conf.

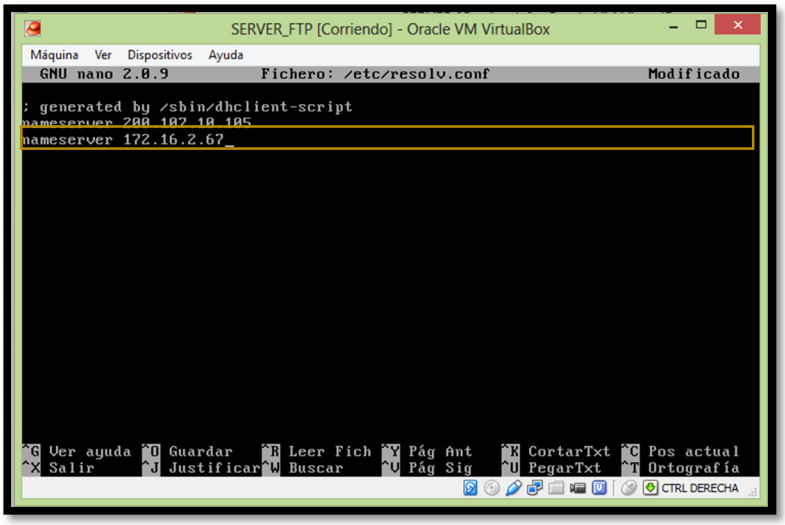

Figura 79. Modificación del fichero resolv
Referencia: Elaboración propia

En el siguiente script se procede a la configuración de la dirección IP del servidor FTP, luego se Guarda y Cerrar.

Se configurará el fichero vsftpd.conf, tras escribir el siguiente comando en el terminal: gedit /etc/vsftpd/vsftp.conf, nos aparecerá el siguiente script en el que configuraremos ciertos parámetros recomendados:

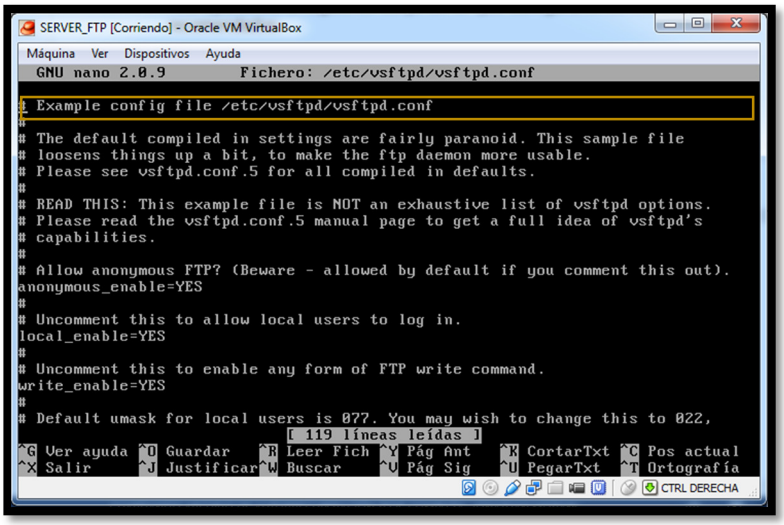

Figura 80. Modificación del fichero vsftpd
Referencia: Elaboración propia

Los parámetros que se configurarán en el script del fichero vsftpd.conf se los realiza bajo las siguientes características que se presentan a continuación:

Tabla 51. *Parámetros a cumplirse*

COMANDOS	CARACTERÍSTICAS
anonymous_enable=YES	Habilita el acceso anónimo al servidor FTP.
local_enable=YES	Habilita los accesos autenticados de los usuarios locales en FTP.
write_enable=YES	Habilita la escritura en el servidor FTP.
chroot_list_enable=YES	Habilita el acceso de invitado para ciertos usuarios de FTP.
chroot_list_file=/etc/vsftpd/chroot_list	Indica la ruta en la cual se encuentra el fichero con los nombres de los usuarios que serán limitados a trabajar en su propia carpeta de trabajo.
Local_umask=022	Indica que los archivos subidos al servidor quedaran con los permisos 022, es decir solo escritura para el grupo y los demás.

Referencia: Elaboración propia

Configuración del script vsftpd.conf con los parámetros descritos anteriormente. Guardar y Cerrar. Ahora se inicializa el servicio de FTP, bajo el siguiente comando: service vsftpd start.

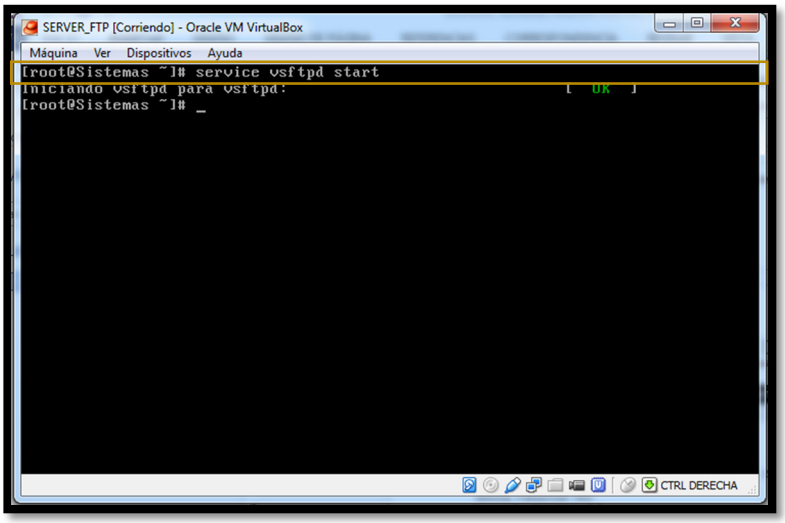

Figura 81. Inicio del archivo vsftpd

Referencia: Elaboración propia

CREACIÓN DE FICHEROS

Para la creación de ficheros, editamos los siguientes comandos en el terminal del sistema.

- mkdir /var/ftp/archivosfinanciero
- cd /var/ftp/archivosfinanciero/
- touch financiero
- ls

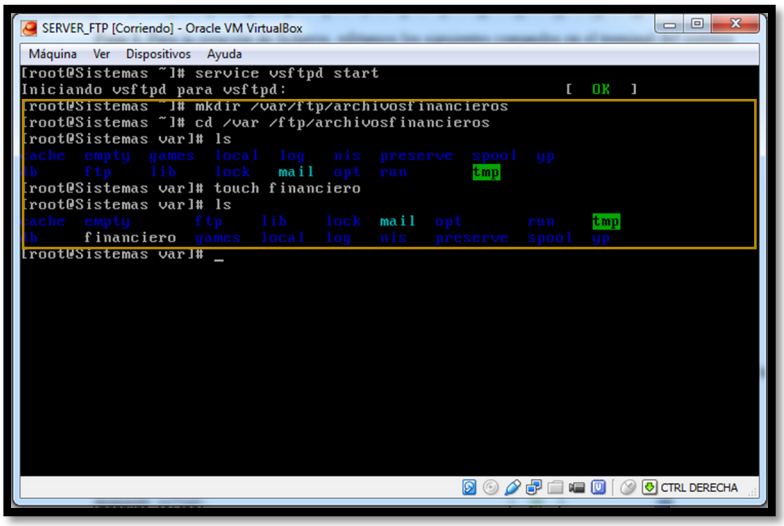

Figura 82. Creación de archivos

Referencia: Elaboración propia

Una vez creado el fichero, se procede a inicializar el servidor FTP con el siguiente comando: /etc/init.d/vsftpd restart.

