# ESCUELA POLITÉCNICA NACIONAL

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

# REDISEÑO DE LA INTRANET MULTISERVICIOS EN LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO", CON POLÍTICAS DE SEGURIDAD UTILIZANDO HACKING ÉTICO E IMPLEMENTACIÓN DE UN PROTOTIPO

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

**JÉSSICA PAOLA HIDALGO YÁNEZ**
pao7_2010@hotmail.com

**DIANA PAULINA TUPIZA LIMA**
diana_tupiza@hotmail.com

**DIRECTOR: ING. TARQUINO SÁNCHEZ A., MBA**
sanchez.tarquino@epn.edu.ec

**Quito, Diciembre 2015**

# DECLARACIÓN

Nosotras, Jéssica Paola Hidalgo Yánez y Diana Paulina Tupiza Lima declaramos bajo juramento que el trabajo aquí escrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Jéssica Paola Hidalgo Yánez Diana Paulina Tupiza Lima

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jéssica Paola Hidalgo Yánez y Diana Paulina Tupiza Lima, bajo mi supervisión.

_____

ING. TARQUINO SÁNCHEZ A., MBA
DIRECTOR DEL PROYECTO

# AGRADECIMIENTOS

A Dios, por ser mi fortaleza y mi refugio a lo largo de mi vida y por permitirme compartir junto a mi familia este sueño.

A mis padres, por todo el amor que me brindan y por el gran sacrificio que realizan para que sus hijas tengamos un mejor futuro y seamos personas de bien, muchas gracias por confiar en mí.

A mis hermanas, Leslie y Daya, porque me han alentado en el transcurso de mi carrera y por que las dos son el motivo de querer ser un mejor ser humano.

Al Ing. Gustavo Correa funcionario de la Administración Zonal Norte Eugenio Espejo, por habernos permitido desarrollar el presente proyecto en su ilustre institución, y por el apoyo incondicional que mostro cada vez que necesitábamos de su ayuda.

A nuestro Director, Ing. Tarquino Sánchez, por haber sido nuestra guía en este proyecto, por motivarnos a ser mejorares profesionales cada día y por siempre recibirnos con una sonrisa.

A Diana, por permitirme ser su compañera en este reto, por haber compartido mis alegrías y tristezas a lo largo de estos años, por ser mi confidente y por decir las palabras precisas en los momentos justos, te quiero mi brujis.

A Vinicio, por creer en mí, por haberme alentado cada día para alcanzar esta meta, por brindarme su apoyo, por haber estado en los momentos que más lo necesitaba, simplemente gracias por ser parte de mi vida.

A mis amig@s, por haber compartido madrugadas de estudio, largos días de clases, proyectos extensos, y por siempre haber estado para darme una mano cuando los necesitaba, gracias por haber hecho de mi carrera universitaria una de las mejores experiencias de mi vida.

Jéssica

# AGRADECIMIENTOS

Mi agradecimiento principalmente a Dios, por permitirme estar de pie, por darme a mis padres que son el pilar fundamental en mi vida.

A mi papi Francisco que con todo su esfuerzo y sacrificio siempre lucha para sacarnos adelante, que nunca importó las malas noches y el cansancio, siempre estuvo conmigo.

A mi mami Luz, que siempre ha estado conmigo en las buenas y malas apoyándome y brindándome tus palabras de aliento para nunca dejarme vencer, siempre supiste que decir y qué hacer cuando más lo necesité, por darme ese amor incondicional. Gracias mami.

Al amor de mi vida, Rafa, no tengo como agradecerte el que estés conmigo, gracias por todos esos empujoncitos que me diste para seguir adelante, por compartir mis sueños y enseñarme a que si se puede lograr lo que uno se propone. Gracias por todo tu amor, respeto, compresión y paciencia. Te amo Amor.

A mis hermanitas, mis gemes, gracias por cada palabra de aliento, por cada abrazo, por cada tu puedes Pao, simplemente son las mejores. A mi familia, por estar siempre unida a pesar de todo, por ser incondicionales siempre en que lo necesité.

A tres personitas que son mi todo, Tía Enma, Abuelita Francisca y sobre todo a mi Abuelito Juan, a ustedes les debo mucho, ustedes que son mi ejemplo de lucha ,sacrificio, y sobre todo de FE. Sé que ahora eres mi angelito Abuelito, gracias por cada visita, historia, consejo que me diste, tus palabras siempre quedarán guardadas en mi corazón. Te quiero mucho Abuelito y como siempre me decías “NI UN PASO ATRÁS, ARRIBA LIMA”.

Al Ingeniero Tarquino Sánchez, por haber guiado este proyecto, y compartir su experiencia y consejos para que esta meta sea una realidad.

A la Administración Zonal Norte, en especial al Ingeniero Gustavo Correa, por abrirme las puertas de su institución y permitirme realizar este proyecto, por brindarme su apoyo y sobre todo su gran amistad. Al Ingeniero Eduardo Catacta y la Ingeniera Norma Benalcázar gracias por todo su apoyo.

A mis amig@s, a todos y cada uno de ustedes gracias, conocerlos fue realmente importante para mí, gracias por estar conmigo en las buenas y malas, sobre todo a mi compañera de risas, mi Jess gracias por poner todo de ti para poder cumplir este sueño, a tu familia por todo el apoyo, sé que conseguiremos grandes cosas y sé que esta amistad jamás se acabará. Te quiero mucho brujita.

Mil gracias a todos los que con un granito de arena siempre estuvieron brindándome todo su apoyo y deseándome lo mejor.

Diana

# DEDICATORIA

A mi familia, porque mis padres y mis hermanas son el motor de mi vida, porque con ellos he aprendido que unidos podemos salir adelante de cualquier adversidad y que todo sueño es alcanzable si le dedicamos esfuerzo y empeño.

*Jéssica*

# DEDICATORIA

A un GRANDE a JUAN LIMA, por tu fortaleza, tu amor, por ser un abuelito excepcional e incomparable. Nunca te olvidaré mi viejito.

A mi mami Luz y mi papi Francisco, que siempre me dieron las fuerzas necesarias para levantarme y seguir caminando.

A mis hermanas, Cris y Vale por su todo su cariño.

A mi amor grandote, Rafa, por todo su amor y paciencia.

A mi Tía Enma por ser una muestra de sacrificio y amor.

A mis Abuelitos por ser la muestra del amor verdadero y FÉ.

A toda mi familia por todo su apoyo.

Diana

# CONTENIDO

# ÍNDICE DE FIGURAS

## CAPÍTULO 1



## CAPÍTULO 2

# ÍNDICE DE TABLAS

## CAPÍTULO 1



## CAPÍTULO 2

**CAPÍTULO 3**

# RESUMEN

Este proyecto de titulación tiene como objetivo el rediseño de la red multiservicios de la Administración Zonal Norte “Eugenio Espejo”, basándose en un análisis de la situación actual de la red, mismo que incluye el rediseño de la infraestructura de la red voz y datos, así como también el establecimiento de políticas de seguridad partiendo del análisis de las vulnerabilidades mediante la utilización de técnicas de hacking ético.

En el primer capítulo se tratarán los aspectos teóricos en los que se fundamenta este proyecto. En el segundo capítulo se realizará una descripción general de la situación actual de la Administración para establecer los requerimientos de la red, además se implementará una Honeynet (red de prueba) donde se aplicarán técnicas de hacking ético para determinar las vulnerabilidades existentes.

En el tercer capítulo se llevará a cabo el rediseño de la intranet multiservicios de voz y datos, se configurará el software para la gestión de monitoreo de la red, además de la determinación de VLANs para la administración de servicios teniendo en cuenta las nuevas políticas de seguridad. En el cuarto capítulo se implementará un prototipo de prueba de la solución propuesta; se utilizarán equipos terminales como máquinas virtuales y el simulador GNS3. Se realizarán pruebas para verificar el correcto funcionamiento del rediseño y se presentarán los resultados respectivos. En el quinto capítulo se determinará la viabilidad del rediseño, realizando una evaluación del proyecto mediante el índice de Costo-Efectividad. En el sexto capítulo se discutirán los resultados obtenidos verificando el cumplimiento de los objetivos planteados, así como las recomendaciones respectivas para otros proyectos. Finalmente se incluye los anexos sobre proyecto orgánico de DMQ, diagramas de la AZNEE actuales, direccionamiento IP, configuración de la honeynet, formato de encuesta, cálculo de escalerilla, informe de cobertura Wifi, configuraciones de routers y switches, archivo de configuración de FTP y Nagios, hoja de datos de softphone, manual de zoiper, pruebas de conectividad y cotizaciones.

# ABSTRACT

This degree project aims to the redesign of the Northern Zonal Administration multi-service network "Eugenio Espejo". An analysis of the current state of the network, including the redesign same infrastructure voice and data network was performed. Were established security policies based on the analysis of vulnerabilities using ethical hacking techniques.

In the first chapter the theoretical aspects in which this project is based will be treated. In the second chapter a general description of the current situation of the management will be held to establish the requirements of the network, will be also implemented a Honeynet (test network) where apply ethical hacking techniques to determine the existing vulnerabilities.

In the third chapter will be held the redesign of intranet multi-service voice and data, you want to configure the software for the management of monitoring of the network, as well as the determination of VLANs for the administration of services taking into account the new security policies.

In the fourth chapter will be implemented a prototype of testing of the proposed solution; be used equipment terminals such as virtual machines and GNS3 Simulator. There will be tests to verify the proper functioning of the redesign and the respective results.

The fifth chapter will determine the viability of the redesign, making an evaluation of the project by the cost-effectiveness index. The results obtained by verifying the fulfilment of the objectives set, as well as the respective recommendations for other projects will be discussed in the sixth chapter.

Finally, the annexes on organic DMQ project, the current AZNEE diagrams, ip address, the honeynet configuration, formatting and survey ladder calculation, report access, router and switch configurations, configuration file includes FTP and Nagios, sotfphone data sheet, manual Zoiper, connectivity tests conducted and quotes.

# PRESENTACIÓN

El objetivo del presente proyecto es rediseñar la intranet multiservicios de la Administración Zonal Norte Eugenio Espejo perteneciente al Distrito Metropolitano de Quito, aprovechando la reciente adquisición de nuevos equipos; por lo que se necesita realizar una eficiente administración y configuración de cada uno de los elementos que compone la infraestructura de conectividad de la red, tomando en cuenta que al ser una entidad pública puede ser blanco de ataques externos que buscan violentar la información que maneja la institución.

Es por ello, que al rediseñar la red de voz y datos con un adecuado sistema de cableado estructurado, se brindará un óptimo manejo de los cambios, adiciones y mantenimientos de los puntos de red, así como también, permitirá disminuir los tiempos de respuesta a las necesidades de los usuarios; acoplándose de esta manera a la tendencia actual de las instituciones del Estado.

Se brindará seguridad contra intrusos en cada uno de los elementos activos de la red, puesto que las configuraciones que se encuentran en los principales equipos de comunicación son relativamente básicas para el tipo de información que manejan los servidores de la entidad, y que al momento no cuentan con un nivel adecuado de seguridad. Por ello, mediante la utilización de hacking ético se determinarán las vulnerabilidades existentes y se establecerán políticas de seguridad que servirán para que el personal del área de informática pueda hacerle frente a los ataques que pudiera sufrir la institución.

En este proyecto de titulación se podrá encontrar temas relacionados a la seguridad mediante la utilización de hacking ético, rediseño de una red LAN y telefonía IP, que servirán como información y base para la implementación en diversas empresas que necesiten mejorar su eficiencia operativa.

# CAPÍTULO I

# FUNDAMENTOS TEÓRICOS

## 1.1 FUNDAMENTOS DE LAS REDES DE DATOS [1]

Una red es la disposición física o virtual de equipos y dispositivos, que permiten compartir información y recursos a través de un medio de comunicación.

Actualmente, las redes permiten garantizar un cierto nivel de servicio (QoS) y asegurar varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, etc.

### 1.1.1 CLASIFICACIÓN DE LAS REDES

Las redes de información no poseen una sola clasificación que se acople a todas las redes existentes. Sin embargo, se ha tratado de clasificarlas dependiendo de la tecnología de transmisión y el área de cobertura.

#### 1.1.1.1 Por la tecnología de transmisión [2]

Se cuenta con dos tipos de tecnologías de trasmisión:

- **Redes por difusión:** Son aquellas que comparten un solo canal de comunicación para todas las máquinas que se encuentren en esa red.
- **Redes punto a punto:** Constan de muchas conexiones entre pares individuales de máquinas, la información viaja por varias máquinas intermedias antes de llegar a su destino.

#### 1.1.1.2 Por el área de cobertura [3]

Según el alcance o cobertura las redes pueden ser clasificadas de la siguiente manera:

- **Personal Area Network (PAN):** Son redes centradas en las personas, la cual está integrada por dispositivos situados en un entorno personal y local del usuario.
- **Local Area Network (LAN):** Son redes de propiedad privada que comparten recursos e intercambian información dentro de una estructura organizacional común.
- **Metropolitan Area Network (MAN):** Son una versión más grande que la LAN y normalmente se basan en una tecnología similar. Pueden abarcar una ciudad.
- **Wide Area Network (WAN):** Son aquellas que abarcan un área geográfica extensa, por lo general un país o continente.
- **INTERNET:** Es la red de redes y presenta un alcance global.

En la tabla 1.1 se presenta un resumen de las redes según el área de cobertura.

**Tabla 1.1** Relación de las redes vs el área de cobertura [1]

| RED | ÁREA DE COBERTURA |
|---|---|
| Personal Area Network (PAN) | 1m |
| Local Area Network (LAN) | 1m – 1Km |
| Metropolitan Area Network (MAN) | 1Km – 10 Km |
| Wide Area Network (WAN) | 10Km – 1000Km |
| INTERNET | 10000Km |

## 1.2 ARQUITECTURA DE RED [2]

Las redes están organizadas en una pila de protocolos o niveles, en donde cada protocolo en la capa inferior proporciona sus servicios a los protocolos de la capa superior para que estos puedan realizar su propia funcionalidad. El propósito de tener una arquitectura por capas, es el de ofrecer servicios a las capas superiores.

[1] (Tanenbaum & Wetherall, 2012)

La comunicación de la capa ***n*** de una máquina con la capa ***n*** de otra máquina se la realiza en base a reglas y convenciones conocida como protocolos. Un protocolo es un acuerdo entre las partes en comunicación, sobre cómo se debe llevar a cabo la misma.

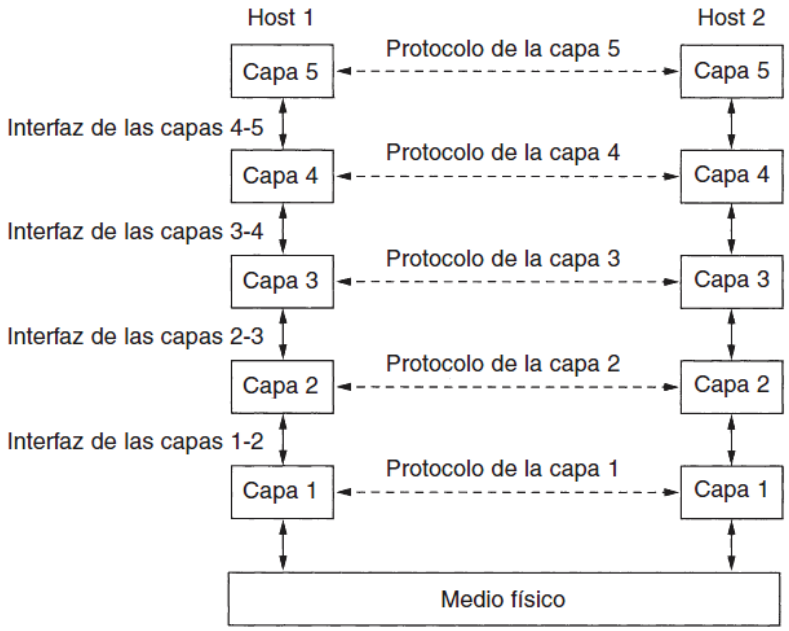



**Figura 1.1** Capas, protocolos e interfaces [2]

Entre cada par de capas adyacentes está una interfaz. Ésta define qué operaciones y servicios primitivos pone la capa más baja a disposición de la capa superior inmediata. La lista de protocolos utilizados por un sistema, se conoce como pila de protocolos. Es así como un conjunto de capas y protocolos se conoce como arquitectura de red.

### 1.2.1 MODELO DE REFENCIA OSI [2][4]

Las capas del modelo de referencia OSI (Open Systems Interconnect) fueron creadas por la ISO (International Organization for Standarization), con el propósito de abrir la comunicación entre diferentes sistemas sin recurrir a cambios en la lógica y

[2] Fuente:(Tanenbaum, 2003)

fundamentos del hardware y software. El modelo de referencia OSI constituido por 7 capas (Figura 1.2) no es un protocolo, es un modelo para entender el diseño de una arquitectura de red que sea flexible, robusta e interoperable.


**Figura 1.2** Modelo de Referencia OSI [3]

**Tabla 1.2** Descripción de las capas del modelo OSI

| MODELO OSI | | |
|---|---|---|
| **CAPAS** | **DESCRIPCIÓN** | **UNIDAD DE DATOS** |
| **CAPA FÍSICA** | Regula aspectos de la comunicación como: tipo de señal, esquema de codificación, sincronización de los bits, tipo de modulación, tipo de enlace, modo de comunicación, tasa de bits (número de bits por segundo) y todas las cuestiones eléctricas, mecánicas y de señalización. | Bit |

[3] Fuente: http://www.textoscientificos.com/redes/tcp-ip

| | | |
|---|---|---|
| **CAPA DE ENLACE** | Se ocupa del direccionamiento físico único (dirección física, ejm: Dirección MAC), topología de la red, acceso a la red, notificación de errores, distribución ordenada de tramas (serie sucesiva de bits) y del control de flujo. | Trama |
| **CAPA DE RED** | Responsable del envío fuente a destino de los paquetes mediante el direccionamiento lógico (dirección lógica, ejm: dirección IP), realiza el enrutamiento y control de congestión de los datos. | Paquete |
| **CAPA DE TRANSPORTE** | Responsable del envío de mensajes desde la fuente al destino verificando la integridad, orden, control de flujo y control de errores, asegurando un servicio confiable. | Segmento |
| **CAPA DE SESIÓN** | Establece, gestiona y finaliza sesiones entre diferentes máquinas proporcionando control de diálogo, administración de token y sincronización. | Dato |
| **CAPA DE PRESENTACIÓN** | Encargada de la representación de la información intercambiada entre dos sistemas, con el fin de interpretar de manera reconocible las diferentes estructuras de datos. | Dato |
| **CAPA DE APLICACIÓN** | Permite al usuario el acceso a la red, provee las interfaces y soporte para servicios como: correo electrónico, páginas web, transferencia de archivos, administración de bases de datos, etc. | Dato |

### 1.2.2 MODELO TCP/IP [5]

El estándar abierto de Internet es el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) (Figura1.3). Este modelo hace posible la comunicación entre dos computadores desde cualquier parte del mundo. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio.

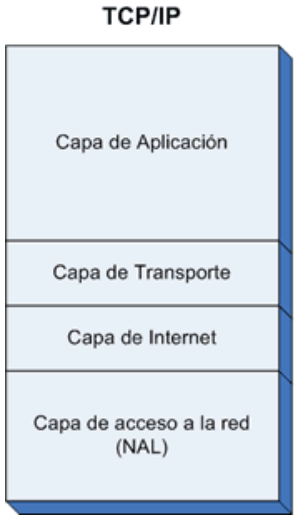



**Figura 1.3** Arquitectura TCP/IP [4]

**Tabla 1.3** Descripción de las Capas del Modelo TCP/IP

| MODELO TCP/IP | | |
|---|---|---|
| **CAPAS** | **DESCRIPCIÓN** | **UNIDAD DE DATOS** |
| **CAPA DE ACCESO A LA RED** | Ofrece la capacidad de acceder a cualquier red física y brinda los recursos que se deben implementar para transmitir datos a través de la red. | Trama |
| **CAPA DE INTERNET** | Empaqueta los datos con la información de las direcciones origen y destino en datagramas IP y realiza el enrutamiento. | Paquete |
| **CAPA TRANSPORTE** | Permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. Maneja dos protocolos para el intercambio de información: TCP (Protocolo de Control de Transmisión) como protocolo confiable y UDP (Protocolo de datagrama de usuario) como protocolo no confiable. | Segmento |
| **CAPA DE APLICACIÓN** | Define los protocolos de aplicación TCP/IP (HTTP, FTP, TELNET, entre otros) y proporciona al usuario la interfaz que interactúa con el sistema operativo. | Dato |

[4] Fuente: http://www.textoscientificos.com/redes/tcp-ip

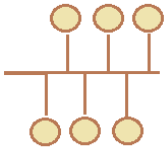
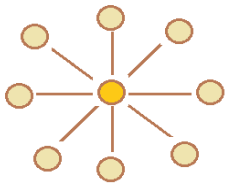
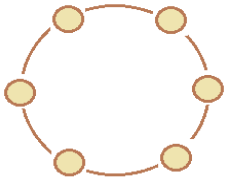
## 1.3 REDES DE ÁREA LOCAL

### 1.3.1 TOPOLOGÍAS LAN [6]

La topología de red es la manera como se interconecta cada nodo dentro de una red de manera física y lógica.

- **Topología física:** Es la disposición real de las máquinas, dispositivos de red y el cableado.
- **Topología lógica:** Es la forma en que las máquinas se comunican a través del medio físico.

**Tabla 1.4** Tipos de Topologías Lógicas y Físicas

| TOPOLOGÍAS | | |
|---|---|---|
| **TIPOS** | **DESCRIPCIÓN** | **Ilustración** |
| **Topología en bus** | Todos los hosts se conectan directamente a un cable principal, lo que ocasiona problemas de tráfico, además un posible corte en el cable interrumpiría todas las transmisiones. |  |
| **Topología en estrella** | Todos los hosts se conectan con un nodo central, el mismo que construye una red punto a punto. Si un host secundario falla la red sigue funcionando, pero si falla el nodo central las transmisiones son interrumpidas. |  |
| **Topología en anillo** | Los nodos se conectan punto a punto formando un anillo físico, la información pasa por cada repetidor hasta llegar al nodo deseado por lo que no existe problemas por la congestión de tráfico, pero si hay una rotura de un enlace, se produciría un fallo general en la red. |  |

### 1.3.2 ARQUITECTURAS LAN MÁS UTILIZADAS

#### 1.3.2.1 Ethernet /IEEE 802.3 [7]

La norma IEEE 802.3 basada en Ethernet define un modelo de red de área local utilizando el protocolo de Acceso Múltiple por Detección de Portadora y Detección de Colisiones (CSMA/CD), donde las estaciones escuchan permanentemente el canal y cuando lo encuentran libre de señal efectúan sus transmisiones inmediatamente. Esto puede llevar a una colisión que hará que las estaciones suspendan sus transmisiones, esperen un tiempo aleatorio y vuelvan a intentarlo.

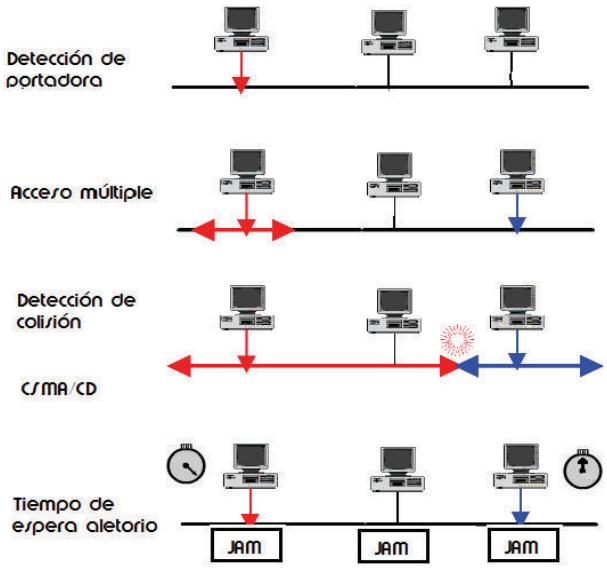



**Figura 1.4** Método de acceso al medio CSMA/CD [5]

En el nivel físico, las redes IEEE 802.3 utilizan codificación Manchester, donde cada período de un bit se divide en dos intervalos iguales. Un bit binario de valor 1 se transmite con valor de tensión alto en el primer intervalo y un valor bajo en el segundo. Un bit 0 se envía al contrario, es decir, una tensión baja seguida de un nivel de tensión alto.

---

[5] Fuente: http://mynewswire.tk/news/csma-cd.html

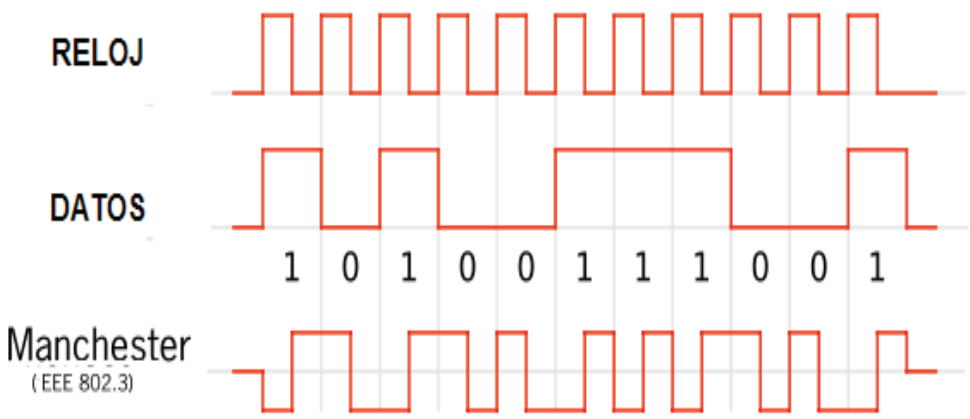



**Figura 1.5** Codificación Manchester [6]

#### 1.3.2.2 Token Ring/802.5 [7]

La norma IEEE 802.5 define una red con topología lógica de anillo con método de paso de testigo como control de acceso al medio. Su funcionamiento consiste en que el testigo circula por la red, cuando alguna estación desea transmitir captura el testigo y envía la trama; cada estación recibe la trama y verifica si la dirección destino coincide con la propia, de no ser así la ignora y la pasa a su vecino, solo la estación destino copia la trama para ser procesada, cambia el bit de copiado a 1 y la devuelve al anillo para que sea retirada por la estación origen.

### 1.3.3 TIPOS DE LAN

#### 1.3.3.1 LAN Inalámbricas [8]

Las redes de Área Local Inalámbrica (WLAN), permiten que los dispositivos con tecnología WIFI que se encuentren dentro del área de cobertura puedan conectarse entre sí, sin necesidad de estar cableados, ya que utilizan ondas de radio para acceder a los servicios de red, esto proporciona comodidad y movilidad a los usuarios.

---

[6] Fuente: https://comunication2011jeff.wordpress.com/2011/01/27/codigo-manchester/

### 1.3.3.2 LAN Virtuales [9]

Una red de área local virtual (VLAN) permite que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica, que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Mediante las VLAN, se puede segmentar de manera lógica las redes conmutadas basadas en equipos de proyectos, funciones o departamentos.

Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. El switch es el encargado de habilitar las VLANs y asignarlas a cada puerto.

#### *1.3.3.2.1 Tipos de VLAN [3]*

Se puede definir las VLAN en función del tipo de tráfico de red o en base a la función específica que desempeña la VLAN.

**Tabla 1.5** Tipos de VLAN

| TIPOS DE VLANs | |
|---|---|
| **VLANs** | **DESCRIPCIÓN** |
| **VLAN de datos (VLAN de usuario)** | Configurada para enviar solo tráfico de datos generado por el usuario. Es una práctica común separar el tráfico de voz de la administración del tráfico de datos. |
| **VLAN predeterminada** | Todos los puertos del switch arrancan siendo miembros de la VLAN predeterminada, la misma que tiene todas las características de cualquier VLAN, excepto que no se la puede volver a denominar ni eliminar. En los switches Cisco lleva el nombre de VLAN 1. |
| **VLAN nativa** | Una VLAN nativa está asignada a un puerto troncal 802.1Q, el cual admite el tráfico que llega de las diferentes VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). |
| **VLAN de administración** | Es cualquier VLAN que se configura para acceder a las capacidades de administración del switch. |
| **VLAN de voz** | VLAN destinada a la administración del tráfico de voz sobre IP (VoIP). |

### 1.3.3.3 WAN [10][11]

Una WAN es una red que permite transportar voz, datos y vídeo entre dos sitios geográficamente distantes. Se pueden identificar las siguientes partes principales:

- **CPE (Equipo Terminal de Abonado):** Equipo ubicado en el lado del usuario (tanto propio como arrendado en caso de servicio WAN contratado).
- **Demarcación:** Fin del CPE e inicio del Loop Local.
- **Loop Local:** Enlace (cableado o no cableado) desde la demarcación hasta el punto de presencia del servicio WAN (CO, Oficina Central)
- **Punto de Presencia:** Es el punto (Switch) de la Oficina central más cercano donde se tiene el servicio WAN.

Las operaciones de una WAN se centran principalmente en las capas física y enlace del modelo OSI.

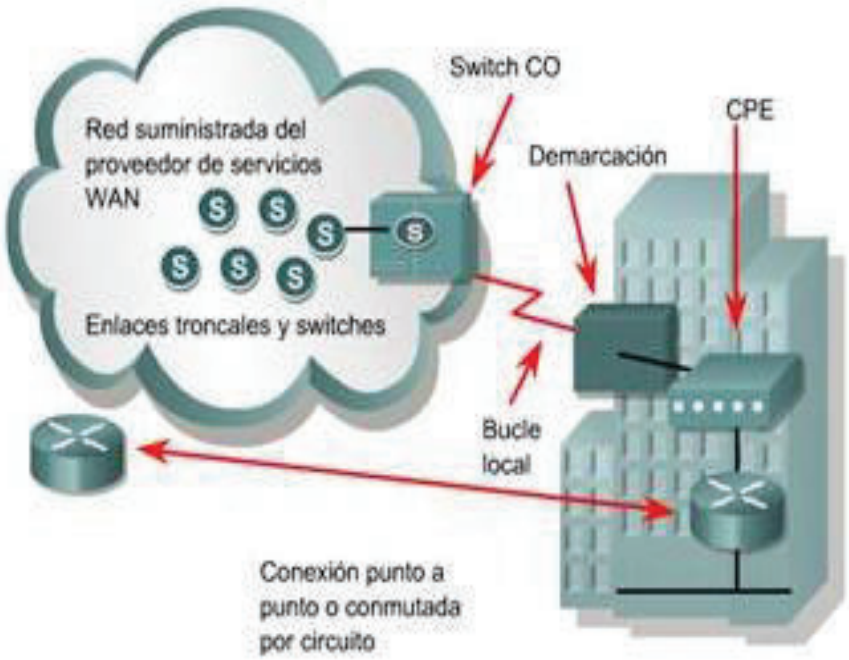



**Figura 1.6** Partes principales de una WAN [7]

[7] Fuente: Cisco Networking Academy CCNA Exploration v4.0. (2008)

## 1.4 FUNDAMENTOS DE CABLEADO ESTRUCTURADO [12]

El cableado estructurado consiste en una serie de pasos y normativas para hacer una red de telecomunicaciones lo más funcional posible y que interconecte equipos activos, de diferentes o igual tecnología, permitiendo la integración de los diferentes servicios que dependen del tendido de cables, como: datos, telefonía, control de acceso, etc., y a su vez proporcionar una conexión física entre todas las zonas de trabajo de una edificación.

El objetivo fundamental del sistema de cableado estructurado es el de cubrir los requerimientos de los usuarios durante la vida útil del edificio sin necesidad de realizar más tendido de cables.

### 1.4.1 SUBSISTEMAS DE CABLEADO ESTRUCTURADO [13]

Hay siete subsistemas relacionados con el sistema de cableado estructurado, como se ve en la Figura 1.7. Cada subsistema realiza funciones determinadas para proveer servicios de datos y voz:

- Área de trabajo.
- Cableado de distribución, también conocido como cableado horizontal.
- Sala de telecomunicaciones.
- Cableado backbone, también conocido como cableado vertical.
- Sala de equipamiento.
- Entrada de facilidades.
- Administración.

### 1.4.2 ESTÁNDARES DE CABLEADO ESTRUCTURADO [14]

La Asociación de Industrias de Telecomunicaciones (TIA) está acreditada por el Instituto Nacional Americano de Normalización (ANSI) para desarrollar estándares referentes a las tecnologías de información y comunicación (TIC),entre las directrices

que desarrollan están las concernientes a: torres celulares, terminales de datos, dispositivos de voz sobre IP, cableado estructurado, centros de datos, entre otros.

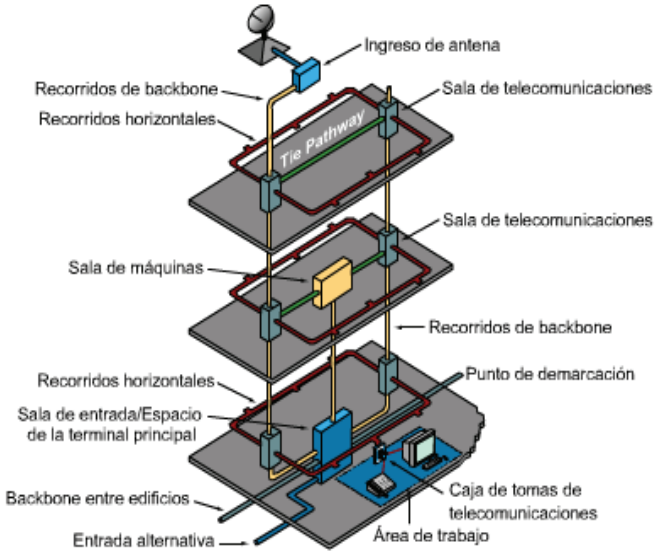



**Figura 1.7** Subsistema de Cableado Estructurado [8]

| | |
|---|---|
| ANSI/TIA 568-C.0 | Cableado de telecomuicaciones genérico para clientes |
| ANSI/TIA 568-C.1 | Cableado de telecomunicaciones para edificios comerciales |
| ANSI/TIA 568-C.2 | Componentes de cableado de par trenzado |
| ANSI/TIA 568-C.3 | Componentes de cableado de fibra óptica |
| ANSI/TIA 568-C.4 | Componentes de cableado coaxial |
| TIA 569-B | Rutas y espacios de telecomunicaciones |
| ANSI/TIA 606-A | Estándar de administración de infraestructura de telecomunicaciones para edificios comerciales |
| ANSI/TIA 607-A | Sistema de puesta a tierra de la infraestructura de telecomunicaciones |

**Figura 1.8** Estándares de Cableado Estructurado [9]

[8] Fuente: Programa de la Academia de Networking de Cisco CCNA 1 v3.1. (2003)

Los estándares mencionados en la Figura 1.8 se dividen en estándares comunes, de instalación y de componentes.

**Estándares Comunes**

- ✓ **ANSI/TIA 568-C.0:** Define la infraestructura general del cableado, además incluye requisitos de instalación y pruebas de campo.
- ✓ **TIA-569-B:** Estándar para recorridos y espacios de telecomunicaciones en edificios comerciales, especifica las prácticas de diseño y construcción dentro y entre los mismos.
- ✓ **ANSI/TIA-606-A:** Estándar de administración para la infraestructura de telecomunicaciones de edificios comerciales incluye especificaciones para la rotulación del cableado. También describe los requisitos de registro y mantenimiento de la documentación para la administración de la red.
- ✓ **ANSI/TIA-607-A:** Estándar sobre requisitos de conexión a tierra de telecomunicaciones para edificios comerciales, admiten un entorno de varios proveedores y productos diferentes, especifica los puntos exactos de interfaz entre el sistema de conexión a tierra y los equipos de telecomunicaciones.

**Estándares de instalación**

- ✓ **ANSI/TIA-568-C.1:** Contiene requisitos que facilitan la planificación y la instalación de un sistema de cableado estructurado en un entorno de edificios comerciales.

**Estándares de componentes**

- ✓ **ANSI/TIA-568-C.2:** Especifica los componentes de cableado, transmisión, modelos de sistemas y los procedimientos de medición necesarios para la verificación del cableado de par trenzado.
- ✓ **ANSI/TIA-568-C.3:** Especifica los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica.

---

[9] Fuente: http://www.origenseguridad.com.mx/

- ✓ **ANSI/TIA-568-C.4:** Especifica los requisitos y recomendaciones para cableado coaxial de banda ancha y el hardware de conexión que se utiliza para soportar la televisión por cable (CATV).

## 1.5 EQUIPOS DE CONECTIVIDAD

**Tabla 1.6** Equipos de conectividad

| EQUIPOS DE CONECTIVIDAD | | |
|---|---|---|
| **EQUIPOS DE CONECTIVIDAD** | **DESCRIPCIÓN** | **GRÁFICO** |
| **BRIDGE**[10] | Es un dispositivo de interconexión de red que opera en la capa de enlace, formando una sola subred y permite conexión entre equipos sin necesidad de routers. |  |
| **GATEWAY** | Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. |  |
| **SWITCH**[11] | Trabaja en la capa 2, 3 y 4 del modelo OSI, distribuye los datos a cada máquina de destino y elimina las eventuales colisiones de paquetes. Las funciones son iguales que el dispositivo Bridge, pero pueden interconectar o filtrar la información entre más de dos redes. |  |
| **ROUTER** [12] | Trabaja en la capa de red del modelo OSI, su principal función es la de enviar y enrutar paquetes de datos de una red a otra, siempre buscando el mejor camino para llegar al destino. |  |

[10] WIKIPEDIA. (s.f.). PUENTE DE RED. Recuperado el 20 de Marzo de 2013, de http://es.wikipedia.org/wiki/Puente_de_red

[11] KIOSKEA. (s.f.). REDES - CONCENTRADOR (HUB), CONMUTADOR (SWITCH) Y ROUTER. Recuperado el 20 de Marzo de 2013, de http://es.kioskea.net/faq/656-redes-concentrador-hub-conmutador-switch-y-router

[12] KIOSKEA. (s.f.). REDES - CONCENTRADOR (HUB), CONMUTADOR (SWITCH) Y ROUTER. Recuperado el 20 de Marzo de 2013, de http://es.kioskea.net/faq/656-redes-concentrador-hub-conmutador-switch-y-router

| | | |
|---|---|---|
| **ACCESS POINT**[13] | Son dispositivos de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica y transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. |  |

## 1.6 SERVICIOS DE LA INTRANET

### 1.6.1 FTP, FILE TRANSFER PROTOCOL

El servicio FTP permite la transferencia de archivos entre ordenadores (local y remoto) conectados a la red. Al utilizar esta aplicación se facilita el intercambio de archivos y se evita problemas como:

- Incompatibilidad de sintaxis
- Formas diferentes de buscar archivos en un directorio.
- Restricciones de acceso a los archivos.

La información que viaja desde el servidor FTP al cliente se lo denomina *descarga* y la que viaja desde el cliente al servidor FTP se lo denomina *carga*; previo a la realización de estas acciones existe un proceso de identificación por parte del cliente con un nombre de usuario y una contraseña.

#### 1.6.1.1 Servidores FTP

Es el software que se encarga de proporcionar el servicio de transferencia de archivos y controlan el acceso de los usuarios a las diferentes carpetas, en su gran mayoría utiliza el lenguaje de programación Unix/Linux.

---

13 Wikipedia. (s.f.). Punto de acceso inalámbrico. Recuperado el 10 de octubre de 2015, de https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico

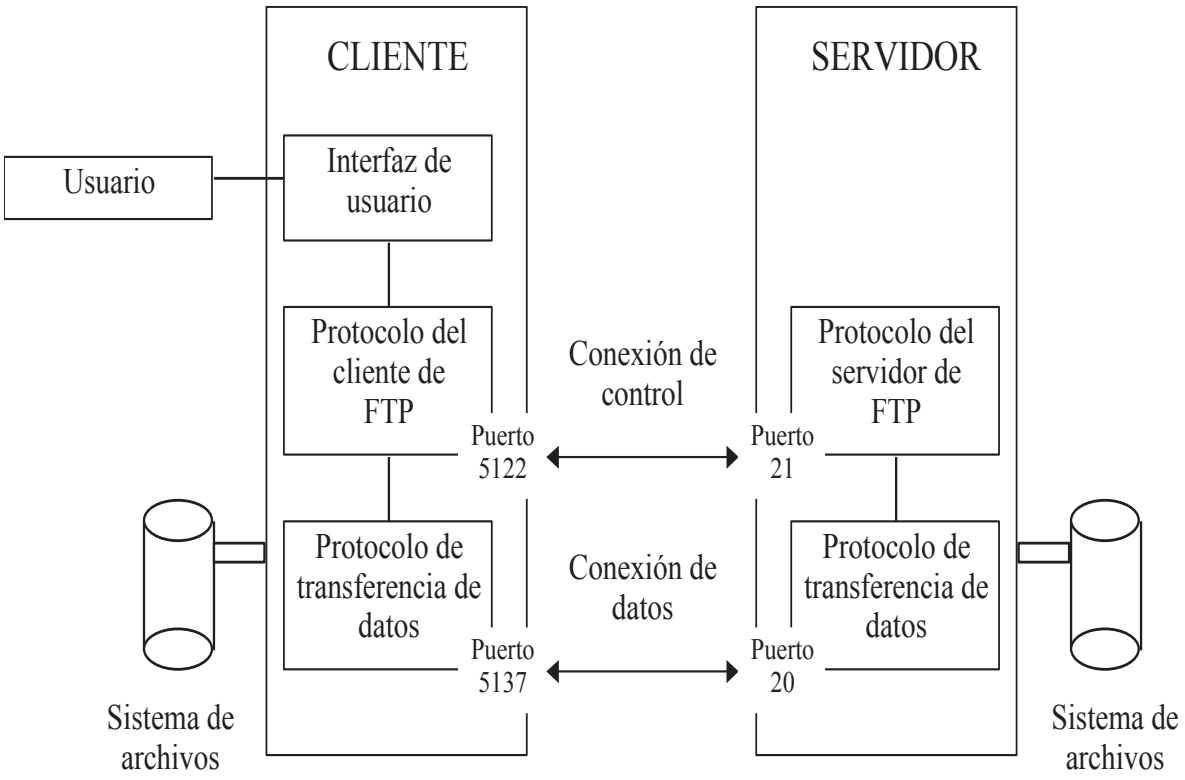



**Figura 1.9** Esquema del funcionamiento de FTP [14]

### 1.6.1.2 Clientes FTP

El acceso a los servidores FTP se realiza a través de programas cliente específico para FTP, los cuales permiten la transferencia de archivos de gran volumen entre el computador y el servidor remoto.

### 1.6.2 DNS - DOMAIN NAME SYSTEM

Este protocolo permite traducir un nombre de dominio (ej. www.google.com ) a una dirección IP (ej.173.194.75.103), lo que facilita al usuario realizar la búsqueda de un determinado servidor en la red.

[14] Fuente: www.informatica.uv.es/it3guia/ARS/apuntes/aplicacion2.rtf

#### 1.6.2.1 Tipos de Servidores DNS

- **Primarios o maestros**: En este tipo de servidores se encuentran guardados los nombres de dominio con su respectiva dirección IP.
- **Secundarios o esclavos:** Estos servidores obtienen los datos a través de una consulta a un servidor primario.
- **Locales o caché:** Almacenan de manera temporal las traducciones realizadas anteriormente, por tal motivo se consigue la respuesta en menor tiempo y sin consumir recursos innecesarios.

#### 1.6.2.2 Consultas DNS

Existen tres tipos de resolución de nombres:

- **Iterativa:** El servidor consultado busca en sus archivos la respuesta, si no la tiene, realiza peticiones iterativamente a los diferentes servidores de la jerarquía a la que pertenece el dominio solicitado.
- **Recursiva:** El servidor consultado está obligado a responder, quiere decir, que realiza consultas recursivas a diferentes servidores DNS hasta encontrar la mejor respuesta.
- **Inversa:** Este tipo de resolución parte de la dirección IP para encontrar el nombre de dominio asociado a la misma.

### 1.6.3 DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL

Permite asignar direcciones IP y otras configuraciones de manera dinámica a los host de una red por un intervalo de tiempo determinado. Su utilidad se presenta en redes con un gran número de equipos, en la cual la asignación de direcciones estáticas implica tiempo y costos.

Los parámetros comunes que un servidor DHCP asigna a un cliente son:

- Dirección IP
- Máscara de subred
- Puerta de enlace
- DNS

#### 1.6.3.1 Asignación DHCP

Existen 3 modos de asignación de direcciones IP:

- **Asignación manual:** El administrador configura de forma manual las direcciones IP del cliente en el servidor DCHP.
- **Asignación automática:** Al cliente DHCP se le asigna una dirección IP aleatoria cuando se conecta por primera vez con el servidor DHCP.
- **Asignación dinámica:** El servidor DHCP asigna una dirección IP a un cliente de forma temporal.

### 1.6.4 PROXY

El servidor proxy actúa como un intermediario entre la intranet y la extranet, permitiendo registrar y bloquear ciertas acciones que llevan a cabo los usuarios de la red corporativa.

- *Actúa como firewall y filtro de contenidos.-* Es usado por el administrador de red para desactivar o filtrar el acceso a páginas ajenas a las actividades corporativas.
- *Mejora el rendimiento.-* Permite guardar en su memoria las páginas web que se utilizan con frecuencia, de esta manera cuando un usuario solicite dicha información, en vez de ir hasta un servidor externo se envía el contenido almacenado en el servidor proxy.

### 1.6.5 SERVIDOR WEB

Los servidores web son aquellos cuya tarea es alojar sitios y/o aplicaciones, las cuales son accedidas por los clientes utilizando un navegador que se comunica con el servidor utilizando el protocolo HTTP (hypertext markup language).

Almacena principalmente documentos HTML (son documentos a modo de archivos con un formato especial para la visualización de páginas web en los navegadores de los clientes), imágenes, videos, texto, presentaciones, y en general todo tipo de información.

### 1.6.6 VOIP

Es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional, como las redes PSTN (Public Switched Telephone Network, red telefónica pública conmutada).

### 1.6.7 PROTOCOLOS DE CORREO ELECTRÓNICO

#### 1.6.7.1 SMTP - Simple Mail Transfer Protocol

Protocolo de la capa aplicación basado en el modelo cliente/servidor, que se utiliza para el intercambio de mensajes. Un cliente SMTP se conecta con el servidor SMTP del host destino y le entrega de forma directa el correo electrónico.

#### 1.6.7.2 POP3 - Post Office Protocol

Protocolo utilizado para recuperar los mensajes guardados, el cliente se conecta con el servidor SMTP, descarga los mensajes y los almacena en el computador del

destinatario borrándolos del servidor, permitiendo visualizarlos posteriormente sin necesidad de establecer conexión.

### 1.6.7.3 IMAP - Internet Message Access Protocol

Protocolo de la capa aplicación que permite visualizar los mensajes que se encuentran en el servidor SMTP de manera remota, sin necesidad de descargarlos. La principal ventaja sobre POP3 radica en la posibilidad de acceder al contenido del correo desde cualquier computador únicamente estableciendo conexión con el servidor.

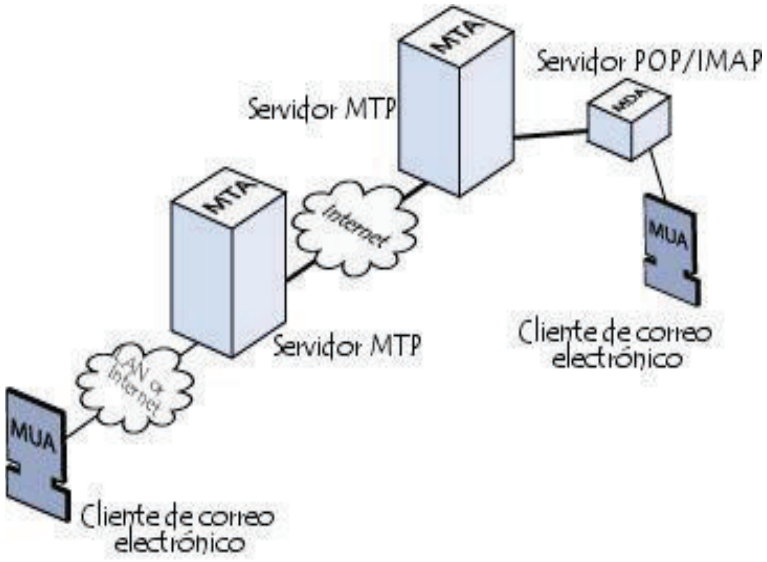



**Figura 1.10** Esquema de funcionamiento del correo electrónico. [15]

## 1.7 SEGURIDAD EN LA RED [2]

En sus inicios las redes de computadoras eran utilizadas por universidades para el intercambio de información (correo electrónico) y a nivel corporativo para la compartición de impresoras, por tal motivo la seguridad quedaba en segundo plano. En la actualidad los múltiples servicios que se prestan a través de las redes

[15] Fuente:http://es.kioskea.net/contents/courrier-electronique/fonctionnement-mta-mua

(servicios bancarios, compras online, homeworkers) dan como resultado que existan ataques a la integridad de las transacciones online. Al viajar la información a través de diferentes medios (cableado e inalámbrico) vuelven vulnerable la confidencialidad de la misma, por tal razón en los últimos años se han encontrado formas de prevenir los ataques a las redes corporativas.

Existen dos tipos de atacantes, los activos son aquellos que provocan daños y modificaciones al funcionamiento normal de la red y los pasivos que no producen ninguna alteración, pero que sin embargo, utilizan la información capturada de manera fraudulenta. Por tal razón la protección de los elementos se debe trabajar en tres ejes fundamentales:

- **Prevención:** Se debe tomar medidas que eviten que la información sea modificada, dañada o hurtada.
- **Detección:** Se debe tomar acciones que permitan identificar cuándo, cómo, dónde y quién dañó un determinado elemento.
- **Reacción:** La capacidad de tomar medidas correctivas una vez ocurrido un ataque a la seguridad de la red.

Para proporcionar la seguridad adecuada a una red de datos es necesario enfocarse en los siguientes servicios:

- **Confidencialidad:** Asegurar que únicamente la persona autorizada tendrá acceso a la información (cifrado/descifrado, privacidad).
- **Integridad:** Asegurar que los datos son correctos, que no han sido modificados en el trayecto del origen al destino (firma digital, intercambio de autenticación).
- **Disponibilidad:** Asegurar que una entidad pueda acceder cuando desea a un recurso o servicio para el que está autorizado (servidores espejo, replicación de datos, enlaces redundantes).

- **Autenticación:** Asegurarse de que la entidad es quien dice ser mediante la identificación, para de esta manera aseverar que las transacciones se efectúan entre entidades legítimas (contraseñas, certificados, biométricos).

### 1.7.1 POLÍTICAS DE SEGURIDAD

Son reglas que se establecen en cada institución (corporación, empresa, organización) para el correcto funcionamiento de la red de datos; son difundidas por las autoridades de manera verbal o escrita y se enfocan en aspectos de infraestructura, procesos y personal. Para tal efecto existen varias técnicas de seguridad:

- Soluciones tecnológicas (equipos)
- Políticas, estándares, normas de servicio
- Planes de contingencia
- Control de calidad (Hacking ético)
- Administración de riesgos

El modelo de seguridad que se desarrollará es el control de calidad a través del hacking ético para determinar las vulnerabilidades existentes en la red actual de la Administración Zonal Norte “Eugenio Espejo” y determinar así las nuevas políticas de seguridad a implementar.

### 1.7.2 HACKING ÉTICO [15]

Hace algún tiempo, los procesos informáticos y lo que implicaban no eran sometidos a ningún tipo de estudio, los administradores y técnicos eran los encargados de realizar pruebas para encontrar posibles agujeros en la seguridad. Este tipo de dificultades presentes en los procesos dieron como resultado la aparición de hackers, personas que tomaban como retos intelectuales corromper la seguridad de los sistemas, descifrar contraseñas y causar daños a la integridad de la información.

En la actualidad, la palabra hacker no se encuentra relacionada únicamente con un delito, sino a la capacidad de encontrar fallos en la seguridad de los sistemas para proporcionar una solución; de esta manera aparece el hacking ético, que no es más que un método basado en el ataque deliberado a los sistemas para encontrar vulnerabilidades en la seguridad para posteriormente corregirlos e impedir que un atacante malicioso cause daños graves a los sistemas informáticos de la organización.

#### 1.7.2.1 Técnicas de vulneración de la seguridad de sitios web

##### *1.7.2.1.1 Enumeration*

Es el proceso de conseguir las cuentas de usuario y vulnerabilidades, como recursos compartidos de la red, grupos, detalles de cuentas y aplicaciones. La enumeración implica conexiones activas a sistemas y consultas directas.

Algunas herramientas orientadas a este propósito son:

- **Net Bios Null Sessions:** Aprovecha un defecto en los protocolos CIFS/SMB (Common Internet File System/Server Messaging Block).
- **Enumeración de Active Directory:** Todos los usuarios y grupos pueden ser obtenidos mediante una simple consulta LDAP, únicamente se debe crear una sesión autenticada vía LDAP.
- **Orientación Border Gateway Protocol:** BGP es utilizado por los routers para ayudarlos a guiar los paquetes a sus destinos, por esta razón lo puede utilizar para encontrar todas las redes asociadas con una empresa en particular.

##### *1.7.2.1.2 SQL Injection*

Consiste en un ataque que se realiza en las aplicaciones web contra la base de datos debido a una falta de filtrado en las consultas. Principalmente se orienta a

vulnerar el proceso de validación de las entradas a los sistemas, mediante artificios que burlan la lógica de las consultas en SQL.

La vulnerabilidad se produce cuando un programa arma inadvertidamente una sentencia SQL en tiempo de ejecución, o durante la fase de desarrollo, cuando el programador inesperadamente ejecuta la sentencia SQL en forma desprotegida. Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podrá realizar cambios, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar otro tipo de código malicioso en el ordenador.

#### *1.7.2.1.3 XSS - Cross Site Scripting*

Esta técnica consiste en inyectar código Java Script o similar (VBScript) en una aplicación web sin que éste deba apegarse a las políticas del sitio web. XSS es un vector de ataque que puede ser utilizado para robar información delicada, secuestrar sesiones de usuario, y comprometer el navegador, quebrantando la integridad del sistema.

Formas en las que se presenta XSS:

- ***Directa o Persistente****:* Consiste en embeber código HTML peligroso en sitios web que lo permitan; incluyendo etiquetas como <script> o <iframe>.
- ***Indirecta o Reflejada:*** Consiste en modificar valores que la aplicación web utiliza para pasar variables entre dos páginas sin iniciar sesiones, y ocurre cuando existe una ruta URL del navegador o cualquier otra cabecera HTTP.

#### *1.7.2.1.4 Session Hijacking*

Hace referencia a la posibilidad de duplicar las credenciales de autorización en una comunicación válida ya establecida entre un servidor y un cliente, para obtener el acceso a la información y los servicios.

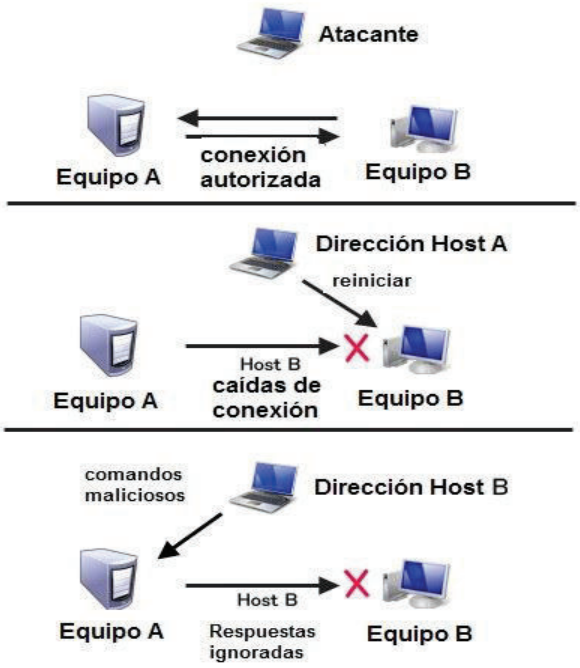



**Figura 1.11** Esquema de funcionamiento session hijacking. [16]

#### *1.7.2.1.5 Ingeniería Social*

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.

Con respecto a la seguridad informática, esta técnica permite obtener contraseñas y una serie de datos a través de las debilidades de las personas más no del software.

## 1.8 ADMINISTRACIÓN DE LA RED

La administración de la red se refiere a las actividades, métodos, procedimientos y herramientas requeridas para mantener en correcto funcionamiento los diferentes servicios que ofrece la red, asegurando de esta manera eficiencia y productividad

[16] Fuente: http://www.hackingloops.com/2011/04/session-hijacking

además de un total conocimiento por parte del administrador de todo lo que sucede dentro de la misma.

Mientras más grandes son las redes (gran número de usuarios y servicios) la complejidad es mayor, por tal razón es conveniente definir los equipos y usuarios que están autorizados para utilizar los servicios de la red, para este efecto se vuelve necesario contar con aplicaciones que permitan tener un completo mapeo de la red (equipos y sus direcciones IP), con el fin de identificar de manera rápida problemas y posibles intrusiones a los sistemas.

Las aplicaciones estándar que permiten administrar la red abarcan servicios, protocolos y bases de información de gestión, este es el caso de los sistemas de gestión de red que se definen como una colección de herramientas para monitoreo y control de las redes, cuyas características son:

- Una interfaz amigable que permite ejecutar un conjunto de comandos para monitorear todas las tareas de la red.
- Tener un completo conocimiento de los equipos que integran la red.

El protocolo de monitoreo de red que se utiliza para la gestión de dispositivos como switches, routers, servidores y estaciones de trabajo es el SNMP (Simple Network Managemente Protocol).

### 1.8.1 SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL

Protocolo utilizado para intercambiar información entre los dispositivos de la red, su principal objetivo es monitorizar y diagnosticar problemas de manera simple y efectiva.

El sistema de administración de red se basa en dos elementos principales: una entidad gestora y agentes. El gestor es la entidad que le permite al administrador realizar solicitudes de supervisión. Los agentes son entidades que se encuentran al nivel de cada interfaz, ellos conectan a la red los dispositivos administrados y permiten recopilar información de las MIB (Management Information Base) de los

diferentes objetos (equipos) además de informar de eventos suscitados inesperadamente a través de mensajes denominados Traps.

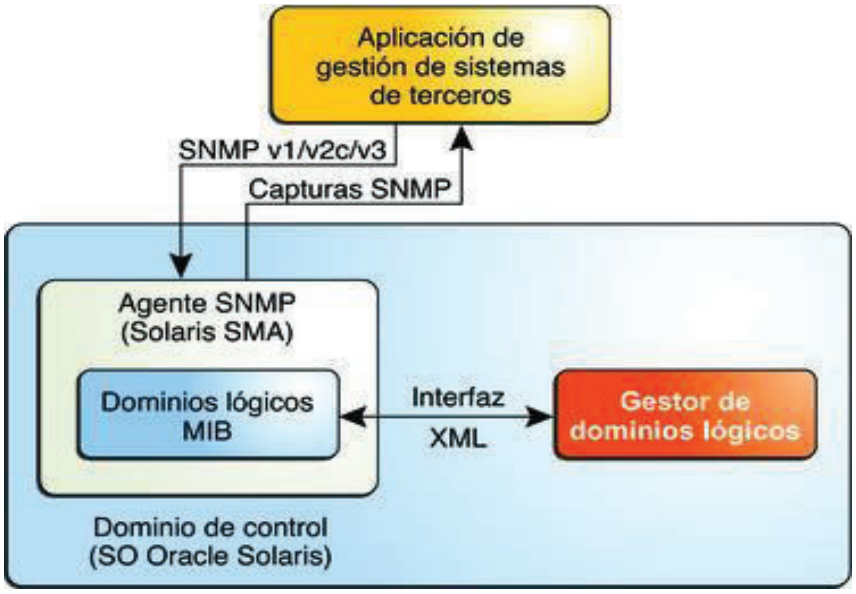



**Figura 1.12** Esquema de funcionamiento Protocolo SNMP [17]

Actualmente SNMP es un protocolo predominante para la gestión de dispositivos, por tal razón la mayoría de equipos de interconexión, enrutamiento y PC ofrecen paquetes de agentes para ser gestionados.

[17] Fuente: http://docs.oracle.com/cd/E38736_01/html/E37596/miboverview.html

# CAPÍTULO II

# ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE LA ADMINISTRACIÓN ZONAL NORTE Y DETERMINACIÓN DE REQUERIMIENTOS.

En este capítulo, se detallará la situación actual de la red de datos de la Administración Zonal Norte "Eugenio Espejo" (AZNEE) de forma física y lógica, así como también se procederá a identificar las vulnerabilidades existentes mediante técnicas de hacking ético, las cuales permitirán posteriormente implementar políticas de seguridad.

## 2.1 UBICACIÓN ACTUAL

La AZNEE está ubicada en la Av. Amazonas 4532 y Pereira del Distrito Metropolitano de Quito (Figura 2.1).

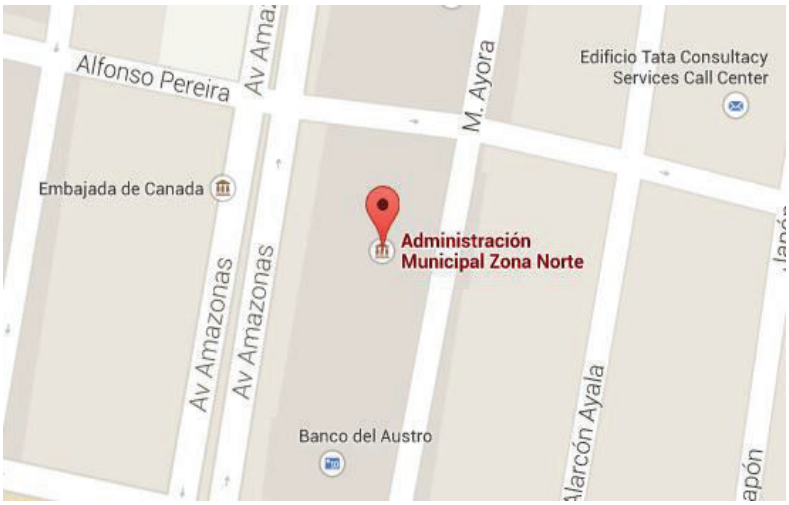



**Figura 2.1** Ubicación geográfica de la Administración Zonal Norte "Eugenio Espejo"[18]

[18] Fuente: https://maps.google. com.ec/

El objetivo de esta Institución es: "*Garantizar los derechos ciudadanos y el acceso a la cultura y al deporte. Planificar el desarrollo integral y garantizar la participación ciudadana. Garantizar la seguridad ciudadana. Establecer un sistema ágil y seguro de movilidad y transporte. Invertir en espacios públicos y obra pública. Rediseñar el gobierno metropolitano y fortalecer la formación - capacitación del servicio civil*."[19]

Su misión es "*Promover una ciudadanía y organización social activa que accede con equidad e inclusión al arte, la cultura, el deporte, la recreación a prácticas y saberes ancestrales, a las tecnologías de la comunicación, entre otros*".[20]

Obtenido del Proyecto de manual Orgánico MDMQ 2014, que se encuentra en el Anexo A.

## 2.2 ANTECEDENTES

El Municipio del Distrito Metropolitano de Quito se encuentra dividido en 8 administraciones zonales (Figura 2.2) para garantizar la descentralización de organismos institucionales y mejorar el sistema de gestión participativa.

Actualmente las administraciones zonales son:

1. Administración Zonal Eugenio Espejo (Norte)
2. Administración Zonal Equinoccio (La Delicia)
3. Administración Zonal Quitumbe
4. Administración Zonal Tumbaco
5. Administración Zonal Valle de los Chillos
6. Administración Zonal Calderón
7. Administración Zonal Manuela Sáenz (Centro)
8. Administración Zonal Eloy Alfaro (Sur)

[19] Documento del plan orgánico .- textual

[20] Página web de la institución.

### 2.2.1 ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO"

La Administración Zonal Norte "Eugenio Espejo" actualmente se encuentra a cargo del Arquitecto Fernando Mauricio Lara Jaramillo e incluye las siguientes parroquias: Concepción, Cochapamba, Kennedy, El Inca, Jipijapa, Belisario Quevedo, Rumipamba, Iñaquito, Mariscal Sucre, Nayón y Zámbiza (Figura 2.2)


**Figura 2.2** Administraciones Zonales del Distrito Metropolitano de Quito[21]

Las principales funciones que realiza esta institución son: [22]

- "*Planificar, organizar, ejecutar, controlar, fiscalizar y evaluar proyectos de desarrollo social, económico y territorial en la jurisdicción zonal integrando la participación ciudadana.*"

[21] Fuente: http://commons.wikimedia.org/wiki/

[22] Proyecto Manual Orgánico MDMQ 2014

- "*Administrar los recursos humanos, materiales, financieros y tecnológicos para una adecuada gestión en procura de la satisfacción de las necesidades de la comunidad de la zona*."
- "*Coordinar con las Secretarías, Direcciones y Empresas Metropolitanas las actividades que permitan mejorar el servicio, con entrega oportuna, de calidad y de alto valor agregado*."
- "*Adecuar y operativizar políticas, planes, programas y proyectos metropolitanos al ámbito local, en las diferentes áreas de intervención Municipal.*"

## 2.3 ORGANIGRAMA ESTRUCTURAL

Cada una de las administraciones zonales del Distrito Metropolitano de Quito tienen la siguiente estructura organizacional:

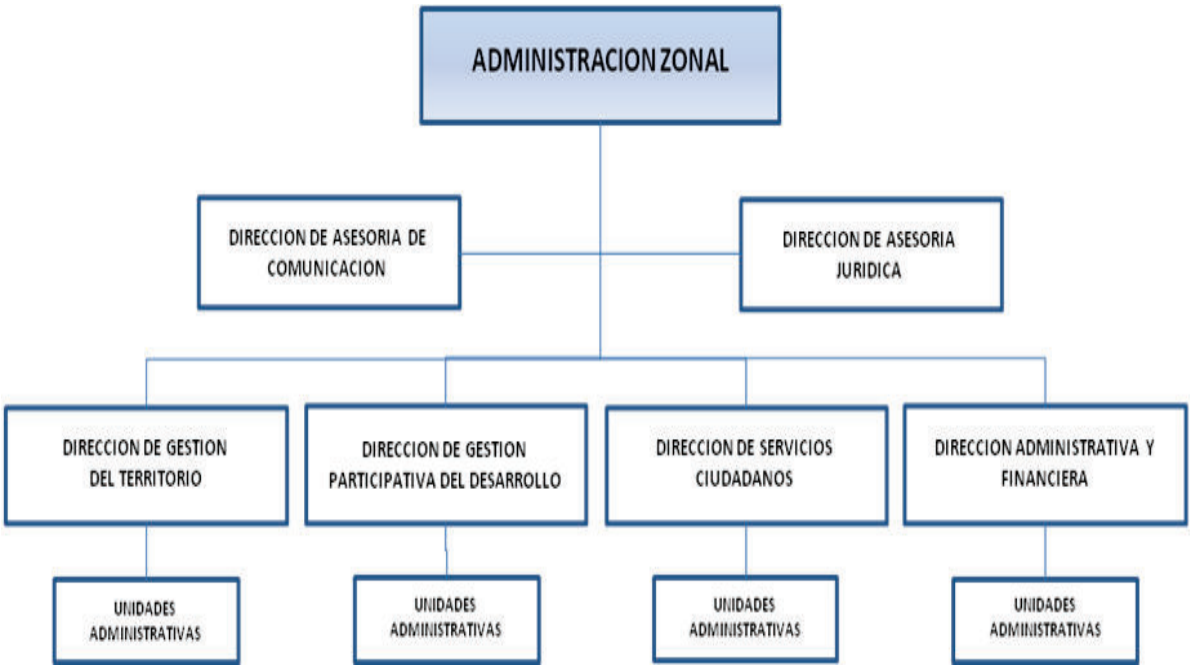



**Figura 2.3** Organigrama estructural de la AZNEE [23]

[23] Proyecto Manual Orgánico MDMQ 2014

# 2.4 SITUACIÓN ACTUAL DE LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO" (AZNEE)

## 2.4.1 DIAGRAMA DE LA RED DE DATOS ACTUAL

La AZNEE posee una infraestructura de red de datos y voz, la cual cuenta en su mayoría con equipos no administrables y con un sistema de cableado que no cumple con los estándares adecuados.

El cableado está constituido por cable UTP categoría 5e, el cual se encuentra en la mayoría de los departamentos por medio del techo del edificio, ya que al no contar con un techo falso estos cables van colocados en los tubos del primer piso y solo ciertos puntos que están colocados con canaletas para los biombos y mamparas que se usan para las áreas de trabajo.

Cuenta con 3 racks en donde se ubican los principales equipos que dan conectividad a la AZNEE, además de existir otros equipos secundarios distribuidos según la necesidad de extender los nuevos puntos para la red.

Debido al crecimiento de usuarios, la AZNEE cuenta con dos subredes: 172.20.5.0/24 y 172.20.112.0/24, las cuales están distribuidas indistintamente sin orden ni gestión. Hoy en día la subred 172.20.112.0/24 presenta problemas de compatibilidad con el antivirus, y solo ese utiliza el 15 % de las direcciones proporcionada por esta subred, según lo informado por el administrador del área de sistemas.

Sus principales servicios son: Correo electrónico, Página Web, Recursos de Impresión, Carpetas Compartidas, Proxy, Antivirus, Servidor de Réplica[24].

En la figura 2.4 se indica el diagrama actual de la red de datos de la AZNEE.

[24] Servidor de Réplica: Este servidor es administrado por la Administración General del Municipio del Distrito Metropolitano de Quito.

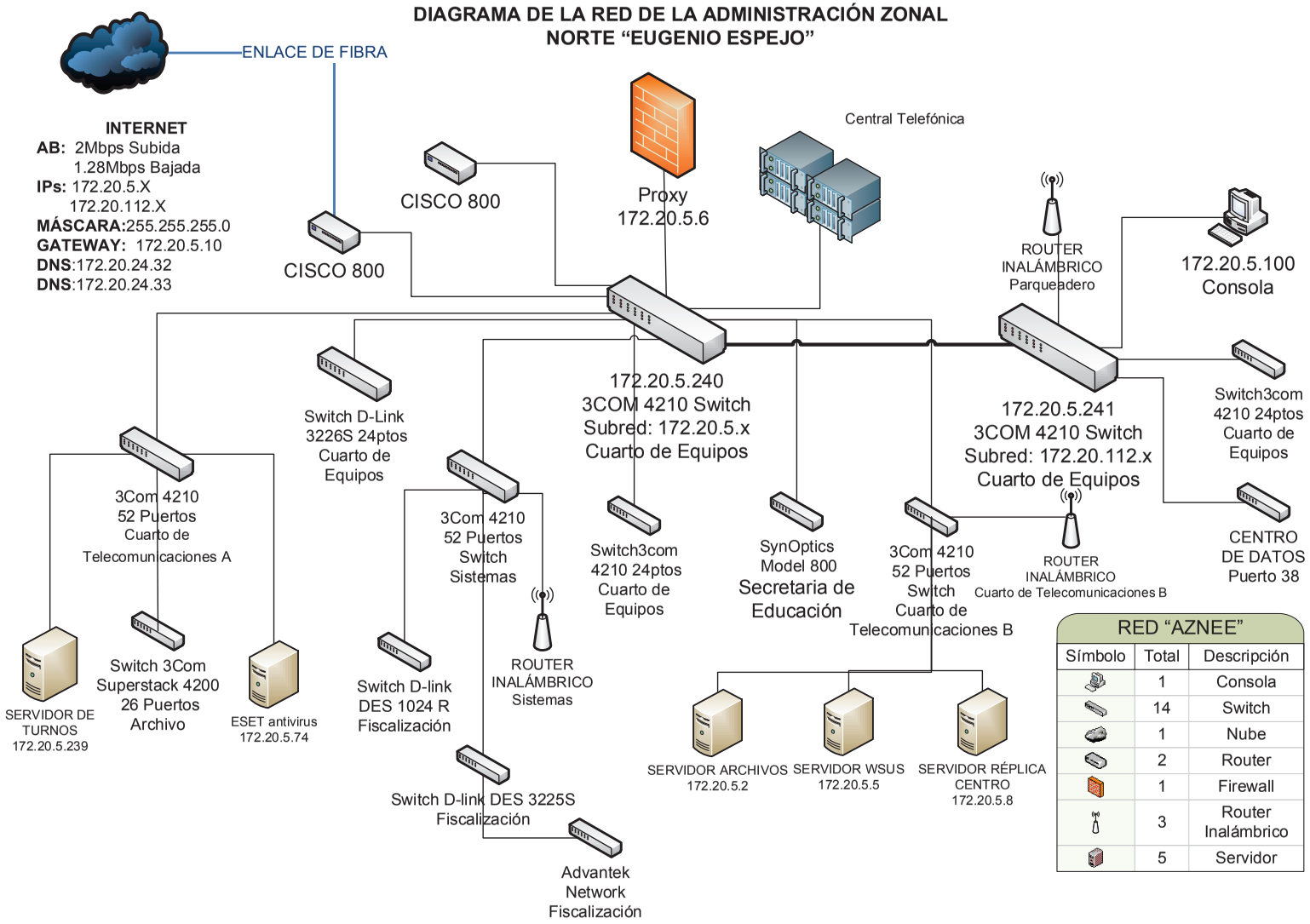



**Figura 2.4** Diagrama de la red de datos de AZNEE

### 2.4.2 SISTEMA DE CABLEADO ESTRUCTURADO

La AZNEE cuenta con un sistema de cableado de par trenzado categoría 5e, que trabaja a una velocidad de 100 Mbps, esta categoría se encuentra en declive debido a que existen aplicaciones que demandan altas prestaciones como por ejemplo, video y voz sobre IP que requieren mayor control de latencia y menores tasas de retransmisión de paquetes para garantizar la calidad del servicio.

Al realizar una inspección a las instalaciones de cableado estructurado de la AZNEE se pudo observar infracciones a los estándares que rigen este sistema.

A continuación se listan los problemas encontrados:

- Los cables no se encuentran enrutados adecuadamente, esto se puede observar en el segundo piso donde los cables cruzan por la estructura metálica perteneciente al techo de la institución. Por tal motivo existen puntos de presión en ciertos tramos, lo que provoca deformaciones en la geometría del cable ocasionando problemas de diafonía[25].
- Varios departamentos no cuentan con canaletas de piso, lo que provoca que el cable este expuesto a aplastamientos y posibles desconexiones, además se infringen los ángulos de curvatura permitidos para cables de cobre.
- Los cuartos de telecomunicaciones no presentan una apropiada organización, se puede observar que existen equipo activos que no se encuentran colocados en el rack por falta de espacio.
- Otro inconveniente encontrado es la ausencia de paneles de conexión entre el equipo activo y el punto de salida de datos, lo que conlleva a la violación del estándar ANSI/TIA 568.C.2.[26]

---

[25] Diafonía: Perturbación electromagnética producida en un canal de comunicación por el acoplamiento de este con otro.

[26] ANSI/TIA 568.C.2: Estándar de componentes y cableado de telecomunicaciones de par trenzado balanceado

La AZNEE cuenta con dos cuartos de telecomunicaciones y un cuarto de equipos como se indica en la tabla 2.1

**Tabla 2.1** Ubicación de las áreas de telecomunicaciones

| IDENTIFICACIÓN | UBICACIÓN |
|---|---|
| **Cuarto de telecomunicaciones A** | Departamento de sistemas. |
| **Cuarto de telecomunicaciones B** | Planta baja cerca del departamento de avalúos y catastros. |
| **Cuarto de equipos** | Cerca del parqueadero interno de la institución |

A continuación se presenta la tabla 2.2, y las figuras 2.5 y 2.6, con todos los puntos de red y localización de los diferentes cuartos de comunicación y un informe detallado del hardware y del software existente en la institución, para tal fin se dividió cada una de las plantas en bloques.

**Tabla 2.2** Descripción de puntos de red de la AZNEE

| BLOQUES | Número de Puntos Actuales | Impresoras de Red | Equipos fuera del cuarto de telecomunicaciones | Número de Racks | Observaciones |
|---|---|---|---|---|---|
| **PRIMER PISO BLOQUE 1** | 23 | 4 | 0 | 1 | Cuarto de Telecomunicaciones A |
| **PRIMER PISO BLOQUE 2** | 38 | 2 | 0 | 0 | Sin Cuarto de Telecomunicaciones |
| **PRIMER PISO BLOQUE 3** | 28 | 4 | 1 | 0 | Sin Cuarto de Telecomunicaciones |
| **PLANTA BAJA BLOQUE 1** | 34 | 5 | 1 | 2 | Cuarto de Telecomunicaciones B |
| **PLANTA BAJA BLOQUE 2** | 27 | 2 | 4 | 1 | Cuarto de Equipos |
| **TOTAL** | **150** | **17** | **6** | **4** | |

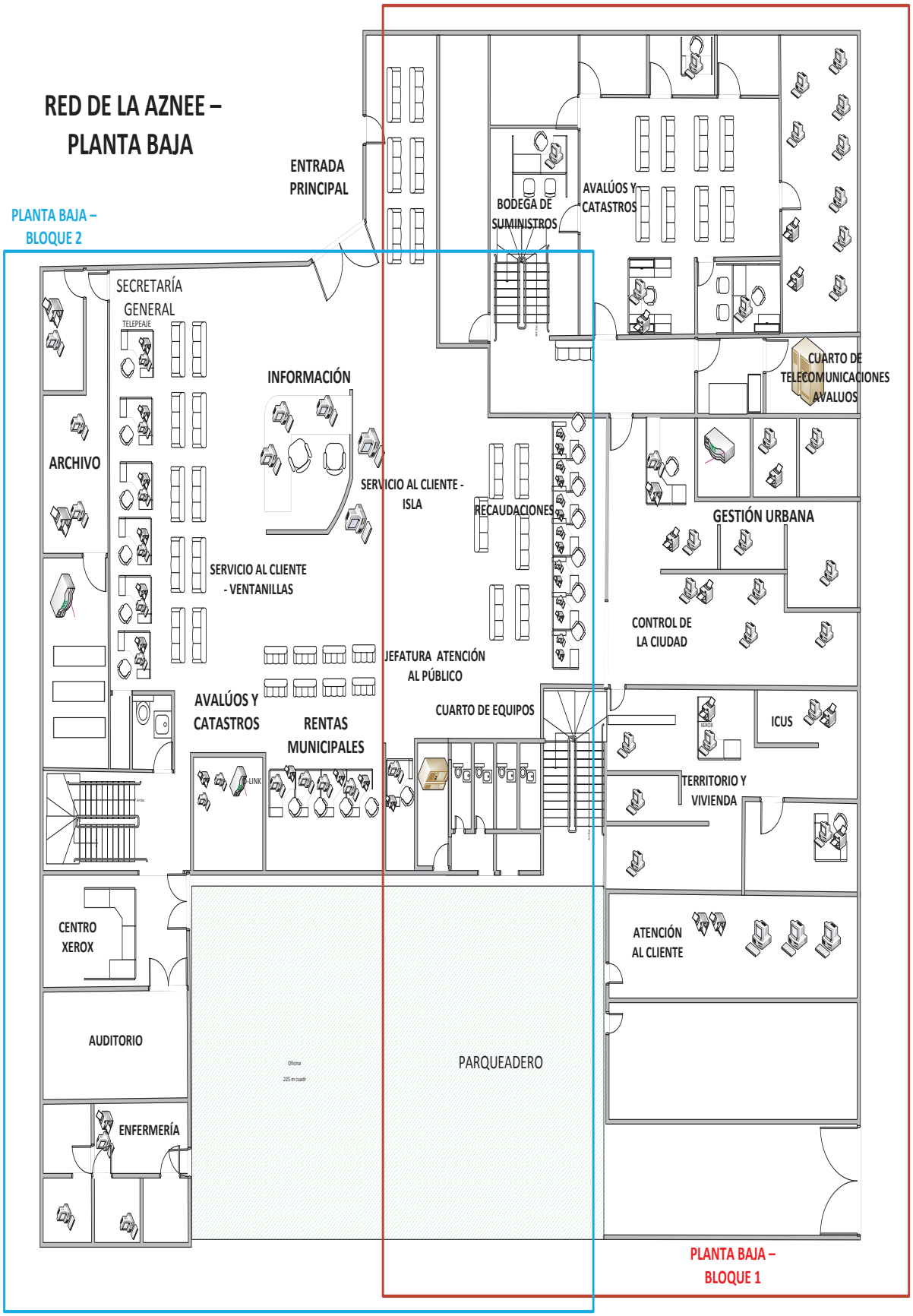



**Figura 2.5** Plano de la AZNEE – Planta Baja

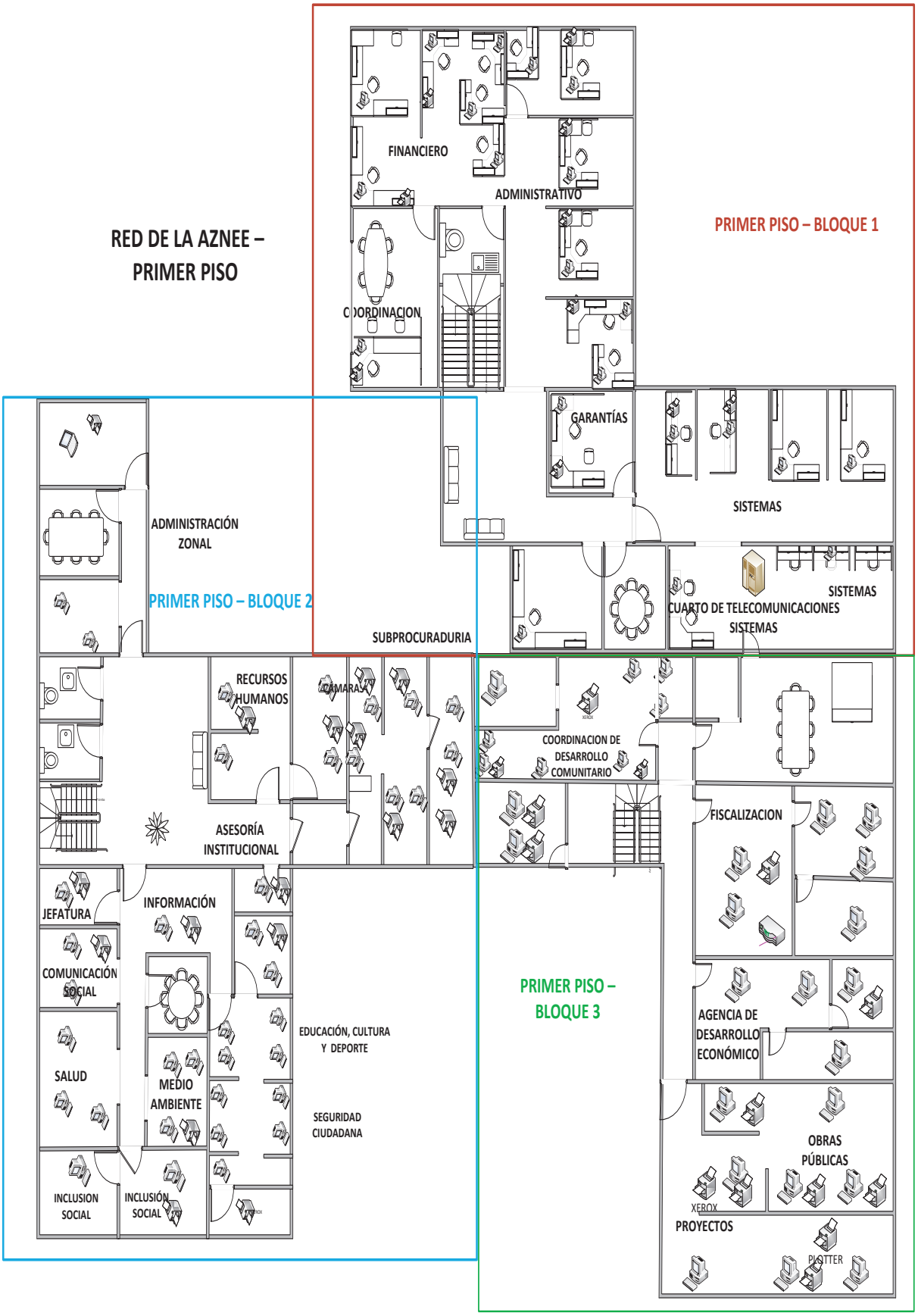



**Figura 2.6** Plano de la AZNEE – Primer Piso

### 2.4.2.1 Primer piso (Bloque 1)

#### *2.4.2.1.1 Descripción de la red*

En este bloque se encuentran los departamentos de Garantías, Sistemas, Administrativo, Financiero, Coordinación, Administración y Servicios (Anexo B). En el departamento de Sistemas se aloja el Cuarto de Telecomunicaciones A, el cual alberga los servidores de actualización de sistema operativo y el servidor de Antivirus ESET (Figura 2.7).


**Figura 2.7** Diagrama del Rack del Cuarto de Telecomunicaciones, Sistemas.

### 2.4.2.2 Primer piso (Bloque 2)

#### *2.4.2.2.1 Descripción de la red*

En este bloque se encuentran los departamentos de Información, Inclusión Social, Salud, Comunicación Social, Jefatura Atención Pública, Administración Zonal, Medio Ambiente, Seguridad Ciudadana, Educación Cultura y Deporte, Asesoría Institucional, Recursos Humanos y Subprocuraduría (Anexo B). Estos departamentos velan por el bienestar y la seguridad de los ciudadanos pertenecientes a su jurisdicción. En la Secretaría de Educación se encuentra ubicado un switch fuera de los racks principales (Figura 2.8).

| Marca | Tipo | Número de Equipos | Equipo |
|---|---|---|---|
| **SynOptis** | Switch 4210 | 1 |  |

**Figura 2.8** Descripción de equipos de red en el primer piso – bloque 2

### 2.4.2.3 Primer piso (Bloque 3)

#### *2.4.2.3.1 Descripción de la red*

En este bloque se encuentran los departamentos de Coordinación de desarrollo comunitario y participación ciudadana, Fiscalización, Agencia de desarrollo económico, Obras públicas y Proyectos (Anexo B). Aquí se concentran

departamentos claves para el desarrollo urbano de la zona norte. En el departamento de fiscalización se encuentra ubicado un switch fuera de los racks principales (Tabla 2.3).

**Tabla 2.3** Descripción de equipos de red en el primer piso – bloque 3

| Marca | Tipo | Número de equipos |
|---|---|---|
| D-link | DES 1024R | 1 |

#### 2.4.2.4 Planta baja (Bloque 1)

##### *2.4.2.4.1 Descripción de la red*

En este bloque se encuentran los departamentos de Avalúos y Catastros, Bodega de suministros, Gestión urbana, Recaudaciones, Control de la ciudad, Territorio y vivienda e ICUS[27] (Anexo B), además se ubica el cuarto de equipos C, mismo que cumple con todas las normas vigentes, y dos switches que se encuentran fuera del rack que están en el departamento de Gestión Urbana (Figura 2. 9).

#### 2.4.2.5 Planta baja (Bloque 2)

##### *2.4.2.5.1 Descripción de la red*

En este bloque se encuentran los departamentos de Enfermería, Auditorio, Archivo, Secretaria General, Avalúos y Catastros 2, Rentas Municipales, Jefatura Atención al Cliente, Servicio al Cliente en Ventanillas, Atención al Cliente e Información (Anexo B), además se ubica el cuarto de telecomunicaciones B, y cuenta con equipos fuera de este cuarto, ubicados en el Departamento de Archivo (Figura 2.10).

[27] ICUS: Informe de compatibilidad de uso de suelo

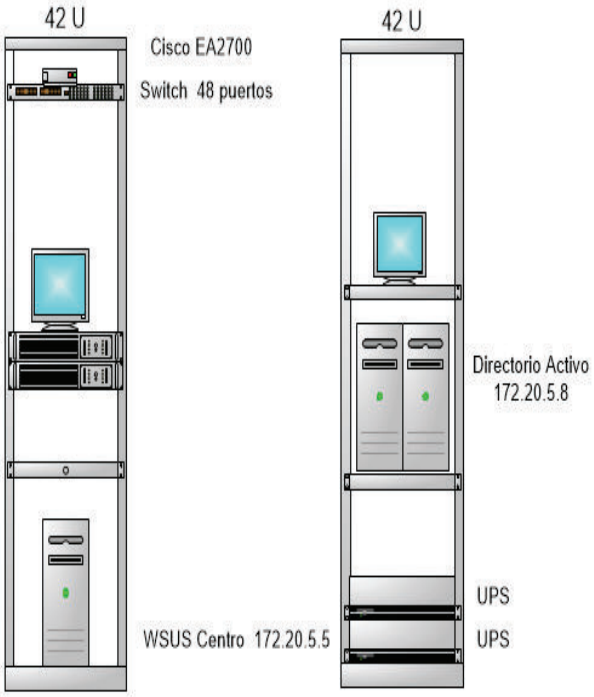
<table>
<tr><th colspan="2">RACK DEL CUARTO DE EQUIPOS C</th></tr>
<tr><td> 
</td><td>  </td></tr>
<tr><td>DEPARTAMENTO DE GESTIÓN URBANA</td><td>  </td></tr>
</table>

**Figura 2.9** Descripción de equipos de red en la planta baja – Avalúos

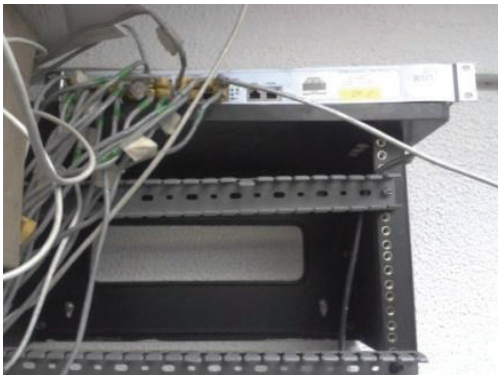
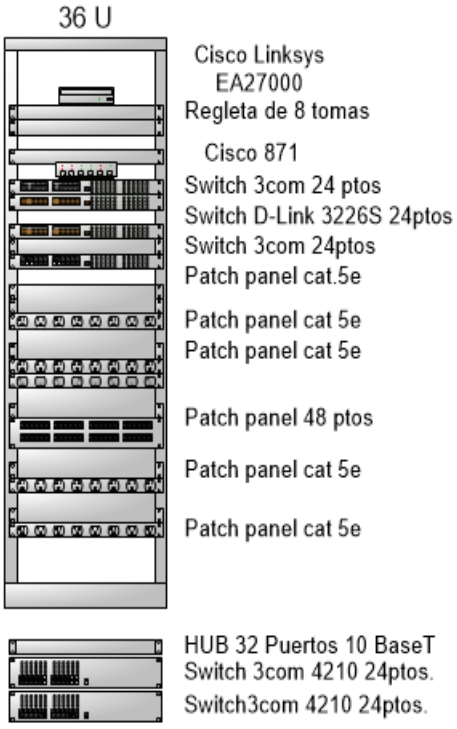
<table>
<tr><th colspan="2">EQUIPOS DE RED EN LA PLANTA BAJA – BLOQUE 2</th></tr>
<tr><td>DEPARTAMENTO<br>ARCHIVO</td><td>  </td></tr>
<tr><th colspan="2">RACK DEL CUARTO DE TELECOMUNICACIONES B - PARQUEADERO</th></tr>
<tr><td> 
</td><td>  </td></tr>
</table>

**Figura 2.10** Descripción de equipos de red en la planta baja– Parqueadero

## 2.4.3 TOPOLOGÍA LÓGICA DE LOS EQUIPOS

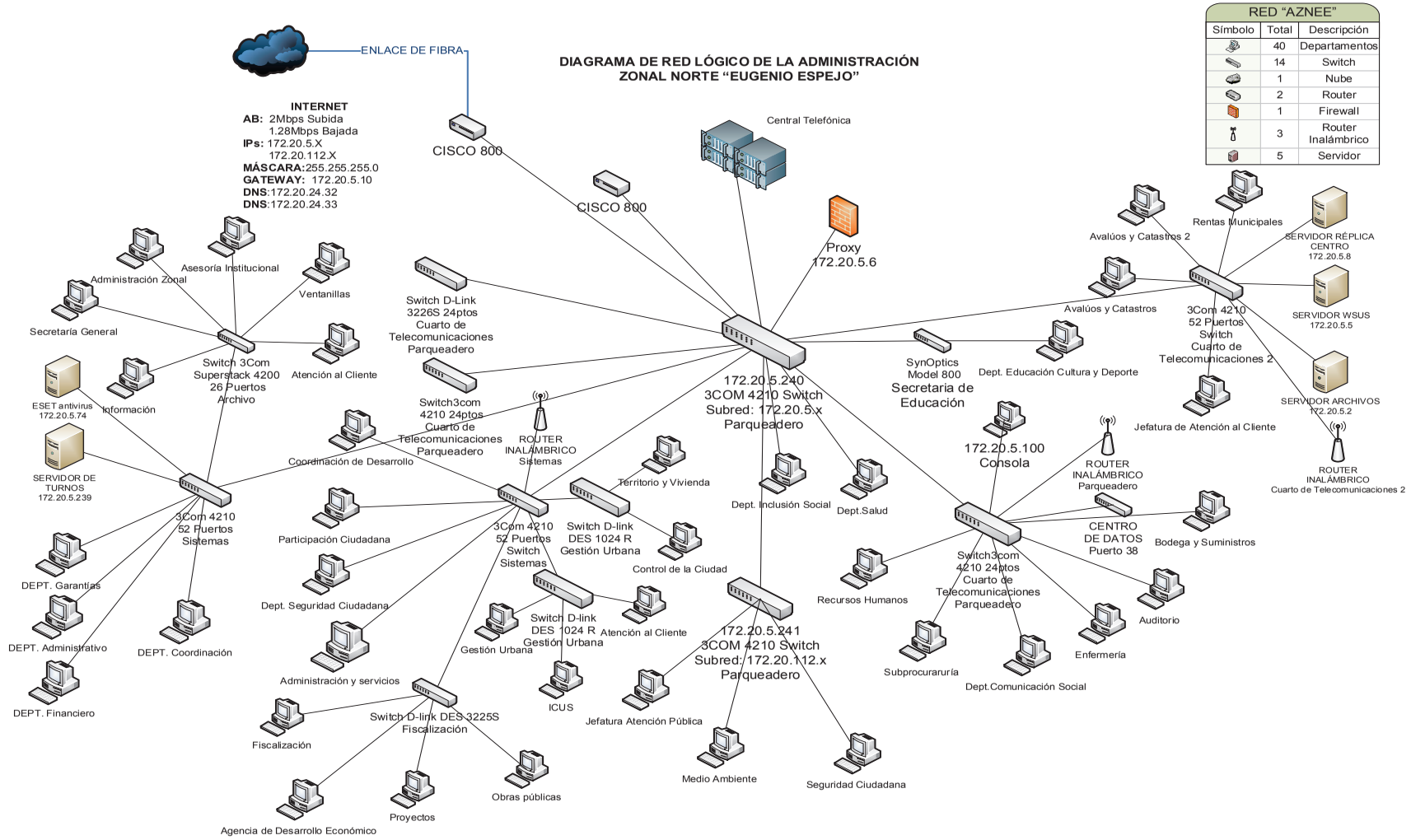



**Figura 2.11** Topología lógica de los equipos

### 2.4.4 DESCRIPCIÓN DEL EQUIPAMIENTO ACTIVO

Los equipos de interconexión pertenecientes a esta Institución facilitan la comunicación entre las diferentes dependencias, a más de permitir una adecuada gestión de la red de datos.