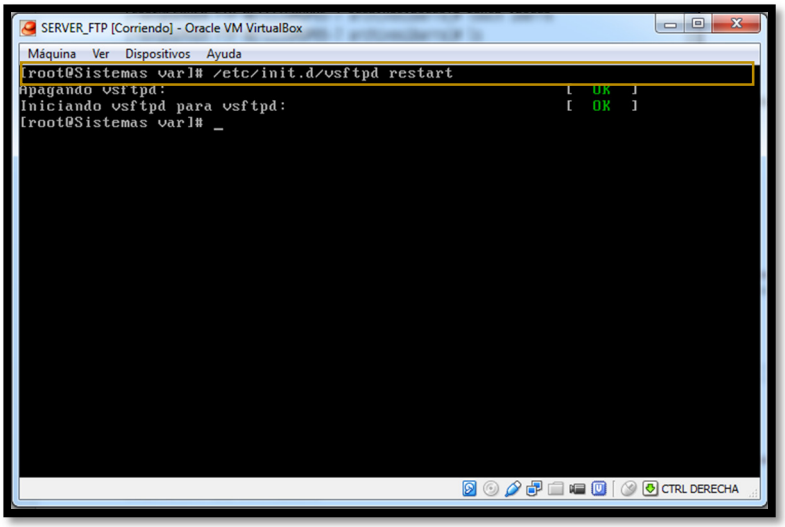

Figura 83. Reinicio del fichero vsftpd

Referencia: Elaboración propia

CREACIÓN DE USUARIOS

La creación de usuarios se guardara en el fichero vsftpd

- useradd mario
- passwd sistemas

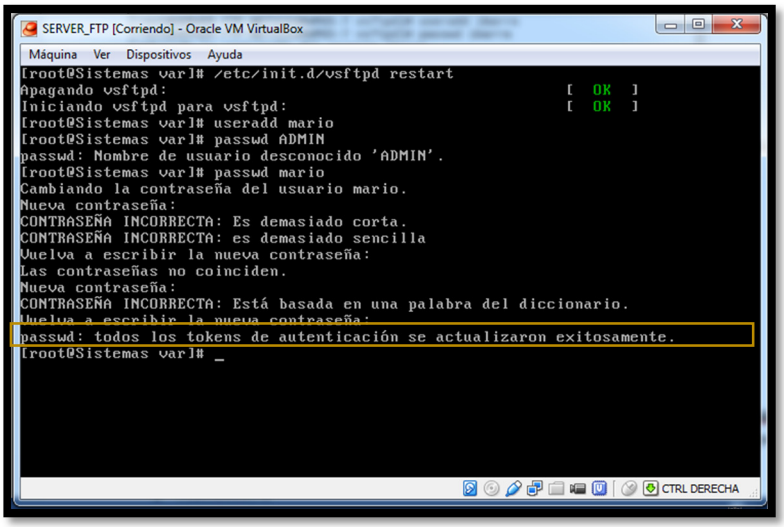

Figura 84. Creación de usuarios

Referencia: Elaboración propia

ANEXO J

ELABORACIÓN DEL SERVIDOR PROXY EN EL GADMU

Instalación de Centos 6.3 en modo texto, se debe ingresar en modo privilegiado para realizar las configuraciones necesarias.

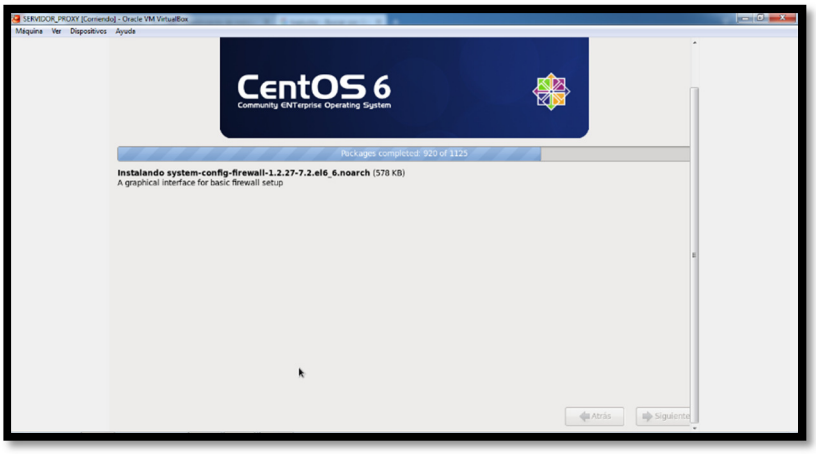

Figura 85. Plataforma Centos 6.3

Referencia: Elaboración propia

Mediante el comando yum install update, se logran actualizar paquetes complementarios.

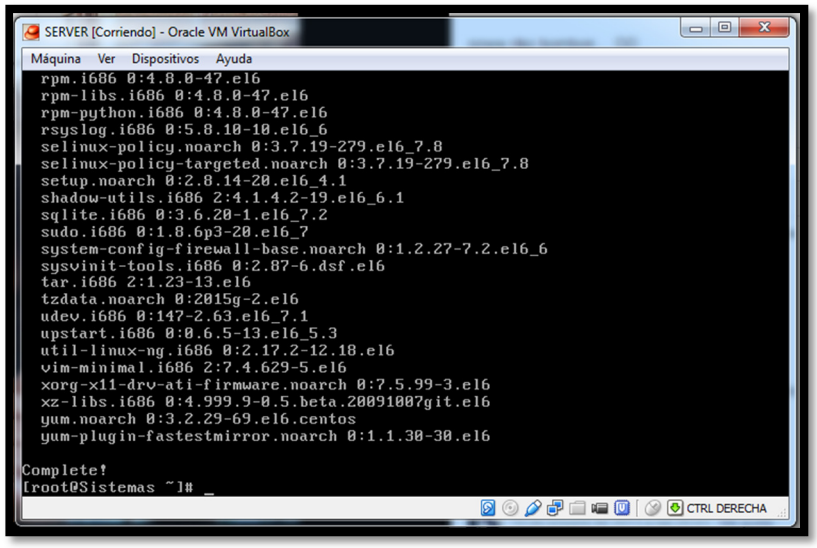

Figura 86. Instalación completa de las actualizaciones.

Referencia: Elaboración propia

Aplicación del paquete squid mediante el comando: yum install squid.

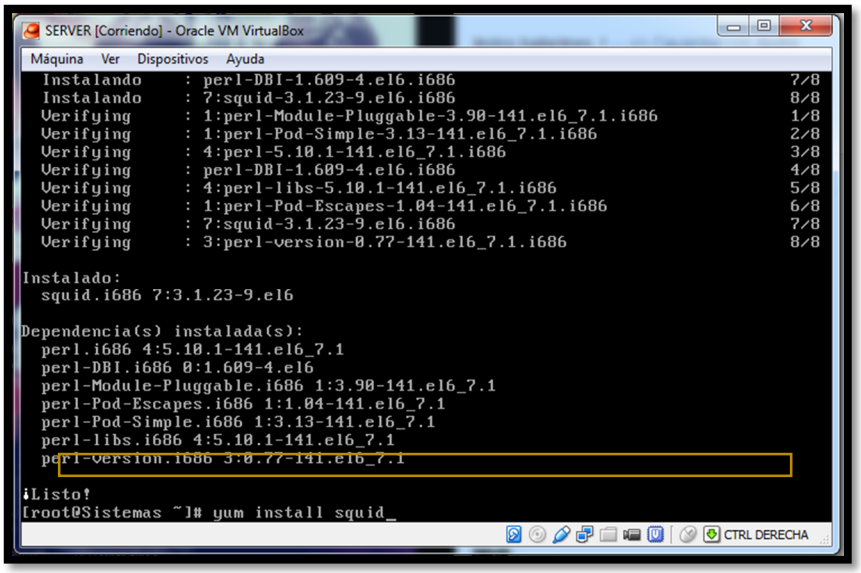

Figura 87. Comando para instalar paquete squid

Referencia: Elaboración propia

Instalación del paquete squid en centos 6.3.

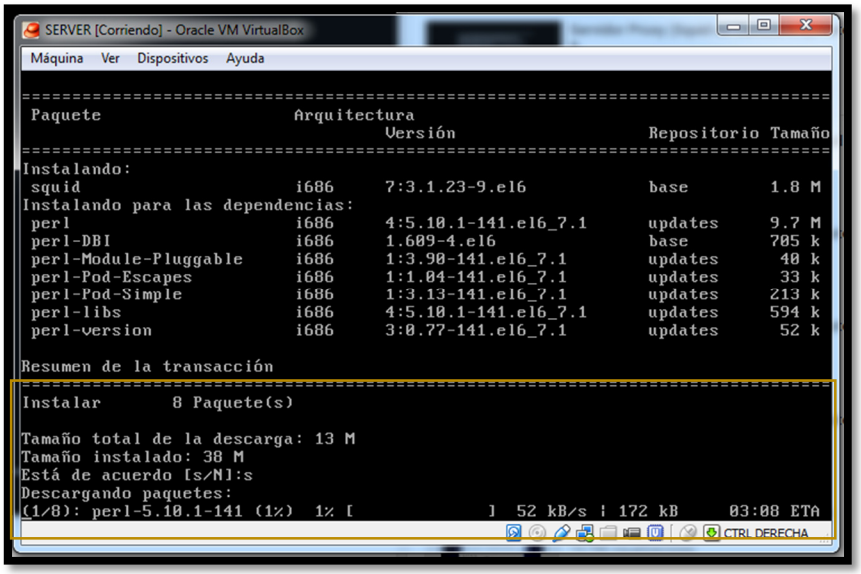

Figura 88. Instalación del paquete squid

Referencia: Elaboración propia

Ingresar al fichero instalado mediante el comando: nano etc/squid/squid.conf.