A continuación en la tabla 2.4 y 2.5 se indican una síntesis de las características de cada uno de los equipos activos.

**Tabla 2.4** Descripción de los equipos de capa 3

| Características | Router Inalámbrico Linksys EA2700 | Router Cisco Serie 870 |
|---|---|---|
| Puertos 10/100 Mbps | × | 4 |
| Puertos Gigabit | 4 | × |
| Banda de operación | 2.4 GHz -5GHz | 2.4 GHz |
| WPS<br>WIFI ProtectedSetupbutton | ✓ | × |
| VPN | × | ✓ |
| IPSec | × | ✓ |
| QoS | ✓ | ✓ |
| Direccionamiento IPv6 | ✓ | ✓ |
| Firewall | ✓ | ✓ |
| VLAN | × | ✓ |
| Número de usuarios | 20 | 20 |
| Enrutamiento estático | ✓ | ✓ |
| Enrutamiento dinámico | ✓ | ✓ |
| Estándares de red | IEEE 802.11n | IEEE 802.11b/g |
| Protocolos de ruteo | No especificados | RIPv1, RIPv2, L2TP, STP, ACLs, PPPoE, PAT, OSPF, BGP, EIGRP. |

**Tabla 2.5** Descripción de los equipos de capa 2

| Características | Switch 3COM 4210 | Switch 3COM 4200 | Switch D-LINK DES- 1024R | Switch D-LINK DES-3226S | Switch Advantek Network |
|---|---|---|---|---|---|
| Número de puertos | 24 | 24 | 24 | 24 | 16 |
| Cantidad de puertos SFP | 2 | 2 | 2 | 2 | …… |
| Velocidad | /100/1000 Mbps | 10/100 Mbps | 10/100 Mbps | 10/100 Mbps | 10/100 Mbps |

| | | | | | |
|---|---|---|---|---|---|
| Soporte PoE | No | No | No | No | No |
| Soporte Vlan | 4094 | 60 | No | 4094 | …… |
| Soporte Telnet | Si | Si | No | Si | …… |
| Soporte IPv6 | Si | No | No | | …… |
| QoS (Calidad de Servicio) | Si | Si | No | Si | …… |
| Soporte de control de flujo | Si | Si | Si | Si | …… |
| IGMP | Si | No | No | Si | …… |
| SNMP | v1, v2,v3 | v1, v2,v3 | …… | v1, v2,v3 | …… |
| SpanningTree Protocol | Si | Si | No | Si | …… |
| Tabla de direcciones MAC | 8192 entradas | 8000 entradas | 4000 entradas | 8000 entradas | 400 entradas |
| Capacidad de conmutación | 8.8 Gbit/s | 8.8 Gbit/s | 5.2 Gbit/s | 8.8 Gbit/s | …… |
| Estándares de red | IEEE 802.1D<br>IEEE 802.1p<br>IEEE 802.1Q<br>IEEE 802.1s<br>IEEE 802.1w<br>IEEE 802.1X<br>IEEE 802.3<br>IEEE 802.3ad<br>IEEE 802.3i<br>IEEE 802.3u<br>IEEE 802.3x<br>IEEE 802.3z | IEEE 802.3<br>IEEE 802.3u<br>IEEE 802.3i<br>IEEE 802.3z<br>IEEE 802.1D<br>IEEE 802.1Q<br>IEEE 802.1p<br>IEEE 802.3x<br>IEEE 802.3ad<br>IEEE 802.1w<br>IEEE 802.1x<br>IEEE 802.3ae<br>IEEE 802.1s | IEEE 802.3 N<br>IEEE 802.3<br>IEEE 802.3u<br>IEEE 802.3x | IEEE 802.3ab<br>IEEE 802.1p<br>IEEE 802.1D<br>IEEE 802.1x<br>IEEE 802.1Q<br>IEEE 802.3u<br>IEEE 802.1w<br>IEEE 802.3z | IEEE 802.3<br>IEEE 802.3u |
| MTBF (Tiempo medio entre fallos) | 359 000 horas | 465 570 horas | 626 992 horas | …… | …… |
| Tipo de Switch | Administrable | Administrable | No administrable | Administrable | No administrable |
| Algoritmos de seguridad | SSH, EAP, 802.1x,RADIUS | 802.1x RADIUS | …… | 802.1x RADIUS,SSH,SSL | …… |

## 2.5 SERVIDORES Y APLICACIONES DE LA ADMINISTRACIÓN NORTE "EUGENIO ESPEJO"

### 2.5.1 SERVIDORES DE LA AZNEE

Los servidores que dispone la AZNEE se encuentran en el cuarto de telecomunicaciones ubicado en la planta baja en el parqueadero y en el departamento de sistemas, ninguno cuenta con las seguridades necesarias para este tipo de equipos.

En la tabla 2.6 se detallan los principales servidores de la AZNEE:

**Tabla 2.6** Servidores de la AZNEE

| Nombre | Marca | Procesador | RAM | Disco Duro | Sistema Operativo | Dirección IP | Ubicación |
|---|---|---|---|---|---|---|---|
| PROXY | HP | Intel Core 2 Quad CPU Q 9550@ 2,863 GHz | 4GB | 500GB | LINUX | 172.20.5.6 | Cuarto de Equipos |
| ANTIVIRUS - SRV02ESET | HP | Intel Core 2 Quad CPU Q 9550@ 2,863 GHz | 4GB | 500GB | WINDOWS 7 - 32bits | 172.20.5.74 | Cuarto de telecomunicaciones A |
| WSUS | HP Proliant ML370 GS | Intel Xeon 2 GHz | 2GB | 200 GB | WINDOWS SERVER 2003 | 172.20.5.120 | Cuarto de telecomunicaciones B |
| ARCHIVOS TRÁMITES | HP Proliant ML370 GS | Intel Xeon 2 GHz | 2GB | 200 GB | WINDOWS SERVER 2003 | 172.20.5.2 | Cuarto de telecomunicaciones B |
| TURNOS | HP | Intel Core i5 3470 CPU @ 3,20 GHz | 2GB | 150GB | WINDOWS 7 - 32bits | 172.20.5.239 | Cuarto de telecomunicaciones A |
| ACTIVE DIRECTORY (RÉPLICA) | ACER | Intel Core i5 3470 CPU @ 3,20 GHz | 4GB | 500GB | WINDOWS 7 - 32bits | 172.20.5.169 | Cuarto de telecomunicaciones A |

Estos servidores se encuentran ubicados de la siguiente manera:

- Switch en el departamento de sistemas: Servidor actualizador del sistema Operativo, Windows Server Update Services (WSUS), Servidor de Antivirus.
- Switch en el parqueadero: Servidor Proxy.
- Switch en el cuarto de Telecomunicaciones B: Servidor Réplica y el Servidor de Archivos y Trámites.

### 2.5.1.1 Servidor de proxy

Las diversas administraciones del Distrito Metropolitano de Quito, tienen servicios que dependen netamente de la Administración General del Municipio de Quito, por ende el servidor en cuestión es usado como un servidor de réplica, el mismo que permite la configuración necesaria para el direccionamiento IP. En la figura 2.12 se muestra la consola de administración.


| Nombre | Tipo | Coincidiendo con... |
|---|---|---|
| QUERY | Expresión Regular de Ruta URL | cgi-bin \? |
| apache | | Server ^Apache |
| all | Dirección de Cliente | 0.0.0.0/0.0.0.0 |
| manager | Protocolo URL | cache_object |
| webserver | Dirección de Cliente | 172.20.5.6/255.255.255.255 |
| localhost | Dirección de Cliente | 127.0.0.1/255.255.255.255 |
| to_localhost | Dirección de Servidor Web | 127.0.0.0/8 |
| SSL_ports | Puerto URL | 443 |
| Safe_ports | Puerto URL | 80 # http |
| Safe_ports | Puerto URL | 21 # ftp |
| Safe_ports | Puerto URL | 443 # https |
| Safe_ports | Puerto URL | 70 # gopher |
| Safe_ports | Puerto URL | 210 # wais |
| Safe_ports | Puerto URL | 1025-65535 # unregistered ports |
| Safe_ports | Puerto URL | 280 # http-mgmt |
| Safe_ports | Puerto URL | 488 # gss-http |
| Safe_ports | Puerto URL | 591 # filemaker |
| Safe_ports | Puerto URL | 777 # multiling http |
| CONNECT | Método de Petición | CONNECT |
| navegcion | Dirección de Cliente | 172.20.5.1-172.20.5.254/255.255.255.255 |
| messenger | Expresión Regular URL | gateway.dll? login:445 meebo iloveim messenger |
| paginas_negadas | Expresión Regular URL | http://www.playboy.com xxx tangas porno anal tetas; http://www.facebook.com http://www.youtube.com http://www.youtoo.com http://twitter.com https://twitter.com laonda |
| descargas | Expresión Regular URL | .zip .exe .wav .mp3 .avi .rar |
| Consola112 | Dirección de Cliente | 172.20.5.100-172.20.5.100/255.255.255.255 |
| garmas19 | Dirección de Cliente | 172.20.5.85-172.20.5.85/255.255.255.255 |
| fdonoso | Dirección de Cliente | 172.20.5.147-172.20.5.147/255.255.255.255 |
| rpallasco | Dirección de Cliente | 172.20.5.63-172.20.5.63/255.255.255.255 |

**Figura 2.12** Consola del servidor Proxy [28]

[28] Fuente: Servidores de la AZNEE

### 2.5.1.2 Servidor y consola de antivirus

El servidor de antivirus cumple la función de proteger los archivos de programas maliciosos que traten de dañar la red de la AZNEE. El antivirus utilizado es el ESET Smart Security Corporativo. En la figura 2.13 se muestra la consola de administración.

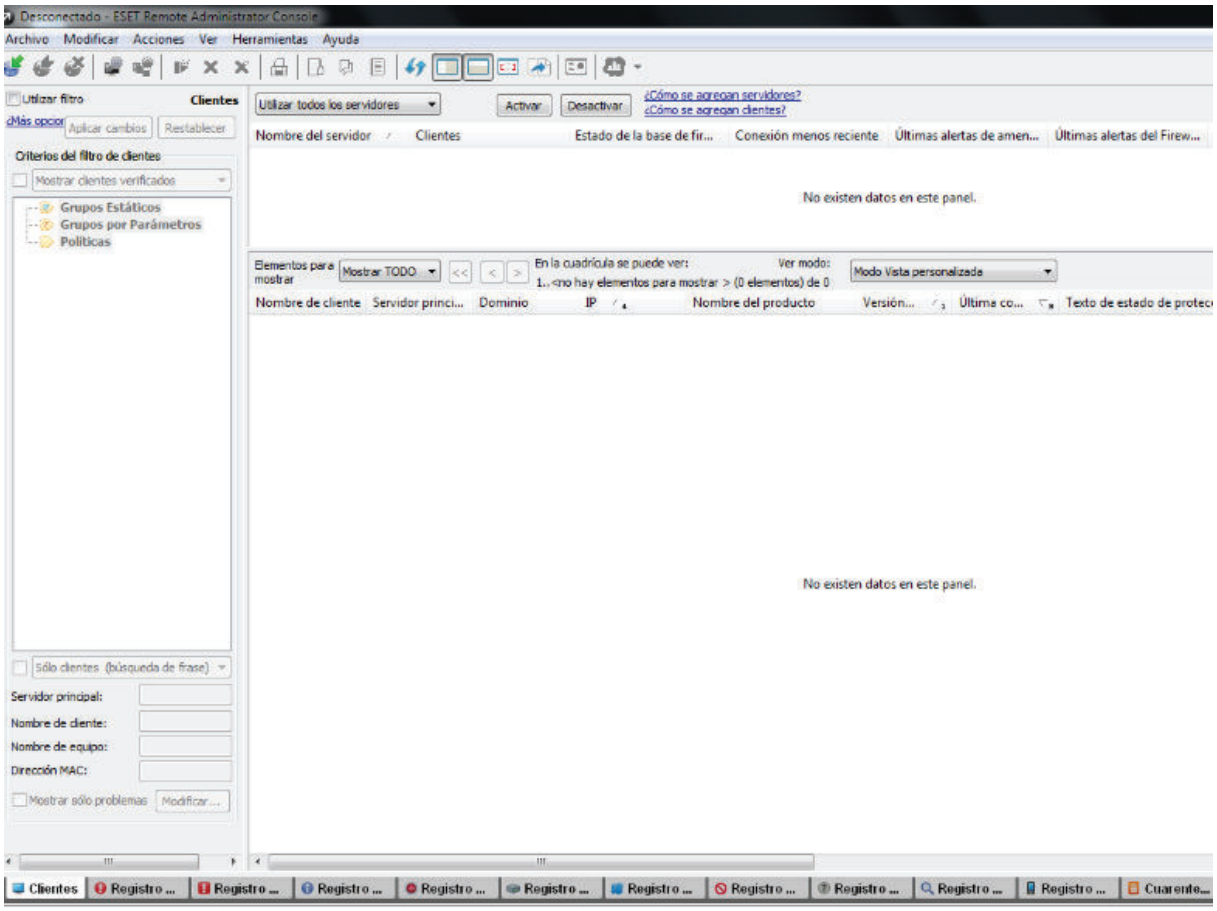



**Figura 2.13** Consola del servidor de Antivirus [29]

### 2.5.1.3 Servidor de archivos

Es conocido como servidor de Trámites, aquí se encuentra toda la información de patentes, planos, programas, instaladores e información de vital importancia para la AZNEE.

[29] Fuente: Servidores de la AZNEE

### 2.5.1.4 Servidor de turnos

El servidor de turnos permite tener una organización de los módulos que brindan servicios en la AZNEE, como son: atención al público y ventanillas. En la figura 2.14 se muestra la consola de administración.

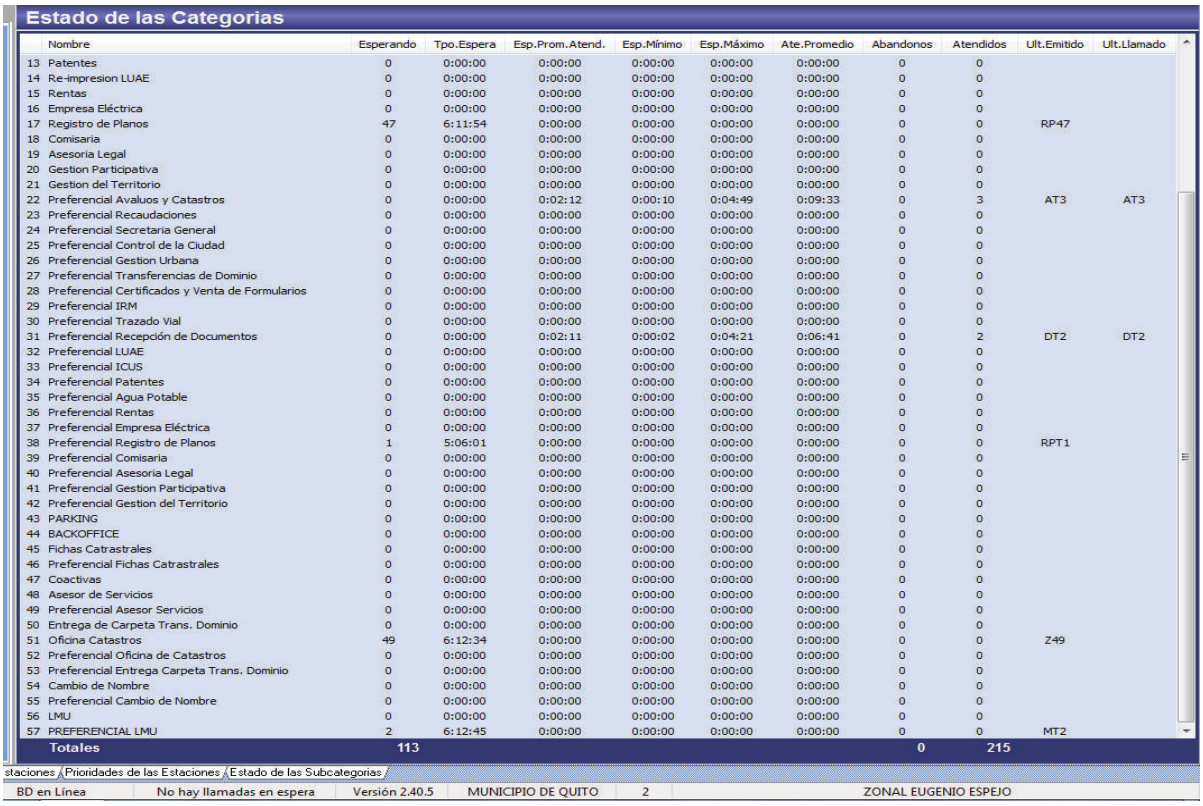


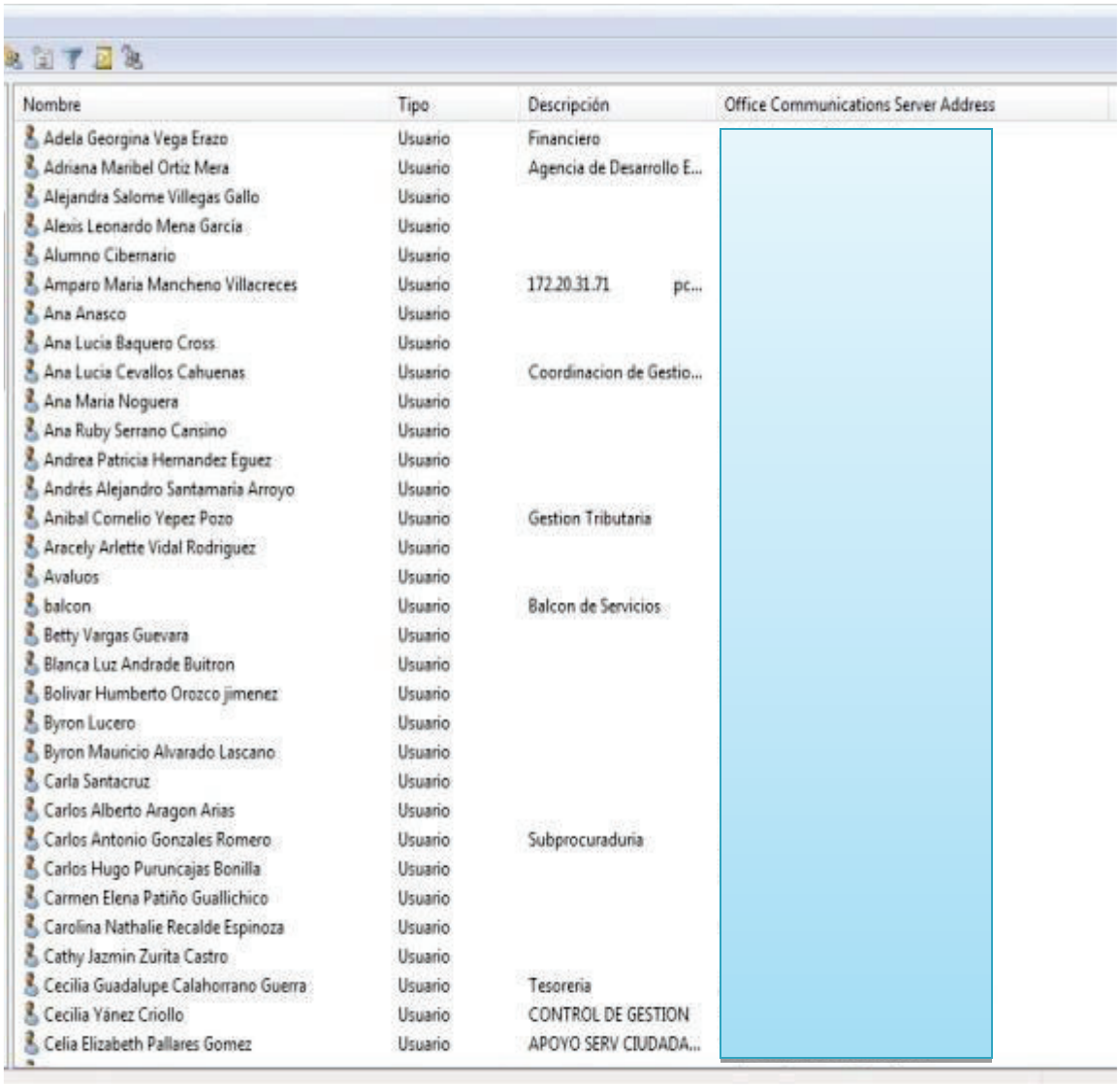

**Figura 2.14** Consola del Servidor de Turnos[30]

### 2.5.1.5 Servidor de réplica

Permite mantener una copia local de la información referente a: control de acceso, servicios de correo electrónico y perfiles de usuarios, grupos y cuentas. El servidor principal se encuentra en la Administración General del Municipio de Quito.

En la figura 2.15 se muestra la consola de administración.

[30] Fuente: Servidores de la AZNEE



| Nombre | Tipo | Descripción | Office Communications Server Address |
|---|---|---|---|
| Adela Georgina Vega Erazo | Usuario | Financiero | |
| Adriana Maribel Ortiz Mera | Usuario | Agencia de Desarrollo E... | |
| Alejandra Salome Villegas Gallo | Usuario | | |
| Alexis Leonardo Mena García | Usuario | | |
| Alumno Cibernario | Usuario | | |
| Amparo Maria Mancheno Villacreces | Usuario | 172.20.31.71 pc... | |
| Ana Anasco | Usuario | | |
| Ana Lucia Baquero Cross | Usuario | | |
| Ana Lucia Cevallos Cahuenas | Usuario | Coordinacion de Gestio... | |
| Ana Maria Noguera | Usuario | | |
| Ana Ruby Serrano Cansino | Usuario | | |
| Andrea Patricia Hernandez Eguez | Usuario | | |
| Andrés Alejandro Santamaria Arroyo | Usuario | | |
| Anibal Cornelio Yepez Pozo | Usuario | Gestion Tributaria | |
| Aracely Arlette Vidal Rodriguez | Usuario | | |
| Avaluos | Usuario | | |
| balcon | Usuario | Balcon de Servicios | |
| Betty Vargas Guevara | Usuario | | |
| Blanca Luz Andrade Buitron | Usuario | | |
| Bolivar Humberto Orozco jimenez | Usuario | | |
| Byron Lucero | Usuario | | |
| Byron Mauricio Alvarado Lascano | Usuario | | |
| Carla Santacruz | Usuario | | |
| Carlos Alberto Aragon Arias | Usuario | | |
| Carlos Antonio Gonzales Romero | Usuario | Subprocuraduria | |
| Carlos Hugo Puruncajas Bonilla | Usuario | | |
| Carmen Elena Patiño Guallichico | Usuario | | |
| Carolina Nathalie Recalde Espinoza | Usuario | | |
| Cathy Jazmin Zurita Castro | Usuario | | |
| Cecilia Guadalupe Calahorrano Guerra | Usuario | Tesoreria | |
| Cecilia Yánez Criollo | Usuario | CONTROL DE GESTION | |
| Celia Elizabeth Pallares Gomez | Usuario | APOYO SERV CIUDADA... | |

**Figura 2.15** Consola del Servidor de Dominio [31]

### 2.5.1.6 Página de la intranet

La página web, figura 2.16, es utilizada por la AZNEE y el resto de administraciones zonales del Distrito Metropolitano de Quito; cuenta con diversos servicios para la ciudadanía quiteña. Su ingreso se lo realiza con el respectivo usuario y contraseña.

[31] Fuente: Servidores de la AZNEE


**Figura 2.16** Intranet de la AZNEE [32]

## 2.5.2 APLICACIONES DE LA AZNEE

Los servicios que presta la AZNEE están basados en aplicaciones las cuales han sido desarrolladas por parte de la Dirección Metropolitana de Informática, encargada de gestionar toda la red del Municipio de Quito.

Entre las aplicaciones que permiten brindar servicios a los clientes se tiene las siguientes:

### 2.5.2.1 Business Process Manager, BPM

La característica principal de esta aplicación es permitir a los usuarios realizar varios trámites, como: obtención de permisos de funcionamiento y construcción, licencias

[32] Fuente: Servidores de la AZNEE

de funcionamiento y construcción, registros de planos, inspecciones de terrenos y negocios.

Los departamentos encargados de dar este servicio son: Gestión Urbana, Salud, Subprocuraduría. Este sistema se encuentra protegido y administrado por la Dirección Metropolitana de Informática, por tal razón su información técnica es reservada.

#### 2.5.2.2 Easyteller

Esta aplicación permite que los usuarios obtengan los certificados de no adeudar al Municipio de Quito. Este sistema se encuentra protegido y administrado por la Dirección Metropolitana de Informática, por tal razón su información técnica es reservada.

#### 2.5.2.3 Rumba

Esta aplicación permite obtener información acerca de partidas presupuestarias, cálculos de presupuestos, consulta de predios, y trámites de transferencia de dominios de los ciudadanos del Distrito Metropolitano de Quito. Este sistema se encuentra protegido y administrado por la Administración Central, por tal razón su información técnica es reservada.

#### 2.5.2.4 Microsoft Office Communication Server, OCS

Es una aplicación utilizada por los usuarios de la AZNEE para comunicarse con sus colegas, ofrece servicios de mensajería instantánea, compartición de documentos, y comunicaciones de voz y video.

#### 2.5.2.5 Informe de Compatibilidad de Uso del Suelo, ICUS

Esta aplicación permite realizar consultas acerca de los predios, claves catastrales que posee la ciudadanía, es usada por el departamento de Territorio y Vivienda. Como las anteriores aplicaciones su información en susceptible por lo cual no puede ser proporcionada.

#### 2.5.2.6 Antivirus

El Municipio de Quito utiliza la plataforma ESET Smart Security Business Edition como un servicio de antivirus, el cual es gestionado por la Administración Central. Se encuentra configurado en servidor SRV02ESET, el cual brinda las actualizaciones necesarias y se comunica con la Administración Central por medio de la dirección IP 172.20.24.120.

#### 2.5.2.7 Correo electrónico

Este servicio permite a los usuarios enviar y recibir correos electrónicos dentro del dominio del Distrito Metropolitano de Quito. El manejo de este servicio se realiza a través de la aplicación Microsoft Office Outlook 2010 y se accede al mismo con las credenciales de cada usuario. Este sistema se encuentra protegido y administrado por la Administración Central, por tal razón su información técnica es reservada.

#### 2.5.2.8 Internet

Este servicio es habilitado dependiendo del perfil de cada usuario, las reglas para su utilización son configuradas en el servidor proxy mediante la asociación de la dirección IP y la restricción de páginas web.

#### 2.5.2.9 DHCP

El servidor de DHCP, es configurado en un servidor de réplica, debido a que este servicio es controlado por la Administración Central, y permite asignar direcciones IP según la administración zonal.

Para la AZNEE los rangos de direcciones IP van desde la 172.20.5.1/24 a 172.20.5.254/24 y desde 172.20.112.1/24 a 172.20.112.254/24, de estas subredes las IPs que no podrán ser utilizadas son las que servirán de gateway (172.20.5.10 - 172.20.112.10) y las direcciones de los servidores.

#### 2.5.2.10 PROXY

La AZNEE cuenta con dos servicios de Proxy, el uno que es propio de la administración, y el segundo que es controlado por la Administración Central, ambos brindan el acceso a internet y limitan el acceso a ciertas páginas, como redes sociales, YouTube, descargas, páginas de contenido para adultos. La configuración mencionada se encuentra en el navegador correspondiente a cada usuario del sistema como lo indica la tabla 2.7

**Tabla 2.7** Proxy de la AZNEE

| | PROXY | PUERTO |
|---|---|---|
| **CENTRO** | proxytmg | 8080 |
| **AZNEE** | 172.20.5.6 | 3128 |

## 2.6 DIRECCIONAMIENTO IP

La AZNEE tiene asignado dos dominio de broadcast TCP/IP. El direccionamiento está disponible en dos subredes 172.20.5.0 y 172.20.112.0 con máscara de subred 255.255.255.0. La puerta de enlace para cada subred es 172.20.5.10 y 172.20.112.10 cuyos DNS tanto primario como secundario son 172.20.24.33 y

172.20.24.32, que están establecidos por la Administración Central. Las direcciones IP disponibles están asignadas a computadores, portátiles, impresoras, switches y routers.

El uso de la subred 172.20.112.0 se debe a un problema de administración de direcciones IP. Además en las diversas remodelaciones que ha tenido la AZNEE no se han retirado los cables de conexión de sus respectivos equipos de comunicación, dando una acumulación de los mismos y la utilización de puertos en los switches.

En el Anexo C se encuentra detallado el direccionamiento de la AZNEE como se encuentra en la actualidad.

## 2.7 ENCUESTA REALIZADA A LOS USUARIOS DE LA AZNEE

La presente encuesta permitió determinar las necesidades y requerimientos de los usuarios de la AZNEE, y de esta manera diseñar una red que brinde servicios de mejor calidad.
Los aspectos que se analizaron en la encuesta fueron:

- Servicios de la red
- Telefonía análoga
- Seguridad de las credenciales de usuario
- Mecanismos de seguridad

Para determinar el tamaño de la muestra de usuarios a ser encuestados se utilizó la recomendación de la UIT-T E802, ecuación 2.1:

$$n = \frac{Z^2 * p * q * N}{N * e^2 + Z^2 * p * q} \qquad Ecuación\ 2.1$$

Dónde:

- n = Tamaño de la muestra

- Z = Nivel de confianza, se estima un valor de 75%, ya que 3 de cada 4 encuestados se tomaron su tiempo para contestar cada pregunta.
- p = Proporción de usuarios que poseen en la población la característica de estudio.
- q = Proporción de usuarios que no poseen en la población la característica de estudio.
- N = Tamaño de la población, total de 150 usuarios (Tabla 2.2)
- e = Error de estimación, seleccionado por el encuestador en un rango de 1% al 10%, se selecciona el 5% debido a que no todos los encuestados podrán contestar de manera acertada.

El nivel de confianza se estima de un 75%, que equivale a un valor de ***Z*** de 1.15. Para los valores de ***p*** y ***q***, se tiene que las personas que conocen más acerca de la seguridad son el personal técnico de la institución que equivale a un 10% dando un valor de ***p*** = 0.1, quedando el valor de ***q*** = 0.9, refiriéndose a los usuarios, ya que para ellos los aspectos de seguridad de la red son transparentes. El valor de ***e*** se estima en un 5%.

Con las variables establecidas se procedió al cálculo de la muestra para realizar la respectiva encuesta, como se indica a continuación:

$$n = \frac{1{,}15^2 * 0.1 * 0.9 * 150}{148 * 0.05^2 + 1{,}15^2 * 0.1 * 0.9}$$

$$n = \frac{17.85375}{0.489025}$$

$$\boldsymbol{n = 36.39\ muestras}$$

Con este resultado se procedió a realizar la encuesta a 36 personas dentro de la Administración Zonal Norte “Eugenio Espejo”.

### 2.7.1 ANÁLISIS DE LOS RESULTADOS

A continuación se presentan los resultados obtenidos en la encuesta realizada al personal de la AZNEE.

**1. ¿En qué intervalo de tiempo usted accede al internet?**

Con el resultado de la figura 2.17 se puede determinar la hora pico para el acceso a internet, y dimensionar un adecuado ancho de banda para la red.

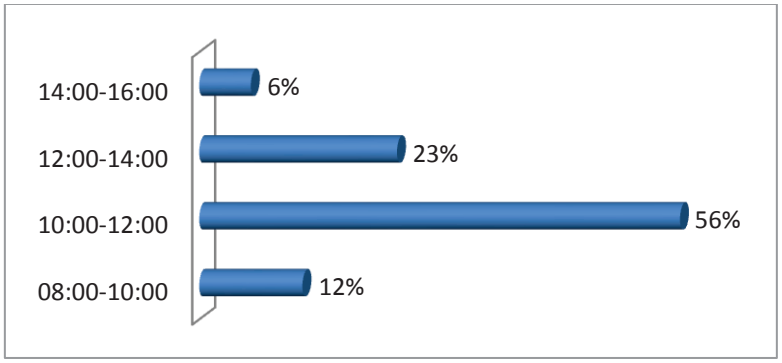



**Figura 2.17** Hora pico de utilización de internet AZNEE

**2. ¿Qué día de semana considera que accede con mayor frecuencia a los recursos de la red?**

Con el resultado de la figura 2.18 se puede determinar el día pico para el acceso a internet, y dimensionar un adecuado ancho de banda para la red.

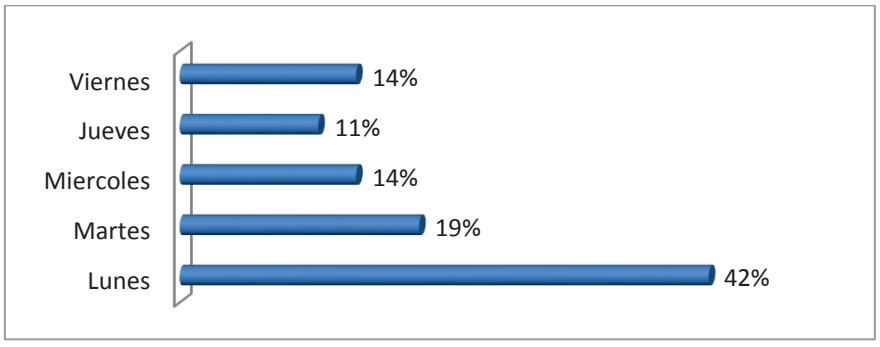



**Figura 2.18** Día pico para el acceso a internet AZNEE

### 3. ¿Cuál es el mes en el que tiene mayor carga de trabajo?

En la figura 2.19 se puede identificar el mes con mayor saturación, que tienen los usuarios de la AZNEE.

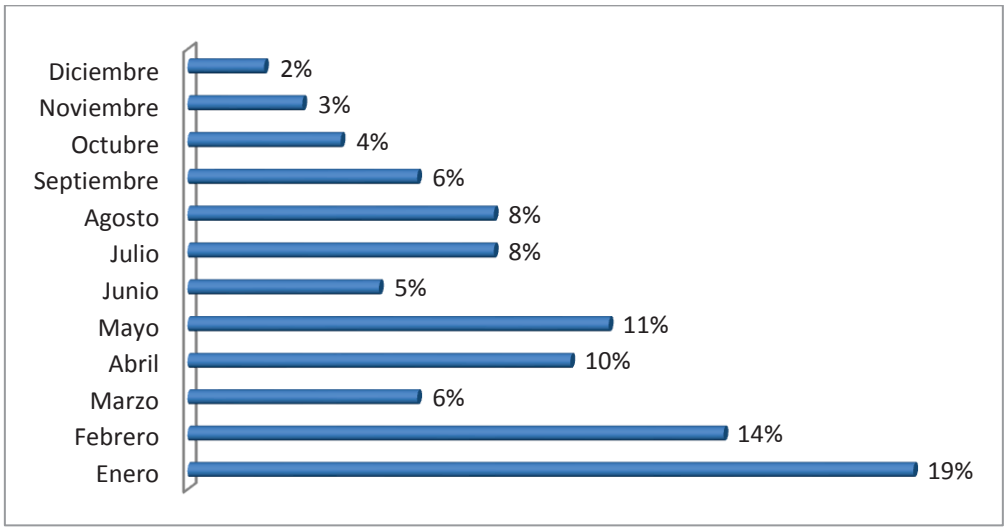



**Figura 2.19** Mes pico de acceso a la red

### 4. ¿Cuántos correos envía en el intervalo de una hora?

El resultado de la figura 2.20 permite dimensionar el tráfico del servicio de correo electrónico para estimar el ancho de banda que ocupa este servicio.

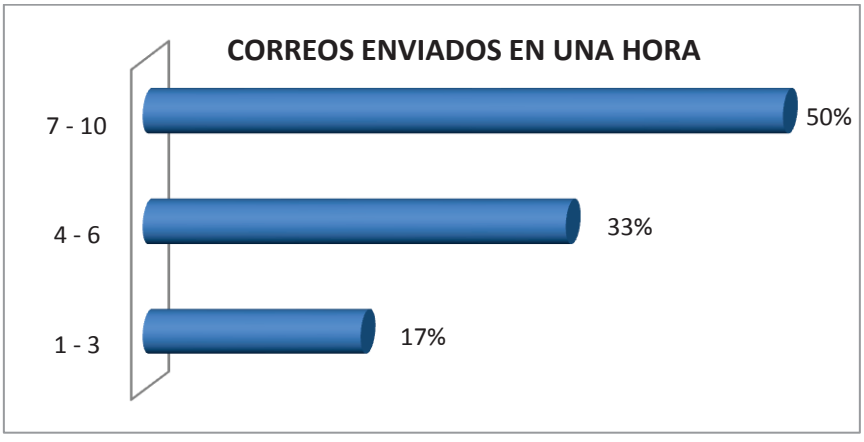



**Figura 2.20** Correos enviados en una hora

**5. ¿Cuantas páginas web visita en el intervalo de una hora?**

El resultado de la figura 2.21 permite dimensionar el tráfico del servicio de páginas web para estimar el ancho de banda que ocupa este servicio.

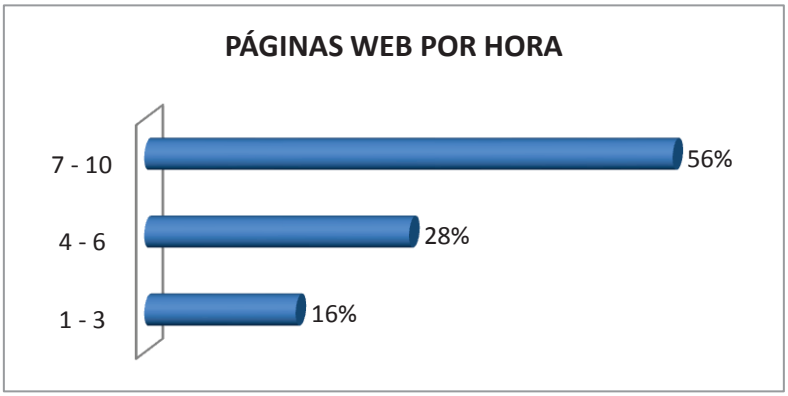



**Figura 2.21** Páginas web visitadas en una hora

**6. ¿Cuántas conversaciones de mensajería instantánea tiene en una hora?**

El resultado de la figura 2.22 permite dimensionar el tráfico del servicio de mensajería instantánea para estimar el ancho de banda que ocupa este servicio.


**Figura 2.22** Número de conversaciones de mensajería instantánea

**7. ¿Cuántas llamadas internas realiza en una hora?**

En la figura 2.23 se observa el número de llamadas promedio que se realizan dentro de la AZNEE.

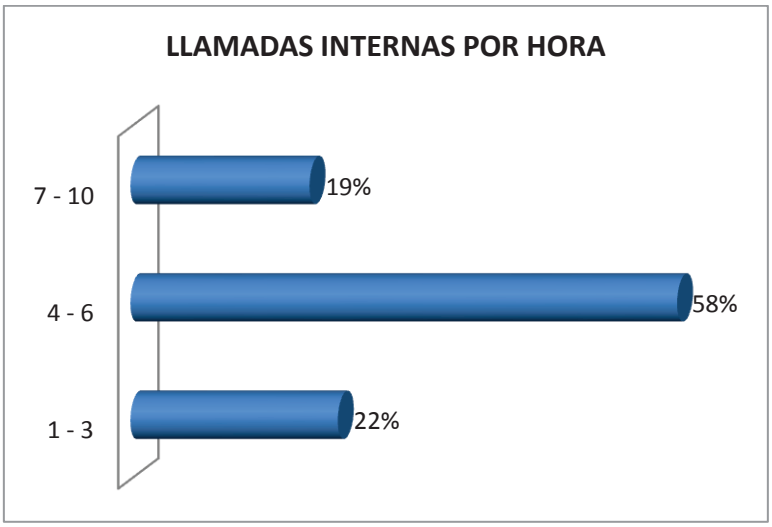



**Figura 2.23** Número de llamadas internas por hora

**9. ¿Cuántas llamadas externas realiza en una hora?**

En la figura 2.24 se puede observar el número de llamadas promedio que se realizan fuera de la AZNEE.

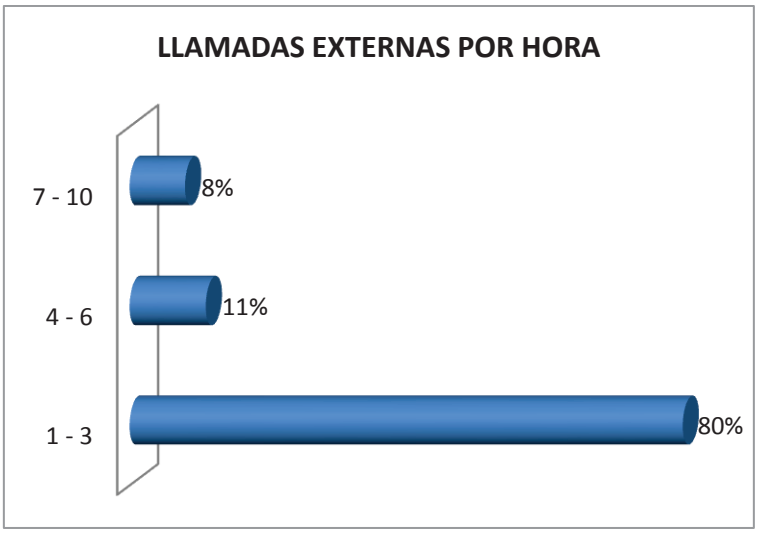



**Figura 2.24** Número de llamadas externas por hora

En base a todos los resultados obtenidos se puede realizar el análisis del tráfico actual de la AZNEE.

## 2.8 ANÁLISIS DEL TRÁFICO DE LA AZNEE

En la actualidad la AZNEE no cuenta con un equipo para monitorizar el tráfico generado tanto interno como externo, por ello se utilizó la herramienta de NTOP[33] para realizar las capturas necesarias para el tráfico de la red, la cual se ubicó en el switch de Core ubicado en el cuarto de equipos.

Sabiendo que la AZNNE cuenta con un enlace asimétrico con una capacidad de 1024 Kbps a través de un enlace de fibra óptica, se recogieron datos en el periodo de agosto – septiembre de 2013, y basándonos en los resultados de la encuesta se dio como resultado la siguiente información.

La recolección de datos realizados por el lapso de un mes llegó a tener una velocidad máxima de 7.5 KBps y una velocidad promedio de 734.4 Bps las cuales se indican en la figura 2.25.

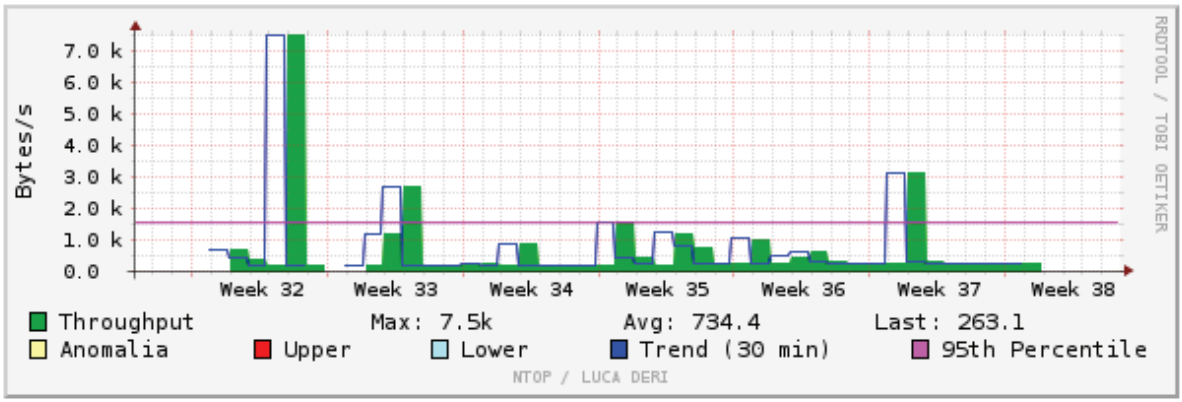



**Figura 2.25** Throughput Agosto – Septiembre 2013 [34]

Además se verificó que el día pico en la AZNEE, en donde los usuarios utilizan más el ancho de banda es el día lunes como se indicó en las respuestas de la encuesta de la sección 2.7 y se verifica en la figura 2.26.

[33] NTOP: http://www.ntop.org/

[34] Fuente: Herramienta de Monitoreo NTOP

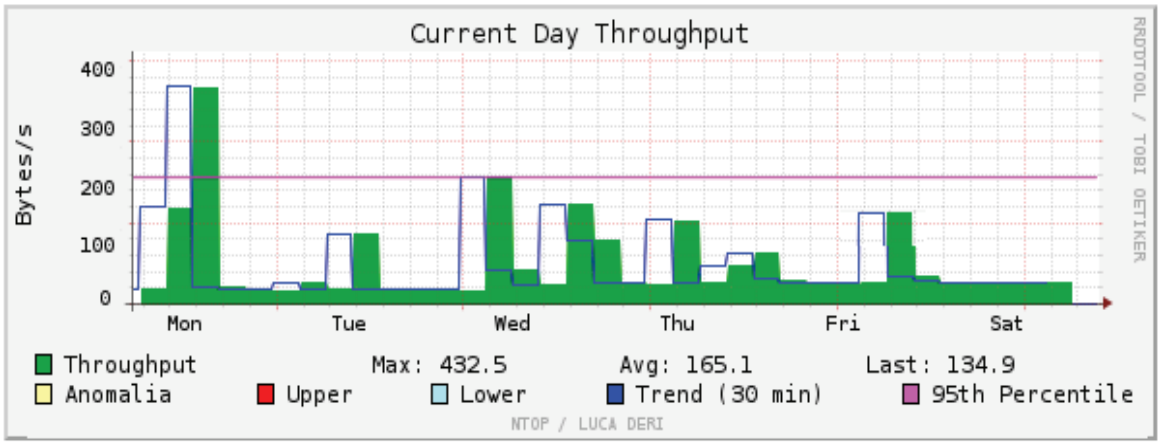



**Figura 2.26** Throughput en el día pico – lunes [34]

Se verificó las horas pico en donde los usuarios acceden al internet, en la figura 2.27 se puede aprecia dos intervalos. El primer intervalo de 10:00 a 12:00 corrobora el resultado de la encuesta y un segundo intervalo de 13:00 a 14:00 horas correspondientes al horario de almuerzo del personal.

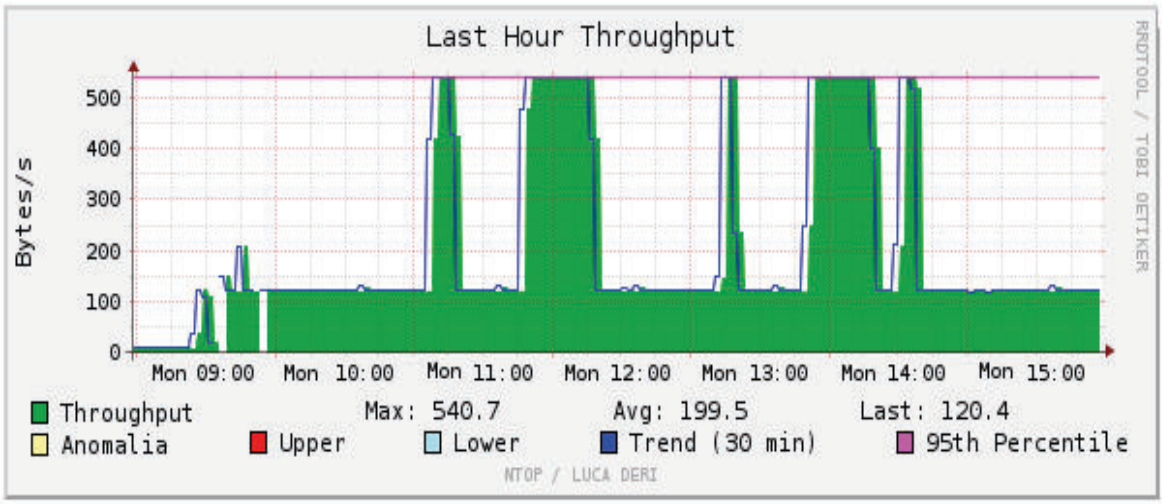



**Figura 2.27** Throughput en las horas pico [34]

Se presenta un historial de tráfico de la red discriminado por protocolo (Figura 2.28), en el cual se puede verificar que la aplicación más utilizada es Proxy seguida por DHCP, HTTP y Telnet protocolos con los cuales se conectan a la red WAN.

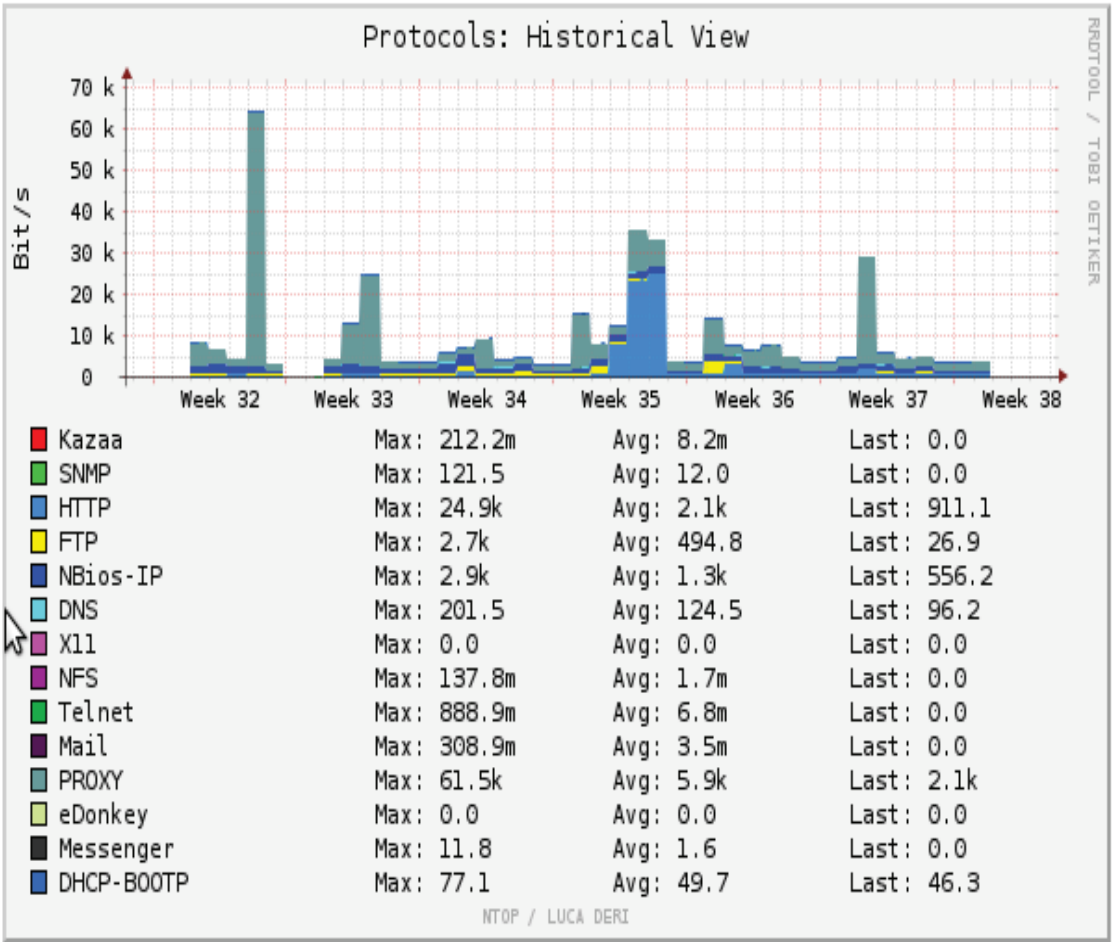



**Figura 2.28** Tráfico de la red de acuerdo a protocolos [34]

## 2.9 DESCRIPCIÓN DEL SISTEMA DE VOZ DE LA AZNEE

La AZNEE cuenta con una central telefónica análoga gestionada por la administración central, este servicio es proporcionado por la Corporación Nacional de Telecomunicaciones CNT.

Los usuarios internos de la AZNEE se comunican mediante una extensión de 3 dígitos, mientras que para las llamadas externas se utiliza un código de salida.

Cabe mencionar que cada llamada está controlada por la D.M.I. (Dirección Metropolitana de Informática), y tienen una duración máxima de 3 minutos.

En la figura 2.29 se observa la central Panasonic que utiliza la AZNEE.


**Figura 2.29** Central Telefónica Panasonic Digital Kx-td1232

La central telefónica Panasonic Kx-td1232 tiene una capacidad máxima hasta 12 líneas externas y 64 líneas internas analógicas, y se ha integrado un armario esclavo para duplicar la capacidad a 24 líneas externas con 128 extensiones analógicas.

Actualmente el sistema trabaja con 112 extensiones internas distribuidas en todo el edificio y 13 líneas troncales conectadas a la red pública de CNT, en el Anexo D se detallan el directorio telefónico de la AZNEE.

## 2.10 DESCRIPCIÓN DEL SISTEMA DE SEGURIDAD

Inicialmente para determinar los parámetros de seguridad que dispone la AZNEE, se entrevistó al personal técnico calificado en base a una serie de preguntas

concernientes a seguridad informática (véase Anexo E), en la tabla 2.8 se describe la información obtenida.

**Tabla 2.8** Resultados obtenidos en la encuesta.

| Parámetro de Seguridad | Descripción | Fortaleza | Debilidad |
|---|---|---|---|
| Backups | Existen copias almacenadas en una empresa privada de los servidores de trámites y de turnos. | Copias almacenadas fuera de la institución. | No existe política que establezca un crono-grama para la realización de backups. |
| Lista de control de acceso | Access Control List (ACLs) implementadas y controladas por la Dirección Metropolitana de informática. | Filtrado de paquetes basando en criterios determinados por la DMI. | Desconocimiento por parte del área de sistemas de la AZNEE del criterio con el que se realiza la configuración de ACLs. |
| Firewall | Controlado por la DMI e implementado en el edificio principal del Municipio de Quito. | Existe una barrera primaria para bloquear el acceso no autorizado. | No se encuentra ubicado dentro de la AZNEE. |
| Antivirus | El software implementado en la institución es ESET Smart Security Corporativo. | Detección de amenazas informáticas. | Software propietario. |
| Antispam | El software implementado en la | Filtrado de correo basura o no | Software propietario. |

| | | | |
|---|---|---|---|
| | institución es ESET Smart Security Corporativo. | deseado. | |
| Proxy | Implementado en la AZNEE donde el acceso a internet es limitado por cargo y por usuario. | Optimización del ancho de banda restringiendo el acceso a páginas definidas por el administrador. | Falta de procedimientos para establecer privilegios de acceso a páginas web. |
| Autenticación | El departamento financiero utiliza un token del Banco Central del Ecuador para firmar electrónicamente y realizar transacciones bancarias. | Disminución en el tiempo de trámites legales y bancarios. | …… |
| | Contraseñas de mediano grado compuesto por números y letras (5 a 8 caracteres). | …… | Cambio de contraseña únicamente cuando el usuario pierde sus credenciales. |

Para realizar un análisis más a detalle de las vulnerabilidades de la institución se procederá a la utilización de técnicas de hacking ético, con este fin se implementará una red de prueba virtual utilizando el software honeynet[35], en la cual se realizarán los ataques informáticos en busca de brechas en la seguridad.

Los pasos a seguir serán los siguientes:

1. Realización de la red de prueba- Honeynet
2. Utilización de técnicas de hacking ético
3. Análisis de resultados

[35] Honeynet: https://www.honeynet.org/

### 2.10.1 REALIZACIÓN DE LA RED DE PRUEBA - HONEYNET

La honeynet es un sistema que permite emular una red de manera física o virtual, diseñada para ser atacada y permitir recolectar información de intrusiones, para el análisis, monitoreo e investigación de vulnerabilidades y a la postre realizar los correctivos sobre la red real.

Para determinar las vulnerabilidades existentes en la AZNEE, se procedió a realizar la honeynet con las configuraciones de los servicios de la red real.

A continuación se detallan los componentes del sistema:

- **Honeypots**: Conjunto de computadores destinados para ser atacados, simulando ser sistemas débiles.
- **Honeywall:** Software basado en Linux que contiene herramientas necesarias para crear una honeynet, con el objetivo de filtrar el trafico producido por los honeypots sin interferir en su normal funcionamiento.
  Las herramientas que utiliza son:

  - ✓ **Iptables:** Es un programa que permite el filtrado de paquetes que ingresan y salen de la honeynet.
  - ✓ **P0f:** Es un programa utilizado para el monitoreo del tráfico que ingresa a la honeynet.
  - ✓ **Snort:** Es un IDS (Intrusion Detection System) de red, que actúa como gateway para toda la información recopilada en honeynet.

  Entre los componentes no estandarizados en la honeywall están:

  - ✓ **Sebek:** Es una herramienta que genera logs de las actividades del atacante en un honeypot, trabaja con la arquitectura cliente-servidor. El software cliente se encuentra instalado en los honeypots y el software

del servidor corre sobre el host donde se encuentra instalado el honeywall.

- ✓ **Walleye**: Es la interfaz de administración gráfica de la honeynet.

### 2.10.2 CONFIGURACIÓN E IMPLEMENTACIÓN DE LA HONEYNET

La implementación de la honeynet se realizará de manera virtual mediante la herramienta de virtualización VirtualBox, donde constarán los sistemas operativos y aplicaciones que se maneja en la red de la AZNEE.

Los honeypots serán configurados en máquinas virtuales con las copias de las imágenes de los discos de dos servidores proporcionados por la AZNEE. ***Cabe recalcar que los servicios principales están instalados en la matriz del Municipio de Quito, por lo que no se puede realizar un análisis más completo sobre la red.***

Las imágenes de los discos duros que se obtuvieron son:

- Antivirus
- Archivos (Windows Server)

Los servicios restantes fueron simulados con la utilización del software ZENTYAL (ZENTYAL, 2014), el cual fue instalado en una máquina virtual y configurado con los siguientes servicios:

- **DNS:** Servicio de nombres de dominio
- **Email:** Servicio de correo electrónico
- **Proxy:** Bloqueo de URLs y puertos no autorizados.
- **Lighweight Directory Access Protocol** (**LDAP):** Servicio de directorio activo para entornos Linux similar a Active Directory en entornos Windows.

En la figura 2.30 se muestra el diseño de la honeynet a implementar, la misma que será ubicada fuera de la red real.

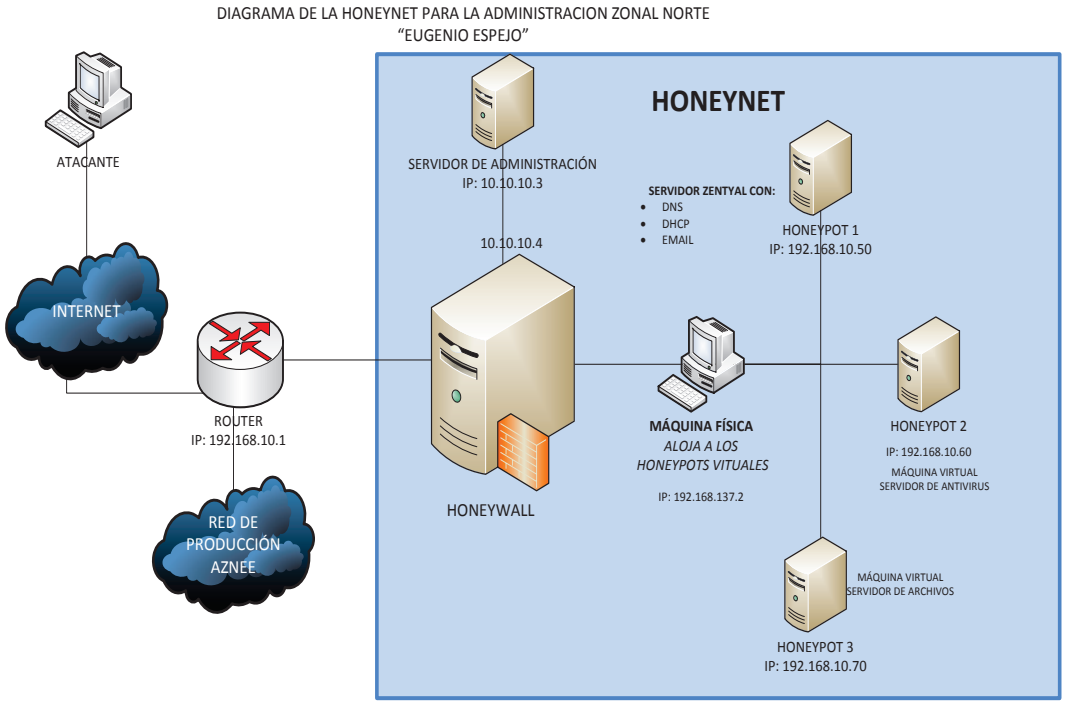



**Figura 2.30** Diagrama de la honeynet para AZNEE.

En el Anexo F, se puede encontrar el archivo de configuración de la honeynet.

### 2.10.3 UTILIZACIÓN DEL HACKING ÉTICO PARA DETERMINAR VULNERABILIDADES

Partiendo de la premisa de que la información en la actualidad es uno de los activos más importantes en cualquier empresa tanto pública como privada, este recurso tiene un valor inconmensurable y para el caso particular de la AZNEE, que gestiona documentos sensibles de diversa naturaleza departamental, como son: catastros, predios, permisos de funcionamiento, patentes, etc. se debe tener mayor precaución con la gestión de los mismos, por lo que para mitigar los riesgos dentro y fuera de la red, se realizará un rediseño total de la infraestructura tecnológica de la institución.

Para realizar un correcto rediseño de la red multiservicios de la AZNEE se debe identificar las vulnerabilidades existentes en la actualidad; para este fin se utilizaron técnicas de hacking ético que no son más que la búsqueda de debilidades mediante el manejo de herramientas informáticas llevadas a cabo por una persona especializada en ataques a sistemas y servicios informáticos.

Los resultados obtenidos a partir de estas técnicas permitirán tomar acciones de prevención necesarias, mitigando posibles ataques maliciosos.

Las técnicas a utilizar son:

- Footprinting
- Scanning
- Enumeration
- Troyanos y puertas traseras
- Ingeniería Social

A continuación el detalle de los ataques realizados y los resultados obtenidos:

### 2.10.3.1 Footprinting

Mediante esta técnica es posible determinar los accesos ocultos o puertas traseras (BackDoors) para poder vulnerar una red. Es la técnica que permite recolectar datos relevantes de una empresa, persona, dominio o cuentas de correo antes de realizar ataques; la herramienta utilizada para ejecutar esta técnica es el software Maltego[36], mismo que permite obtener información concerniente al dominio del Municipio de Quito, que se indica en la figura 2.31.

El proceso que sigue el software Maltego es el siguiente:

[36] Maltego: https://www.paterva.com/web6/

1. Maltego envía la petición del cliente a los servidores de semilla[37]en formato XML a través de HTTPS.
2. La petición del servidor de semilla es entregada a los servidores TAS[38] para que realicen el proceso de descubrimiento en los proveedores de servicios.
3. Los resultados se envían al cliente Maltego.

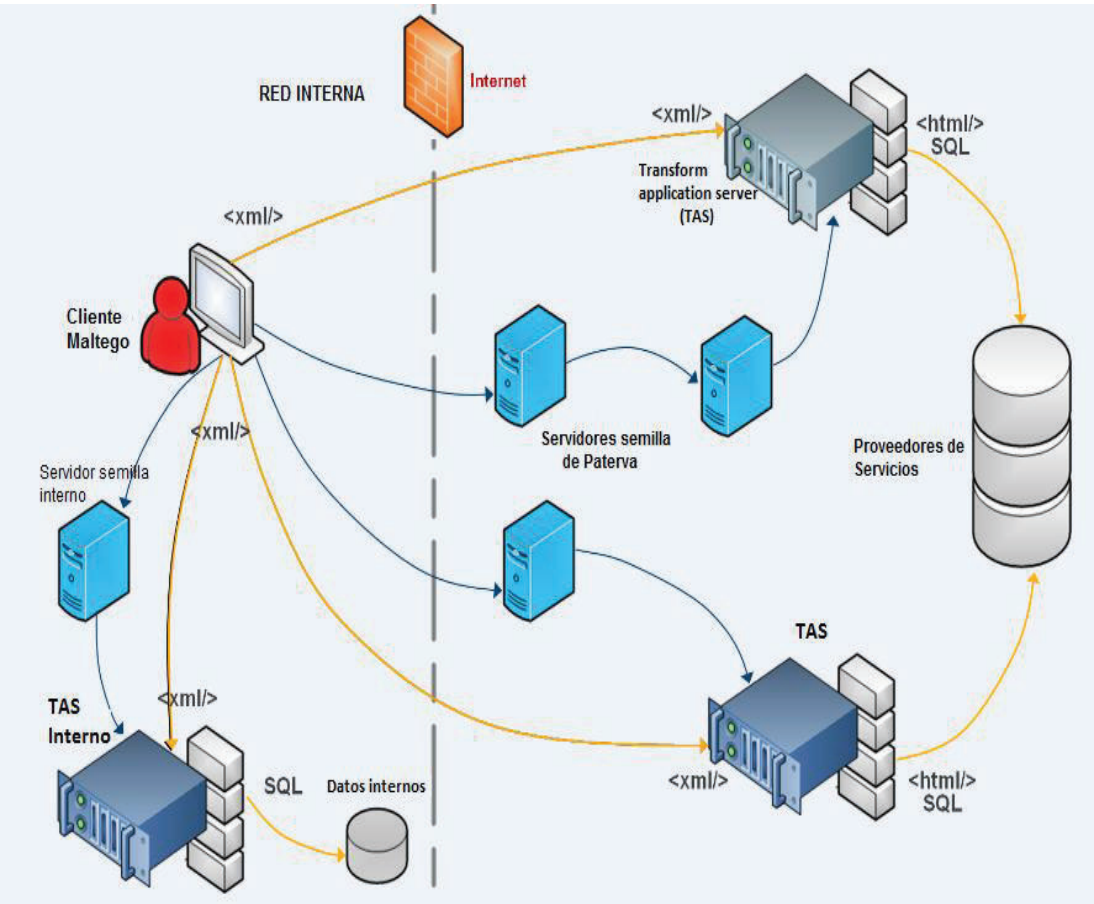



**Figura 2.31** Funcionamiento Software Maltego

Para el caso del Municipio de Quito se procedió a ingresar el dominio de la institución como entidad de búsqueda, obteniendo los resultados mostrados en la figura 2.32.

- Herramienta utilizada Maltego

[37] Semilla: Son pequeñas piezas de XML que le indican al cliente de Maltego donde se ubican los servidores TAS, se asemeja al índice de un libro.

[38] TAS: Transform Application Server

Main View | Bubble View | Entity List

| Nodes | Type | Value | Weight | Incoming | Outgoing |
|---|---|---|---|---|---|
| quito.gob.ec | Domain | quito.gob.ec | 0 | 0 | 29 |
| root.andinanet.net | DNS Name | root.andinanet.net | 100 | 1 | 0 |
| hostmaster@andinanet.net | Email Address | hostmaster@andinanet.net | 100 | 1 | 0 |
| www.quito.gob.ec | Website | www.quito.gob.ec | 50 | 2 | 0 |
| mail.quito.gob.ec | DNS Name | mail.quito.gob.ec | 100 | 1 | 1 |
| intranet.quito.gob.ec | DNS Name | intranet.quito.gob.ec | 100 | 1 | 1 |
| geoportal.quito.gob.ec | Website | geoportal.quito.gob.ec | 26 | 1 | 0 |
| omsc.quito.gob.ec | Website | omsc.quito.gob.ec | 32 | 1 | 0 |
| citaprevia.quito.gob.ec | Website | citaprevia.quito.gob.ec | 32 | 1 | 0 |
| cargaliviana.quito.gob.ec | Website | cargaliviana.quito.gob.ec | 36 | 1 | 0 |
| archivos.quito.gob.ec | Website | archivos.quito.gob.ec | 11 | 1 | 0 |
| www.responsabilidadsocial.quito.gob.ec | Website | www.responsabilidadsocial.quit... | 12 | 1 | 0 |
| www.patrimonio.quito.gob.ec | Website | www.patrimonio.quito.gob.ec | 13 | 1 | 0 |
| archivoqhistorico.quito.gob.ec | Website | archivoqhistorico.quito.gob.ec | 20 | 1 | 0 |
| consultamdmq.quito.gob.ec | Website | consultamdmq.quito.gob.ec | 100 | 1 | 0 |
| ao.quito.gob.ec | Website | ao.quito.gob.ec | 56 | 1 | 0 |
| epmhv.quito.gob.ec | Website | epmhv.quito.gob.ec | 65 | 1 | 0 |
| www.registrodelapropiedad.quito.gob.ec | Website | www.registrodelapropiedad.quit... | 79 | 1 | 0 |
| www.patronato.quito.gob.ec | Website | www.patronato.quito.gob.ec | 99 | 1 | 0 |
| www7.quito.gob.ec | Website | www7.quito.gob.ec | 0 | 1 | 0 |
| www.educacion.quito.gob.ec | Website | www.educacion.quito.gob.ec | 0 | 1 | 0 |
| agenciadecontrol.quito.gob.ec | Website | agenciadecontrol.quito.gob.ec | 0 | 1 | 1 |
| educacion.quito.gob.ec | Website | educacion.quito.gob.ec | 0 | 1 | 1 |
| smiq.quito.gob.ec | Website | smiq.quito.gob.ec | 11 | 1 | 0 |
| www.epmhv.quito.gob.ec | Website | www.epmhv.quito.gob.ec | 5 | 1 | 0 |
| sid.quito.gob.ec | Website | sid.quito.gob.ec | 0 | 1 | 0 |
| sthv.quito.gob.ec | Website | sthv.quito.gob.ec | 0 | 1 | 0 |
| pam.quito.gob.ec | Website | pam.quito.gob.ec | 0 | 1 | 0 |
| serviciosciudadanos.quito.gob.ec | Website | serviciosciudadanos.quito.gob.ec | 0 | 1 | 0 |
| 200.107.60.5 | IPv4 Address | 200.107.60.5 | 100 | 1 | 1 |
| 190.152.144.56 | IPv4 Address | 190.152.144.56 | 100 | 1 | 1 |
| 190.152.144.4 | IPv4 Address | 190.152.144.4 | 100 | 1 | 1 |
| 190.152.144.125 | IPv4 Address | 190.152.144.125 | 100 | 1 | 1 |
| 190.152.144.0-190.152.144.255 | Netblock | 190.152.144.0-190.152.144.255 | 100 | 3 | 1 |
| 200.107.60.0-200.107.60.255 | Netblock | 200.107.60.0-200.107.60.255 | 100 | 1 | 1 |
| 14420 | AS | 14420 | 100 | 2 | 0 |

**Figura 2.32** Listado de dominios ligados al Municipio de Quito. [39]

Este es uno de los primeros pasos para determinar qué tan expuesta se encuentra una organización en el internet, y con esta información tratar de proporcionar seguridad a cada entrada al sistema de la institución.

[39] Fuente: Información obtenida utilizando Maltego.

### 2.10.3.2 Scanning

Es una técnica pre-ataque que permite escanear puertos y vulnerabilidades de los diferentes equipos dentro de una red para identificar posibles agujeros de seguridad, el comando utilizado para ejecutar esta técnica es Nmap[40].

Se realizó el escaneo de puertos de los servidores de la AZNEE, obteniendo la información necesaria para determinar políticas de seguridad que mejoren la administración de acceso a los puertos, como se indicada en la figura 2.33.

- Herramienta utilizada Nmap

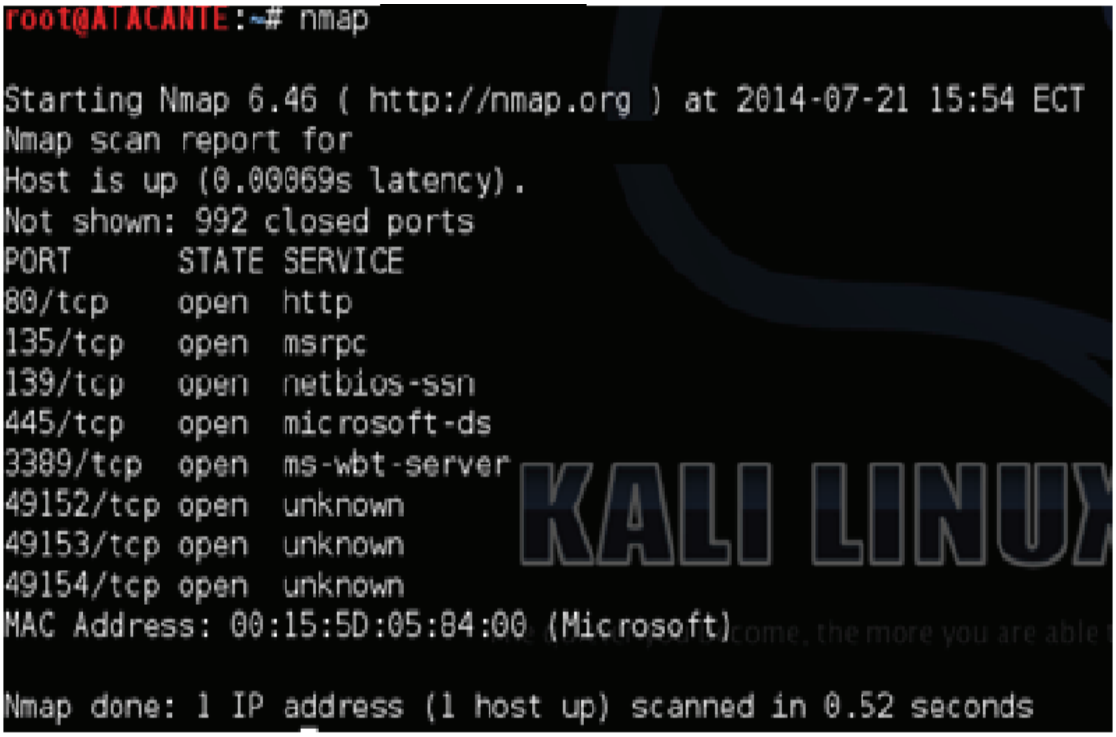



**Figura 2.33** Ejemplo de puertos abiertos en uno de los servidores

Este análisis se realizó en cada uno de los servidores de la red de la AZNEE. El resumen consolidado de los puertos abiertos por servidor se muestra en la tabla 2.9.

[40] Nmap: Network Mapper (Mapeador de puertos de red)

**Tabla 2.9** Puertos abiertos dentro de los servidores de la AZNEE

| Servidor | Puertos abiertos |
|---|---|
| DHCP | 80, 135, 139, 445, 3389, 49152, 49153, 49154. |
| DNS1 | 53, 88, 135, 139, 389, 445, 593, 636, 3268, 3269, 3389, 49152, 49153, 49154. |
| DNS2 | 22, 23, 53, 88, 135, 139, 389, 445, 464, 593, 636, 1026, 1433, 1434, 1443, 1500, 1501, 1503, 1521, 1503, 1521, 1524, 1533, 3268, 3269, 3389, 5555, 5900, 49152, 49153, 49154, 49155, 49157, 49158. |
| Turnos | 21, 80, 90, 135, 139, 445, 500, 990, 1947, 5000, 5001, 5002, 5432, 5500, 5800, 5900, 5901, 7001, 49152, 49153, 49154, 49155, 49157, 49158. |
| Aplicaciones | No se tuvo acceso al servidor dado que es una réplica del servidor de la matriz. |

A continuación se presentan las capturas de pantalla correspondientes a los puertos abiertos en los servidores especificados en la tabla 2.9.

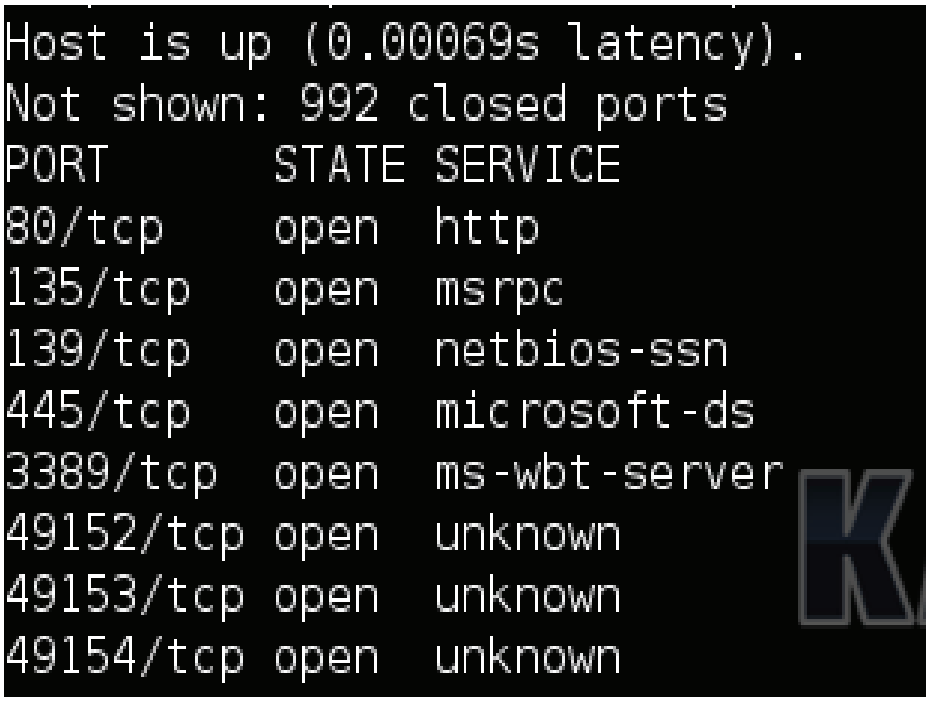



**Figura 2.34** Puertos abiertos Servidor DHCP

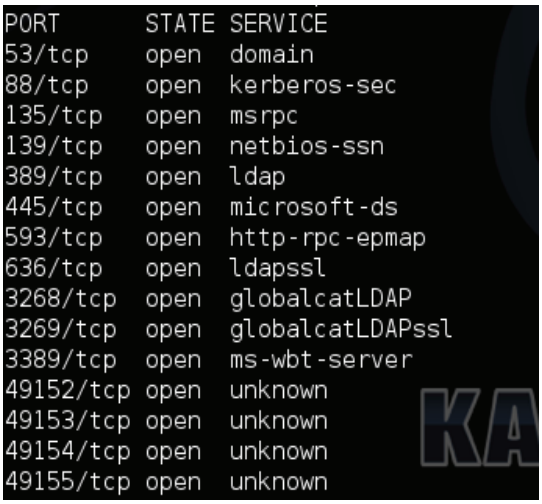



**Figura 2.35** Puertos abiertos Servidor DNS1

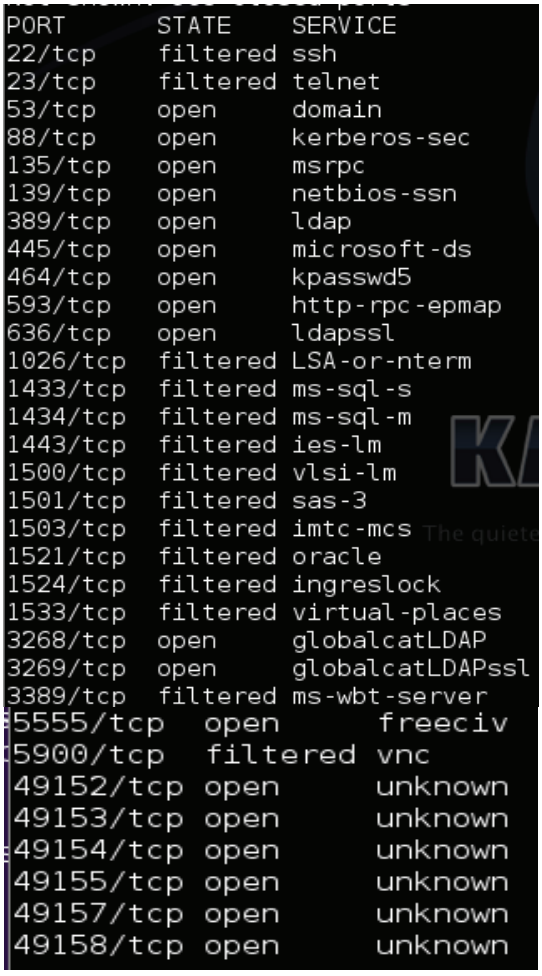



**Figura 2.36** Puertos abiertos DNS2

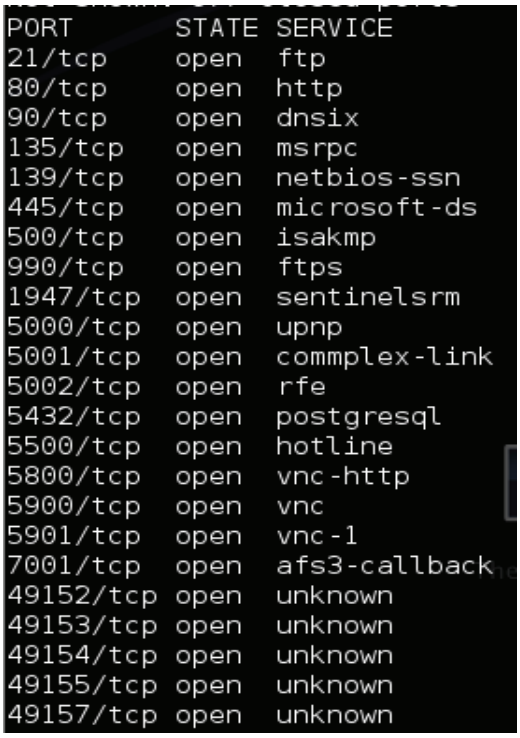



**Figura 2.37** Puertos abiertos Servidor de turnos

En la tabla 2.10 se muestra el listado de los puertos abiertos encontrados en los servidores de la AZNEE ligados a las vulnerabilidades que representan cada uno de ellos y el grado de incidencia en el sistema.

Esta información permitirá determinar los puertos que deben permanecer abiertos para que los procesos se desarrollen con normalidad y los que necesitan ser cerrados para minimizar posibles violaciones de seguridad.

**Tabla 2.10** Puertos abiertos sensibles a ataques

| Puerto abierto | Servicio | Vulnerabilidad | Grado |
|---|---|---|---|
| **23/tcp** | telnet | Las contraseñas de Telnet no se encuentran encriptadas por lo que son vulnerables a ataques de sniffing[41]. | Alto |

[41] Sniffing: Técnica de escucha del tráfico de la red.

| | | | |
|---|---|---|---|
| **135/tcp** | msrpc | Funcionaría como puerta trasera dando acceso al servidor de manera remota, este puerto viene habilitado por defecto. | Alto |
| **139/tcp** | netbios-ssn | Establece un servicio de sesión que emula TCP con un equipo remoto y permite sondear el tráfico compartido como archivos e impresoras | Medio |
| **445/tcp** | microsoft-ds | Permite la transferencia de archivos de forma remota, y un atacante puede utilizarlo para provocar desbordamiento de memoria. | Medio |
| **3389/tcp** | ms-wbt-server | Permite acceso remoto al equipo y la manipulación de los archivos del sistema. | Alto |
| **5555/tcp** | freeciv | Permite acceso por puerta trasera mediante una secuencia de comandos para causar fallos. | Medio |
| **5900/tcp** | VNC | Permite conexión remota a los servidores. | Alto |
| **1521/tcp** | Oracle database | Puerta de escucha del servidor de base de datos Oracle. | Alto |
| **5432/tcp** | PostgreSQL | Puerto de escucha del servidor de base de datos PostgreSQL | Alto |
| **80/tcp** | HTTP | Puerto de acceso web. | Alto |
| **21/tcp** | FTP | Puerto de transferencia de archivos. | Medio |
| **49152,49153, 53, 49154,49155,88, 593, 636, 3268, 3269,22,23,389, 464,1026, 1434 433,1443, 1500, 90,1501,1503, 1524, 1533, 5900, 49158,500, 9157, 990,1947, 5000, 5002,5500, 5800.** | | Puertos de uso general manejados por Windows Server, Active Directory y LDAP. | Bajo o nulo |

Como se puede apreciar en la tabla 2.10 existen puertos de escucha que permiten conectarse a base de datos del municipio central, sin embargo, son réplicas que deberían ser accedidas a través de los servicios requeridos y no visibles para todos, y más bien presentan un grado de vulnerabilidad alto, por lo que en el capítulo 3 se procederá a realizar las acciones correctivas necesarias para mitigar o eliminar los puertos que mantengan un riesgo de seguridad alto.

#### 2.10.3.3 Enumeration

Este pre-ataque permite enumerar los recursos dentro del objetivo como por ejemplo: identificar grupos, cuentas de usuario, contraseñas y recopilar información de recursos compartidos (impresoras, dispositivos de almacenamiento externo, etc.), con esta información un atacante podría conseguir escalar privilegios hasta llegar al nivel del administrador e instalar software malicioso que le permitirá tener control sobre la máquina, recolectar o robar datos y dejar puertas traseras para próximas intrusiones.

- Herramienta utilizada Dnsmap

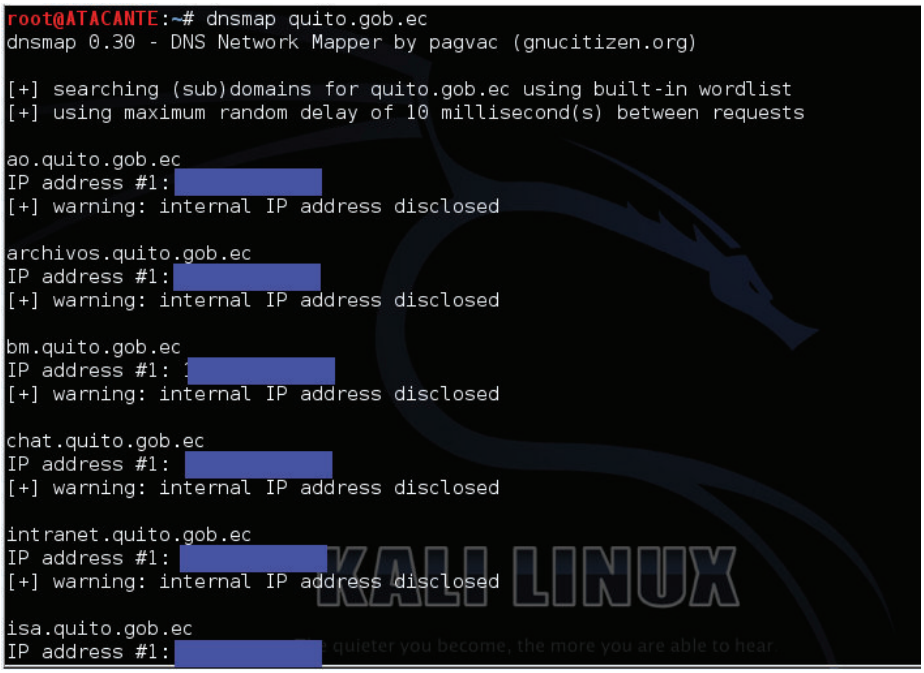



**Figura 2.38** Ejemplo de información encontrada con Dnsmap

En la figura 2.38 se muestran los subdominios pertenecientes a www.quito.gob.ec que son invisibles para el público pero que existen en los registros de DNS y que pueden ser explotados mediante ataques basados en dominios, por confidencialidad no se muestran las direcciones IP respectivas.

Este es el siguiente paso que ejecuta un atacante cuando no ha podido acceder a información de la institución mediante footprinting o scanning, regularmente son archivos o dominios que no están siendo usados por los administradores de la red y que cuentan con información útil para el atacante.

En el capítulo 3 se establecerán políticas en las que se especifique el tiempo y las condiciones para realizar una depuración de los dominios que no van a ser utilizados, de esta manera se disminuirán los agujeros en la seguridad de la red.

#### 2.10.3.4 Troyanos y Puertas Traseras

Los troyanos son programas que se hacen pasar por genuinos, cuyo verdadero objetivo es ejecutar software malicioso en el equipo donde sean instalados. Al ejecutarse se auto incluye en la rutina de inicio del equipo y desde ese instante, puede vigilar el equipo hasta que el usuario se conecta a Internet.

Las puertas traseras o backdoors por su parte son bugs[42] que permiten acceso a un equipo de forma remota, aprovechan la arquitectura de internet que se basa en el modelo cliente-servidor.

Para determinar qué tan expuesta se encuentra la red de la AZNEE a un ataque de esta naturaleza se utilizó la herramienta Ettercap[43], en la figura 2.39 se muestran las diferentes alternativas que posee la herramienta para permitir capturar información.

- Herramienta utilizada Ettercap

[42] Bugs: Debilidad, error o defecto en un sistema informático.

[43] Ettercap: http://ettercap.github.io/ettercap/

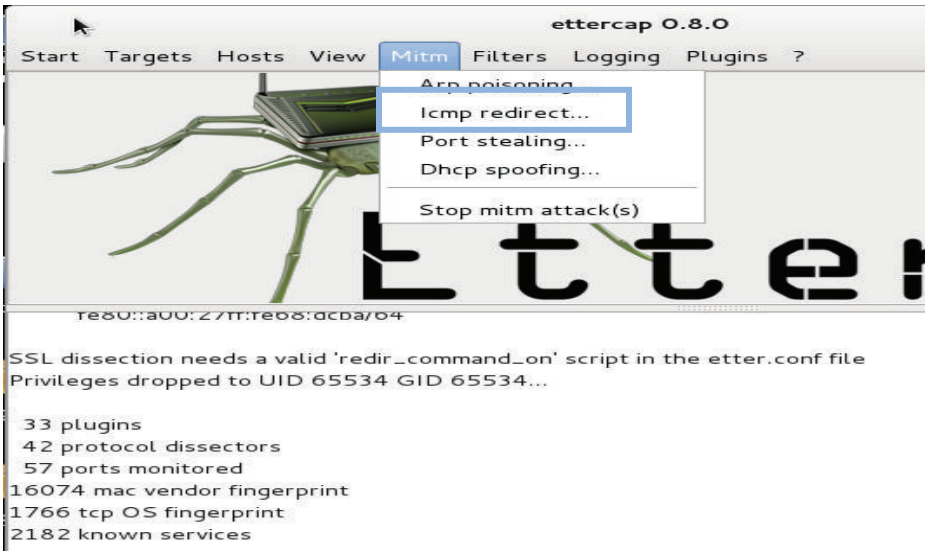



**Figura 2.39** Pantalla principal de Ettercap

Con este software se envenenó la red con paquetes ARP[44] para producir un desbordamiento de la memoria caché de los equipos de red y capturar paquetes de información bajo la técnica de hombre en el medio. Esta técnica fue bloqueada por el antivirus instalado en las máquinas de la AZNEE, como se indica en la figura 2.40.