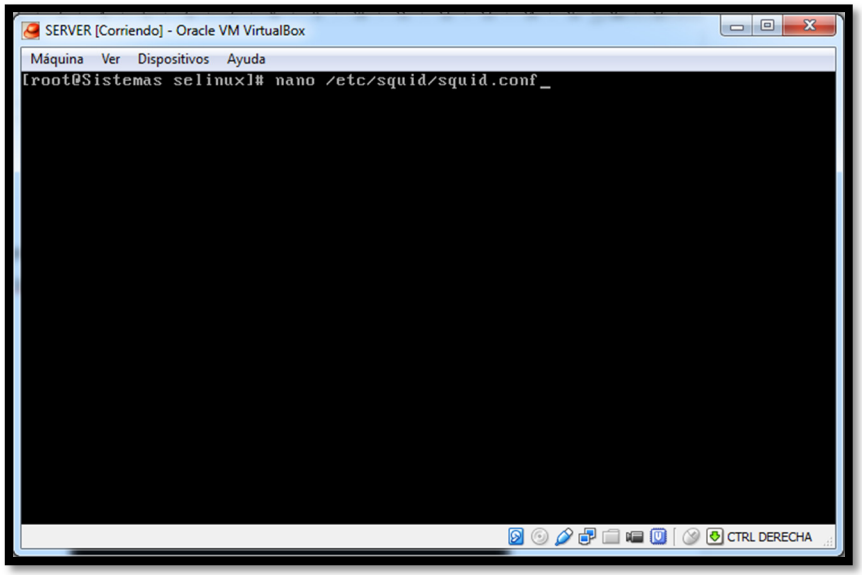

Figura 89. Ingreso al fichero squid

Referencia: Elaboración propia

En el cual agregaremos las siguientes líneas de control:

- acl blocksites dstdomain “/etc/squid/blocksites.squid”
- acl blockkeywords url_regex –i “/etc/squid/blockkeywords.squid”
- acl blockip src “/etc/squid/blockip.squid”

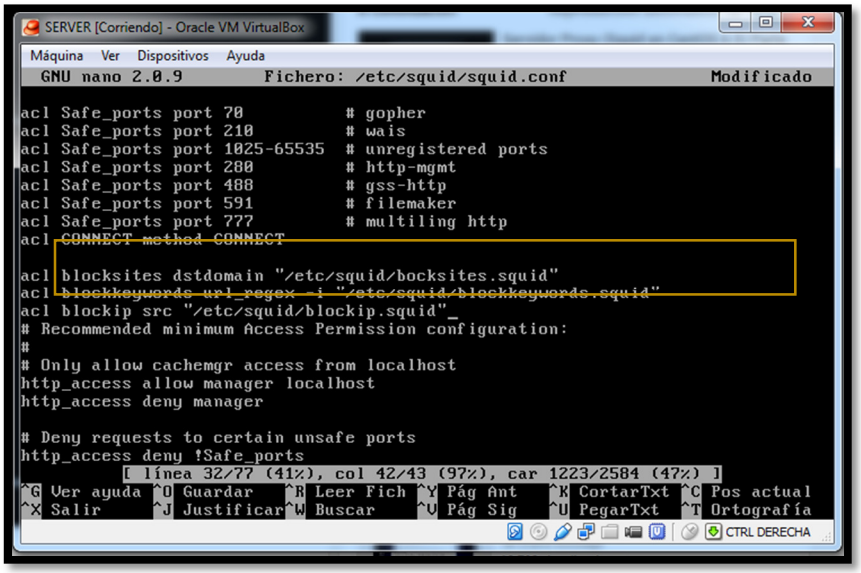

Figura 90. Modificación del fichero squid

Referencia: Elaboración propia

Con las siguientes líneas se deniega el acceso a páginas mediante los ficheros anteriores.

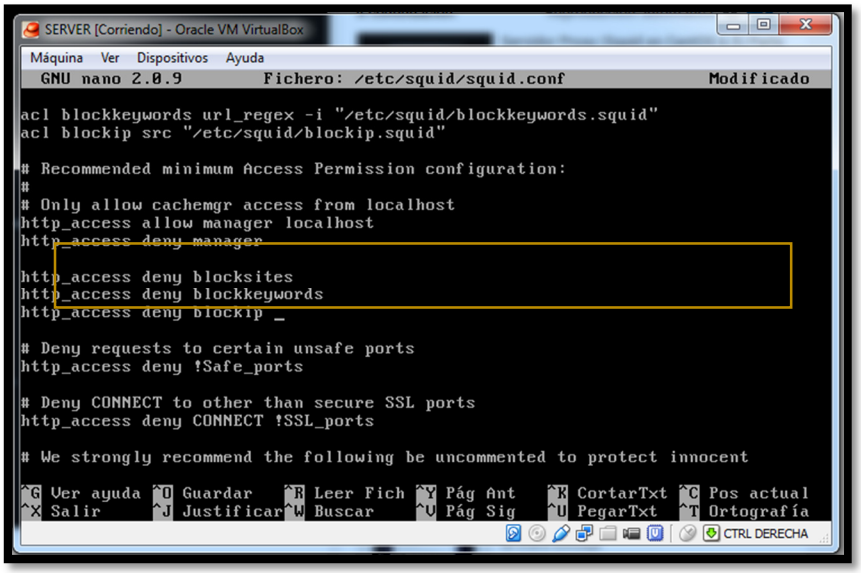

Figura 91. Agregación de fichero para denegar acceso a usuarios

Referencia: Elaboración propia

Habilitación del puerto 3128

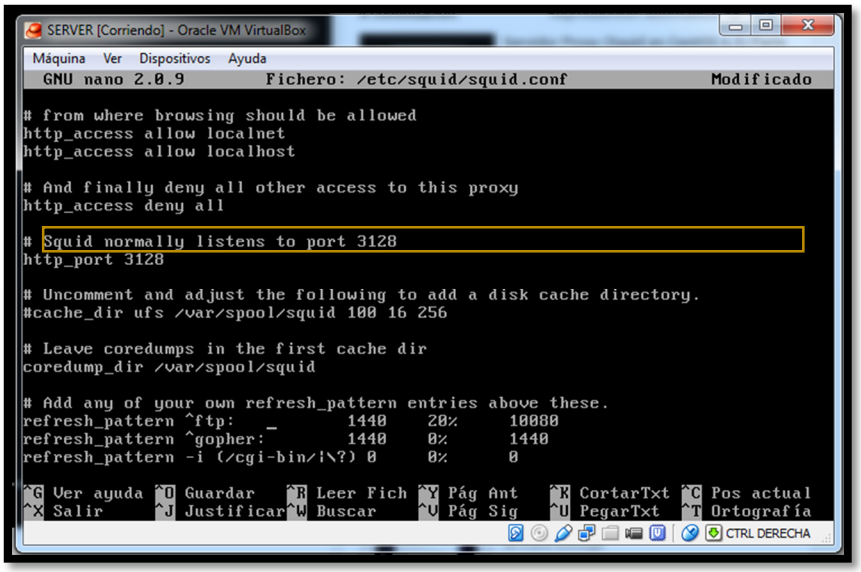

Figura 92. Habilitación del puerto.

Referencia: Elaboración propia

Verificamos mediante el comando (ls), los ficheros instalados.

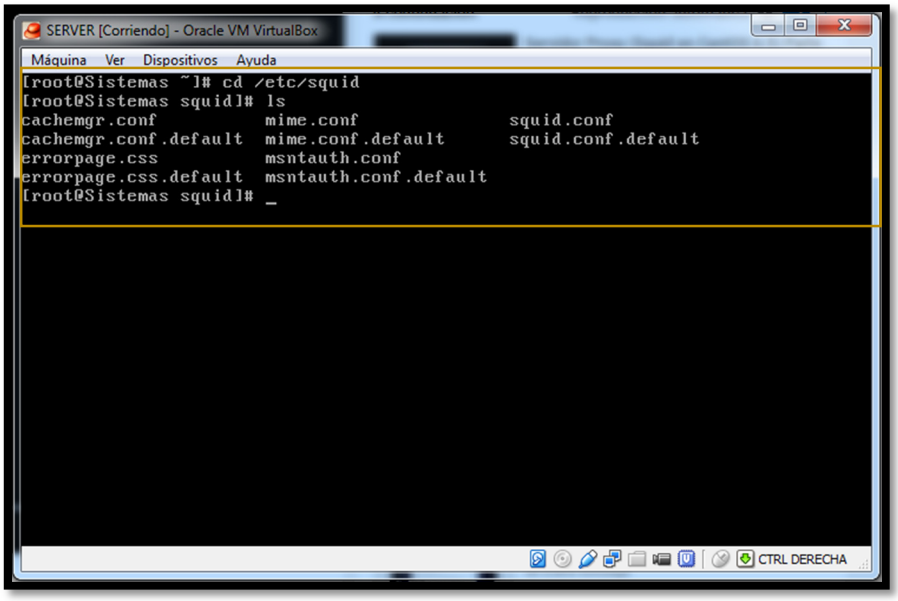

Figura 93. Verificación de archivos creados

Referencia: Elaboración propia

Editamos el fichero “/etc/squid/blocksites.squid”, en el cual se describe las paginas a bloquearse.

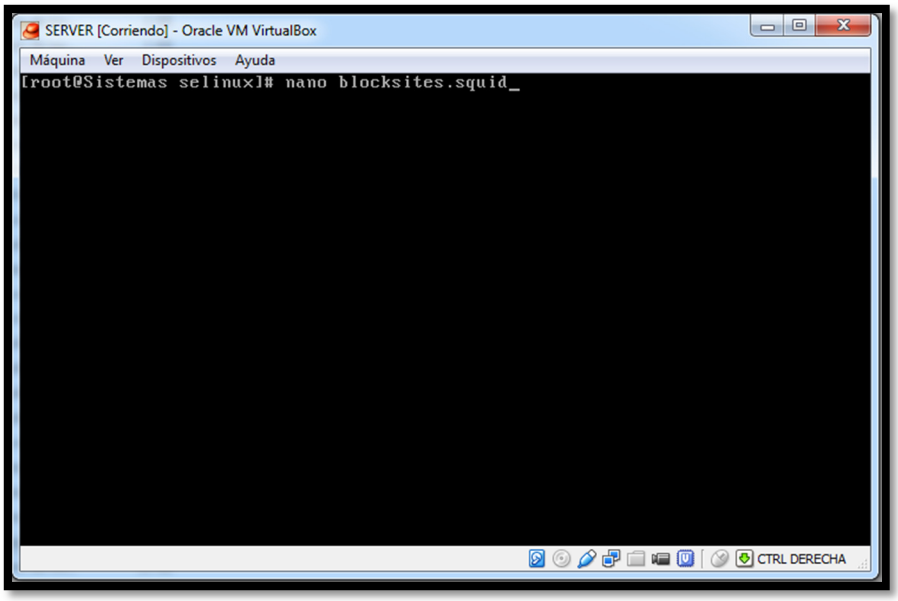

Figura 94. Ingreso al archivo de bloqueo de páginas web

Referencia: Elaboración propia

Editamos el fichero añadiendo las siguientes líneas.

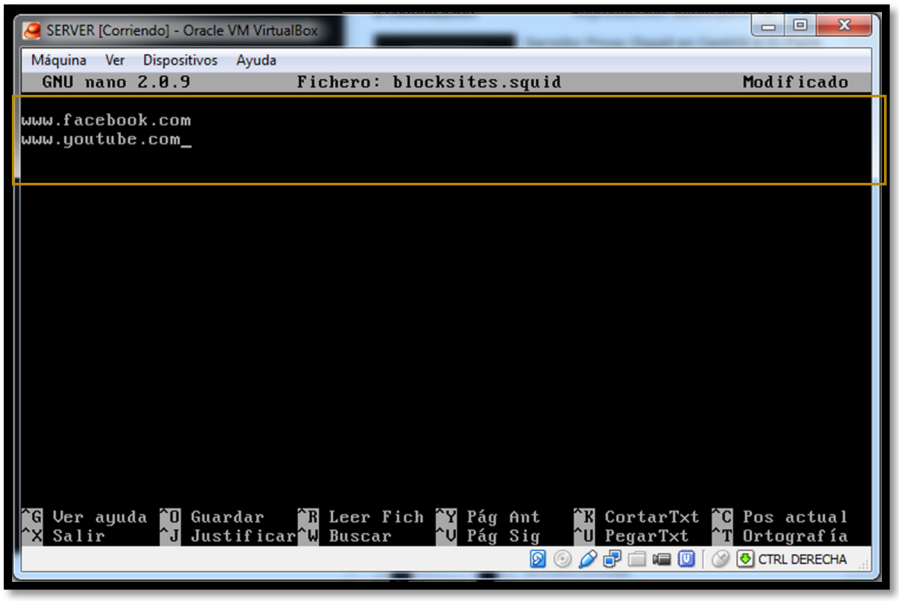

Figura 95. Agregación de páginas web a bloquearse

Referencia: Elaboración propia

Editamos el fichero “/etc/squid/blockkeywords.squid”, en el cual se describe las palabras claves a bloquearse en el navegador.

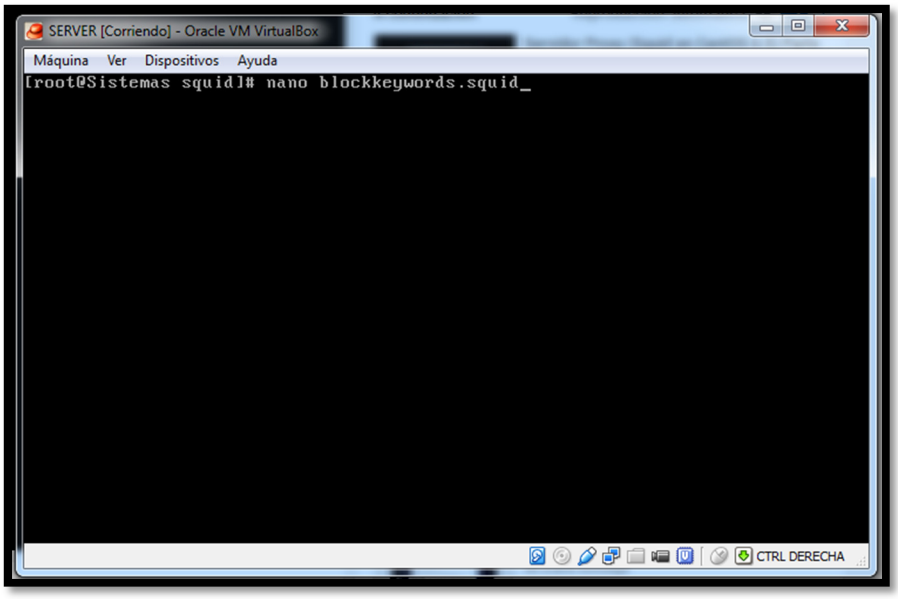

Figura 96. Ingreso al fichero de bloqueo por enunciados

Referencia: Elaboración propia

Editamos el fichero añadiendo las siguientes líneas.

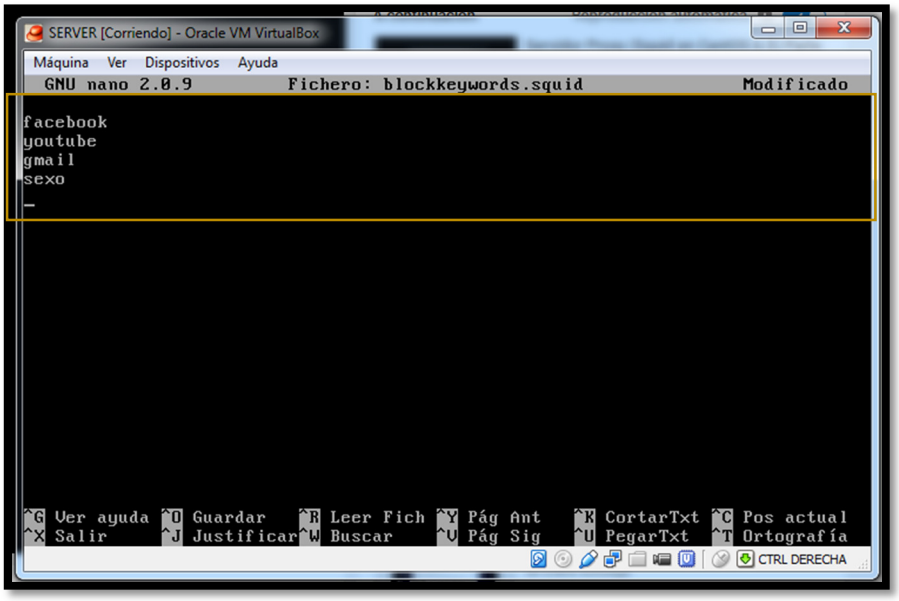

Figura 97. Agregación de bloqueo por las siguientes palabras

Referencia: Elaboración propia

Editamos el fichero "/etc/squid/blockkeywords.squid", en el cual se describe la dirección IP a bloquearse.