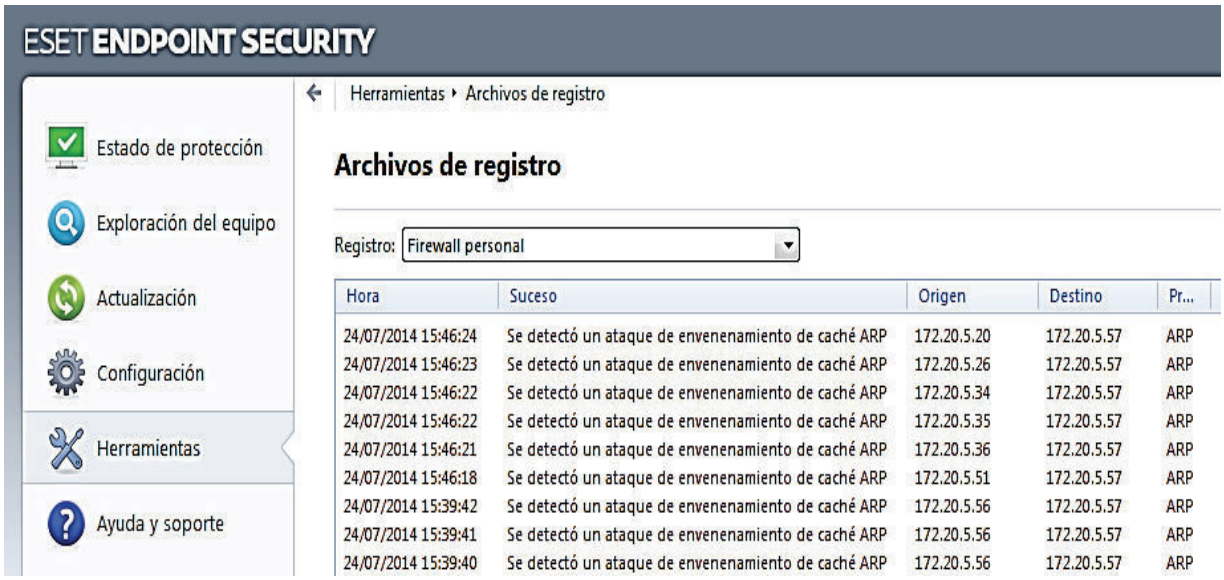



**Figura 2.40** Archivo de registro del antivirus

[44] ARP: Address Resolution Protocol , permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP.

#### 2.10.3.5 Ingeniería Social

La ingeniería social es una técnica que se basa en el engaño o abuso de confianza de personas inescrupulosas que obtienen información sensible de los usuarios y personal de la entidad, y la utilizan para realizar ataques maliciosos a la integridad de la institución.

En la AZNEE existe personal ajeno a la institución que de una u otra forma tiene acceso a información sensible o confidencial, por citar un ejemplo se encuentran estudiantes secundarios realizando pasantías; estos sujetos son fáciles de atacar.

Un ejemplo de la aplicación de esta técnica fue obtener información relevante de la institución como contraseñas de equipos, direcciones IPs y claves de acceso a ciertos servicios que maneja la AZNEE y que por motivos de confidencialidad los resultados no pueden ser expuestos en este proyecto.

#### 2.10.3.6 Conclusiones Hacking Ético

**Tabla 2.11** Resultados de Hacking Ético

| Técnica de hacking ético | Herramienta utilizada | Datos obtenidos | Vulnerabilidad encontrada | Observaciones |
|---|---|---|---|---|
| **Footprinting** | Maltego | Dominios ligados a quito.gob.ec que se encuentran expuestos en el internet. | 26 dominios que podrían ser blancos de ataques. | Los dominios listados con esta herramienta muestran únicamente los expuestos en internet, mas no los que se obtuvieron con Dnsmap. |
| **Scanning** | Nmap | Puertos abiertos en los servidores de la institución. | Puertos innecesarios abiertos en los servidores de DNS, DHCP y Turnos. | Se debe habilitar únicamente los puertos necesarios para realizar las transacciones específicas de cada servidor. |

| | | | | |
|---|---|---|---|---|
| **Enumeration** | Dnsmap | Subdominios pertenecientes a quito.gob.ec invisibles para el público pero que existen en los registros del DNS. | Subdomininios que podrían ser explotados mediante la técnica de ataques basados en dominios para escalar privilegios dentro de la red. | Es recomendable eliminar los subdominios que van a dejar de ser utilizados para disminuir la probabilidad de ataques. |
| **Troyanos y puertas traseras** | Ettercap | No se pudieron obtener datos debido a que el antivirus bloqueó el ataque de paquetes ARP. | No se pudo capturar mensajes enviados entre equipos de la red. | La institución cuenta con el antivirus ESET ENDPOINT SECURITY que bloquea ataques de troyanos en el sistema. |
| **Ingeniería social** | Indagación | Contraseñas de switches y routers | Información sensible sin la debida codificación y protección física. | Esta información no puede ser expuesta por motivos de confidencialidad. |

Las medidas para mitigar los riegos encontrados se muestran en el capítulo 3.

## 2.11 ANÁLISIS DE REQUERIMIENTOS

En bases a la información recolectada se rediseñará la red multiservicios de tal manera que satisfaga las necesidades existentes actualmente en la AZNEE. Con este fin se listan los requerimientos de la red multiservicios con una escalabilidad mínima de 5 años.

### 2.11.1 CABLEADO ESTRUCTURADO

Para la AZNEE se planea implementar una nueva solución de cableado estructurado que permita mejorar la relación señal a ruido y de esta manera tener mayor fiabilidad en la aplicaciones actuales y mejor velocidad en las aplicaciones futuras.

Los lineamientos base para el rediseño del cableado estructurado son:

- ✓ La norma ANSI/TIA 568.C que fue pública en el 2009 y que agrupa los requerimientos actuales de los sistemas, tanto en características y rendimiento de los componentes como en su estructura.
- ✓ La norma ANSI/TIA 569.B determina los requerimientos de rutas y espacios de telecomunicaciones.
- ✓ Para el sistema de cableado estructurado se utilizará cable categoría 6 UTP que brinda una velocidad de 1 Gbps y un ancho de banda de 250 MHz, lo que permitirá tener una infraestructura que se adapte a aplicaciones que demanden mayores recursos de la red.
- ✓ La norma ANSI/TIA 606.A define la documentación y administración para el etiquetado y registro de las distintas secciones de la red, sean éstos cables, patch panel, patch cords, espacios de telecomunicaciones y ductos.
- ✓ Reubicación de la acometida de servicios de telecomunicaciones hacia el cuarto de equipos, de esta forma se asegura la no manipulación de los enlaces de datos, que son el eje principal de funcionamiento de la institución.
- ✓ Reubicación de los equipos activos instalados en los gabinetes de pared ubicados actualmente en las oficinas hacia el cuarto de telecomunicaciones para la gestión adecuada de los enlaces.
- ✓ Proveer de la seguridad física necesaria a los cuartos de telecomunicaciones para que no sean sensibles a ataques malintencionados.
- ✓ Provisión de enlaces de fibra óptica multimodo para comunicar los cuartos de telecomunicaciones con el cuarto de equipos de la institución.

### 2.11.2 REQUERIMIENTOS PARA LA RED INTERNA

- ✓ Dar un adecuado sistema de gestión y monitoreo para los equipos de telecomunicaciones de la AZNEE.
- ✓ Definir grupos de usuarios con requisitos en común y agruparlos en VLANs para mejorar la administración de la red de datos y voz.
- ✓ Determinar las características necesarias para equipos de telecomunicaciones y servidores para que cumplan con las funciones establecidas.
- ✓ Realización de respaldos de los componente del sistema, y tener duplicados de los mismos para que cualquiera de sus instancias pueda ser utilizada en caso de falla.
- ✓ La información de los componentes del sistema deberá estar protegida para su acceso y la no divulgación por el personal de informática.

### 2.11.3 REQUERIMIENTO DE VOZ

Se plantea una solución que permita sustituir la central telefónica análoga por una central basada en telefonía IP, la misma que funcionará con los mismos puntos de datos expuestos en este rediseño, debido a que la infraestructura de la AZNEE no permite una excesiva aglomeración de cables UTP.

Por tal razón se utilizarán teléfonos IP que constan de 2 puertos de conmutación, que permiten hacer una interconexión con la computadora y de esta manera correr las dos aplicaciones por un solo punto de red, se plantea en primera instancia la instalación de 40 teléfonos IP que pertenecerán a cada departamento.

La razón de hacer el cambio de una telefonía análoga por una telefonía IP es el ahorro en costos, y la integración de servicios. A través del empleo de la tecnología IP se puede obtener como beneficio adicional la posibilidad de integrar al servicio de transmisión de voz otros servicios adicionales como los son la transmisión paralela de datos, videos y otros archivos.

### 2.11.4 REQUERIMIENTOS DE LA WLAN

- ✓ No existe cobertura en ciertas áreas de la AZNEE por lo que es necesario realizar un escaneo de la intensidad de señal de la wlan existente.
- ✓ Determinar si los equipos existentes cumplen con los requerimientos planteados para el rediseño de la red inalámbrica.
- ✓ Definir perfiles de usuario de acuerdo a las aplicaciones a las que podrán tener acceso para optimizar los recursos de la red.
- ✓ Establecer cambios periódicos de contraseñas de acceso para garantizar que solo el personal autorizado utilice los recursos de la red, por lo que la distribución de las nuevas claves estará a cargo del personal de sistemas de la institución.

### 2.11.5 REQUERIMIENTOS DE SEGURIDAD

En base a las vulnerabilidades encontradas mediante la implementación de la honeynet y utilizando las técnicas respectivas se requiere lo siguiente:

- ✓ Implementar políticas de seguridad para la administración y gestión de los servidores.
- ✓ Implementación de políticas de seguridad para la administración y gestión de usuarios en el Active Directory[45] y LDAP.
- ✓ Creación de un instructivo para la gestión y administración de los espacios de telecomunicaciones, redes alámbricas e inalámbricas y las posibles medidas de seguridad a tener en cuenta para mitigar riesgos de seguridad en las mismas.
- ✓ Establecer lineamientos para el manejo de copias y respaldos de seguridad de los servidores que manejen información sensible.
- ✓ Políticas de actualizaciones de antivirus y equipos de escritorio.

[45] Active Directory: Es el servicio de directorio de una red Windows

# CAPÍTULO III

# REDISEÑO DE LA RED DE LA AZNEE

En este capítulo se plantea una solución viable para realizar la red multiservicios y satisfacer los requerimientos y necesidades de los usuarios de la AZNEE.

Se observa que las redes de las administraciones del Distrito Metropolitano de Quito no cuentan con un diseño basado en estándares, por el contrario, cada uno se ha ido adaptando según el movimiento del personal (despidos, traslados, ingresos, etc.) como es el caso de la AZNEE, que debido al crecimiento de usuarios se convirtió en un ambiente desorganizado.

## 3.1 CRECIMIENTO DE USUARIOS

Para el rediseño de la red de la AZNEE se debe considerar el número de usuarios actuales y establecer un crecimiento a futuro para poder brindar escalabilidad a la nueva red.

El departamento de recursos humanos proporcionó estadísticas del crecimiento de usuarios, como se puede ver en la figura 3.1.

Existe un incremento del 5%, mismo que se debe a varias modificaciones en la estructura del edificio, además de ciertas reubicaciones del personal a nuevas instalaciones del Municipio del Distrito Metropolitano de Quito.

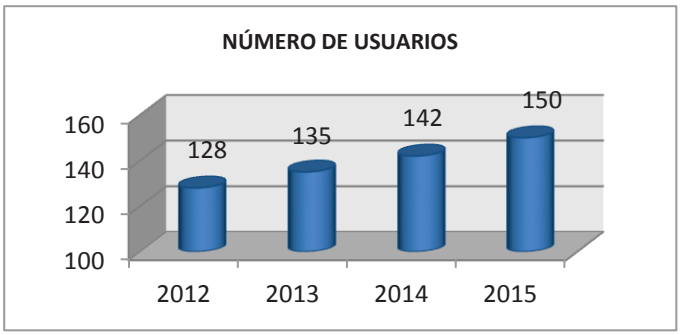



**Figura 3.1** Estadísticas de usuarios de la AZNEE.

Estos datos se pueden verificar en base a fórmula de valor futuro, en donde:

$$V_f = V_o(1+i)^n$$

$V_f$ = Número de usuarios en un determinado año

$V_o$ = Número de usuarios iniciales en determinado año

$i$ = Porcentaje de crecimiento de usuarios al año

$n$ = Número de años

Realizando el cálculo para el año 2015 se tiene:

$$V_f = 142(1+0.1)^1$$

$$V_f = 150\ usuarios$$

Con estos resultados se estima un crecimiento de usuarios de red del 5 % con una escalabilidad a 5 años. En la tabla 3.1 se muestra el cálculo respectivo para cada año.

**Tabla 3.1** Estimación de usuarios de red.

| AÑOS | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|---|---|---|
| USUARIOS | 128 | 135 | 142 | **150** | 157 | 164 | 172 | 181 | **190** |

## 3.2 REDISEÑO DE LA RED MULTISERVICIOS

### 3.2.1 DIMENSIONAMIENTO DEL TRÁFICO

Para calcular el ancho de banda que se necesitará para este rediseño, se analizarán los servicios utilizados por la AZNEE y el nuevo servicio de telefonía IP.

Los servicios a analizar en base a la encuesta realizada son:

- Correo Electrónico
- Páginas web
- Servicio de Mensajería
- Servicio de actualizaciones
- Antivirus
- Telefonía IP

#### 3.2.1.1 Ancho de banda para servicio de correo electrónico

El servicio de correo electrónico que posee la AZNEE, tiene un tamaño promedio de los paquetes de 200 KB (dato obtenido con Ntop), el número de correos enviados por hora es de 10, dato que se obtuvo mediante la encuesta realizada (véase sección 2.7), por lo que el ancho de banda aproximado es:

$$\mathrm{AB}_{\mathrm{correo-usuario}} = \frac{200\ \mathrm{KB}}{\mathrm{correos}} * \frac{1024\ \mathrm{Byte}}{1\ \mathrm{KByte}} * \frac{8\ \mathrm{bits}}{1\ \mathrm{Byte}} * \frac{10\ \mathrm{correos}}{1\ \mathrm{hora}} * \frac{1\ \mathrm{hora}}{3600\ \mathrm{seg}}$$

$$\mathrm{AB}_{\mathrm{correo-usuario}} \approx 4551{,}1\ \mathrm{bps}$$

Considerando los resultados obtenidos en la figura 2.20 donde se evidencia un 50% de usuarios accediendo al servicio de correo a la vez y adicionando un 10% para un crecimiento futuro, se establece una simultaneidad del 60%.

El número de usuarios actualmente es de 150 y aplicando un porcentaje de simultaneidad del 60% se obtiene 90 usuarios concurrentes en la red que están accediendo al servicio de correo de la institución.

$$\mathrm{AB}_{\mathrm{correo-total}} = \mathrm{AB}_{\mathrm{usuario}} * \#\mathrm{Usuarios}_{\mathrm{simultáneos}}$$

$$\mathrm{AB}_{\mathrm{correo-total}} = 4551{,}1\ \mathrm{bps} * 90 = 409599\ \mathrm{bps}$$

$$\mathrm{AB}_{\mathrm{correo-total}} = 518825{,}4\ \mathrm{bps} * \frac{1\mathrm{kbps}}{1024\mathrm{bps}} = 400\ \mathrm{Kbps}$$

### 3.2.1.2 Ancho de banda para servicio de páginas web

El servicio de páginas web es el más utilizado por los usuarios de la AZNEE, el tamaño promedio de los paquetes de este servicio es de 850 KB (dato obtenido con Ntop), en base a la encuesta se obtuvo que los usuarios ingresan a alrededor de 10 páginas web hora (véase sección 2.7), por lo que el ancho de banda aproximado es:

$$\mathrm{AB}_{\mathrm{páginas-usuario}} = \frac{850\ \mathrm{KB}}{\mathrm{páginas}} * \frac{1024\ \mathrm{Byte}}{1\ \mathrm{KByte}} * \frac{8\ \mathrm{bits}}{1\ \mathrm{Byte}} * \frac{10\ \mathrm{páginas}}{1\ \mathrm{hora}} * \frac{1\ \mathrm{hora}}{3600\ \mathrm{seg}}$$

$$\mathrm{AB}_{\mathrm{páginas-usuario}} \approx 19342{,}22\ \mathrm{bps}$$

Considerando un promedio del 35% del total de usuarios que acceden a páginas web en base a la figura 2.21 y agregando una holgura del 5%, se estima un 40% de simultaneidad de usuarios. Este porcentaje multiplicado por el total de usuarios (150 usuarios) da como resultado 60 usuarios concurrentes que utilizan el servicio web.

$$\mathrm{AB}_{\mathrm{páginas-total}} = \mathrm{AB}_{\mathrm{usuario}} * \#\mathrm{Usuarios}_{\mathrm{simultáneos}}$$

$$\mathrm{AB}_{\mathrm{páginas-total}} = 19342{,}22\ \mathrm{bps} * 60 = 1160533{,}2\ \mathrm{bps}$$

$$\mathrm{AB}_{\mathrm{páginas-total}} = 1160533{,}2\ \mathrm{bps} * \frac{1\mathrm{kbps}}{1024\mathrm{bps}} \approx 1133{,}33\ \mathrm{kbps}$$

### 3.2.1.3 Ancho de banda para servicio de mensajería

El servicio de mensajería es un servicio que es muy usado para las conversaciones en línea y asesoramiento online en la AZNEE, el tamaño promedio de los paquetes de este servicio es de 120 KB (dato obtenido con Ntop), en base a la encuesta se

obtuvo que los usuarios tienen alrededor de 6 conversaciones por hora (véase sección 2.7), por lo que el ancho de banda aproximado es:

$$\mathrm{AB}_{\mathrm{conversaciones-usuario}} = \frac{120\ \mathrm{Kbytes}}{\mathrm{conversaciones}} * \frac{1024\ \mathrm{Byte}}{1\ \mathrm{KByte}} * \frac{8\ \mathrm{bits}}{1\ \mathrm{Byte}} * \frac{6\ \mathrm{conversaciones}}{1\ \mathrm{hora}} * \frac{1\ \mathrm{hora}}{3600\ \mathrm{seg}}$$

$$\mathrm{AB}_{\mathrm{conversaciones-usuario}} = 1638{,}4\ \mathrm{bps}$$

Considerando que el servicio de mensajería instantánea es utilizado por la AZNEE en diferentes periodos de tiempo con picos variados en base a las encuestas realizadas, se ha estimado un total de 40% de usuarios que acceden simultáneamente al servicio durante el día. Este porcentaje multiplicado por el total de usuarios (150 usuarios) da como resultado 60 usuarios concurrentes.

$$\mathrm{AB}_{\mathrm{conversaciones-total}} = \mathrm{AB}_{\mathrm{usuario}} * \#\mathrm{Usuarios}_{\mathrm{simultáneos}}$$

$$\mathrm{AB}_{\mathrm{conversaciones-total}} = 1638{,}4\ \mathrm{bps} * 60 = 98304\ \mathrm{bps}$$

$$\mathrm{AB}_{\mathrm{conversaciones-total}} = 124518{,}4\ \mathrm{bps} * \frac{1\mathrm{kbps}}{1024\mathrm{bps}} = 96\ \mathrm{kbps}$$

#### 3.2.1.4 Servicio de actualizaciones

Considerando que todas las máquinas de la AZNEE mantienen un sistema operativo Windows 7, las actualizaciones tienden a ser pesadas para ser descargadas por la red por lo que las mismas se deberán de gestionar en un horario diferido en donde no se encuentren desempeñando actividades los usuarios de la red.

El servicio de actualizaciones usa un protocolo UDP (User Datagram Protocol) y QoS (Quality of Service ) por lo que ancho de banda de la red no se verá afectado de ninguna manera.

### 3.2.1.5 Ancho de banda para servicio de antivirus

El servicio de antivirus permite brindar la seguridad necesaria para los equipos de la AZNEE; tomando en cuenta el tamaño promedio de los paquetes para las actualizaciones respectivas se tiene un valor de 2 MB, en los cuales se receptan alrededor de una actualización por hora, por lo que la tasa aproximada para la actualización del antivirus es:

$$AB_{\substack{actualización \\ antivirus}} = \frac{2\ MB}{actualización} * \frac{1024\ KByte}{1\ MByte} * \frac{1024\ Byte}{1\ KByte} * \frac{8\ bits}{1\ Byte} * \frac{1\ actualización}{1\ hora} * \frac{1\ hora}{3600 seg}$$

$$\mathrm{AB}_{\text{actualización antivirus}} = 4660.34\ \text{bps}$$

$$\mathrm{AB}_{\substack{\text{actualización} \\ \text{servidor antivirus}}} = \#\text{usuarios} * \mathrm{AB}_{\text{usuario}}$$

$$\mathrm{AB}_{\substack{\text{actualización} \\ \text{servidor antivirus}}} = 1 * 4660{,}34\ \text{bps}$$

$$\mathrm{AB}_{\substack{\text{actualización} \\ \text{servidor antivirus}}} = 4660{,}34\text{bps} * \frac{1\text{kbps}}{1024\text{bps}} = 4{,}55\ \text{kbps}$$

### 3.2.1.6 Capacidad del Tráfico de voz

Para el ancho de banda necesario para la VoIP, se determinará la tasa y el tamaño del paquete que dependerá de codificador que se utilice y el encabezado de los protocolos que intervienen en la encapsulación de la trama de voz. Se encapsula primero en RTP (Protocolo de Transporte en tiempo real), luego en UDP o TCP, antes de ser transmitida en una trama IP. LA figura 3.2 se encuentran los códecs más utilizados para la telefonía IP.

| Codec Information | | | | Bandwidth Calculations | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Codec & Bit Rate (Kbps) | Codec Sample Size (Bytes) | Codec Sample Interval (ms) | Mean Opinion Score (MOS) | Voice Payload Size (Bytes) | Voice Payload Size (ms) | Packets Per Second (PPS) | Bandwidth MP or FRF.12 (Kbps) | Bandwidth w/cRTP MP or FRF.12 (Kbps) | Bandwidth Ethernet (Kbps) |
| G.711 (64 Kbps) | 80 Bytes | 10 ms | 4.1 | 160 Bytes | 20 ms | 50 | 82.8 Kbps | 67.6 Kbps | 87.2 Kbps |
| G.729 (8 Kbps) | 10 Bytes | 10 ms | 3.92 | 20 Bytes | 20 ms | 50 | 26.8 Kbps | 11.6 Kbps | 31.2 Kbps |
| G.723.1 (6.3 Kbps) | 24 Bytes | 30 ms | 3.9 | 24 Bytes | 30 ms | 33.3 | 18.9 Kbps | 8.8 Kbps | 21.9 Kbps |
| G.723.1 (5.3 Kbps) | 20 Bytes | 30 ms | 3.8 | 20 Bytes | 30 ms | 33.3 | 17.9 Kbps | 7.7 Kbps | 20.8 Kbps |
| G.726 (32 Kbps) | 20 Bytes | 5 ms | 3.85 | 80 Bytes | 20 ms | 50 | 50.8 Kbps | 35.6 Kbps | 55.2 Kbps |
| G.726 (24 Kbps) | 15 Bytes | 5 ms | | 60 Bytes | 20 ms | 50 | 42.8 Kbps | 27.6 Kbps | 47.2 Kbps |
| G.728 (16 Kbps) | 10 Bytes | 5 ms | 3.61 | 60 Bytes | 30 ms | 33.3 | 28.5 Kbps | 18.4 Kbps | 31.5 Kbps |
| G722_64k(64 Kbps) | 80 Bytes | 10 ms | 4.13 | 160 Bytes | 20 ms | 50 | 82.8 Kbps | 67.6Kbps | 87.2 Kbps |
| ilbc_mode_20(15.2Kbps) | 38 Bytes | 20 ms | NA | 38 Bytes | 20 ms | 50 | 34.0Kbps | 18.8 Kbps | 38.4Kbps |
| ilbc_mode_30(13.33Kbps) | 50 Bytes | 30 ms | NA | 50 Bytes | 30 ms | 33.3 | 25.867 Kbps | 15.73Kbps | 28.8 Kbps |

**Tabla 3.2** Tabla de códecs para telefonía IP [46]

El ancho de banda para del servicio de Telefonía IP viene dado por la siguiente ecuación.

$$BW = Tamaño\ \ total\ del\ paquete * PPS$$

Dónde:

- $Tamaño\ \ total\ del\ paquete = Encabezado\ \ RTP + Encabezado\ \ UDP + Encabezado\ \ IP + Encabezado\ \ Ethernet + tamaño\ de\ carga\ útil\ de\ voz$
- $PPS$ = Representa el número de paquetes que es preciso transmitir por segundo para enviar la velocidad de bits del códec.

Para calcular la longitud del paquete se debe tener en cuenta que la señal de voz se encapsula en RTP, luego en UDP y este en se encapsula en IP y todo en conjunto se encapsula en la capa de enlace a utilizar sobre la LAN y el tipo de códec a usar.

[46] Fuente: https://www.sinologic.net/blog/tag/codec

Para este rediseño se eligió el códec G.729, debido a que es utilizado en su mayoría para aplicaciones VoIP por su bajo requerimiento de ancho de banda 8Kbit/s.

En la tabla 3.3 se encuentra las cabeceras de cada uno de los protocolos que forman parte de la trama de VoIP sobre la LAN.

**Tabla 3.3** Cabecera para Telefonía IP

| Protocolo | Longitud de Cabecera |
|---|---|
| RTP | 12 bytes |
| UDP | 8 bytes |
| IP | 20 bytes |
| Ethernet | 20 bytes |
| G.729 | 20 bytes |

$$Tamaño\ \ total\ del\ paquete = 12\ bytes + 8\ bytes + 20\ bytes + 20\ bytes + 20\ bytes$$

$$Tamaño\ \ total\ del\ paquete = 80\ bytes * 8bits/byte$$

$$\boldsymbol{Tamaño\ \ total\ del\ paquete = 640\ bits}$$

Para calcular el PPS se utiliza la siguiente fórmula en base a la tabla 3.2:

$$PPS = \frac{Velocidad\ de\ bits\ del\ códec}{Tamaño\ de\ la\ carga\ útil\ de\ voz}$$

$$PPS = \frac{tamaño\ del\ códec/intervalo\ del\ códec}{Tamaño\ de\ la\ carga\ útil\ de\ voz}$$

$$PPS = \frac{80\ bits/10\ ms}{160\ bits}$$

$$PPS = 8\ kbps/160bits$$

$$\boldsymbol{PPS = 50\ pps}$$

Por lo tanto el ancho de banda cuando se utiliza la capa de enlace Ethernet es:

$$BW = Tamaño\ \ total\ del\ paquete * PPS$$

$$BW = 640\ bits * 50\ pps$$

$$\boldsymbol{BW = 32\ kbps}$$

La trama de VoIP también puede viajar sobre la WAN y para calcular la longitud del paquete se debe se debe tener en cuenta que la señal de voz se encapsula en RTP, luego en UDP y este en se encapsula en IP y todo en conjunto se encapsula en la capa de enlace de PPP (Protocolo Punto Punto)[47] que viajará sobre la WAN y el tamaño de carga útil de voz del códec G.729

En la tabla 3.4 se encuentra las cabeceras de cada uno de los protocolos que forman parte de la trama de VoIP sobre la WAN.

**Tabla 3.4** Cabecera para Telefonía IP

| Protocolo | Longitud de Cabecera |
|---|---|
| RTP | 12 bytes |
| UDP | 8 bytes |
| IP | 20 bytes |
| PPP | 4 bytes |
| G.729 | 20 bytes |

$$Tamaño\ \ total\ del\ paquete = 2\ bytes + 4\ bytes + 20\ bytes$$

$$Tamaño\ \ total\ del\ paquete = 26\ bytes * 8bits/byte$$

$$\boldsymbol{Tamaño\ \ total\ del\ paquete = 208\ bits}$$

Para calcular el PPS se utiliza la siguiente fórmula en base a la tabla 3.2:

[47] PPP: Es un protocolo de WAN utilizado con frecuencia y proporciona conexiones de LAN a WAN a varios protocolos

$$PPS = \frac{Velocidad\ de\ bits\ del\ códec}{Tamaño\ de\ la\ carga\ útil\ de\ voz}$$

$$PPS = \frac{tamaño\ del\ códec/intervalo\ del\ códec}{Tamaño\ de\ la\ carga\ útil\ de\ voz}$$

$$PPS = \frac{80\ bits/10\ ms}{160\ bits}$$

$$PPS = 8\ kbps/160 bits$$

$$\boldsymbol{PPS = 50\ pps}$$

Por lo tanto el ancho de banda cuando se utiliza la capa de enlace Ethernet es:

$$BW = Tamaño\ \ total\ del\ paquete * PPS$$

$$BW = 208\ bits * 50\ pps$$

$$\boldsymbol{BW = 10,4\ kbps}$$

El ancho de banda total que se estima para el rediseño con los datos calculados anteriormente se encuentra en la tabla 3.5.

**Tabla 3.5** Enlace de datos requerido

| **CÁLCULO DEL ANCHO DE BANDA** | |
|---|---|
| Correo Electrónico | 400 Kbps |
| Páginas web | 1133,33 Kbps |
| Servicio de Mensajería | 96 Kbps |
| Actualizaciones del Antivirus. | 4,55 Kbps |
| Telefonía IP (40 usuarios) | 1280 Kbps |
| **TOTAL** | **2913.88 Kbps** |
| **ANCHO DE BANDA MÍNIMA DEL PROVEEDOR** | **3 Mbps** |

### 3.2.2 DISEÑO LAN PASIVA

La AZNEE no cuenta con un sistema de cableado estructurado que cumpla con normas internacionales, debido a que en sus inicios la red estuvo diseñada para manejar alrededor de 90 usuarios; con el paso del tiempo y la diversidad de servicios ofrecidos por la AZNEE, la red creció de manera indiscriminada sin ninguna planificación.

Para el rediseño de la red se contemplan los siguientes lineamientos:

- El sistema se basará en la norma ANSI/TIA 568.C.0 - Generic Structure Cabling
- De acuerdo al dimensionamiento del tráfico se plantea la migración de categoría 5e a categoría 6, la misma que permite manejar un ancho de banda de 250 MHz y una velocidad de transmisión de 1 Gbps a 100 metros.

A continuación se detallan los parámetros que deberán cumplir cada uno de los subsistemas que conforman el sistema de cableado estructurado.

#### 3.2.2.1 Áreas de trabajo

Es el espacio donde los usuarios interactúan con los dispositivos de telecomunicaciones (computadoras, teléfonos IP, impresoras, fax, etc.), se colocará un punto de red por cada usuario, puesto que el rediseño contempla el paso de telefonía análoga a telefonía IP.

Cada área de trabajo deberá disponer de un patch cord de 5 metros como máximo, para este rediseño se utilizará un patch cord de 2 metros para conectarse con los diferentes dispositivos.

### 3.2.2.2 Cableado horizontal

El cableado horizontal corre desde la salida de telecomunicaciones del área de trabajo hasta el punto de interconexión horizontal que se encuentra en el cuarto de telecomunicaciones, este subsistema debe seguir una topología en estrella.

La distancia de recorrido del cable estará limitado por la norma ANSI/TIA 568C.1 en la cual se especifica una longitud máxima de 90 metros.

El cable deberá cumplir con los siguientes requerimientos:

- Cable categoría 6.
- Conductores de cobre sólido de 24 AWG aislado con polietileno de alta densidad HDPE.
- Chaqueta tipo CMR[48].
- Poseer una barra plástica tipo cruceta para minimizar la interferencia electromagnética entre los pares trenzados.

### 3.2.2.3 Cableado vertical o Backbone

Este subsistema provee la interconexión entre los cuartos de telecomunicaciones y el cuarto de equipos, además debe ser parte de la topología de estrella jerárquica.

Para definir el tipo de medio que se utilizará para el backbone se debe tener en cuenta que la velocidad de transmisión del cableado vertical debe ser igual o mayor que la del cableado horizontal, para este rediseño se utilizará fibra óptica multimodo tipo OM3 que provee una velocidad de 10Gbps a una distancia máxima de 300 metros. En la figura 3.2, se puede observar los enlaces de fibra que se colocarán entre los cuartos de telecomunicaciones y el cuarto de equipos.

[48] CMR: Chaqueta tipo Riser para aplicaciones en las cuales los cables sobrepasen más de un piso para evitar que el fuego se propague de uno a otro.

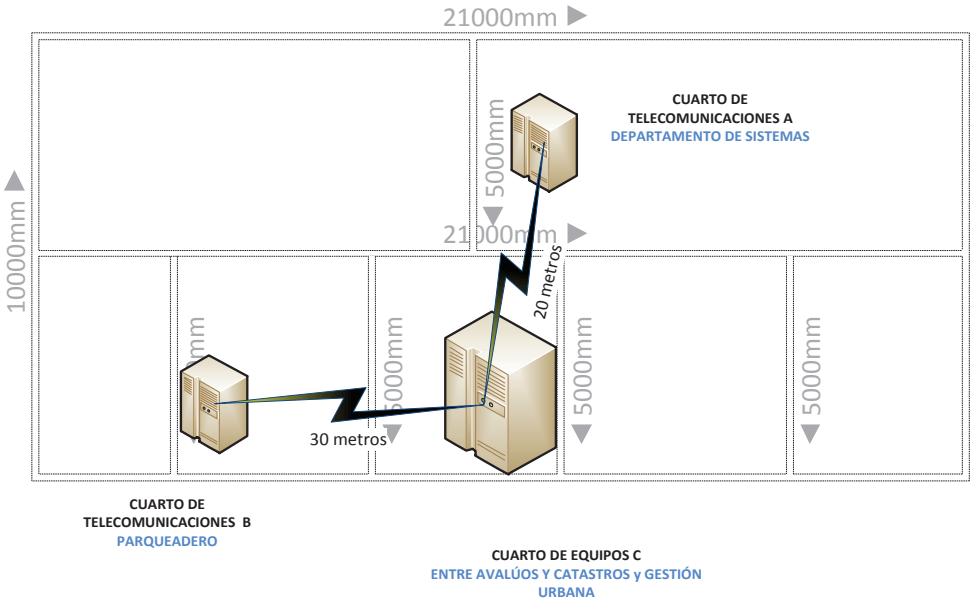



**Figura 3.2** Diagrama de cableado vertical

### 3.2.2.4 Rutas y espacios de telecomunicaciones para edificios comerciales

La norma ANSI/TIA 569A define la infraestructura para rutas de cableado estructurado a través de escalerillas, bandejas, canaletas y tuberías.

A continuación un breve listado de los lineamientos de esta norma:

- El radio de curvatura para cable UTP debe ser mayor a 4 veces el diámetro del cable.
- El radio de curvatura para fibra óptica debe ser 20 veces el diámetro del cable durante la instalación y mayor a 10 veces en reposo.
- Ninguna sección de cable debe ser mayor a 30 metros y no debe tener más de dos curvas de 90 grados entre cajas de paso.
- La tensión máxima que se puede ejercer sobre un cable al momento de tenderlo es de 25lbf.
- Se debe evitar colocar amarras demasiado ajustadas ya que pueden causar deformidades en los cables, es recomendable utilizar cinta velcro.
- El grado de relleno máximo de los conductos es del 40%.

- Si en un conducto debe ir tendido cable de datos y eléctrico es conveniente colocar una división entre ellos.

Para el rediseño de la AZNEE se enrutará el cable con escalerilla metálica a través de los cuartos de telecomunicaciones y en los tramos que conducen gran cantidad de cables y para llegar a cada una de las estaciones de trabajo se utilizará canaleta decorativa con sus respectivos accesorios.

#### 3.2.2.5 Cuarto de telecomunicaciones y cuarto de equipos

Los espacios de telecomunicaciones deben estar ubicados en lugares idóneos en los cuales los equipos activos no estén expuestos a humedad, polvo o rayos solares, puesto que estos factores dañan a los mismos.

Las áreas de los cuartos de telecomunicaciones y del cuarto de equipos deben estar acordes con la capacidad que van a soportar, considerando los equipos que cada cuarto va albergar así como un margen de escalabilidad.

A continuación parámetros a tener en cuenta al momento de diseñar los cuartos de telecomunicaciones:

- Se recomienda colocar un cuarto de telecomunicaciones por piso.
- Ubicar los cuartos de telecomunicaciones en el centro del área a servir para no exceder la norma de los 100 metros.
- Las puertas de acceso deben ser de apertura completa, con llave y con medidas de al menos 91 centímetros de ancho y 2 metros de alto.
- Para que los equipos activos no sufran daños la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente entre 18 y 35 grados centígrados y en el cuarto de equipos entre 18 y 24 grados centígrados.
- La humedad relativa del cuarto debe ser menor al 85% en cuartos sin equipos electrónicos y entre 30% - 55% en aquellos que si los tienen.
- Se debe evitar el uso de cielo falso.

- No debe haber tuberías de agua pasando por dentro o sobre el cuarto de telecomunicaciones para evitar inundaciones.
- Se debe proporcionar una iluminación de mínimo 500 luxes a un metro del piso.
- Las paredes deben estar pintadas de color claro para mejorar la iluminación.

De acuerdo al rediseño los espacios de telecomunicaciones deben tener las medidas, que indica la tabla 3.6.

**Tabla 3.6** Área de los cuartos de telecomunicaciones

| BLOQUES | DEPARTAMENTO | ÁREA RECOMENDADA |
|---|---|---|
| **PRIMER PISO BLOQUE 1 (Cuarto de telecomunicaciones A)** | SISTEMAS | 3m x 2.4m |
| **PLANTA BAJA BLOQUE 1 (Cuarto de equipos C)** | AVALÚOS | 3m x 3.5m |
| **PLANTA BAJA BLOQUE 2 (Cuarto de telecomunicaciones B)** | PARQUEADERO | 3m x 2.4m |

### 3.2.2.6 Entrada de Servicios

Es el punto en el que se une el cableado externo del proveedor de servicios de telecomunicaciones con el cableado de backbone del edificio, esto permite delimitar responsabilidades entre el proveedor y el cliente.

Se debe tener en cuenta que la distancia máxima que puede penetrar el cable dentro del edificio es 15 metros, debido a que la chaqueta del mismo no posee características antiflama.

En el caso de la AZNEE la entrada de servicios se encuentra en el cuarto de telecomunicaciones ubicado en el parqueadero, el rediseño contempla el traslado de este subsistema al cuarto de equipos ubicado cerca del departamento de avalúos.

### 3.2.2.7 Administración

El estándar ANSI/TIA 606A proporciona la guía y los conceptos básicos para una correcta administración del sistema instalado incluyendo patch cords, patch panels, salida de telecomunicaciones y racks.

Los tres conceptos básicos que comprenden la administración son:

- Identificadores
- Registros
- Etiquetas

A continuación se detalla cada uno de conceptos mencionados:

- **Identificador**: Es un ítem de información que permite vincular un elemento de la infraestructura de cableado estructurado con su respectivo registro.
- **Registro**: Es una colección de información correspondiente a un elemento de la infraestructura de telecomunicaciones, que contiene datos acerca del mismo, como por ejemplo tipo de cable, distancia, última fecha de certificación, etc.
- **Etiqueta**: Es un elemento de marcación que permite identificar los elementos instalados.

El esquema de identificación que se va a manejar en la AZNEE es el que se indica en las tablas 3.7 y 3.8.

#### *3.2.2.7.1 Identificación de cableado horizontal*

**Tabla 3.7** Etiquetado del cableado horizontal

| ID piso | ID cuarto de telecomunicaciones | - | ID patch panel | | ID posición | |
|---|---|---|---|---|---|---|
| 1 | A | - | PP | A | 1 | 5 |

**Ejemplo**: 1A-PPA15

- Piso 1
- Cuarto de telecomunicaciones A
- Patch Panel A
- Posición 15

#### *3.2.2.7.2 Identificación del backbone*

**Tabla 3.8** Etiquetado del cableado backbone

| ID cuarto de telecomunicaciones | / | ID cuarto de equipos | - | ID cable | |
|---|---|---|---|---|---|
| A | / | C | - | 0 | 2 |

**Ejemplo**: A/C-02

- Origen: Cuarto de telecomunicaciones A
- Destino: Cuarto de equipos C
- Cable 02

### 3.2.3 DIMENSIONAMIENTO DE LOS ELEMENTOS DEL CABLEADO

#### 3.2.3.1 Dimensionamiento de rutas de cableado

Para el enrutamiento de los cables en los cuartos de telecomunicaciones se utilizará escalerilla metálica debido a que se va a manejar un promedio de 81 cables a la salida de los racks como se indica en la tabla 3.6 y para llegar a cada área de trabajo se colocará canaleta decorativa, dado que la infraestructura de la AZNEE es modular y las divisiones entre las oficinas son de mampara.

La AZNEE no cuenta en sus archivos con los planos de la institución, razón por la cual se realizaron planos con medidas aproximadas tomadas en las inspecciones realizadas en esta dependencia.

El estándar ANSI/TIA 569-B recomienda que el enrutamiento sea diseñado para permitir el 50% de expansión de la instalación inicial, además el llenado no deberán exceder el 40% de las rutas de cableado. De acuerdo a lo mencionado se presenta la tabla 3.9, con las dimensiones y cantidades necesarias para este rediseño.

Los cálculos para la determinación de las dimensiones de la escalerilla metálica se encuentran en el Anexo G.

**Tabla 3.9** Cálculo de elementos de enrutamiento

| **CÁLCULO ESCALERILLA METÁLICA** | | | | |
|---|---|---|---|---|
| **DIMENSIONES (alto x ancho) 100mm x 150mm** | **DISTANCIA (m)** | **NÚMERO DE CABLES /ESCALERILLA** | **HOLGURA DEL 10% (m)** | **TOTAL (m)** |
| **CUARTO DE TELECOMUNICACIONES A (SISTEMAS)** | 35 | 75 | 3.5 | 38.5 |
| **CUARTO DE EQUIPOS C** | 30 | 81 | 3 | 33 |
| **80mm x 100 mm** **CUARTO DE TELECOMUNICACIONES B ( PARQUEADERO)** | 40 | 34 | 4 | 44 |
| **CÁLCULO CANALETA DECORATIVA** | | | | |
| **DIMENSIONES** | **DISTANCIA (m)** | **NUMERO DE CABLES /CANALETA** | **HOLGURA DEL 20% (m)** | **TOTAL (m)** |
| **32mm X 12mm** | 189.6 | 5 | 37.92 | 227.52 |

Para el cálculo de la escalerilla metálica se contempló una holgura del 10% necesario para cubrir las curvas que tendrá la instalación a lo largo del trayecto, y para el caso de las canaletas se requirió una holgura del 20% ya que se debe rodear las paredes de las oficinas para que las canaletas no queden a la vista de los usuarios y así cuidar la estética del edificio.

### 3.2.3.2 Cálculo del número de rollos de cable

Para realizar el cálculo del número de rollos se toma en cuenta el punto más cercano ($d_{min}$) y el punto más lejano ($d_{max}$) con respecto al cuarto de telecomunicaciones.

A continuación se indica un ejemplo con el cual se realizaron los cálculos para los diferentes departamentos de la AZNEE.

- Determinar la distancia media con los datos del punto más cercano y más lejano.

$$d_{med} = \frac{d_{max} + d_{min}}{2}$$

$$d_{med} = \frac{70m + 30m}{2}$$

$$d_{med} = 50m$$

- Añadir un 10% de holgura al resultado anterior para obtener la distancia ajustada ($d_{adj}$)

$$d_{adj} = d_{med} + 10\%$$

$$d_{adj} = 50m + 5m$$

$$d_{adj} = 55m$$

- Calcular el número de corridas por rollo, con la relación de la longitud de cable UTP (305m), la distancia promedio, aproximándola al inmediato inferior.

$$\#corridas\ x\ rollo = \frac{L}{d_{adj}} = \frac{305m}{55m} = 5.54$$

$$\#corridas\ x\ rollo = 5$$

- Calcular el número de rollos con la relación del número de puntos de red y el número de corridas aproximándolo al inmediato superior.

$$\#rollos = \frac{\#puntos}{\#corridas} = \frac{31}{5} = 6.2$$

$$\#rollos = 7$$

Según los cálculos realizados para cada sección de la red se presenta la tabla 3.10 con el número total de rollos que se utilizarán para el rediseño.

**Tabla 3.10** Número total de rollos para el rediseño

| BLOQUES | Número de Puntos Actuales | Número de Puntos Rediseño al 5% | dmax | dmin | dmed | dadj | #corridas | #rollos |
|---|---|---|---|---|---|---|---|---|
| **PRIMER PISO BLOQUE 1** | 25 | 31 | 70 | 30 | 50 | 55 | 5 | 7 |
| **PRIMER PISO BLOQUE 2** | 35 | 45 | 52 | 25 | 38,5 | 42,35 | 7 | 7 |
| **PRIMER PISO BLOQUE 3** | 29 | 36 | 45 | 15 | 30 | 33 | 9 | 4 |
| **PLANTA BAJA BLOQUE 1** | 35 | 45 | 45 | 18 | 31,5 | 34,65 | 8 | 6 |
| **PLANTA BAJA BLOQUE 2** | 26 | 33 | 65 | 20 | 42,5 | 46,75 | 6 | 6 |
| **TOTAL** | **150** | **190** | | | | | **35** | **30** |

Para los enlaces de backbone se utilizará fibra óptica multimodo tipo OM3 de 6 hilos para interiores y se conectorizarán el total de hilos para proveer de redundancia al sistema.

La distancia de cada enlace hace referencia a la figura 3.3, para que el cálculo de la cantidad de cable de fibra óptica sea correcto se debe tener una reserva del 20%

para posibles re-terminaciones, debido a que puede existir rupturas al momento de realizar mantenimientos. En la tabla 3.11 se indica el cálculo correspondiente.

Al momento de la instalación existe una cantidad de material que se desperdicia por diferentes motivos, el principal es la habilidad que posee el instalador y el estado de las herramientas utilizadas, debido a la delicadeza del medio de transmisión.