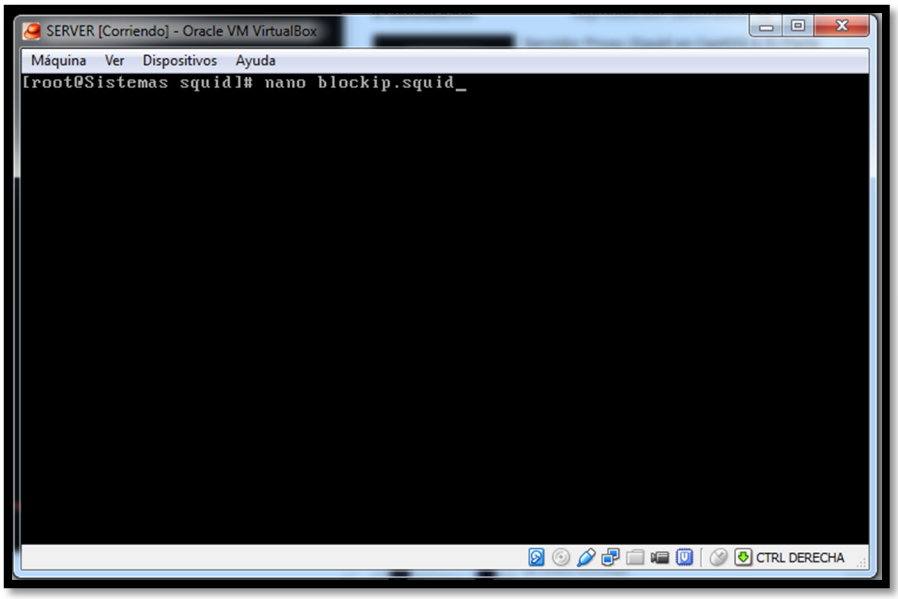

Figura 98. Ingreso al fichero del destinatario

Referencia: Elaboración propia

Ingresamos al archivo “selinux”.

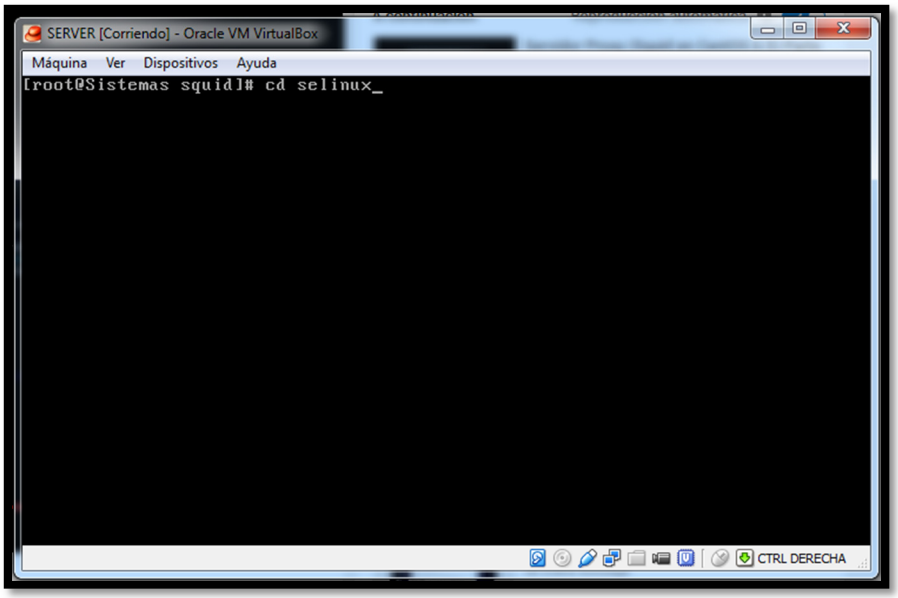

Figura 99. Ingreso al archivo selinux

Referencia: Elaboración propia

Mediante el comando “ls”, verificamos los archivos existentes.

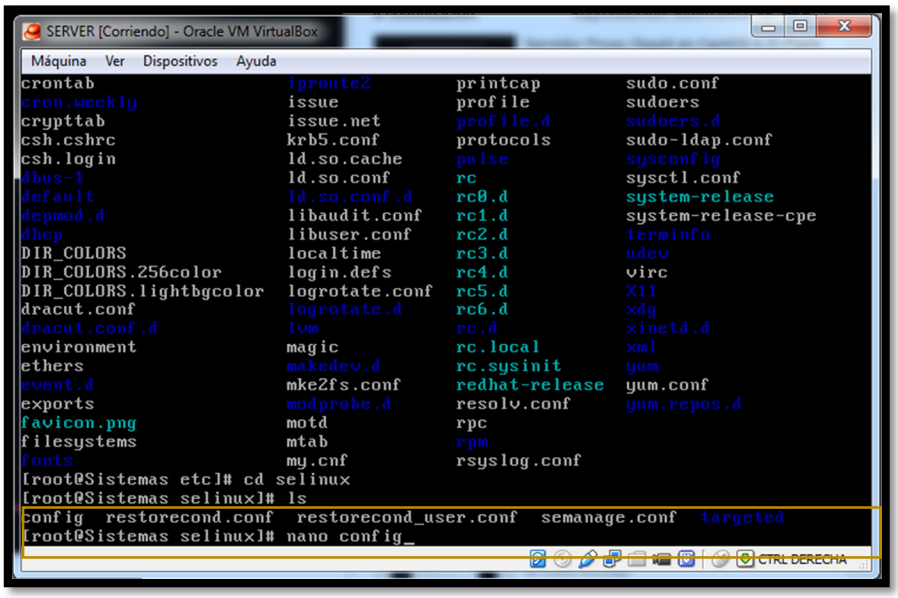

Figura 100. Visualización de ficheros en selinux

Referencia: Elaboración propia

Editamos el archivo “config”

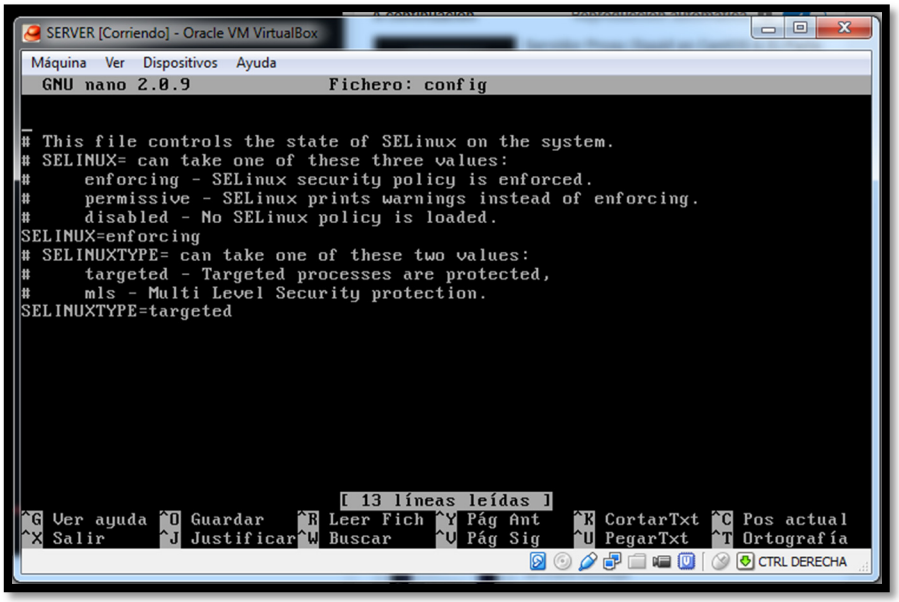

Figura 101. Modificación del fichero config

Referencia: Elaboración propia

Detenemos el fichero iptables

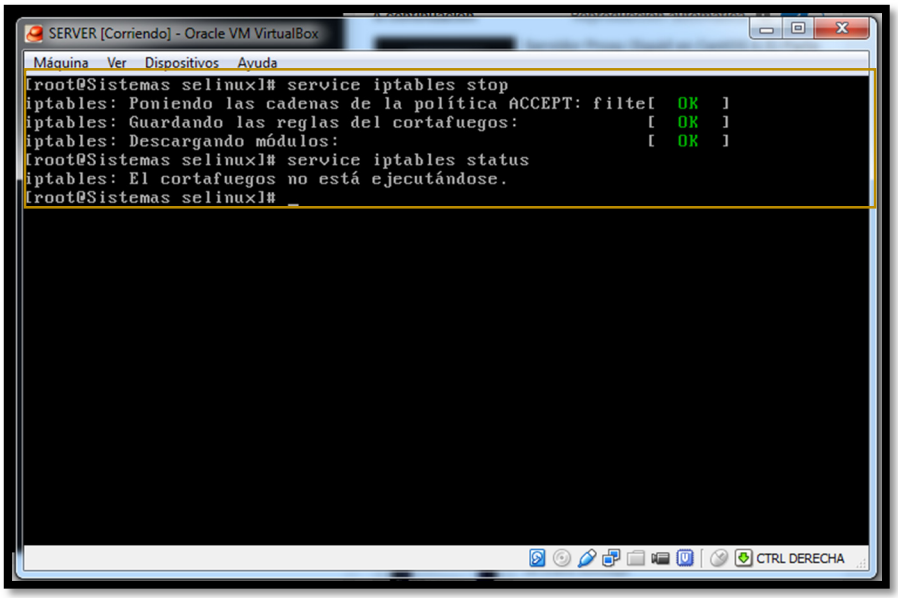

Figura 102. Comando para detención del squid

Referencia: Elaboración propia

Iniciamos el archivo “iptables”

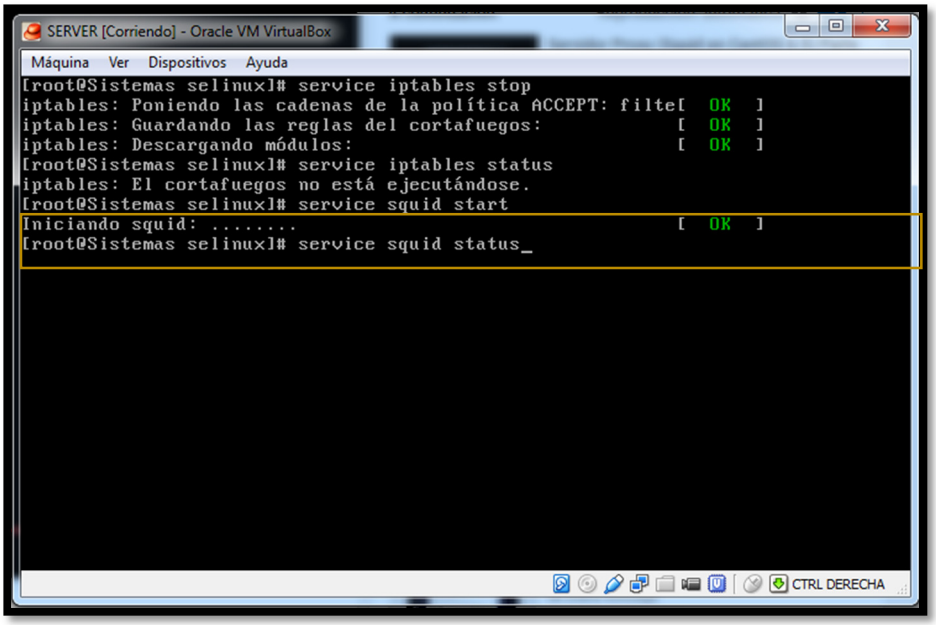

Figura 103. Inicialización del squid

Referencia: Elaboración propia

Verificamos lo archivos que contiene el fichero squid, mediante el comando ls

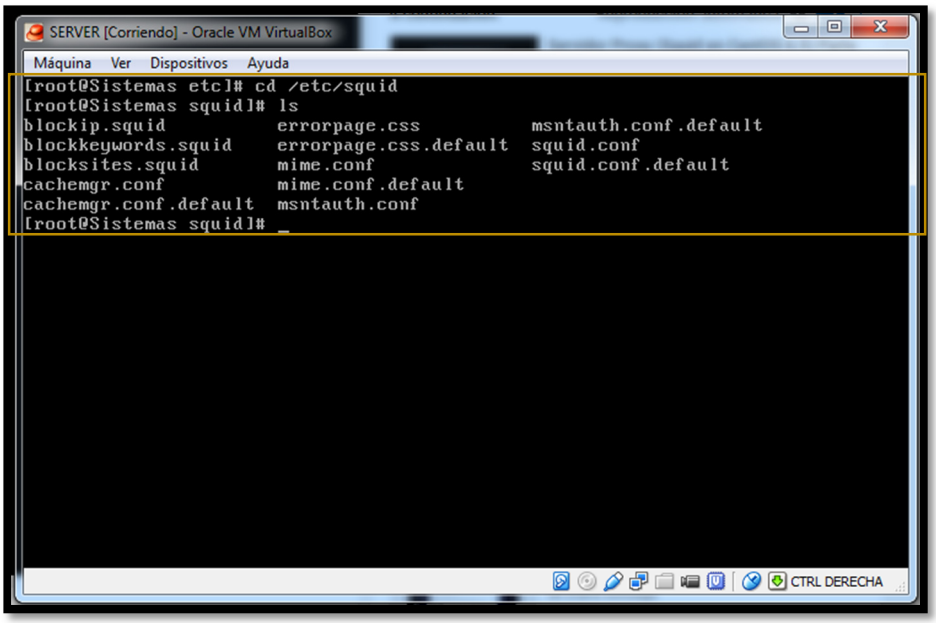

Figura 104. Visualización de ficheros

Referencia: Elaboración propia

Verificamos el estado del servidor proxy mediante la siguiente figura, el servidor proxy se encuentra en funcionamiento.

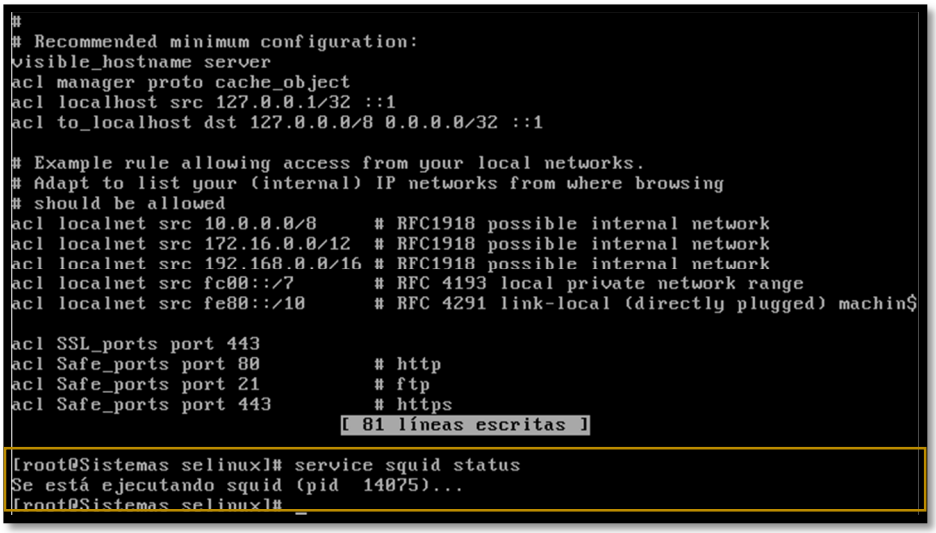

Figura 105. Estado del servidor squid

Referencia: Elaboración propia

ANEXO K

ANÁLISIS DE LA NORMA ISO/IEC/IEEE 29148:2011 (SISTEMAS E INGENIERÍA DE SOFTWARE - CICLOS DE VIDA PROCESOS - INGENIERÍA DE REQUISITOS)

El estándar IEEE830 de la versión del año 1998 y conjuntamente con la actualización ISO/IEC/IEEE para especificación de requisitos de Software, permite la elección de un 29148 sistema operativo, en este caso para el servidor PROXY mediante la evaluación de ciertos parámetros.

INTRODUCCIÓN

Para la elección del sistema operativo donde se va a instalar el servidor FIREWALL, los siguientes sistemas analizará mediante la norma ISO/IEC/IEEE 29148 serán los siguientes: CENTOS (6.3), UBUNTU (14.04.2), DEBIAN (7)

Propósito

El propósito que debe cumplir el software es que brinde un servicio óptimo para control de tráfico interno y está orientado al personal de administración de la red interna del Gobierno Autónomo Descentralizado San Miguel de Urcuquí.

Ámbito

El sistema operativo que se utilizará para el servidor PROXY SQUID y FTP, con el fin de limitar el tráfico interno de la institución, además sus herramientas deben acoplarse al modelo jerárquico implementado, con el fin de logrando mejorar la administración.

Definición y abreviaturas

- Sistema operativo: Programa básico de una computadora que brinda una interfaz gráfica fácil de utilizar sin discriminación de nivel de aprendizaje
- FIREWALL: Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos.
- PROXY: Son firewall que filtran aplicaciones, se ubican en la capa 7 del modelo OSI
- Modelo Jerárquico: Utiliza capas para facilitar las tareas solicitadas para la red de datos, este modelo representa un ahorro en costos, mediante la distribución correcta de ancho de banda para cada capa. Utiliza protocolos de enrutamiento para controlar ancho de banda, además la detección de errores y solución de problemas es inmediata.