**Tabla 3.11** Cantidad de fibra óptica para el backbone

| Enlaces de Backbone | Distancia (m) | Reserva del 20% (m) | Holgura (m) | Total (m) |
|---|---|---|---|---|
| **Enlace Cuarto de Telecomunicaciones A – Sistemas / Cuarto de equipos C** | 20 | 4 | 2 | 26 |
| **Enlace Cuarto de Telecomunicaciones B – Parqueadero / Cuarto de equipos C** | 30 | 6 | 2 | 38 |
| **TOTAL** | | | | **64** |

### 3.2.3.3 Dimensionamiento de racks

La unidad en que se mide los racks son los UR (**U**nidades de **R**ack) y su equivalencia es 1 UR = 4.44cm, la manera más fácil de dimensionar la altura adecuada del rack es definir el número de equipos que se instalarán en su interior y la altura en UR que ocupa cada uno, (Tabla 3.12 y Figura 3.4).

Para este rediseño se contempla la instalación de racks cerrados con llave tipo Yale y puerta de malla, esto permite tener control sobre la manipulación de los equipos y conexiones de telecomunicaciones, además permitirá que el aire circule adecuadamente para que los equipos activos no sufran daños por variación en la temperatura interna del rack.

**Tabla 3.12** Cantidad de elementos para los racks de telecomunicaciones

| Elementos | Cuarto de telecomunicaciones A - Sistemas | Cuarto de telecomunicaciones B - Parqueadero | Cuarto de Equipos C - Avalúos | Total unidades |
|---|---|---|---|---|
| Rack cerrado con puerta de malla de 42 UR (2200mm x 800mm x1000mm) | 1 | 1 | 2 | 4 |
| Patch panel modular Cat. 6 | 4 | 2 | 4 | 10 |
| Organizador horizontal (80mm x80mm) | 4 | 2 | 4 | 10 |
| Multitoma horizontal con 4 tomas dobles | 1 | 1 | 2 | 4 |
| Bandeja de fibra óptica para 24 hilos | 1 | 1 | 1 | 3 |
| Bandeja metálica | 1 | 1 | 2 | 4 |
| Organizador vertical de 87" | 2 | 2 | 2 | 6 |
| Ventilador para rack | 1 | 1 | 2 | 4 |

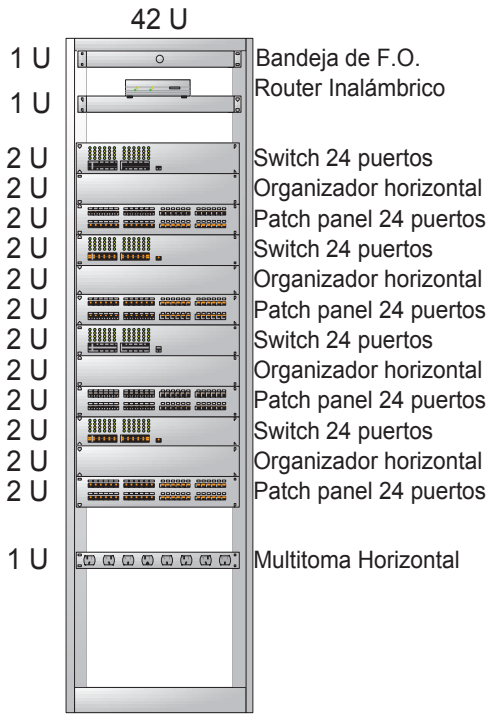



**Figura 3.3** Diagrama de elevación del rack del Cuarto de Telecomunicaciones A – Sistemas

### 3.2.3.4 Cálculo de elementos complementarios

En la tabla 3.13 se especifica todos los elementos adicionales que se requieren para dejar en funcionamiento el sistema de cableado estructurado. Se debe recordar que el rediseño contempla un solo punto de red para la solución de voz y datos respectivamente, por esta razón se requieren 3 patch cord por punto.

**Tabla 3.13** Cantidad de elementos para los racks de telecomunicaciones

| Elementos | Cuarto de telecomunicaciones A (Sistemas) | Cuarto de telecomunicaciones B (Parqueadero) | Cuarto de Equipos C (Avalúos) | Total unidades |
|---|---|---|---|---|
| Elementos complementarios cableado horizontal | | | | |
| Jack Cat. 6 | 150 | 68 | 162 | 380 |
| Patch cord cat.6 1m | 150 | 68 | 162 | 380 |
| Patch cord cat.6 2m | 75 | 34 | 81 | 190 |
| Faceplate 1 posición | 75 | 34 | 81 | 190 |
| Caja sobrepuesta | 75 | 34 | 81 | 190 |
| Elementos complementarios cableado vertical | | | | |
| Pigtail OM3 1m | 6 | 6 | 12 | 24 |
| Patch cord duplex OM3 2m | 3 | 3 | 6 | 12 |
| Panel adaptador LC duplex 6 hilos OM3 | 1 | 1 | 2 | 4 |
| Cassette portafusión 12 hilos | 1 | 1 | 1 | 3 |
| Tubillos termocontráctiles | 6 | 6 | 12 | 24 |

## 3.2.4 DISEÑO LAN ACTIVA

El modelo que más se ajusta a las características de la red es un modelo estrella jerárquica, el mismo que permitirá una mayor escalabilidad, organización, administración y mejores servicios para la AZNEE. Este modelo de red consta de tres capas: la cada de núcleo, capa de distribución y la capa de acceso. Cada capa cumple con una función determinada, la cual permitirá implementar una red confiable

y segura. A continuación se detalla cómo está constituida cada capa para nuestro rediseño.

#### 3.2.4.1 Capa de núcleo

"*La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante*." [16]

Por ende esta capa estará constituida por dos switch multicapa que cumplan con las siguientes características:

- Interfaces 100/1000 Mbps para conectarse con el router del ISP (Proveedor de servicio de internet), la intranet y el backup.
- Soporta el protocolo de etiquetado IEEE 802.1Q[49].
- Protocolos de enrutamiento como OSFP (Open Shortest Path First), RIPv2 (Routing Information Protocol version 2) o BGP (Border Gateway Protocol), mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, la conexión entre las administraciones zonales y la administración central del DMQ.
- Capacidad para Fibra Óptica.
- Administración y monitoreo mediante el protocolo SNMP (Simple Network Management Protocol) v1, v2, v3, SSH[50] y telnet.

#### 3.2.4.2 Capa de distribución

"*La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa de núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red y realiza el enrutamiento de las funciones entre VLANs definidas en la capa de acceso*." [16]. Para el rediseño se emplearán 4 switches de distribución, ubicados en: Sistemas,

[49] IEEE 802.1Q: El protocolo de etiquetado de las VLAN

[50] SSH: Secure Shell Protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor

Data Center, Parqueadero y el Archivo, estos contarán con las siguientes características:

- 24 puertos 100/1000 Mbps
- Soporta el protocolo de etiquetado VLANs
- Soporte de ACL's (Listas de Control de Acceso)
- Agregación de enlaces con el estándar 802.3ad[51]

#### 3.2.4.3 Capa de acceso

"*La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red."[16]*

Para el rediseño se utilizarán 10 switches de acceso para cubrir la demanda de usuarios, no todos los puertos de un switch estarán utilizados debido a la distribución de las estaciones de trabajo. Las características de estos switches serán las siguientes:

- Soporte de VLANs , 802.1q
- Filtrado de MACs, para la seguridad mediante control de acceso
- Puertos Gigabit Ethernet
- Puertos con Auto-sense y POE
- QoS
- Seguridad de puerto
- Agregado de enlaces

### 3.2.5 DISEÑO LÓGICO

Para el dimensionamiento IP se empleará VLSM (Variable Length Subnet Mask), para evitar el desperdicio de direcciones IP, asignando VLANs de acuerdo a cada departamento y las funciones que se realicen.

#### 3.2.5.1 Direccionamiento IP

La AZNEE en base al direccionamiento dado por la Dirección Metropolitana de Informática cuenta con dos redes clase C.

---

[51] 802.3ad: Agregación de enlaces paralelos

- 172.20.5.0/24
- 172.20.112.0./24

En el análisis realizado se determinó un total de 190 puntos de red, tomando en cuenta esta información se procede a la asignación de IPs, según los bloques establecidos en el capítulo 2.

El servidor de DHCP asignará direcciones IP dinámicas a las estaciones de trabajo. Los servidores, impresoras, teléfonos IP, router inalámbricos y controles biométricos serán asignados a diferentes subredes, como se indica en la tabla 3.14.

**Tabla 3.14** Direccionamiento IP para el rediseño de la AZNEE

| BLOQUES | NÚMERO DE HOST | SUBRED / MÁSCARA | GATEWAY |
|---|---|---|---|
| PRIMER PISO BLOQUE 2 | 45 | 172.20.112.0/26 | 172.20.112.62 |
| TELEFONOS IP | 40 | 172.20.112.64/26 | 172.20.112.126 |
| PLANTA BAJA BLOQUE 1 | 44 | 172.20.112.128/26 | 172.20.112.190 |
| PRIMER PISO BLOQUE 3 | 36 | 172.20.112.192/26 | 172.20.112.254 |
| PLANTA BAJA BLOQUE 2 | 33 | 172.20.5.64/27 | 172.20.5.94 |
| PRIMER PISO BLOQUE 1 | 24 | 172.20.5.96/27 | 172.20.5.126 |
| SERVIDORES | 8 | 172.20.5.160/28 | 172.20.5.174 |
| WIFI | 6 | 172.20..5.176/29 | 172.20.5.182 |
| LECTOR DE HUELLAS | 2 | 172.20.5.184/29 | 172.20.5.190 |

### 3.2.5.2 VLANS

El propósito de utilizar VLAN's es agrupar usuarios con características en común y asociarlos en una subred lógica sin importar su ubicación.

Cada una de estas redes virtuales serán configuradas en los switches de acceso y su información se transmitirá a través de enlaces troncales al resto de la red.

Las VLAN's que se asignaron para el rediseño están en la tabla 3.15 con sus respectivos rangos de IPs.

**Tabla 3.15** Grupos de Usuarios por bloques

| VLANS | NÚMERO DE VLAN | SUBRED | MÁSCARA | RANGO DE IPS VALIDAS | DIRECCIÓN DE BROADCAST | GATEWAY |
|---|---|---|---|---|---|---|
| VL_PPB2 | 10 | 172.20.112.0/26 | 255.255.255.192 | 172.20.112.1 – 172.20.112.62 | 172.20.112.63 | 172.20.112.62 |
| VL_TLF | 20 | 172.20.112.64/26 | 255.255.255.192 | 172.20.112.65 – 172.20.112.126 | 172.20.112.127 | 172.20.112.126 |
| VL_PBB1 | 30 | 172.20.112.128/26 | 255.255.255.192 | 172.20.112.129 – 172.20.112.190 | 172.20.112.191 | 172.20.112.190 |
| VL_PPB3 | 40 | 172.20.112.192/26 | 255.255.255.192 | 172.20.112.193 – 172.20.112.254 | 172.20.112.255 | 172.20.112.254 |
| VL_PBB2 | 50 | 172.20.5.64/27 | 255.255.255.224 | 172.20.5.65 – 172.20.5.94 | 172.20.5.95 | 172.20.5.94 |
| Enlaces | | 172.20.5.0/30 | 255.255.255.252 | 172.20.5.1 – 172.20.5.2 | 172.20.5.3 | |
| VL_ADM | 99 | 172.20.5.32/27 | 255.255.255.224 | 172.20.5.33- 172.20.5.62 | 172.20.5.63 | 172.20.5.62 |
| VL_PPB1 | 60 | 172.20.5.96/27 | 255.255.255.224 | 172.20.5.97 – 172.20.5.126 | 172.20.5.127 | 172.20.5.126 |
| VL_SERV | 80 | 172.20.5.160/28 | 255.255.255.240 | 172.20.5.161 – 172.20.5.174 | 172.20.5.175 | 172.20.5.174 |
| VL_WIFI | 90 | 172.20.5.176/29 | 255.255.255.248 | 172.20.5.177– 172.20.5.182 | 172.20.5.183 | 172.20.5.182 |

### 3.2.6 REDISEÑO DE LA ZONA WIFI PARA LA AZNEE

La AZNEE cuenta en la actualidad con 4 routers inalámbricos modelo Cisco Linksys EA2700, los mismos que han sido ubicados en los cuartos de telecomunicaciones y el cuarto de equipos. Se realizó un análisis con la herramienta INSSIDE[52] que permite monitorear la cobertura y la intensidad de señal de los routers inalámbricos, y se identificó que no son suficientes para cubrir todas las áreas de la AZNEE, a continuación se muestra el escaneo de las redes inalámbricas en varios puntos de la administración.

Las redes escaneadas pertenecientes a la AZNEE son:

- **Norte Comunica,** Cuarto de Equipos, Parqueadero.
- **ZNorte,** Departamento de Sistemas.
- **Eugenio Espejo**, Departamento de Educación, Cultura y Deporte.
- **EEspejo,** Cuarto de Telecomunicaciones.

En la figura 3.4 se pueden observar la señal de las 4 redes inalámbricas, tomadas desde el cuarto de telecomunicaciones.

**Tabla 3.16** RSSI desde cuarto de telecomunicaciones

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **NorteComunica** | -77 | 6 |
| **ZNorte** | -62 | 11 |
| **Eugenio Espejo** | -89 | 1 |
| **EEspejo** | -91 | 11 |

De acuerdo a los RSSI (Indicador de fuerza de la señal recibida), descrita en la tabla 3.16 , se puede observar que la mejor señal es de la red ZNorte con -62 db, ya que nos permite tener un enlace bueno, las dos redes inalambricas (NorteComunica y

[52] INSSIDE: Es una herramienta que permite buscar redes inalámbricas en una zona determinada y controlar, de un modo gráfico, la intensidad de sus señales.

Eugenio Espejo), presentan un enlace normal – bajo y -89db muestra una señal aceptable para la conexión, pero puede sufrir caídas.


**Figura 3.4** Intensidad de las señales desde el cuarto de telecomunicaciones

En la figura 3.5 se puede observar la señal del router inalámbrico ZNorte (color verde), por encima de los -30db que indica una señal ideal para la conexión, tomada desde el departamento de sistemas. También podemos observar que en este punto de la medición las señales de EEspejo ubicado en el departamento de Educación, cultura y deporte nos da una señal por encima de los -70 db (color morado) con un enlace normal. Mientras que las señales de NorteComunica y Eugenio Espejo son muy débiles debido a la distancia en la que se encuentran.

**Tabla 3.17** RSSI desde el Departamento de Sistemas

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **NorteComunica** | -85 | 6 |
| **ZNorte** | -30 | 11 |
| **Eugenio Espejo** | -90 | 1 |
| **EEspejo** | -70 | 11 |


**Figura 3.5** Intensidad de las señales desde el departamento de sistemas

En la figura 3.6 se puede observar la señal del router inalámbrico ZNorte (color verde) , por encima de los -60db que indica un enlace bueno, tomada desde el departamento de sistemas, en el punto más lejano. La red inalámbrica Eugenio Espejo muestra un RSSI de -75 que indica un enlace normal, que es señal mediadamente buena.

**Tabla 3.18** RSSI desde el Departamento de Sistemas – punto lejano

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **ZNorte** | -61 | 11 |
| **Eugenio Espejo** | -75 | 1 |

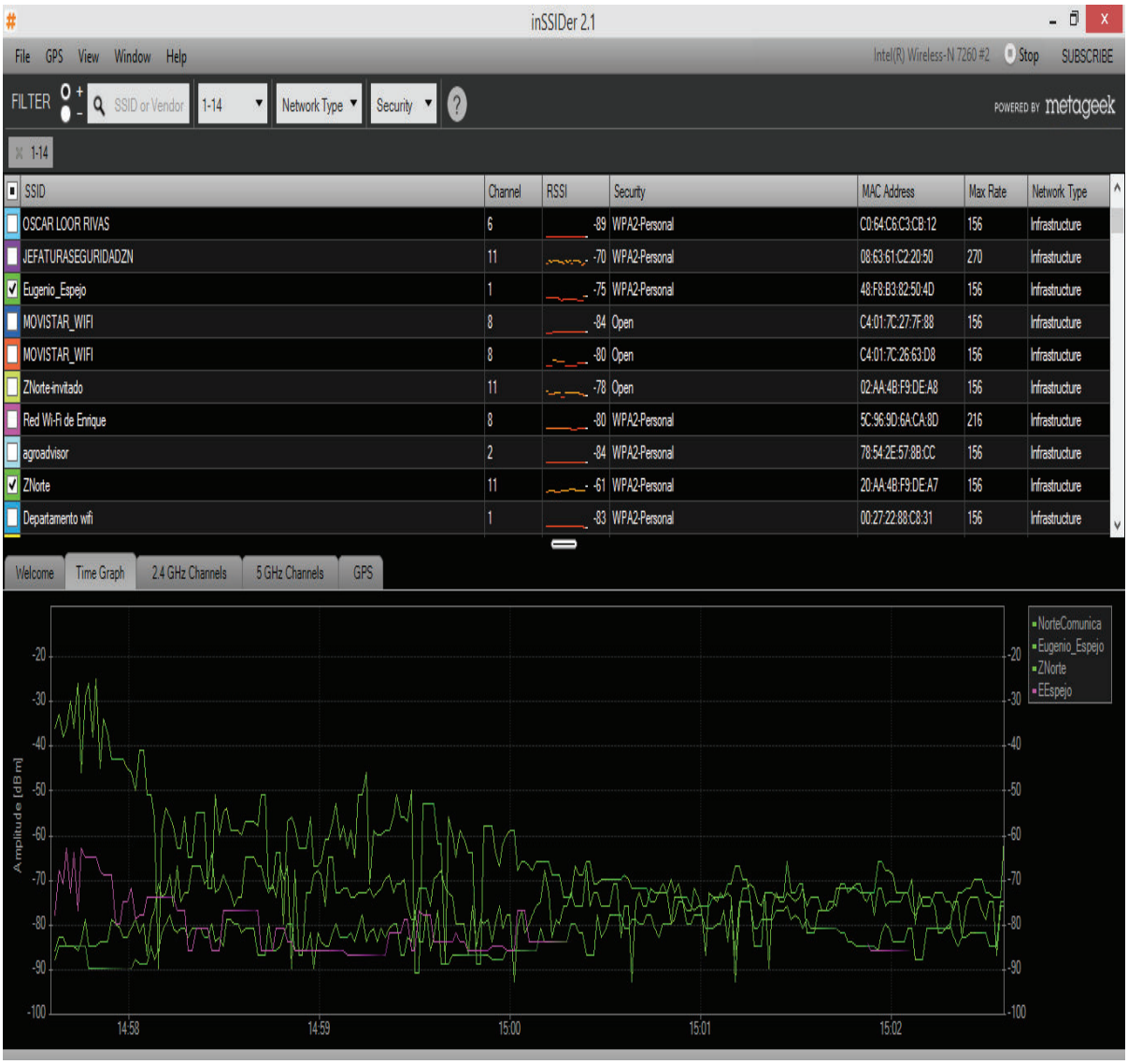



**Figura 3.6** Señal del router inalámbrico ZNorte, desde el punto más lejano.

En la figura 3.7 se puede observar los canales que ocupan las diferentes redes inalámbricas dentro de la AZNEE, lo cual también se debe tomar en cuenta para que las redes deben ser colócalas en diferentes bandas de frecuencia para aprovechar mucho más su potencial. Como se verifica en el gráfico la señal de la red inalámbrica ZNorte y EEspejo están trabajando en el canal 11, lo que genera interferencias con estas dos señales y se debe buscar otro canal para ajustar cualquiera de las dos señales para brindar un servicio de buena calidad.

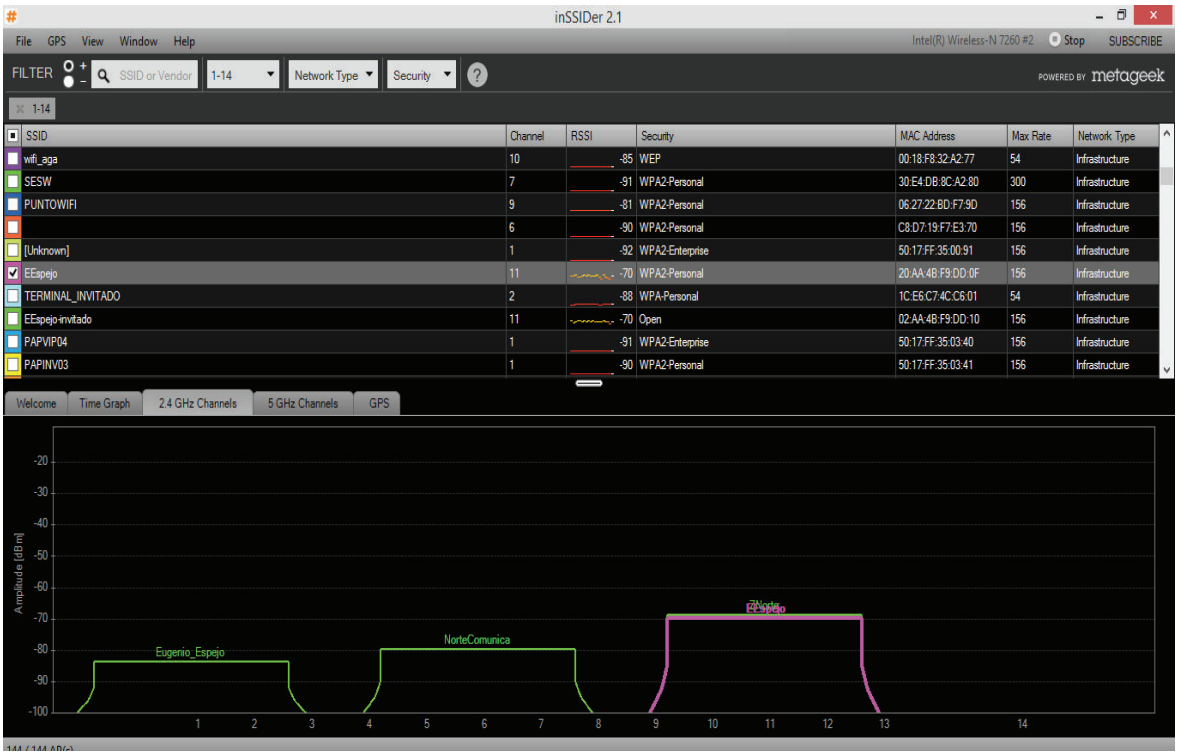



**Figura 3.7** Bandas de frecuencia de las redes inalámbricas de la AZNEE.

En la figura 3.8 se puede observar la señal del router inalámbrico EEspejo (color morado), indica un RSSI de -76 db que es un enlace normal – bajo con una señal medianamente buena, tomada desde el datacenter. También se puede observar que la intenisdad de señal del router ZNorte es buena dedibo a que se encuentra en el departamento de sistemas ubicado arriba del datacenter; las medición señales de los dos routers están con una señal mínima para poder establecer una conexión produciendo cortes en la comunicación.

**Tabla 3.19** RSSI desde el Cuarto de Telecomunicaciones

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **NorteComunica** | -80 | 11 |
| **ZNorte** | -61 | 1 |
| **Eugenio Espejo** | -85 | 6 |
| **EEspejo** | -76 | 11 |


**Figura 3.8** Señal del router inalámbrico EEspejo

En la figura 3.9 se puede observar la señal del router inalámbrico ZNorte (color verde), por encima de los -80db que indica una señal mínima aceptable donde pueden ocurrir cortes en la comunicación, esta señal fue tomada desde el Departamento de ventanillas de atención al público. La señal que da una mejor cobertura es Eugenio Espero con -51db que indica una señal idónea. Mientras que las señales de NorteComunica y EEspejo son muy débiles debido a la distancia que las separa. En esta parte de la AZNEE, las señal es muy débil de cualquiera de los 3 routers inalámbricos y la única señal aceptable solo cubre cierta parte de la atención al público.

**Tabla 3. 20** RSSI desde las Ventanillas

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **ZNorte** | -84 | 11 |
| **Eugenio Espejo** | -51 | 1 |


**Figura 3.9** Señal del router inalámbrico Eugenio Espejo

En la figura 3.10 se puede observar la señal del router inalámbrico NorteCominuca (color verde) , por encima de los -50db que indica una señal idónea para el establecimiento de conexiones, esta señal fue tomada desde la zona del parqueadero. Las señal abastece desde ese punto a la parte posterior de la AZNEE. En cuanto a las redes ZNorte y Eugenio Espejo sus señales son medianamente buenas, aunque pueden sufrir ciertas caidas en la comunicación.

**Tabla 3.21** RSSI desde el parqueadero de la AZNEE

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **NorteComunica** | -51 | 6 |
| **ZNorte** | -78 | 11 |
| **Eugenio Espejo** | -70 | 1 |


**Figura 3.10** Señal del router inalámbrico NorteCominuca

En la figura 3.11 se puede observar la señal del router inalámbrico Znorte (color verde), por encima de los -80db que indica una señal mínima aceptable para establecer una conexión,que puede presentar cortes en la comunicación, pérdida de datos,etc, esta señal fue tomada desde los departamentos de Proyectos, donde la señal es no llega adecuadamente. Para las otras tres señales la intensidas en mas baja que no pueden cubrir totalmente esta área.

**Tabla 3.22** RSSI desde el Departamento de Proyectos

| RED INALÁMBRICA | RSSI | CANAL |
|---|---|---|
| **ZNorte** | -87 | 11 |
| **Eugenio Espejo** | -76 | 1 |


**Figura 3.11** Señal del router inalámbrico Znorte desde Departamento de Proyectos.

Como conclusión se plantea añadir dos equipos que no se encuentran en uso actualmente para satisfacer la demanda de los usuarios. A continuación en la figura 3.12 y 3.13 se detalla la ubicación de los routers inalámbricos y las zonas que cubrirán, de tal manera que la AZNEE cuente con una red inalámbrica para uso del personal interno y público en general.

Existirán dos SSID (Service Set Identifier) basados perfiles como indica la tabla 3.23.

**Tabla 3.23** Determinación de SSID según perfiles

| PERFIL | SSID |
|---|---|
| Personal de la AZNEE | Waznee |
| Público en general | EE-invitado |

Los routers que se encuentran en la parte central de la AZNEE tendrán configurado el perfil de invitado, mismo que no requiere de autenticación. Estos brindarán servicio a las personas que acudan a realizar trámites en la institución. Las claves para acceder a la red inalámbrica de la institución serán distribuidas por el personal de informática. Se establece como política de seguridad realizar el cambio de contraseñas de acceso cada 3 meses.

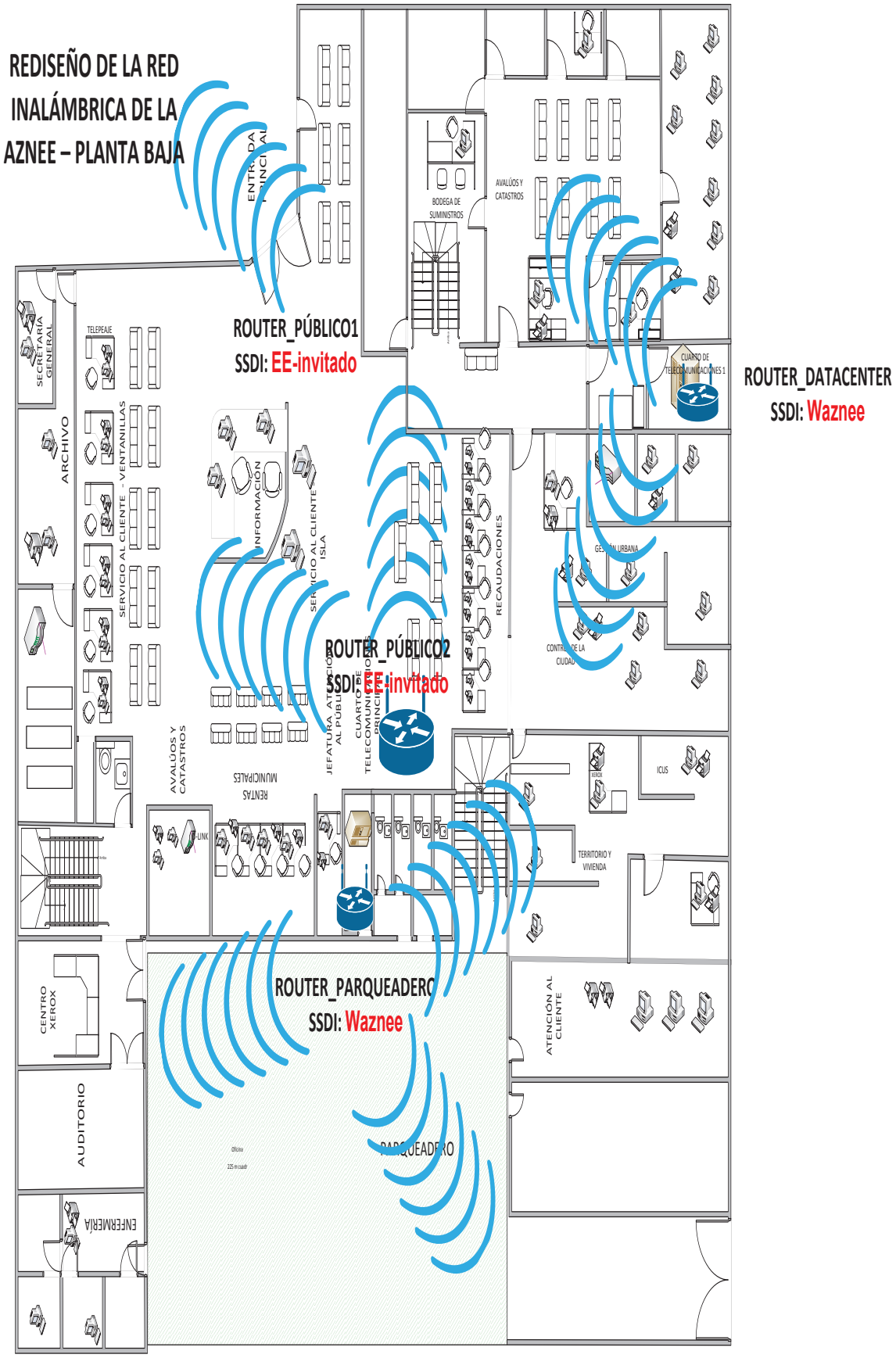



**Figura 3.12** Rediseño de la red inalámbrica para la AZNEE planta baja.

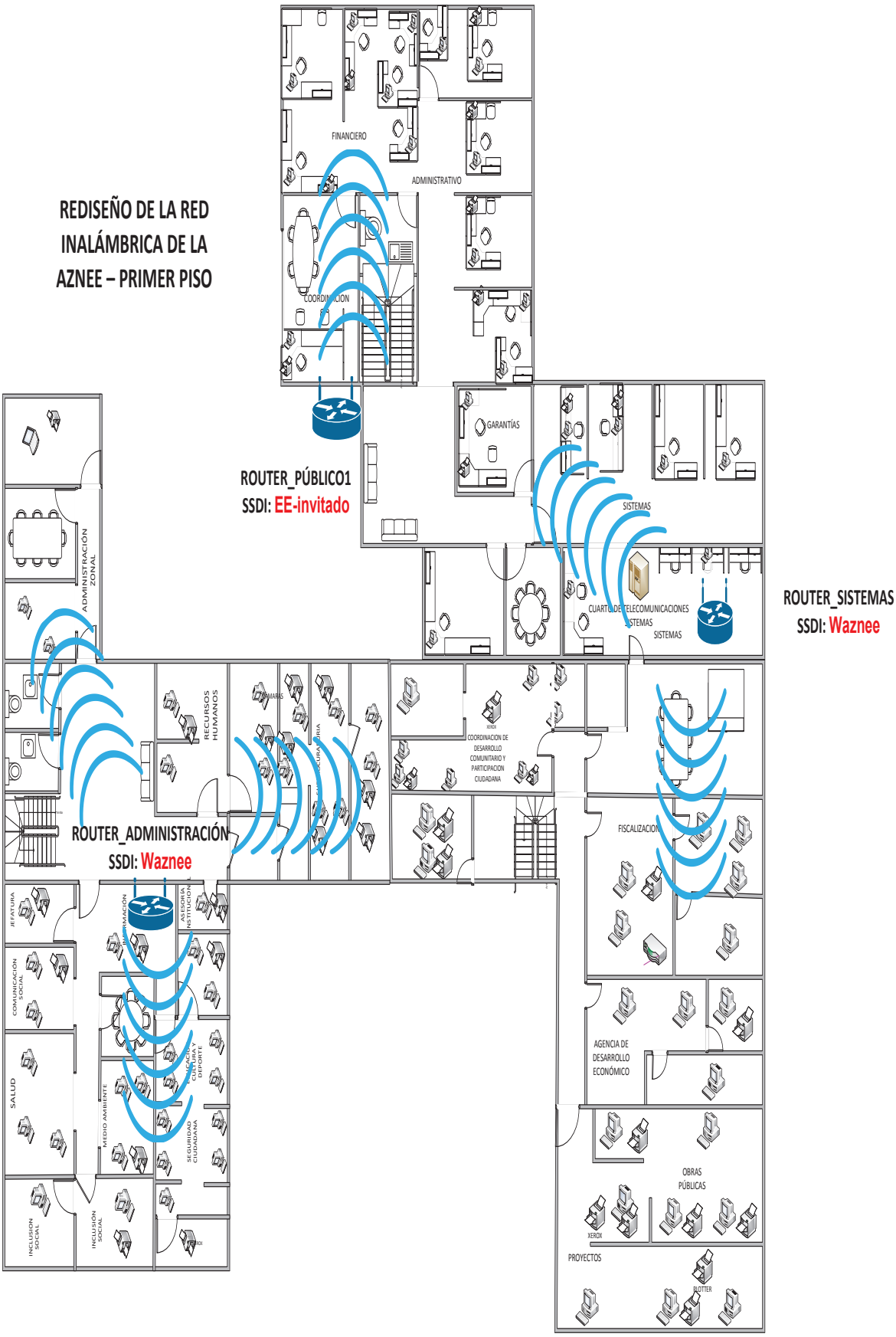



**Figura 3.13** Rediseño de la red inalámbrica para la AZNEE primer piso.

### 3.2.7 TELEFONÍA IP

La telefónica IP permite ofrecer servicios como: registro de llamadas, identificación de llamadas, desvío de llamadas, llamadas en espera y llamadas simultáneas. Inicialmente se planea colocar un teléfono IP por cada departamento, el cual será asignado al jefe del área. La conexión de los teléfonos se realizará como indica la figura 3.14

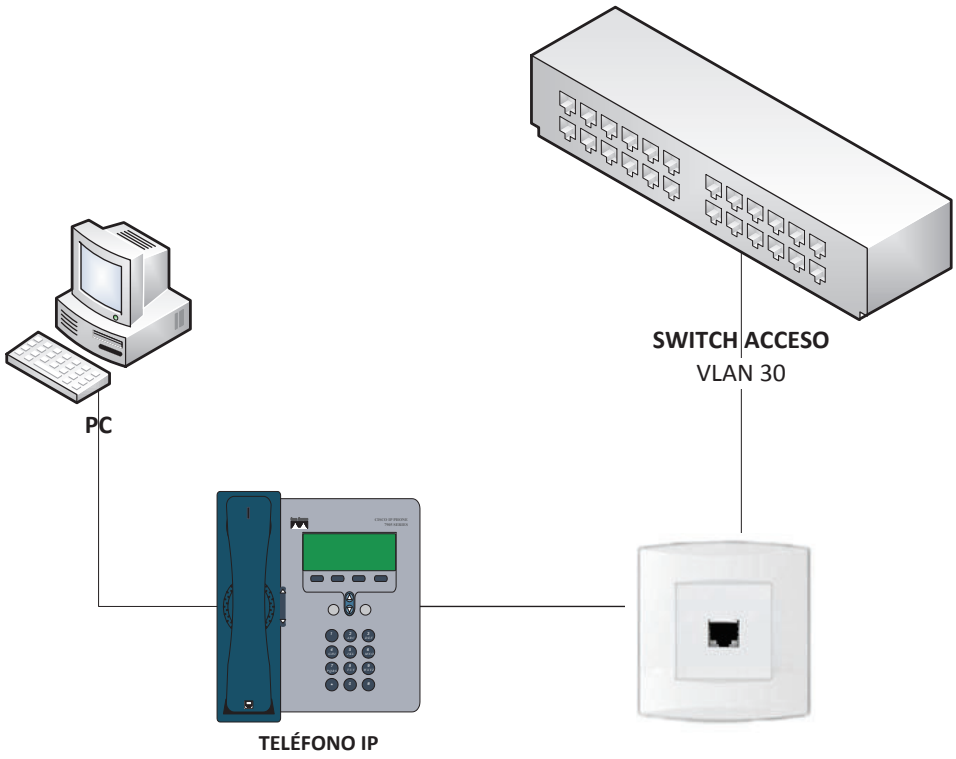



**Figura 3.14** Conexión del teléfono IP.

#### 3.2.7.1 Requerimientos de voz

Para determinar la intensidad de tráfico de voz se utilizará la ecuación 3.1, además de los datos obtenidos en la encuesta (sección 2.6).

$$A = C * T[\text{Erlangs}] \qquad \text{Ecuación 3.1}$$

Dónde:

A = Intensidad del Tráfico en Erlangs

C= Número de llamadas realizadas en la hora pico

T = Tiempo promedio de duración de una llamada

El número de llamadas obtenidas por hora es 6, y el tiempo promedio de llamada es establecido por Dirección Metropolitana de Informática que es de 3 minutos.

$$\mathrm{A_{usuario}} = 6\ \frac{\text{llamadas}}{1\ \text{hora}} * \frac{1\ \text{hora}}{60\ \text{minutos}} 3\ \text{minutos[Erlangs]}$$

$$\mathrm{A_{usuario}} = 0.3\ [\text{Erlangs}]$$

Considerando que el servicio de telefonía es utilizado para llamadas internas y externas como se muestra en las figuras 2.23 y 2.24, se ha estimado un total de 40% de usuarios que acceden simultáneamente al servicio durante el día.

$$\mathrm{Usuarios_{simultáneos}} = \mathrm{Usuarios\ _{totlales}} * \text{Indice de simultaneidad}$$

$$\mathrm{Usuarios_{simultáneos}} = 40 * 40\%$$

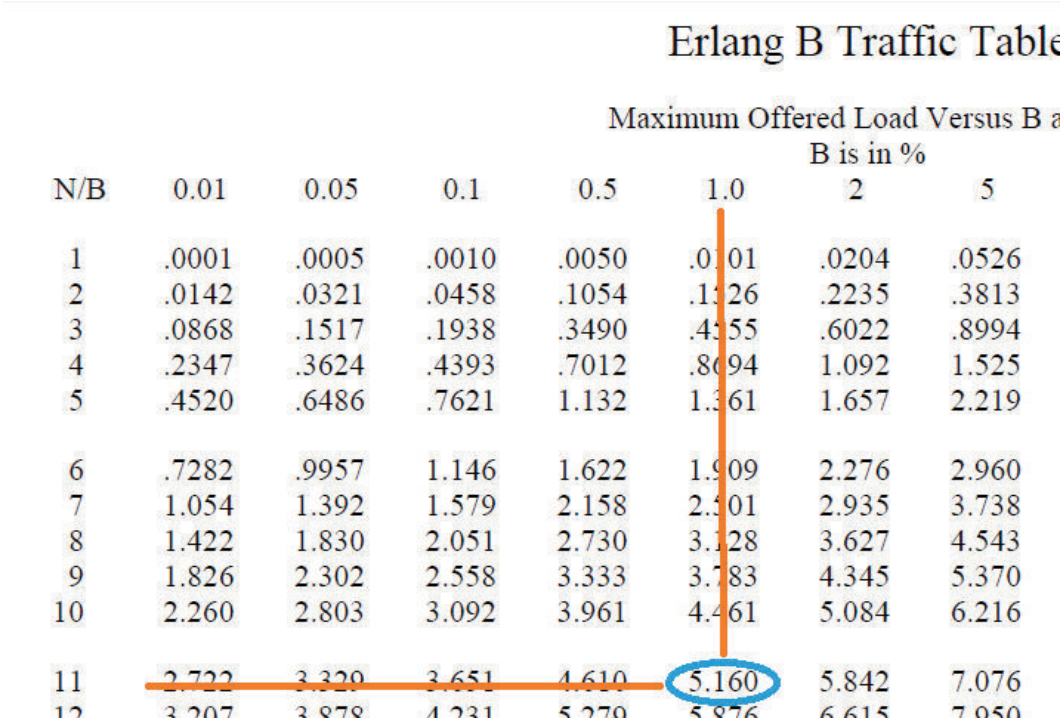
$$\mathrm{Usuarios_{simultáneos}} = 16$$

$$\mathrm{A_{Total}} = \mathrm{A_{usuario}} * \mathrm{Usuarios_{simultaneos}}$$

$$\mathrm{A_{Total}} = 0.3 * 16 = 4{,}8\ [\text{Erlangs}]$$

Considerando una probabilidad de pérdida del 1% y verificando en la tabla de Erlang B (Figura 3.15), se tiene que la AZNEE necesitará 11 líneas troncales.

Para la implementación del servicio de VoIP se analizaron dos alternativas las cuales se encuentran escritas en la tabla 3.24 y se eligió el software de Asterisk por presentar un mayor rendimiento y estabilidad.



Erlang B Traffic Table

Maximum Offered Load Versus B a
B is in %

| N/B | 0.01 | 0.05 | 0.1 | 0.5 | 1.0 | 2 | 5 |
|---|---|---|---|---|---|---|---|
| 1 | .0001 | .0005 | .0010 | .0050 | .0101 | .0204 | .0526 |
| 2 | .0142 | .0321 | .0458 | .1054 | .1526 | .2235 | .3813 |
| 3 | .0868 | .1517 | .1938 | .3490 | .4555 | .6022 | .8994 |
| 4 | .2347 | .3624 | .4393 | .7012 | .8694 | 1.092 | 1.525 |
| 5 | .4520 | .6486 | .7621 | 1.132 | 1.361 | 1.657 | 2.219 |
| 6 | .7282 | .9957 | 1.146 | 1.622 | 1.909 | 2.276 | 2.960 |
| 7 | 1.054 | 1.392 | 1.579 | 2.158 | 2.501 | 2.935 | 3.738 |
| 8 | 1.422 | 1.830 | 2.051 | 2.730 | 3.128 | 3.627 | 4.543 |
| 9 | 1.826 | 2.302 | 2.558 | 3.333 | 3.783 | 4.345 | 5.370 |
| 10 | 2.260 | 2.803 | 3.092 | 3.961 | 4.461 | 5.084 | 6.216 |
| 11 | 2.722 | 3.329 | 3.651 | 4.610 | 5.160 | 5.842 | 7.076 |
| 12 | 3.207 | 3.878 | 4.231 | 5.279 | 5.876 | 6.615 | 7.950 |

**Figura 3.15** Líneas troncales según la tabla de Erlang B

**Tabla 3.24** Comparación de software para telefonía IP

| Asterisk | Elastisk |
|---|---|
| Software Open Source | Sistema todo en uno propietario |
| Total control | Instala muchos componentes por default |
| Compilador ajustable a la arquitectura de la PC | Su interfaz gráfica es muy lenta y pesada en comparación con FreePBX |
| Programación por líneas de comandos | Algunos componentes no son actualizados con frecuencia |
| Uso de FreePBX para la configuración gráfica | Ha sido víctima de errores de seguridad por tener componentes extras. |

### 3.2.7.2 Direccionamiento IP y Plan de numeración

La AZNEE contará con 40 extensiones para el servicio de telefonía IP dentro de la VLAN como se indica en la sección 2.11.3.

**Tabla 3.25** Direccionamiento para el servicio de telefonía IP.

| CANTIDAD DE TELÉFONOS IP | SUBRED / MÁSCARA | VLAN |
|---|---|---|
| 40 | 172.20.112.64/26 | VL_TLF – 30 |

El plan de numeración estará dado según el bloque donde se encuentre el departamento, al mismo que sé le otorgará un sufijo para su correcta ubicación.

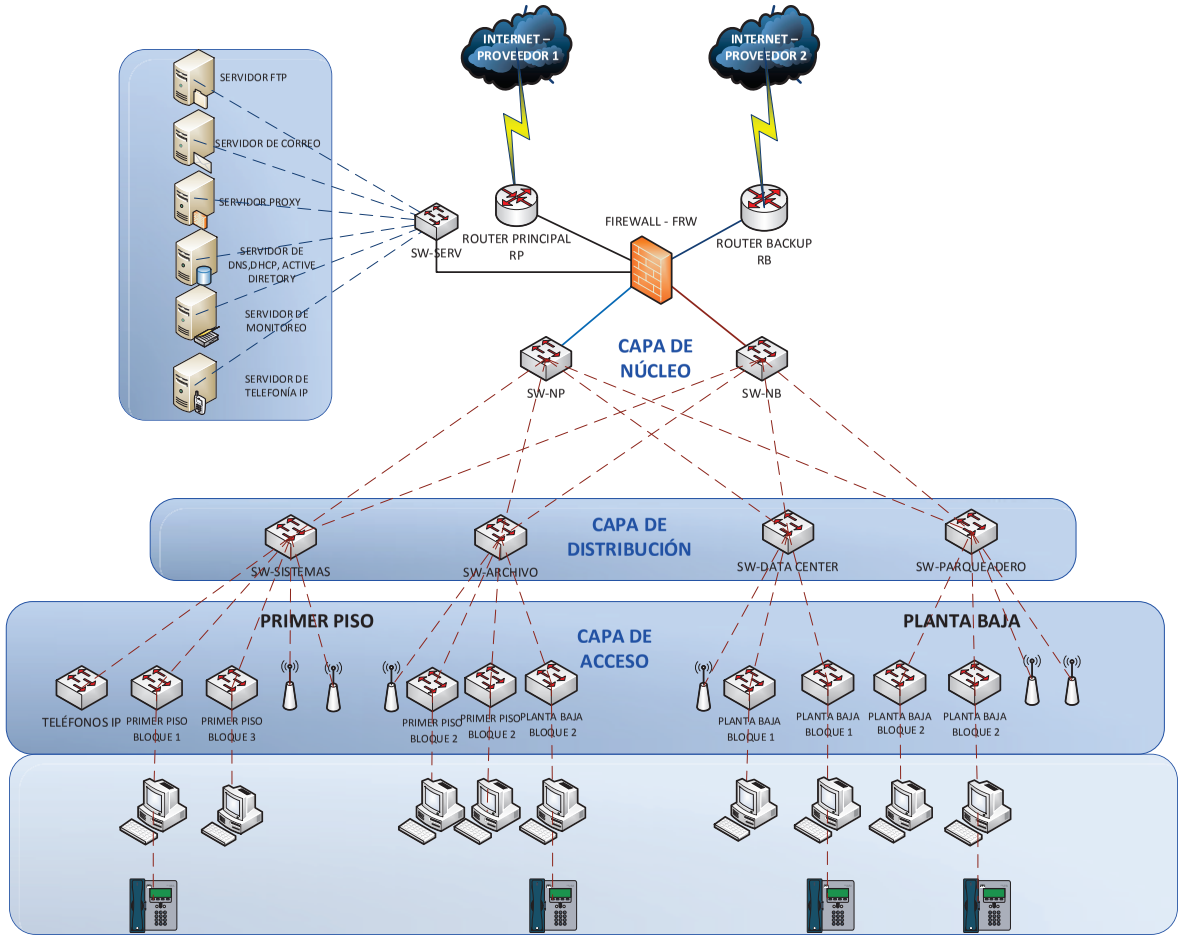
En la tabla 3.26 se observa la numeración que se implementará con el software ASTERISK[53] para poder realizar las configuraciones respectivas.