Referencias

Para realizar el documento se ha tomado en cuenta l siguiente referencia:

1. Martínez Cadena, A. M., (2015, Febrero). Diseño del sistema de telefonía IP bajo una plataforma de software libre para la industria FLORALP S.A de la ciudad de Ibarra.
2. Norma ISO/IEC/IEEE 29148 (2011) Especificación de Requisitos de Software
3. IEEE-STD-830-1998: Especificaciones de los requerimientos del software.

Visión general

Este documento se basa en dos secciones en la primera se realiza un análisis de general y en la segunda sección se describe los requisitos específicos.

DESCRIPCION GENERAL

En este caso sirve para un análisis comparativo para la mejor elección del sistema operativo, que servirá para la implementación del PROXY.

Perspectiva

Las plataformas de sistema operativos libres, debe adaptarse e instalarse en cualquier equipo, con lo elementos de red que disponga la institución.

Características de los usuarios

El software a utilizarse debe adaptase al nivel de los usuarios, dentro de la institución GADMU son pocos los usuarios que tienen un nivel educativo alto, con experiencia en el manejo de estos sistemas.

Restricciones

Las restricciones sometidas los sistemas operativos son:

- El software debe ser libre.
- Sus aplicaciones al integrarse deben ser libres
- Compatibilidad con interfaces ETHERNET.

ANEXO L

TABLA DE REMUNERACIONES EN EL GADMU

Nº	CÉDULA	APELLIDOS NOMBRES	REMUNERACIÓN BÁSICA UNIFICADA
1	1002907796	AGUILAR CADENA JAIME DAVID	1.412,00
2	1707262653	ALCEDO SAA LUIS FRANSISCO	675,00
3	1007623939	ALVAREZ MORILLO DIANA KARINA	901,00
4	1007276453	ANANGONO NAVAS FABRICIO JAIRO	901,00
5	1003329008	ANDRADE CIFUENTES DIEGO PATRICIO	1.412,00
6	1003481551	ANRRANGO VARGAS CARMEN MARITZA	675,00
7	400515151	ARMAS BENAVIDES BYRON AUGUSTO	1.760,00
8	1003318555	ARMAS NAZARENO FREDDY SAUL	901,00
9	1712826294	BENAVIDES ALBUJA GIOVANNA PAOLO	675,00
10	1002273738	ARRELLANO TAPIA PATRICIO SANTIAGO	675,00
11	1003775887	BENAVIDES MORALES ESTRELLA ELI	675,00
12	1001273935	BOLAÑOS GUERRA MARCO VINICIO	1.412,00
13	1001288394	BORJA PATRICIA CONSUELO	1.760,00
14	1001285624	CAICEDO ZAMORA JULIO CESAR	901,00
15	1002872016	CALDERON GOMEZ MIRIAN ROCIO	675,00
16	1099283831	CALDERON MENESES NANCY MARIA	901,00
17	1002039996	CARANQUI LEON FAUSTO RODRIGO	817,00
18	1001843000	CARRILLO ESPINOZA RODRIGO EFREN	2.380,00
19	103441580	CHICA ARICHABALA JESY LORENA	901,00
20	1001933975	CHUMA REALPE MARIA DEL ROSARIO	733,00
21	1002248514	CHUQUIN PERUGACHI WILLIAM EDGAR	901,00
22	1001313921	CIFUENTES REYES LUIS GERMAN	2.380,00
23	1002992400	COBOS TERAN CECILIA MARINA	2.380,00
24	1001626263	CRUZ FLORES XIMENA CRISTINA	675,00
25	1709135659	CRUZ PONCE VICTOR JULIO	3.520,00
26	1002828838	CRUZ ROSERO CARLA ESTEFANIA	1.412,00
27	1007728239	DIAZ CERON FERNANDO JIMMY	1.760,00
28	1702827138	DIBUJES ERAZO MARTIN WILLIAN	1.412,00
29	1002002473	DUEÑAS TORRES FAUSTO PATRICIO	675,00
30	1003288469	DUEÑAS TORRES HECTOR EFREN	733,00
31	1002070462	ECHEVERRIA MORALES CECILIA	1.412,00
32	1001539624	ECHEVERRIA RECALDE ORLANDO ATA	1.412,00
33	1001362472	ENRIQUEZ CASTRO EDVIO ROGNER	901,00

Nº	CÉDULA	APELLIDOS NOMBRES	REMUNERACIÓN BÁSICA UNIFICADA
34	1008737371	ESTRADA MONCAYO MICHELLE KARLA	675,00
35	1002343398	FARINANGO TORRES MARIO ROBERTO	901,00
36	1001397312	FELIX SALVADOR AURA BERTHA	675,00
37	1002253258	FLORES CALVACHE MARIA CRISTINA	1.920,00
38	1003005251	FLORES CALVACHE MARIA CRISTINA	1.412,00
39	1001706876	GALLEGOS TRUJILLO JACINTO IVAN	2.380,00
40	485858999	GOMEZ TAMBACO SANDRO MARIO	1.920,00
41	1002604138	GORDILLO MEDRANO LUCIA MAGDALENA	817,00
42	1002577938	GORDON REASCOS LUZ GUADALUPE	675,00
43	1003242078	GUANCHA VENEGAS JUAN PABLO	1.412,00
44	1716333834	HERRERA SASI HENRY ROBERTO	901,00
45	1003092549	HERRERA VINUEZA PATRICIA ELIZA	675,00
46	1704747623	HURTADO CHACON LUIS HOMERO	901,00
47	1002278339	ILES CHUMA EDGAR GEOVANNI	733,00
48	1001561701	JATIVA RAMIREZ DAICY ALEXANDRA	817,00
49	1008288239	LARA IPILALES JORGE EDWIN	1.760,00
50	1001348703	LARA QUILCA MILTON SEGUNDO FABIAN	1.412,00
51	1001710852	MANRIQUE ALOMIA EDISON RAUL	733,00
52	1002838731	MENESES CERON MARCO SCOOT	700,00
53	1003125877	MICHILENA LARA MARCELA DEL ROCIO	675,00
54	1009828373	MIRANDA CALDERÓN EDISON ORLANDO	901,00
55	1003014147	MONTENEGRO LARA ANA MARIA	901,00
56	1099283745	MORAN NOGUERA MAURICIO EMILIO	901,00
57	1001897451	MORETA QUILCA GUSTAVO	1.760,00
58	1703883445	NAVAS VELEZ BYRON EFREN	1.676,00
59	1006527339	OBANDO GOMEZ CRISTOBAL FERNANDO	2.380,00
60	1001454584	OBANDO GOMEZ LUIS ANIBAL	1.760,00
61	1006253341	OBANDO RUALES ERICK ITAN	2.380,00
62	1706387485	OÑA SARZOSA EDWIN ANIBAL	817,00
63	483839292	ORMAZA MEJIA JOSE MANUEL	817,00
64	1008383447	PANTOJA RIVERA JESYCA MARIA	1.760,00
65	1006373832	PANTOJA ZURA BETSY KARINA	2.380,00
66	1001057379	PAREDES VALENZUELA IVAN ENRIQU	2.380,00
67	1002727273	PARRA ERAZO KATHERINE YOMAIRA	675,00
68	1003146451	PINTO REVELO CESAR OSWALDO	2.380,00

Nº	CÉDULA	APELLIDOS NOMBRES	REMUNERACIÓN BÁSICA UNIFICADA
69	1709293832	PIÑAN HIDROBO LORENA ESTEFANIA	675,00
70	1002485322	QUILCA DE LA TORRE LUIS ROBERT	1.760,00
71	1002683207	QUIMBIAMBA ANRRANGO MARIA DORA	1.760,00
72	1002451480	QUITO ARRAYAN ROCIO DEL PILAR	675,00
73	1002753992	REA ENRIQUEZ PATRICIA ALEXANDR	675,00
74	1002861597	RECALDE BOLAÑOS MARIA FERNANDA	675,00
75	1001400686	RECALDE LARA MARIA MAGDALENA	1.412,00
76	1005353548	RECALDE MENESES CLARA SORAYA	901,00
77	1004888923	RECALDE REASCOS LILIAN OLIVA	901,00
78	1002535362	RIVERA DIANA CAROLINA	901,00
79	1001827236	RIVERA FARINAGO GONZALO MARIO	2.380,00
80	1001972890	SALAS MARCILLO SILVANA DEL PILAR	901,00
81	1000881415	SALTOS VARELA WILSON ENRIQUE	675,00
82	1002609137	SANTACRUZ BELTRAN ENMA GABRIEL	1.412,00
83	1002597662	SILVA ATARIHUANA WILLIAM ROBERTO	901,00
84	1007272637	SUAREZ ERAZO SARA DIANA	1.412,00
85	1003747479	TAFUR VELASCO JIMENA YOLANDA	2.380,00
86	1001196771	TAMAYO DAVILA CARLOS ALFONSO	901,00
87	1007373728	TINAMA CAÑAMAR JUAN MANUEL	675,00
88	1008273731	TORRES GONZALES EMILIO FABIAN	901,00
89	1003737462	TORRES SULTAN MARIELA ANA	675,00
90	1001829930	UBIDIA GONZALES LENIN ALBERTO	901,00
91	1007272636	VALENCIA ROMERO JHONNY ALBERTO	901,00
92	1003198924	VALLES ANDRADE SONIA JANETH	901,00
93	1792727363	VALLES CUENCA SONIA ADRIANA	2.380,00
94	1001791654	VARELA CALDERON ROSA ANITA	675,00
95	1707318430	VASCONEZ FLORES MARCO TULIO	2.380,00
96	1002272738	VERDEZOTA MAYORGA VALERIA FERNANDA	2.380,00
97	1004627383	VILLALBA FARINANGO CLEMENCIA ROSA	2.380,00
98	1002254660	YALAMA DIBUJES ANITA ROSAURA	675,00
99	1001093770	YASELGA TERAN OSCAR ELOY	700,00
100	1007822391	ZULETA ALVAREZ JAIME EMILIO	901,00
		SUELDO DE 100 EMPLEADOS	125.399,00
		PARA 125 EMPLEADOS EXTERNOS	31.349,75
		TOTAL	156.748,75