**Tabla 3.26** Plan de numeración para la AZNEE

| BLOQUES | SUFIJO | RANGO DE EXTENSIONES |
|---|---|---|
| PRIMER PISO BLOQUE 2 | 1400 | 1401-1450 |
| PLANTA BAJA BLOQUE 1 | 1500 | 1501-1550 |
| PRIMER PISO BLOQUE 3 | 1600 | 1601-1650 |
| PLANTA BAJA BLOQUE 2 | 1700 | 1701-1750 |
| PRIMER PISO BLOQUE 1 | 1800 | 1801-1850 |

[53] ASTERISK: http://www.asterisk.org/

## 3.3 REDISEÑO GENERAL DE LA RED




| INFORMACIÓN | | |
|---|---|---|
| REDISEÑO DE LA RED DE LA AZNEE | | |
| Símbolo | Total | Descripción |
| | 1 | SERVIDOR FTP |
| | 1 | SERVIDOR DE CORREO ELÉCTRONICO |
| | 1 | SERVIDOR DE PROXY |
| | 1 | SERVIDOR DNS, DHCP, ACTIVE DIRECTORY |
| | 1 | SERVIDOR DE MONITOREO |
| | 1 | SERVIDOR DE TELEFONÍA IP |
| | 3 | ENLACE DE FIBRA |
| | 2 | NUBE DE INTERNET |
| | 1 | FIREWALL |
| | 2 | ROUTERS DE BORDE |
| | 17 | SWITCHES DE ACCESO Y DISTRIBUCIÓN |
| | 6 | ROUTERS INALÁMBRICOS |
| | 9 | USUARIOS AZNEE |

**Figura 3.16** Rediseño de la Red de la Administración Zonal Norte

## 3.4 HERRAMIENTA DE MONITOREO

Un sistema de monitoreo permite tener el control y vigilar los recursos de telecomunicaciones en busca de componentes defectuosos o fallos en los servicios de red, los cuales serán reportados mediante alarmas programadas por el administrador y enviadas a las cuentas de correo del personal de informática, quienes tomarán las medidas correctivas necesarias.

Para la gestión de la red de la AZNEE se plantea la utilización del software NAGIOS[54], el cual permitirá realizar las siguientes funciones:

- Identificar y resolver problemas que puedan afectar el normal funcionamiento de la red.
- Monitorear la infraestructura de red para asegurar que los sistemas, aplicaciones y servicios funcionen correctamente.
- En caso de reportar una alarma la aplicación enviará un correo de notificación al personal técnico.

## 3.5 DISEÑO DE LA SOLUCIÓN PARA MEJORAR EL SISTEMA DE SEGURIDAD

En base al análisis previo realizado en el capítulo 2, se procederá al diseño de la solución de seguridad considerando los siguientes aspectos:

### 3.5.1 SEGURIDAD A NIVEL DE SERVIDORES

Se eligió Linux como el sistema operativo base de los servidores, por ser una plataforma de libre distribución con altas prestaciones por su gran soporte para drivers, herramientas de desarrollo, programas para usuario y flexibilidad para realizar instalaciones complejas.

[54] NAGIOS: http://www.nagios.org/

Adicionalmente, en esta sección se configurarán los servicios necesarios para proteger los equipos informáticos, que son utilizados como estaciones de trabajo y servidores en general. Para ello se utilizará:

- Iptables
- Active directory
- LDAP

Actualmente, en la AZNEE están abiertos un gran número de puertos, como se pudo apreciar en el análisis previo realizado en el capítulo 2, que se deberían controlar en base a reglas que ayuden a mitigar los riesgos de seguridad para la red. Considerando estos antecedentes, se procederá a generar un conjunto de políticas de seguridad para garantizar la seguridad del equipo y la integridad de la información manejada por los mismos

En base a las buenas prácticas en servidores se recomienda:

- Inicialmente cerrar todos los puertos, para posteriormente abrir aquellos que sean requeridos por los servicios y aplicativos utilizados por los usuarios de la red.
- Mantener a los equipos informáticos con las últimas actualizaciones de seguridad, se debe tener en cuenta que al realizar este tipo de actualizaciones garantizamos un grado elevado de seguridad.
- No se debe actualizar los servidores de aplicaciones a menos que sea íntegramente necesario para el buen funcionamiento de los servicios que mantiene. Se debe considerar que una actualización innecesaria podría afectar el buen funcionamiento de los servicios y aplicaciones, esto no es deseable.
- Se recomienda cambiar las credenciales de acceso en periodos de tiempo no muy extensos, véase pág. 120 y 121. Adicionalmente, se sugiere que las claves se las almacene en un gestor de contraseñas, un buen punto de partida

es el software KeePassX[55], que ayuda a mantener las claves encriptados en un repositorio local libre de la vista de intrusos.

- Se considera necesario mantener un cronograma activo para la gestión de backups y respaldos de información, que pueden generarse en cintas magnéticas, cds o algún dispositivo electrónico de almacenamiento de información.
- Todos los servidores deberán ser monitoreados constantemente para evitar cualquier pérdida de información o problemas de disponibilidad que pueda afectar el trabajo de los usuarios en la red.

A continuación se procederá a detallar criterios para desarrollar las buenas prácticas antes mencionadas:

#### 3.5.1.1 Mecanismos de bloqueo de puertos

Se procederá a instalar dependiendo de la distribución de Linux que se utilice, el sistema de firewall denominado Iptables[56].

Para ambientes en base a una distribución Debian - Ubuntu, el procedimiento será el siguiente:

*sudo apt-get install ufw*

Para ambientes basados en plataformas Red Hat, se instalará de la siguiente manera:

*yum install Iptables*

Después de haber instalado el sistema, se muestra la manera de cómo interactuar

[55] KeePassX: https://www.keepassx.org/

[56] Iptables: Es una herramienta que permite controlar el flujo de paquetes y establecer reglas para el control de acceso a los puertos y servicios que disponga el equipo informático.

con las políticas de seguridad necesarias para cada servidor, mismas que se pueden contrar a detalle en el Anexo H.

Las instrucciones para bloquear los puertos que no son necesarios en el servidor DHCP se enumeran a continuación:

- Inicialmente se cierran todos los puertos

  $ sudo ufw default deny

- Se añaden reglas para abrir los puertos, en este caso se deben abrir los puertos 67 (envío de respuesta) y 68 (recepción de petición).

  $ sudo ufw allow 67

  $ sudo ufw allow 68


**Figura 3.17** Puertos abiertos en el servidor DHCP[57].

[57] Fuente: http://protocolo-dhcp.blogspot.com/p/puertos-udp-67-y-68.html

#### 3.5.1.2 Mecanismos de respaldos de información

La información sensible dentro de la AZNEE se la podría respaldar de la siguiente manera:

- **Cintas magnéticas**: La información almacenada en este tipo de medio, se la debe realizar en periodos de tiempo cortos o largos que dependerán exclusivamente de la sensibilidad de la información que se gestione en la dependencia. En la AZNEE, se deberían realizar respaldos en periodos de tiempo que fluctúan entre 15 días a un mes como máximo, dado que las documentación que se maneja no es tan sensible y no está sujeta a cambios constantes como es el caso de documentos de catastros, planos y trámites de permisos de funcionamiento.

### 3.5.2 SEGURIDAD A NIVEL DE SERVICIOS

Considerando los servicios que se gestiona en la AZNEE, se procederá a desarrollar un conjunto de ideas que ayudarán a mitigar los riesgos de la red.

#### 3.5.2.1 Políticas de seguridad para el Active Directory

Al utilizarse en la red el servicio proporcionado por la administración central del Municipio de Quito, se observó ciertos inconvenientes, como es la falta de caducidad de contraseñas y la desorganización que existe a nivel de grupos de usuarios, por lo que esto afecta al rendimiento y seguridad de la red. Pensando en esto se ha generado las siguientes políticas:

- Las contraseñas deberán tener un periodo de caducidad de entre 3 a 6 meses máximo.

- Se deberán crear contraseñas que mantengan una longitud no menor a ocho caracteres entre números, letras y símbolos especiales.
- Se deberá generar grupos de trabajo que se encuentren acordes a las actividades que desempeñan los usuarios, un buen punto de partida sería catalogar a los usuarios por coordinación y por departamento.

Adicionalmente, al no haber tenido acceso a este servidor se procederá a emular el servicio utilizando Zentyal[58] en conjunto con LDAP y los clientes que se manejan en la AZNEE.

### 3.5.2.2 Políticas de seguridad para servicios de uso general

Entre los servicios de uso general tenemos:

#### *3.5.2.2.1 FTP*

Solo los usuarios que estén dentro del dominio deberán tener accesos a las carpetas y directorios compartidos en la red interna de la AZNEE.

#### *3.5.2.2.2 Telefonía IP*

Únicamente se deberá colocar teléfonos IP para los usuarios que lo ameriten considerando el cargo, coordinaciones y administraciones generales.

Se deberá evitar mantener abiertas líneas que permitan realizar llamadas de índole personal sin previo consentimiento de un superior. Se configurará un código de salida que sea de una complejidad media y se lo asignará a un grupo de personas bajo un formulario de requerimiento.

#### *3.5.2.2.3 Proxy*

Para mantener a los usuarios de la red libre de distracciones que afecten su rendimiento, se debe proceder a instalar un servidor de proxy que ayude a bloquear

[58] Zentyal: http://www.zentyal.org/

urls y sitios web no deseables. La AZNEE, mantiene un servidor proxy que se encuentra ubicado en la administración central y el cual, como ya se mencionó anteriormente, no se tuvo acceso. Sin embargo, se procederá a emular el servidor utilizando el servicio proxy que brinda Zentyal.

Zentyal utiliza Squid[59], como base para la implementación del proxy. La implementación de las políticas y reglas de configuración del mismo se detalla en el capítulo 4.

[59] Squid: Servidor proxy para web con caché.

# CAPÍTULO IV

# IMPLEMENTACIÓN DE UN PROTOTIPO, PRUEBAS Y RESULTADOS

En este capítulo se detallará la implementación del prototipo que tendrá una topología semejante a la establecida en el capítulo anterior, con sus servicios y configuraciones; cabe recalcar que el prototipo no permitirá reflejar en su totalidad el rediseño de las LAN pasiva y activa planteado para la red multiservicios de la AZNEE.

## 4.1 DISEÑO LÓGICO Y FÍSICO DE LA RED

En el prototipo se configurarán los equipos terminales así como los equipos de conectividad. En la Figura 4.1 se indica el diagrama que se implementó para la comprobación de servicios de voz y datos.

### 4.1.1 DIRECCIONAMIENTO IP

En el prototipo, los equipos de conectividad y los servidores tendrán el direccionamiento IP, descrito en la tabla 4.1.

**Tabla 4.1** Direccionamiento IP del Prototipo

| BLOQUES | SUBRED / MÁSCARA | MÁSCARA | GATEWAY |
|---|---|---|---|
| PRIMER PISO BLOQUE 2 | 172.20.112.0/26 | 255.255.255.192 | 172.20.112.62 |
| TELÉFONOS IP | 172.20.112.64/26 | 255.255.255.192 | 172.20.112.126 |
| PLANTA BAJA BLOQUE 2 | 172.20.5.64/27 | 255.255.255.224 | 172.20.5.94 |
| ENLACES | 172.20.5.0/30 | 255.255.255.252 | |
| SERVIDORES | 172.20.5.160/28 | 255.255.255.240 | 172.20.5.174 |
| WIFI | 172.20.5.176/29 | 255.255.255.248 | 172.20.5.182 |

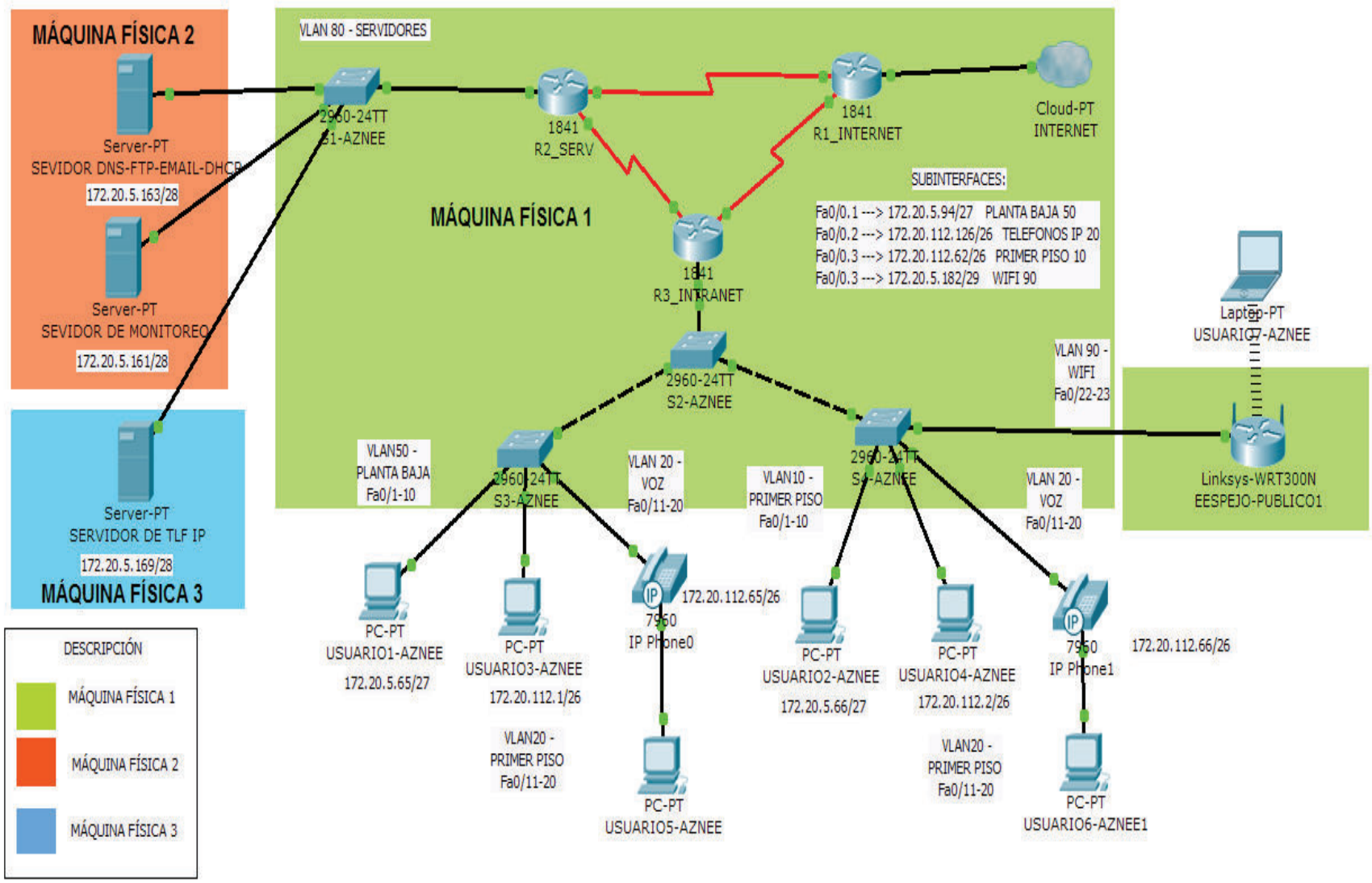



**Figura 4.1** Diagrama de red del prototipo.

Las VLANs que se implementarán para este prototipo se describen en la tabla 4.2.

**Tabla 4.2** Direccionamiento IP según cada interfaz

| DISPOSITIVOS | INTERFAZ | DIRECCIÓN IP | MÁSCARA | GATEWAY |
|---|---|---|---|---|
| | ROUTER EXTERNO | | | |
| R1_INTERNET | Fa0/0 | DCHP | DHCP | |
| R1_INTERNET | Serial 1/0 | 172.20.5.14 | 255.255.255.252 | - |
| R1_INTERNET | Serial 1/1 | 172.20.5.10 | 255.255.255.252 | - |
| | ROUTER SERVIDORES | | | |
| R2_SERV | Serial 1/0 | 172.20.5.13 | 255.255.255.252 | - |
| R2_SERV | Serial 1/1 | 172.20.5.6 | 255.255.255.252 | - |
| | ROUTER DE LA RED INTERNA | | | |
| R3_ INTRANET | Serial 1/0 | 172.20.5.5 | 255.255.255.252 | - |
| R3_ INTRANET | Serial 1/1 | 172.20.5.9 | 255.255.255.252 | - |
| | SWITCHES - SW -SERVIDORES | | | |
| ZENTYAL | NIC | 172.20.5.163 | 255.255.255.240 | 172.20.5.174 |
| NAGIOS | NIC | 172.20.5.161 | 255.255.255.240 | 172.20.5.174 |
| ELASTISK | NIC | 172.20.5.170 | 255.255.255.240 | 172.20.5.174 |
| | EQUIPOS TERMINALES | | | |
| USUARIO1-AZNEE | NIC | 172.20.5.65 | 255.255.255.224 | 172.20.5.94 |
| USUARIO2-AZNEE | NIC | 172.20.5.66 | 255.255.255.224 | 172.20.5.94 |
| USUARIO3-AZNEE | NIC | 172.20.112.1 | 255.255.255.240 | 172.20.112.62 |
| USUARIO4-AZNEE | NIC | 172.20.112.2 | 255.255.255.240 | 172.20.112.62 |
| USUARIO5-AZNEE | NIC | 172.20.112.65 | 255.255.255.192 | 172.20.112.126 |
| USUARIO6-AZNEE | NIC | 172.20.112.66 | 255.255.255.192 | 172.20.112.126 |
| USUARIO7-AZNEE | | 172.20.5.177 | 255.255.255.248 | 172.20.5.182 |
| | | ROUTER DE SERVIDORES | | |
| R2_SERV | Fa0/0.1 | 172.20.5.174 | 255.255.255.240 | - |

| | | ROUTER DE LA RED INTERNA | | |
|---|---|---|---|---|
| R3_ INTRANET | Fa0/0.1 | 172.20.112.62 | 255.255.255.192 | PRIMER-PISO |
| R3_ INTRANET | Fa0/0.2 | 172.20.5.94 | 255.255.255.224 | PLANTA-BAJA |
| R3_ INTRANET | Fa0/0.3 | 172.20.112.126 | 255.255.255.192 | VOZ |
| R3_ INTRANET | Fa0/0.4 | 172.20.5.182 | 255.255.255.248 | WIFI |

## 4.2 INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

Para la realización del prototipo se utilizaron máquinas físicas con las siguientes configuraciones:

- **Máquina Física 1:** PC con sistema operativo Linux donde se instaló el software GNS3[60] para la emulación de los routers R1_INTERNET, R2-SERV y R3-INTRANET y los switches S1-AZNEE, S2-AZNEE,S3-AZNEE Y S4-AZNEE.
- **Máquina Física 2:** PC con sistema operativo Windows 8 donde se instaló el software VirtualBox, se crearon dos máquinas virtuales, una que contiene al servidor Zentyal y otra con el servidor de monitoreo Nagios.
- **Máquina Física 3:** PC con sistema operativo Windows 8, donde se creó una máquina virtual que contiene el servidor de telefonía IP Asterisk.

De esta manera se procedió a la implementación cada uno de los servicios que utilizarán la red, así como las configuraciones de seguridad.

A continuación se detalla cada uno de los dispositivos y servicios que se manejaron para la implementación del prototipo de prueba.

### 4.2.1 EQUIPOS TERMINALES

Existen dos usuarios denominados USUARIO1-AZNEE y USUARIO2-AZNEE configurados con sistema operativo Windows 7. Las direcciones IP y de DNS, serán proporcionadas directamente por el servidor de DHCP.

[60] GNS3: http://www.gns3.com/

Para la simulación de teléfonos IP se utilizó softphones con el software 3CXphone[61] versión 6 para las pruebas de comunicación.

### 4.2.2 EQUIPOS DE CONECTIVIDAD

Los equipos de conectividad que se utilizaron en este prototipo fueron:

#### *4.2.2.1 Routers*

Los routers utilizados para la implementación de este prototipo son de la marca Cisco serie 7200, para soportar el protocolo BGP. El archivo de configuración se encuentra en el Anexo I.

A continuación se detalla las configuraciones realizadas:

- Configuraciones básicas de un router (hostname, encriptación de claves.)
- Configuración de interfaces (Serial y Fastethernet)
- Configuración de subinterfaces para la respectiva VLAN.
- Pool de direcciones para el servicio de DCHP por cada subred.
- Configuración del protocolo BGP (Border Gateway Protocol).

En la figura 4.2 se puede verificar la tabla de enrutamiento que tendrán los routers.

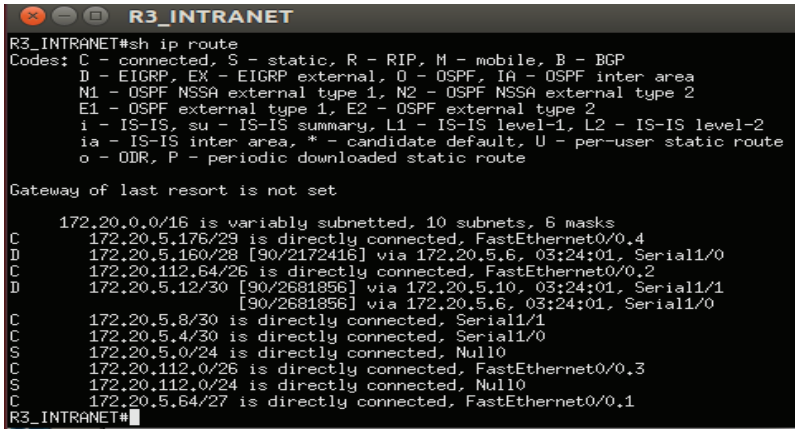



**Figura 4.2** Tabla de enrutamiento de R3_ INTRANET

[61] 3CXphone: http://www.3cx.com/voip/voip-phone/

El direccionamiento dinámico se lo implementó en cada uno de los routers para que ellos asignen el pool de direcciones IP respectivas. En la figura 4.3 se puede observar el pool de direcciones del R3_INTRANET.

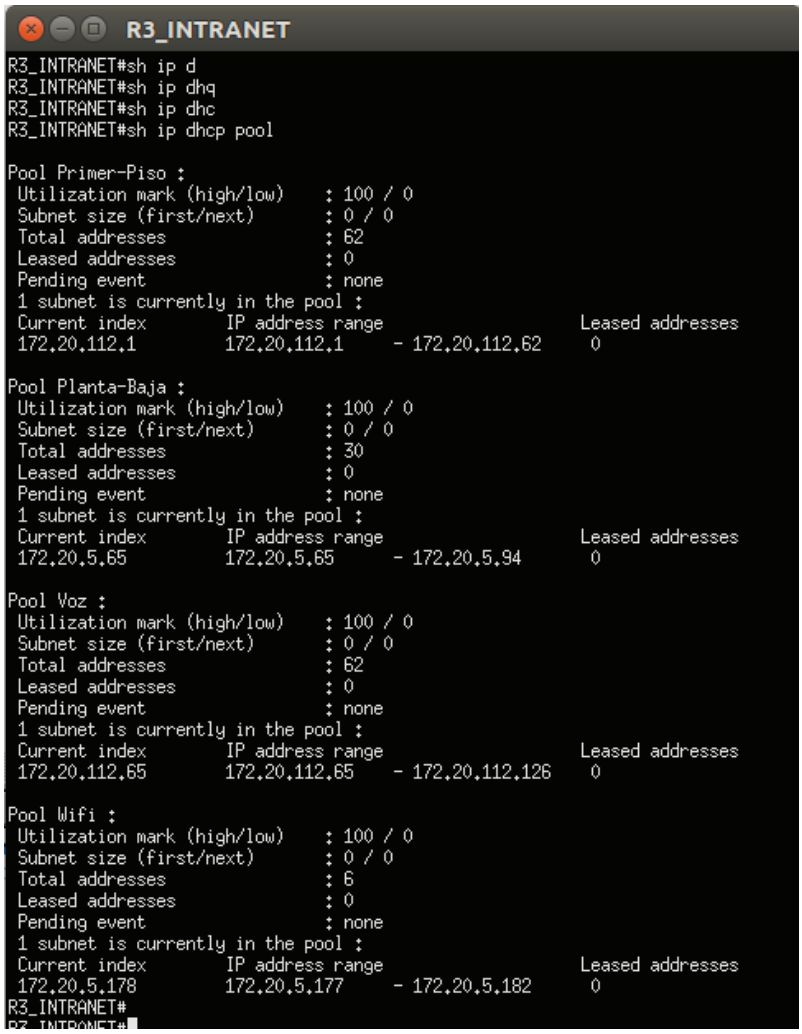



**Figura 4.3** Pool de direcciones del R3_INTRANET

#### *4.2.2.2 Switches*

Los switches que se usaron para el prototipo fueron de la marca Cisco serie 3745, los archivos de configuración de cada uno se encuentran en el Anexo I.

A continuación se detalla las configuraciones realizadas:

- Configuraciones básicas de un switch (hostname, encriptación de claves.)

- Creación de VLANs.
- Descripción de cada VLAN.
- Asignación de puertos para cada VLAN.
- Asignación de puertos troncales.
- Configuración de una IP para la interfaz de administración.
- Desactivación de puertos no usados.

En la figura 4.4 se muestra la tabla de VLANs que se implementaron en el switch S4_AZNEE del prototipo.

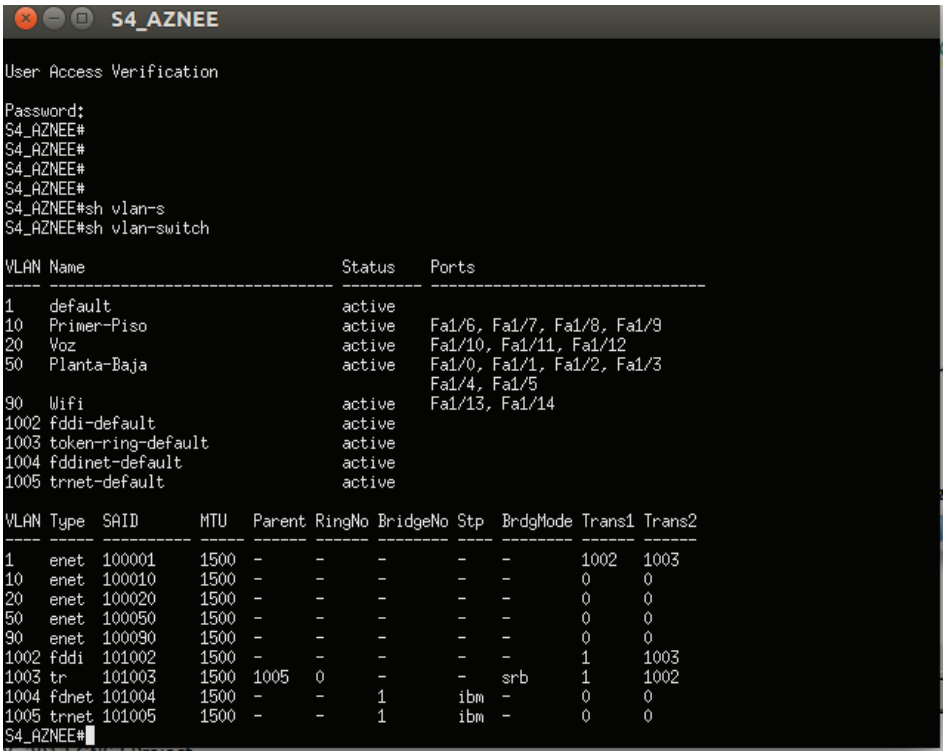



**Figura 4.4** Tabla de direccionamiento de VLANs en S4_AZNEE

#### *4.2.2.3 Routers inalámbricos*

Para la realización de la red inalámbrica se desarrolló una Red Ad-hoc[62], en la cual se utilizó el dispositivo wireless de la Máquina Física 1, permitiendo que se conecten los dispositivos inalámbricos dentro de la red.

[62] Red Ad-Hoc: Red Inalámbrica Descentralizada

Los parámetros configurados fueron:

- Configuración de SSID – Waznee
- IP de administración, Gateway y DNS

### 4.2.3 SERVIDORES

Para la instalación y configuración de los servidores se utilizó software libre específicamente las distribuciones de Ubuntu y Centos. En la tabla 4.3 se indican los servidores y sus características.

**Tabla 4.3** Servidores a implementar en el prototipo.

| SERVIDOR | SERVICIOS | SISTEMA OPERATIVO |
|---|---|---|
| ZENTYAL | DNS,FTP,CORREO,IDS | Linux Ubuntu Server 3.14 |
| ASTERISK | Telefonía IP | Linux CentOS 3.11 |
| NAGIOS | Sistema de Monitorización de Red | Linux Ubuntu 2.6.32 |

#### 4.2.3.1 Servidor Zentyal

Zentyal es un servidor basado en el sistema operativo Linux, utilizado para pequeñas y grandes empresas, en este caso se decidió su utilización para la implementar los servicios planteados en el capítulo anterior, los cuales se numeran a continuación:

- DNS
- Servidor de Dominio LDAP
- FTP
- Correo
- Sistema de Detección de Intrusos (IDS)

La instalación de Zentyal se realizó sobre una máquina virtual en la cual se configuró los siguientes parámetros:

- Lenguaje de instalación
- Zona horaria
- Distribución de teclado
- Configuración de la red
- Usuario y contraseña de administración

Una vez terminada la instalación de Zentyal, el sistema presenta la interfaz gráfica que permitirá la administración a través de una página web (Figura 4.5).

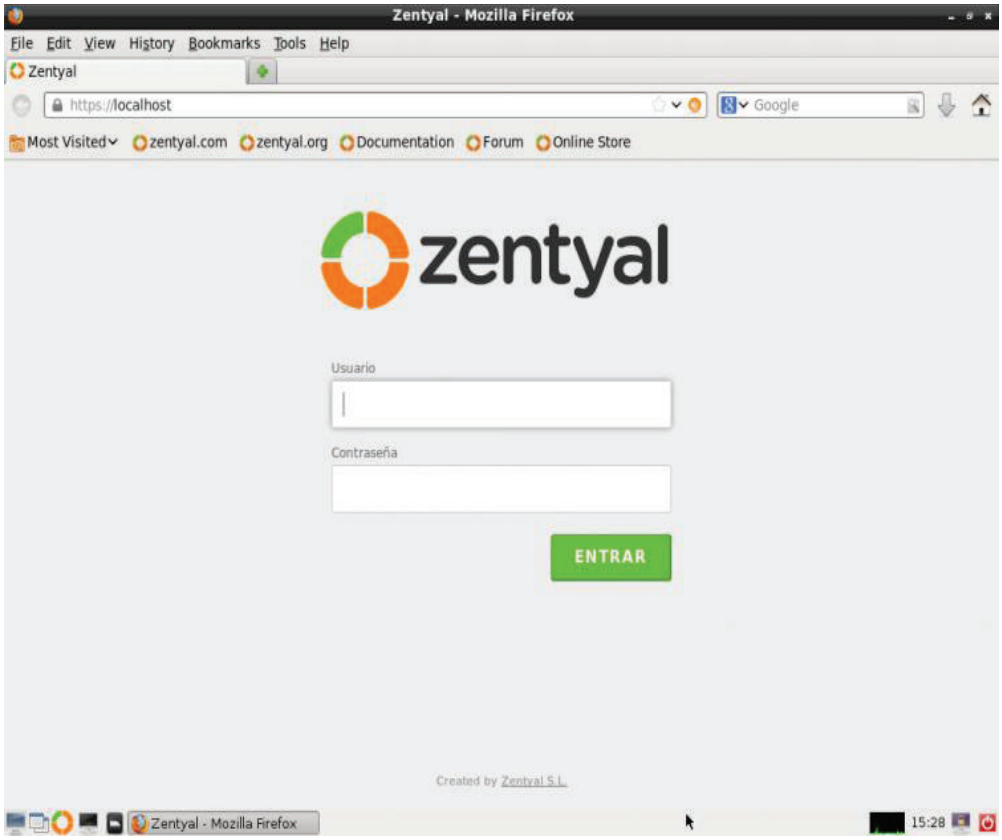



**Figura 4.5** Página de inicio del servidor Zentyal

Después de autenticarnos, se procede a la instalación de los paquetes de los servicios listados anteriormente, y se realiza la configuración inicial de los parámetros del servidor Zentyal.

#### *4.2.3.1.1 Interfaz de Red*

La dirección IP y la máscara de la interfaz de red del servidor Zentyal se la configuró de manera estática (Figura 4.6).


**Figura 4.6** Configuración de la interfaz de red

#### *4.2.3.1.2 DNS*

Para la configuración del servidor de DNS en Zentyal, se especificó la dirección IP 172.20.5.163. En la figura 4.7 se indica la creación del dominio **quito.gob.ec**, mismo que simulará el dominio del Municipio de Quito.


**Figura 4.7** Creación del dominio quito.gob.ec

#### *4.2.3.1.3 Servidor de Dominio*

Zentyal integra el uso de Samba4[63] como servidor de dominio, el cual se relaciona con la implementación de Microsoft Active Directory, que permitirá la compartición de información del directorio a clientes asociados al mismo dominio, además permitirá la compartición de ficheros.

En Zentyal una vez activado el módulo de usuarios y equipos se podrá observar la configuración de LDAP como se puede indicar en la figura 4.8.


**Figura 4.8** Configuración de LDAP

[63] Samba4: Controlador Active Directory

Se activa la opción de PAM (Pluggable Authentication Modules)[64] para permite a los usuarios un acceso con autenticación para verificar su identidad.

En el menú de usuarios y equipos podemos gestionar el árbol LDAP, en donde se puede crear o eliminar nodos del árbol. En la figura 4.9 se indica los usuarios y grupos que se crearon para la realización de pruebas.

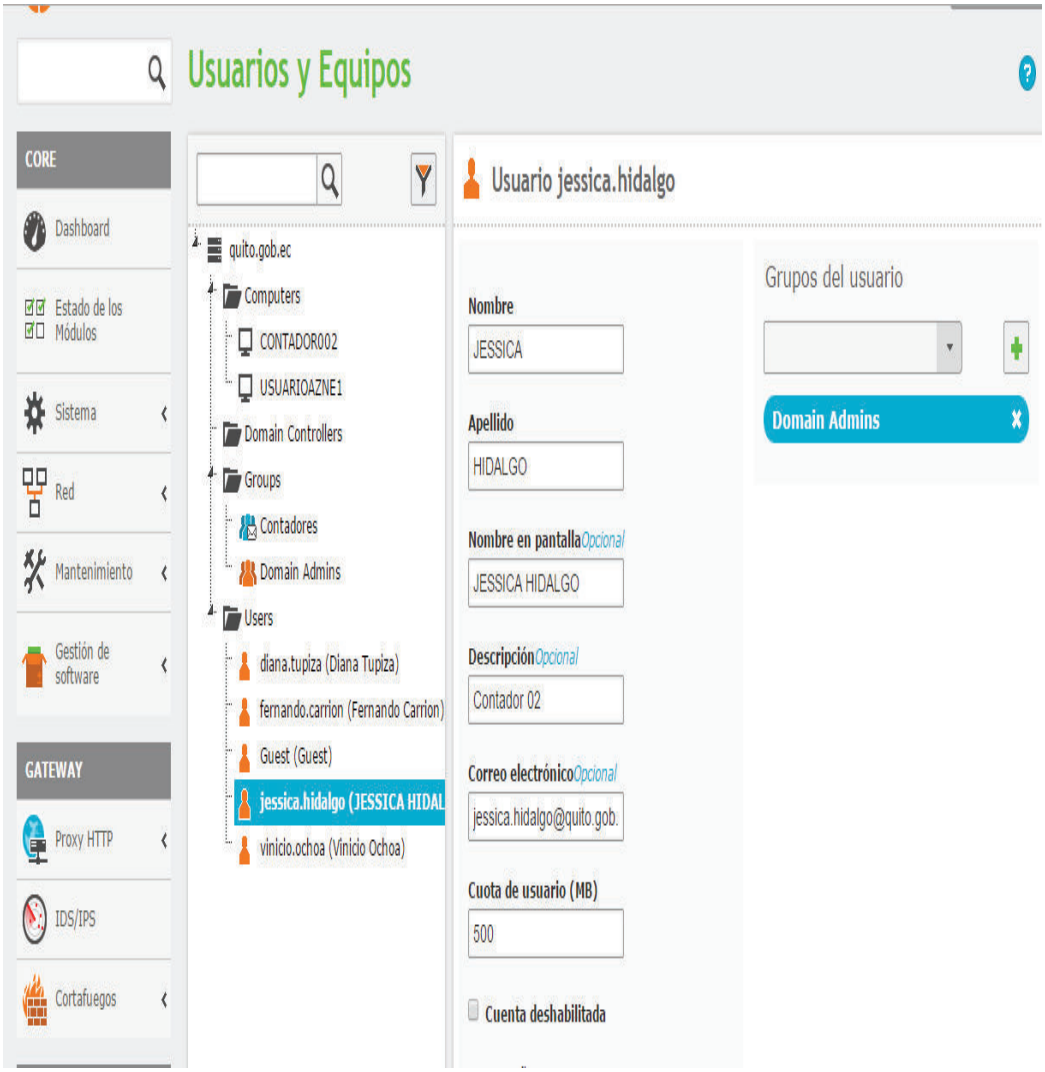



**Figura 4.9** Creación de nodos en el árbol de LDAP

[64] PAM: Es un mecanismo de autenticación flexible que permite abstraer las aplicaciones y otro software del proceso de identificación

En la figura 4.10 se indican los equipos creados y asociados al dominio quito.gob.ec.

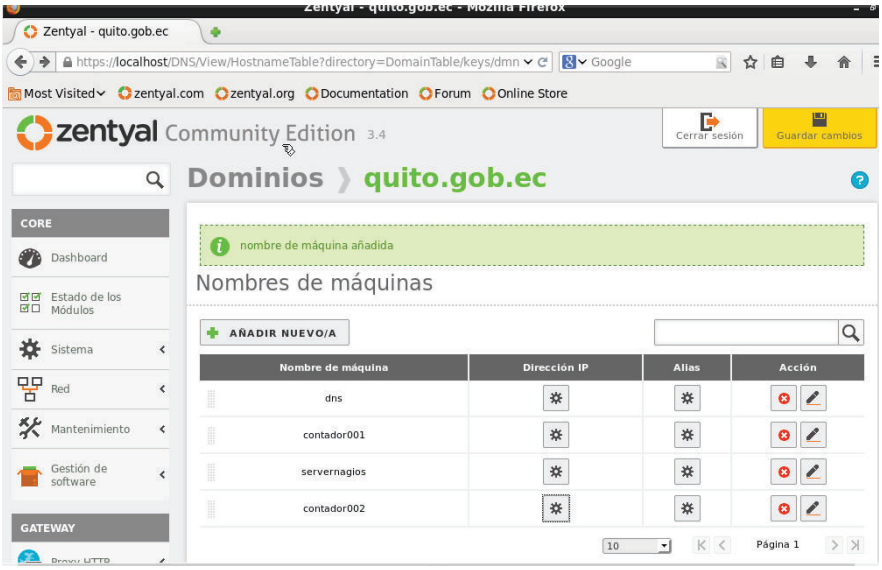



**Figura 4.10** Equipos creados para la realización de pruebas.

Desde el módulo de usuarios y equipos se puede modificar la configuración por defecto que tienen los usuarios, por ejemplo las cuentas de correo como se indica en la figura 4.11.

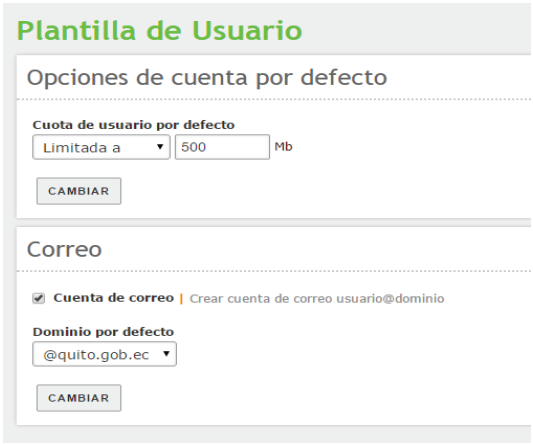



**Figura 4.11** Configuración de la plantilla de usuarios

Zentyal por medio de LDAP crea un directorio personal en */home/zentyal/temporal,* el mismo que estará disponible para los usuarios unidos

al dominio. Para la creación de un directorio compartido se realizará la configuración que se muestra en la figura 4.12


**Figura 4.12** Creación del directorio compartido.

#### *4.2.3.1.4 Servidor de Correo*

En la figura 4.13 se muestra la configuración del servidor de correo con los parámetros que se indica.

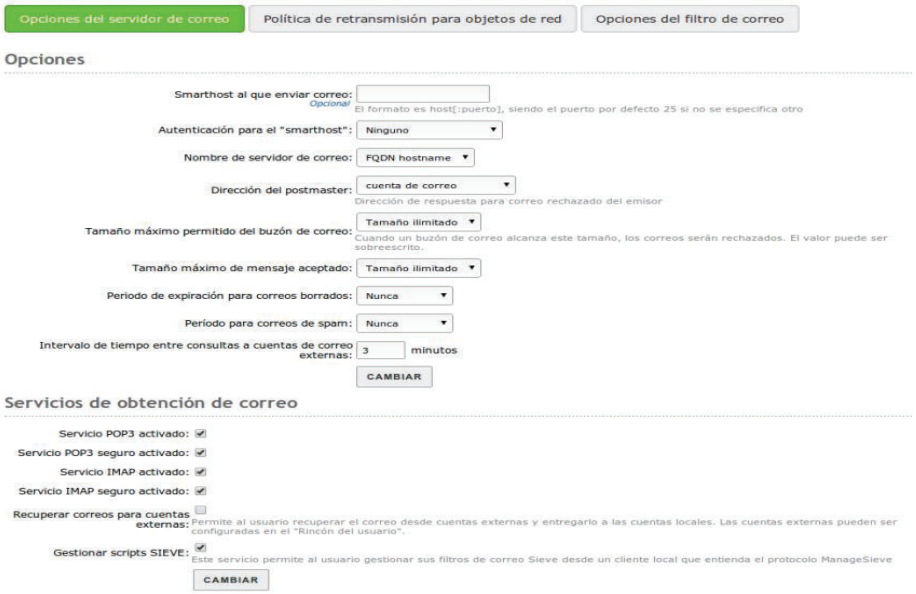



**Figura 4.13** Configuración del servidor de Correo

Para la creación de cuentas de correo se deberá tener usuarios creados (véase, figura 4.9) y un dominio de correo virtual que se encuentran en la figura 4.14.


**Figura 4.14** Creación de dominios virtuales

#### *4.2.3.1.5 Servidor FTP*

Los archivos de configuración del servidor FTP se encuentran en las siguientes direcciones:

- /etc/vsftpd.conf
- /etc/pam.d/vsftpd

En la figura 4.15 se puede verificar la configuración general del servidor FTP y en el Anexo J se encuentra el archivo de configuración.


**Figura 4.15** Configuración del Servidor FTP.

#### *4.2.3.1.6 Sistema de Detección de Intrusos*

En la configuración del sistema de detección de intrusos lo primero que se realizó es la identificación de la interfaz de red, en donde se habilitó la escucha del IDS como se indica en la figura 4.16.


**Figura 4.16** Interfaz habilitada para la escucha del IDS

Para determinar las reglas del sistema de detección de intrusos Zentyal tiene preconfigurados un conjunto de reglas de Snort[65], que permiten bloquear y registrar el origen del tráfico sospechoso.

En la figura 4.17 se indican las reglas que fueron habilitadas para el IDS.

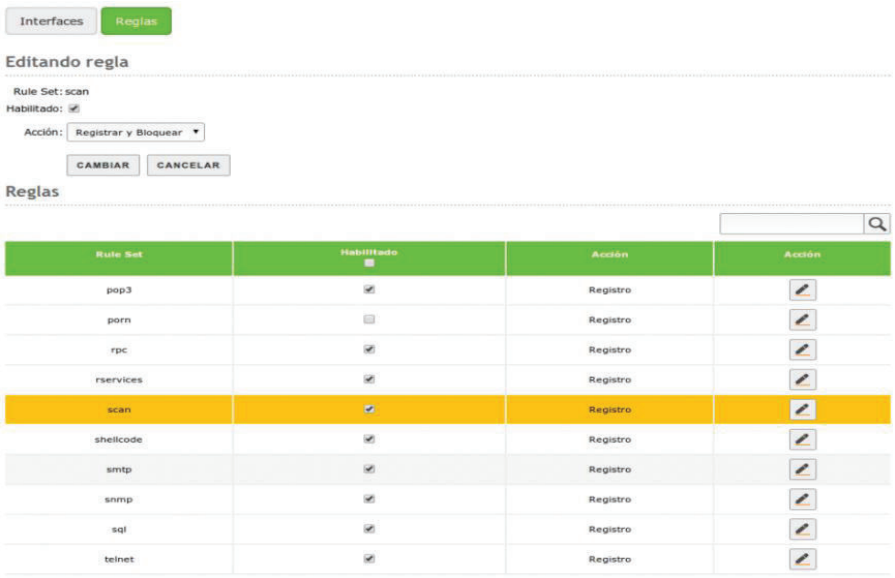



**Figura 4.17** Reglas configuradas para el sistema de detección de intrusos

[65] Snort: Es un sniffer de paquetes y un detector de intrusos basado en red.

#### *4.2.3.1.7 Proxy*

La configuración del Proxy mediante Zentyal proporciona máxima seguridad entre la red interna y el router conectado al internet. Zentyal proporciona varias reglas para establecer políticas para el filtrado de paquetes como lo indica la figura 4.18.


**Figura 4.18** Tipos de reglas para el manejo del proxy en Zentyal

A continuación en la figura 4.19, se indican las reglas configuradas en Zentyal.