ANEXO M

ENCUESTA PARA ANÁLISIS DE LA RED LÓGICA INTERNA DEL EN EL GADMU

Nombre: ……....

Cargo: ……..

Departamento: ……..

¿Tiene acceso a los recursos de red como: base de datos, impresora, correo institucional, entre otros?

Si ……

No …….

¿Según su opinión, considera usted que la red que utiliza el GADMU, permite trabajar de una manera eficaz, sin retrasos y de una manera continua?

Si ------

No ------

A veces -------

En horas pico, El sistema que usted maneja en línea le permite trabajar:

Adecuadamente ……

Con retrasos ……

Inadecuadamente ……

¿Qué porcentaje al día usted considera que la red se encuentra en mal estado, es decir tiene problemas con los sistemas que usted maneja, no puede enviar o recibir información, entre otros?

5% --------- 10% --------- 15% ---------

TABULACIÓN

¿Tiene acceso a los recursos de red como: base de datos, impresora, correo institucional, entre otros?

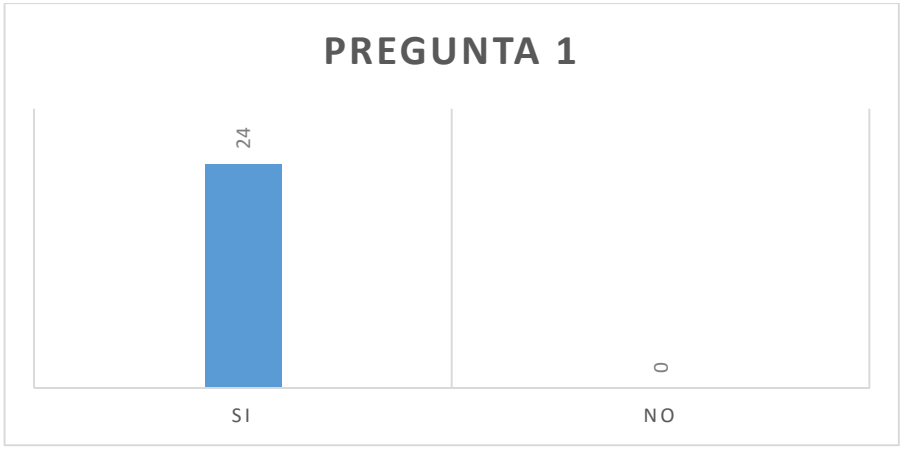

Figura 106. Acceso a los recursos de Red

Referencia: Elaboración propia

¿Según su opinión, considera usted que la red que utiliza el GADMU, permite trabajar de una manera eficaz, sin retrasos y de una manera continua?

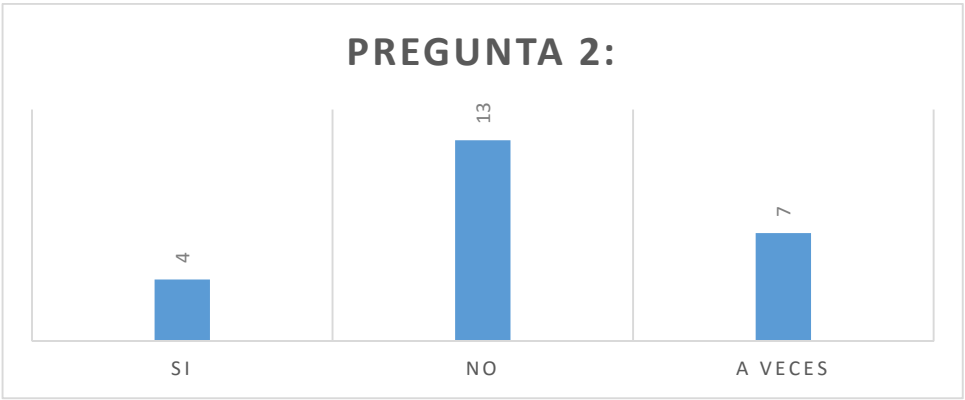

Figura 107. Opinión del funcionamiento de la red del GADMU

Referencia: Elaboración propia

En horas pico, El sistema que usted maneja en línea le permite trabajar:

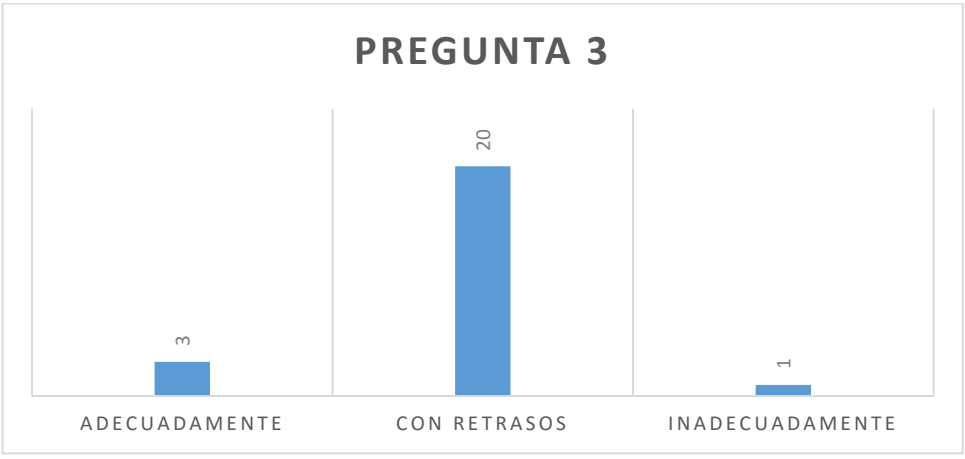

Figura 108. Forma de trabajo de la red GADMU

Referencia: Elaboración propia

¿Qué porcentaje considera que la red se encuentra en mal estado, es decir tiene problemas con los sistemas que usted maneja, no puede enviar o recibir información, entre otros?

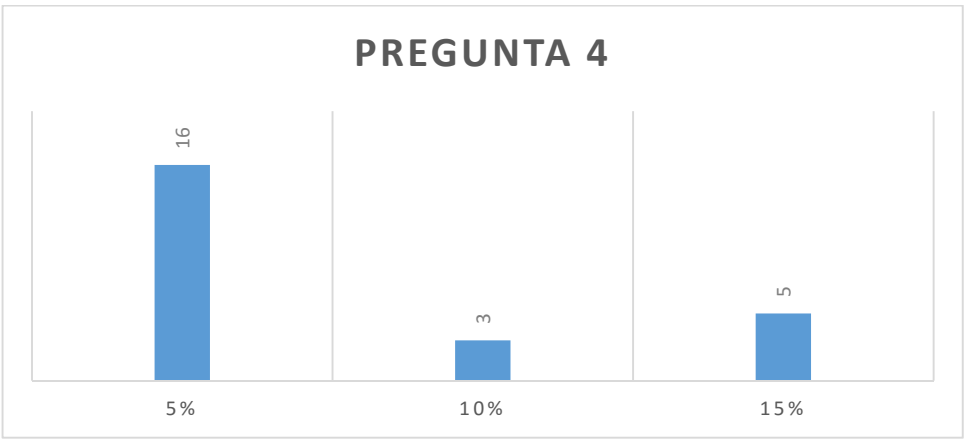

Figura 109.Porcentaje de problemas de red

Referencia: Elaboración propia