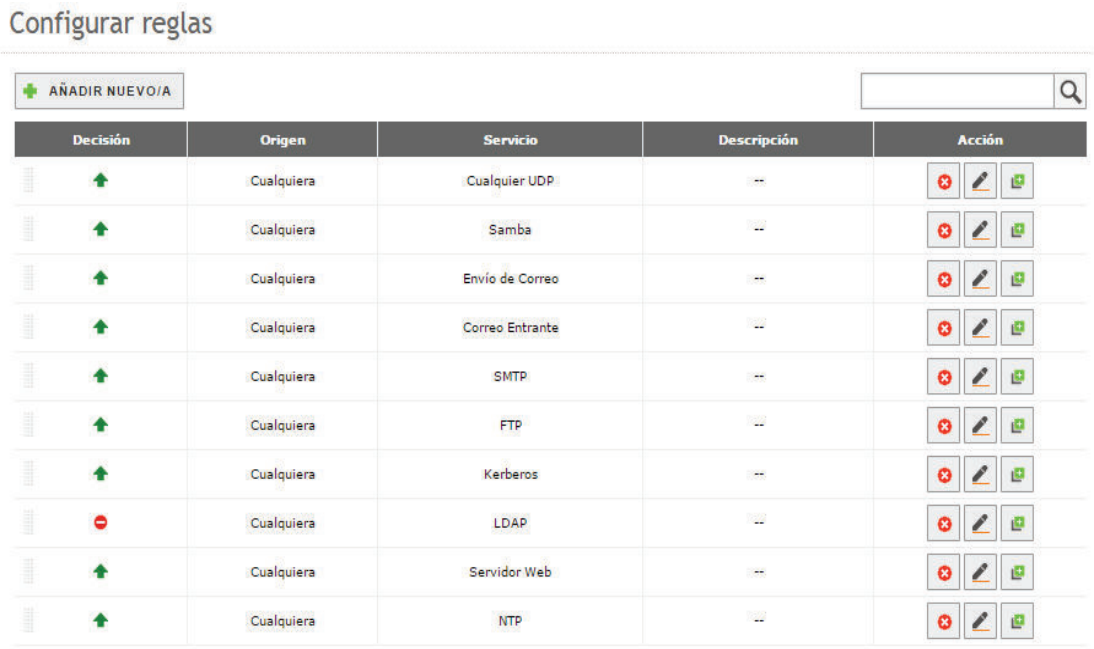



**Figura 4.19** Reglas del proxy

#### 4.2.3.2 Nagios

El sistema de monitoreo implementado es Nagios, el cual se instaló sobre el sistema operativo Ubuntu 12.04.

El primer paso es instalar los servicios básicos que son: apache2, PHP y build (compilador).

```
sudo apt-get install apache2
sudo apt-get install libapache2-mod-php5
sudo apt-get install build-essential
sudo apt-get install mysql-server mysql-client
sudo apt-get install php-pear
sudo apt-get install rrdtool
sudo apt-get install librrds-perl
sudo apt-get install php5-gd
```

Se creará un usuario y un grupo para el servidor Nagios.

```
sudo useradd -m -s /bin/bash nagios
sudo passwd nagios
sudo groupadd nagcmd
sudo usermod -a -G nagcmd nagios
sudo usermod -a -G nagcmd www-data
```

Se descarga, descomprime e instala el paquete que contiene el software Nagios.

```
sudo wget
http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-
3.3.1.tar.gz
sudo tar -xvzf nagios-3.3.1.tar.gz
cd nagios/
sudo ./configure --prefix=/srv/nagios --with-command-user=nagios --
with-command-group=nagcmd  --with-nagios-user=nagios --with-nagios-
group=nagcmd
```

Una vez terminada la instalación de Nagios, se puede acceder a la interfaz gráfica de administración, que para este caso es http://172.20.5.161/nagios, como se indica en la figura 4.20.

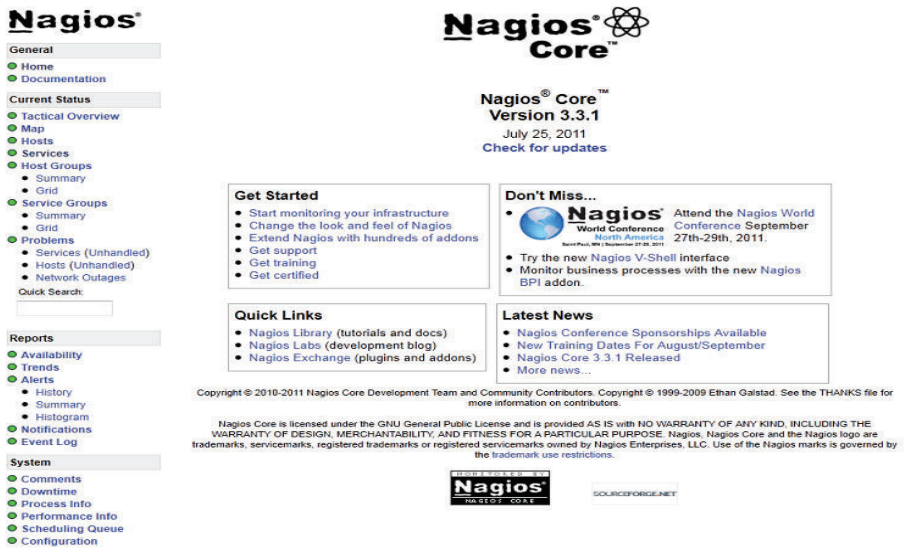



**Figura 4.20** Interfaz gráfica de administración de Nagios.

Se instalará la herramienta NagiosQL que permite el registro de host y equipos que se van a monitorear.

```
sudo wget http://sourceforge.net/projects/nagiosql/files/nagiosql
/NagiosQL%203.1.1/nagiosql_311.tar.gz
sudo tar -xvzf nagiosql_311.tar.gz
sudo mv nagiosql /srv/nagios/nagiosql
sudo ln -s /srv/nagios/nagiosql /var/www/nagiosql
sudo pear install HTML_Template_IT
sudo mkdir /srv/nagios/etc/objects/hosts
sudo mkdir /srv/nagios/etc/objects/services
sudo mkdir /srv/nagios/etc/objects/backup
```

```
sudo mkdir /srv/nagios/etc/objects/backup/hosts
sudo mkdir /srv/nagios/etc/objects/backup/services
sudo chown -R nagios:nagcmd /srv/nagios
sudo chmod 770 /srv/nagios/nagiosql/config
sudo chmod g+w /srv/nagios/nagiosql/
sudo chmod g+w /srv/nagios/etc/objects/hosts
/srv/nagios/etc/objects/services /srv/nagios/etc/objects/backup
/srv/nagios/etc/objects/backup/hosts
/srv/nagios/etc/objects/backup/services
```

Una vez finalizada la instalación de los repositorios ingresamos a la página http://172.20.5.161/nagiosql para continuar con el proceso de instalación como indica la figura 4.21.

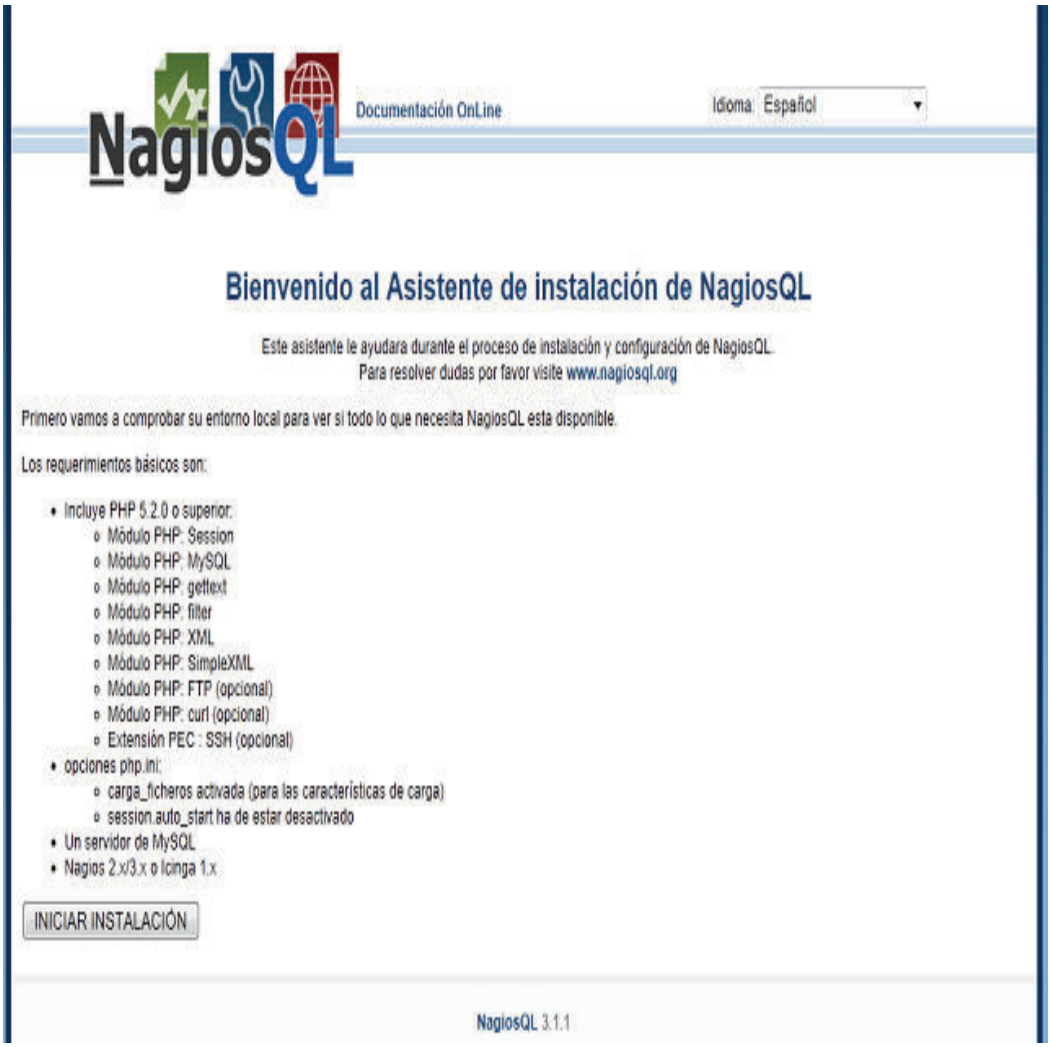



**Figura 4.21** Página de instalación de NagiosQL

En la figura 4.22 se indica la comprobación de los requisitos del servicio NagiosQL.

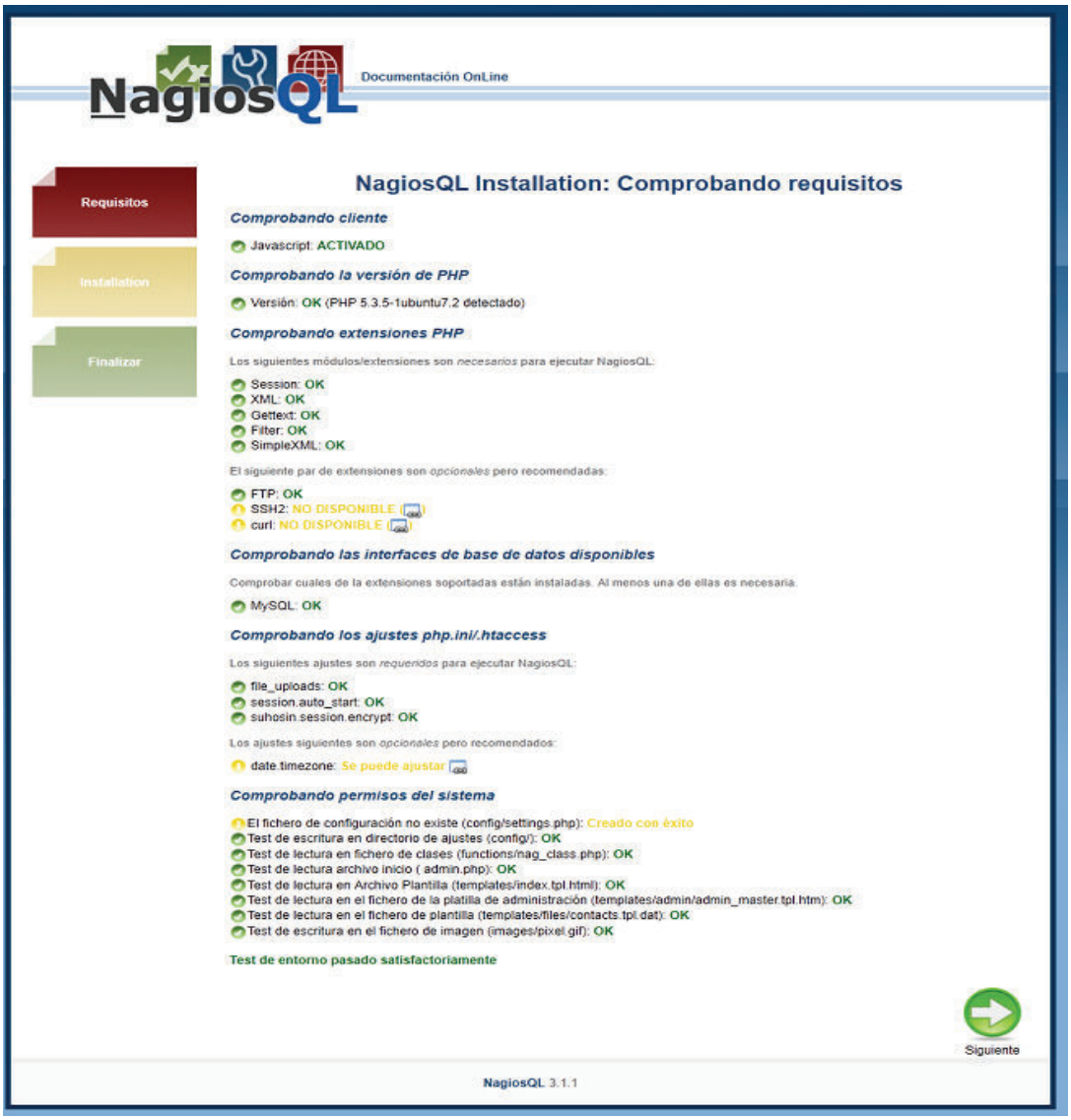



**Figura 4.22** Comprobación de requisitos para NagiosQL

Se colocan las claves correspondientes y las credenciales de inicio en la aplicación, para finalizar la instalación se tendrá una ventana de confirmación y otra para la autenticación.

Se procederá a configurar los archivos de NagiosQL para el registro de equipos y dispositivos a ser monitoreados.

En el prototipo los equipos a monitorear son:

- Router R1_INTERNET
- Router R2_SERV
- Router R3_INTRANET
- Servidor de Monitoreo Nagios
- Servidor Zentyal
- Servidor de Telefonía IP ASTERISK

En la figura 4.23 se indica los hosts que fueron configurados en el archivo host.cfg.

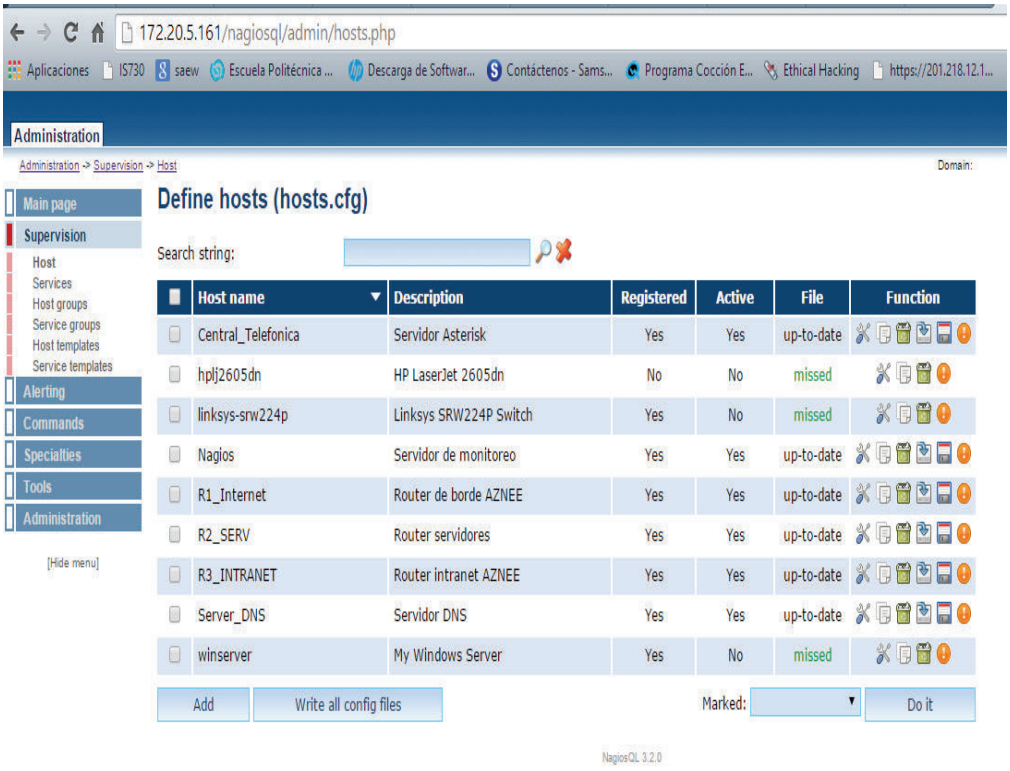



**Figura 4.23** Hosts configurados para el monitoreo.

Se configuró el protocolo SNMP en los routers para tener una gestión adecuada de la red. Una vez que se agregan los hosts se puede verificar en el servidor el estado de los mismos como se indica en la figura 4.24. En el Anexo K se muestran los archivos de configuración para el servidor Nagios.

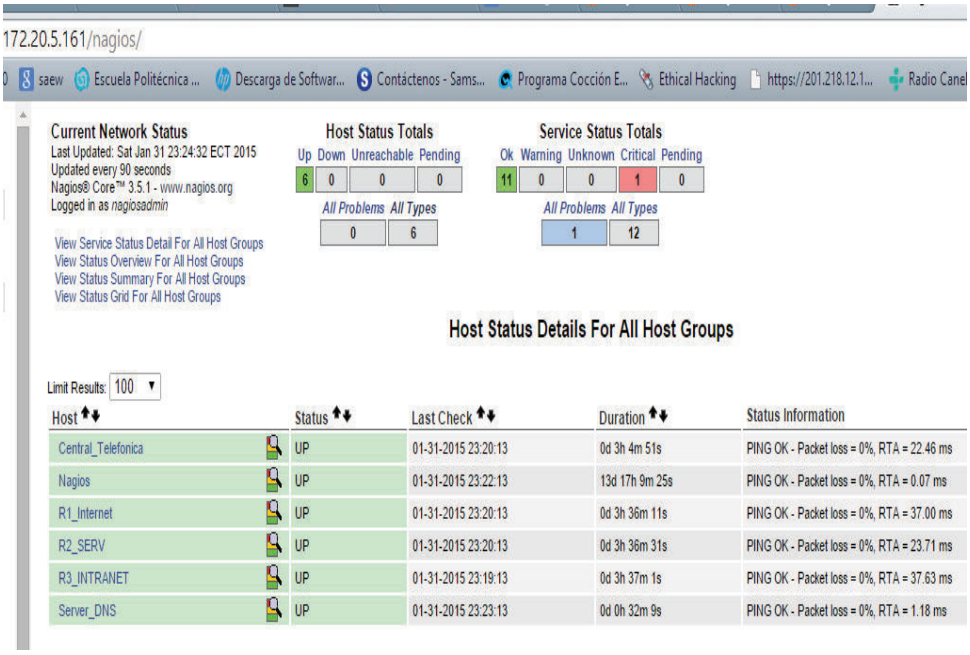



**Figura 4.24** Estado de los equipos configurados

#### 4.2.3.3 Configuración de central telefónica IP - Asterisk

El servidor Asterisk será implementado sobre una máquina virtual, mediante la utilización de la imagen .iso de AsteriskNOW.

En la instalación del servidor los parámetros a tomar en cuenta son:

- Selección del idioma
- Distribución del teclado
- Configuración de la dirección IP de forma manual o por DHCP.
- Huso horario
- Contraseña de administración

El asistente de instalación se encarga de realizar una configuración previa antes de la instalación de Asterisk y una vez terminado este proceso, el servidor se reiniciará y nos mostrará una pantalla en modo consola, figura 4.25, donde se indica la dirección IP con la cual se debe acceder a la interfaz gráfica para realizar las configuraciones respectivas.

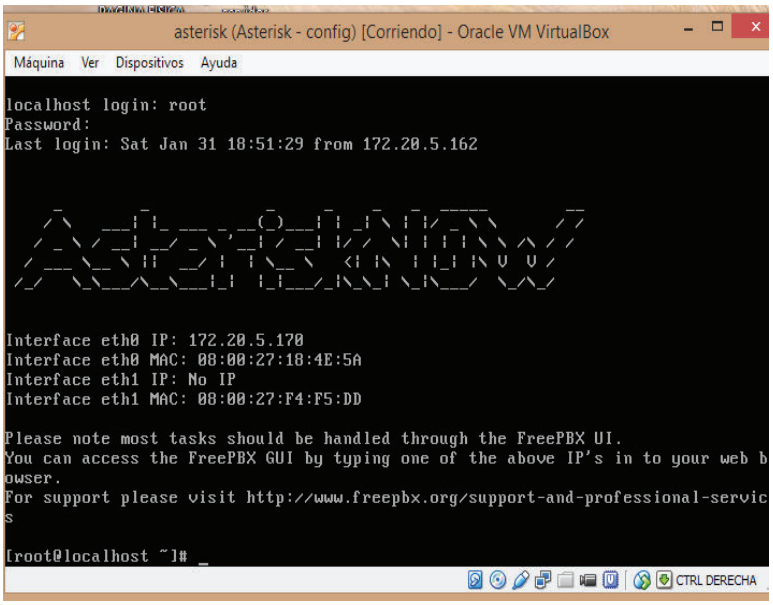



**Figura 4.25** Interfaz de consola de Asterisk.

En la figura 4.26 se indica la configuración de extensiones y usuarios según la tabla 3.11.

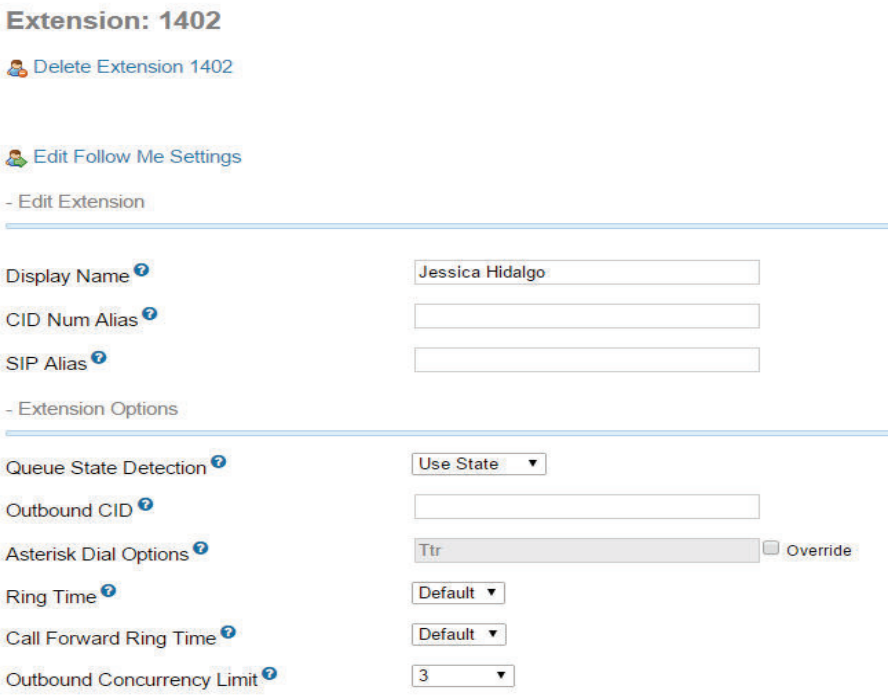



**Figura 4.26** Configuración de extensiones

#### 4.2.3.4 Configuración del teléfono IP

El software que se utilizó para simular los teléfonos IP es el 3CX PHONE versión 6, cuyas especificaciones técnicas se encuentran en el Anexo L.

En la figura 4.27 se indica la configuración básica de un softphone, cuyos parámetros a configurar fueron:

- Nombre
- Credenciales(extensión y password)
- Dirección IP del servidor de telefonía

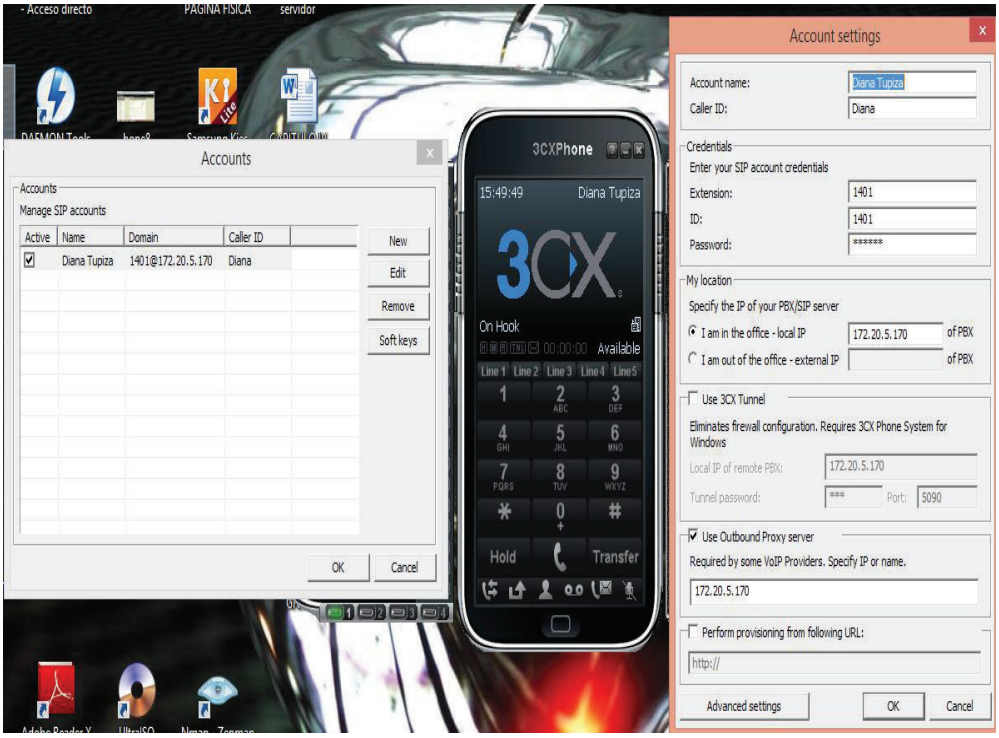



**Figura 4.27** Configuración de softphone 3CX phone.

Para probar las características que brinda el servidor de telefonía IP, se instaló en un smartphone, el software ZOIPER, cuyas especificaciones técnicas se encuentran en el Anexo M, en la figura 4.28 se muestra a configuración básica de esta aplicación.

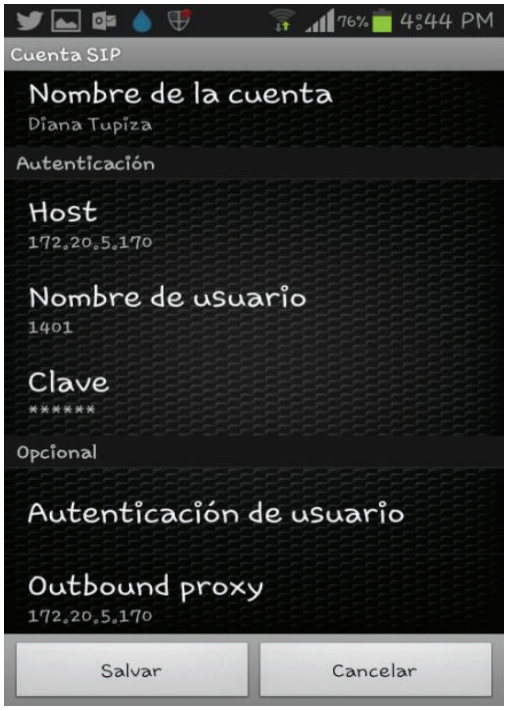



**Figura 4.28** Configuración de Zoiper en un celular smartphone

## 4.3 CONFIGURACIONES DE SEGURIDAD

Las configuraciones a nivel de seguridad se las realizaron con la herramienta IPTABLES en cada uno de los servidores, para evitar accesos inesperados y así mejorar la seguridad.

Los archivos de configuración de IPTABLES de cada uno de los servidores se encuentran a continuación en donde se cerraron puertos según su grado de vulnerabilidad.

### 4.3.1 SERVIDOR DE TELEFONÍA IP

Las configuraciones que se realizaron al servidor de asterisk en la parte de seguridad se indican a continuación:

# Generated by iptables-save v1.4.7 on Sun Jan 25 03:02:46 2015
*mangle

```
:PREROUTING ACCEPT [83145:120824770]
:INPUT ACCEPT [83145:120824770]
:OUTPUT ACCEPT [46823:2584014]
:POSTROUTING ACCEPT [46823:2584014]
COMMIT
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
#-A INPUT -j ACCEPT
#-A INPUT -p udp -m udp --dport 5060 -j ACCEPT
#-A OUTPUT -j ACCEPT
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
#-A INPUT -p tcp --tcp-flags FIN,SYN,RTS,PSH,ACK,URG
FIN,SYN,RST,PSH,ACK,URG -J
-A INPUT -i eth0 -p tcp -m tcp  --dport 4445 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp  --dport 443 -m state --state NEW -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp  --dport 5060 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp  --dport 5060 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp  --dport 10000:20000 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp  --dport 5061 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp  --dport 5061 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp  --dport 4469 -j ACCEPT

-A INPUT -i eth0 -p udp -m udp  --dport 161 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -m state --state NEW -j ACCEPT
COMMIT
*nat
```

Las configuraciones realizadas se dieron para las siguientes restricciones:

- SSH se escucha en el puerto 22. Permite el acceso remoto de manera segura a través de la red.
- El puerto 4445 permite tener acceso al Panel de operador de Flash.
- El puerto 443 HTTPs es usado solo para acceder a FreePBX en su servidor.
- Los puertos 5060 y 5061 son usados para el tráfico del protocolo SIP[66].
- Está utilizando el puerto estándar, 4569, para tráfico IAX2[67]

### 4.3.2 SERVIDOR ZENTYAL

En la figura 4.29 y 4.30 se muestran las configuraciones del firewall para el servidor Zentyal.

```
  GNU nano 2.2.6                File: firewall.conf

# firewall.conf - configuration file for zentyal-firewall
#
# This file contains the most basic settings, most other stuff is configured
# using the web interface.
#
# Everything after a '#' character is ignored
#
# All whitespace is ignored
#
# Config keys are set this way:
#
# key = value
#
# They may contain comments at the end:
#
# key = value # this is ignored

# Limit of logged packets per minute.
iptables_log_limit = 50

# Burst
iptables_log_burst = 10

# Logs all the drops
iptables_log_drops = yes

# Extra iptables modules to load
# Each module should be sperated by a comma, you can include module parameters
iptables_modules = nf_conntrack_ftp, nf_nat_ftp, nf_conntrack_h323, nf_nat_h323, nf_conntrac$

# Enable source NAT, if your router does NAT you can disable it
nat_enabled = yes

# Uncomment the following to show the from External to Internal section
#show_ext_to_int_rules = yes
```

**Figura 4.29** Configuración de firewall de Zentyal

[66] SIP: estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

[67] IAX2: Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

```
root@dns:/# sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
preinput   all  --  anywhere             anywhere
idrop      all  --  anywhere             anywhere             state INVALID
iaccept    all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
inospoof   all  --  anywhere             anywhere
iexternalmodules  all  --  anywhere             anywhere
iexternal  all  --  anywhere             anywhere
inoexternal  all  --  anywhere             anywhere
imodules   all  --  anywhere             anywhere
iglobal    all  --  anywhere             anywhere
iaccept    icmp !f  anywhere             anywhere             icmp echo-request
state NEW
iaccept    icmp !f  anywhere             anywhere             icmp echo-reply st
ate NEW
iaccept    icmp !f  anywhere             anywhere             icmp destination-u
nreachable state NEW
iaccept    icmp !f  anywhere             anywhere             icmp source-quench
 state NEW
iaccept    icmp !f  anywhere             anywhere             icmp time-exceeded
 state NEW
iaccept    icmp !f  anywhere             anywhere             icmp parameter-pro
blem state NEW
idrop      all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
preforward  all  --  anywhere             anywhere
fdrop      all  --  anywhere             anywhere             state INVALID
faccept    all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
fnospoof   all  --  anywhere             anywhere
```

**Figura 4.30** Configuración de firewall de Zentyal

### 4.3.3 SERVIDOR DE MONITOREO

En la figura 4.31 y 4.32 se muestra la configuración del firewall para el servidor de Monitoreo.


**Figura 4.31** Configuración de firewall del servidor de monitoreo

```
root@quito-VirtualBox:/# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@quito-VirtualBox:/#
```

**Figura 4.32** Configuración de firewall del servidor de monitoreo

## 4.4 PRUEBAS

Se realizaron pruebas para comprobar el funcionamiento de los siguientes servidores:

- Servidor de DNS
- Servidor DHCP
- Servidor Proxy
- Servidor de Correo
- Servidor de Monitoreo
- Servidor de Telefonía IP
- Pruebas de conectividad

### 4.4.1 SERVIDOR DNS

Para comprobar su funcionamiento el cliente introdujo el nombre de dominio en vez de la dirección IP como se indica en la figuras 4.33 y 4.34


**Figura 4.33** Funcionamiento del Servidor DNS - directo


**Figura 4.34** Funcionamiento del Servidor DNS - inverso

Se utilizó el comando nslookup para verificar el nombre y la dirección del servidor DNS, como se indica en figura 4.35.

```
[root@asterisk ~]# nslookup  quito.gob.ec
Server:         172.20.5.163
Address:        172.20.5.163#53

Name:   quito.gob.ec
Address: 172.20.5.163
Name:   quito.gob.ec
Address: 10.2.2.5
```

**Figura 4.35** Resultado del comando nslookup

### 4.4.2 SERVIDOR DHCP

Los clientes obtuvieron una dirección IP dinámicamente dentro del rango establecido, además del gateway y la dirección IP del servidor de DNS.

Para verificar esta información se introduce el comando *ipconfig* en el usuario1_aznne obteniendo la siguiente información (figura 4.36).

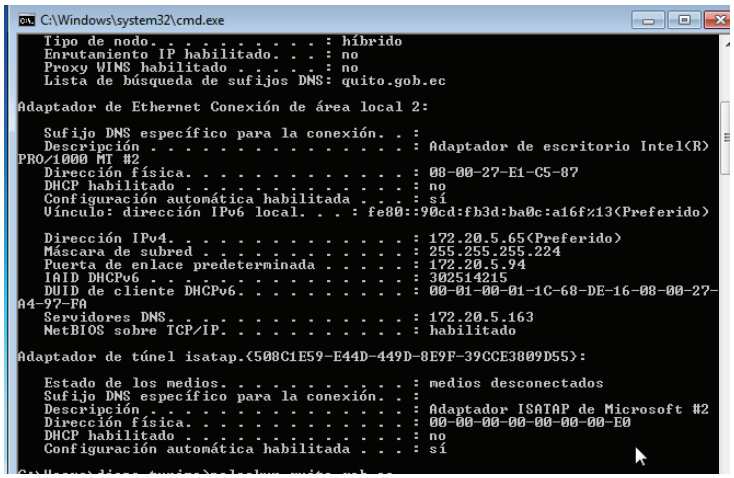



**Figura 4.36** Resultado del comando ipconfig

Para la verificar el funcionamiento del servidor de DHCP, se introduce el comando *show ip dhcp pool* en el router R3_INTRANET, como se indica en la figura 4.37.

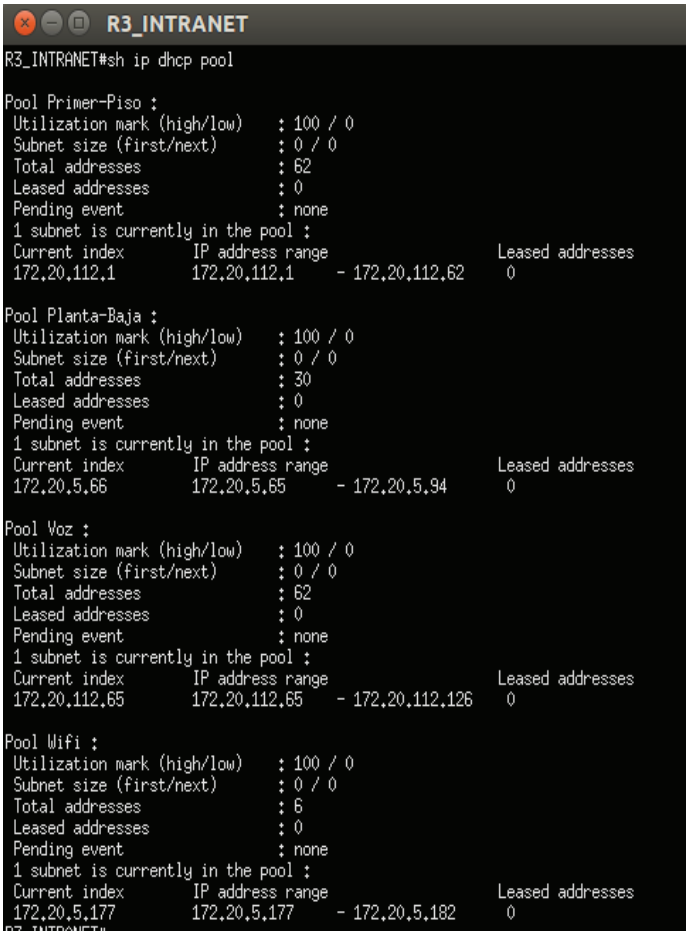



**Figura 4.37** Funcionamiento del servidor de DHCP

### 4.4.3 SERVIDOR PROXY

En el proxy se establecieron reglas para el bloqueo de las siguientes páginas:

- Facebook
- Youtube
- Skype
- Hotmail

En la figura 4.38 se observa un ejemplo de aplicación de las reglas del proxy.

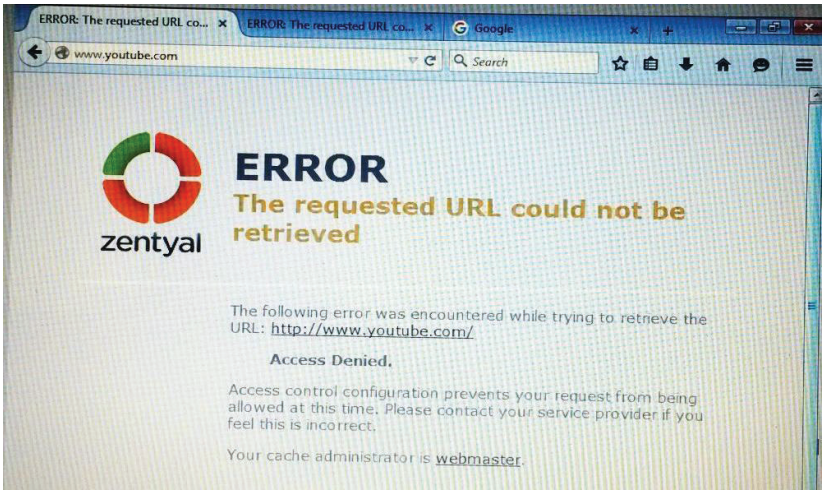



**Figura 4.38** Página con acceso restringido.

### 4.4.4 SERVIDOR DE CORREO

Para comprobar este servicio se procedió a configurar las cuentas de correo en el software Thunderbird[68] que es una aplicación de correo gratuita.

En la figura 4.39 se puede comprobar el funcionamiento del servidor tanto en el envío y recepción de correos.

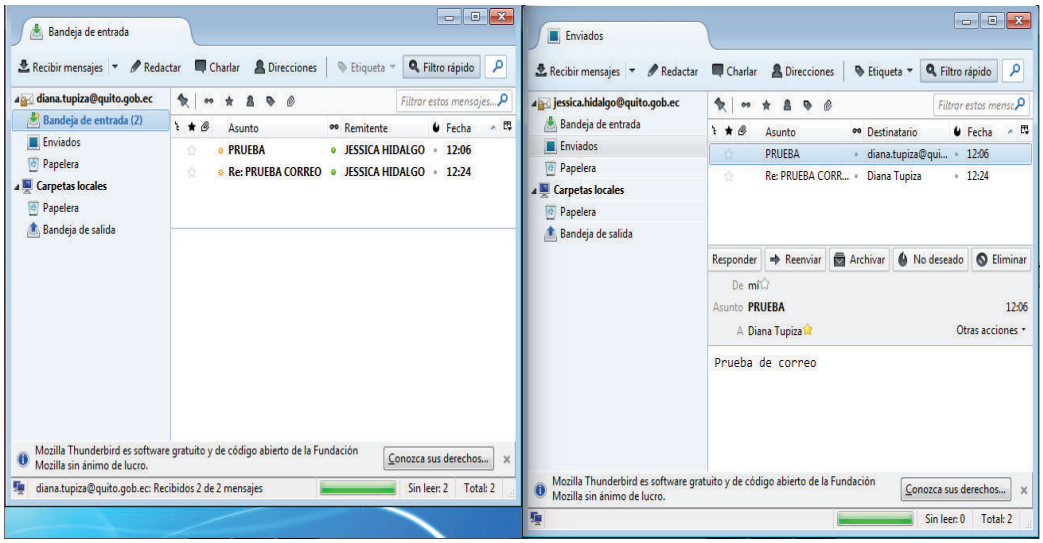
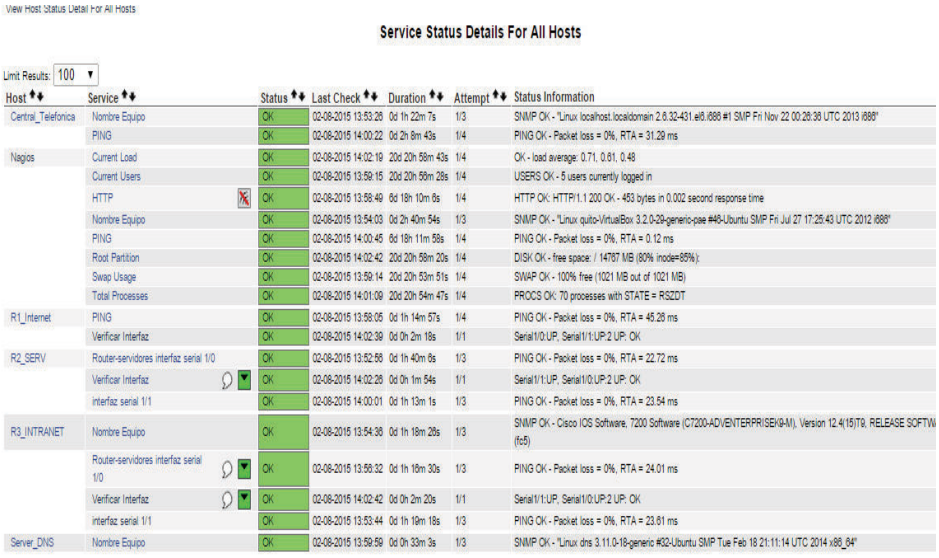



**Figura 4.39** Comprobación del servidor de correo.

[68] Thunderbird: https://www.mozilla.org/es-ES/thunderbird/

### 4.4.5 SERVIDOR DE MONITOREO

Nagios crea automáticamente un mapa de los equipos que se encuentran monitoreados como se indica en la figura 4.40


View Host Status Detail For All Hosts

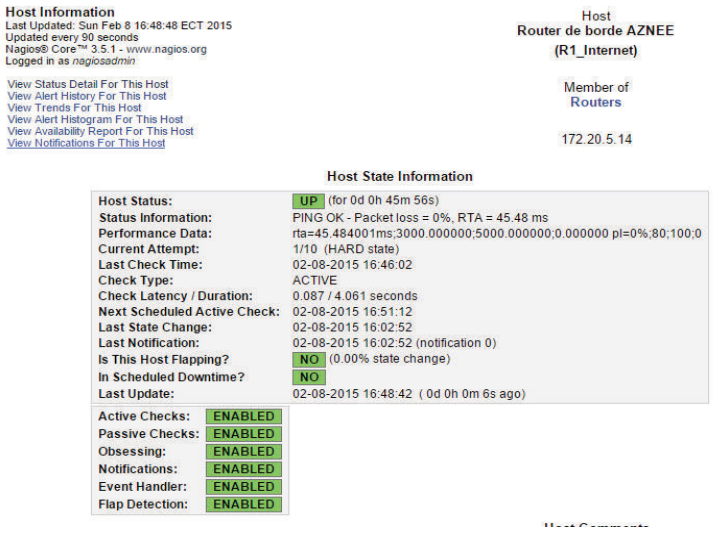
**Service Status Details For All Hosts**

Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| Central_Telefonica | Nombre Equipo | OK | 02-08-2015 13:53:28 | 0d 1h 22m 7s | 1/3 | SNMP OK - "Linux localhost.localdomain 2.6.32-431.el6.i686 #1 SMP Fri Nov 22 00:26:36 UTC 2013 i686" |
| | PING | OK | 02-08-2015 14:00:22 | 0d 2h 8m 43s | 1/4 | PING OK - Packet loss = 0%, RTA = 31.29 ms |
| Nagios | Current Load | OK | 02-08-2015 14:02:19 | 20d 20h 58m 43s | 1/4 | OK - load average: 0.71, 0.61, 0.48 |
| | Current Users | OK | 02-08-2015 13:59:15 | 20d 20h 56m 28s | 1/4 | USERS OK - 5 users currently logged in |
| | HTTP | OK | 02-08-2015 13:58:49 | 6d 18h 10m 6s | 1/4 | HTTP OK: HTTP/1.1 200 OK - 453 bytes in 0.002 second response time |
| | Nombre Equipo | OK | 02-08-2015 13:54:03 | 0d 2h 40m 54s | 1/3 | SNMP OK - "Linux quito-VirtualBox 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686" |
| | PING | OK | 02-08-2015 14:00:45 | 6d 18h 11m 58s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.12 ms |
| | Root Partition | OK | 02-08-2015 14:02:42 | 20d 20h 58m 20s | 1/4 | DISK OK - free space: / 14787 MB (80% inode=85%): |
| | Swap Usage | OK | 02-08-2015 13:59:14 | 20d 20h 53m 51s | 1/4 | SWAP OK - 100% free (1021 MB out of 1021 MB) |
| | Total Processes | OK | 02-08-2015 14:01:09 | 20d 20h 54m 47s | 1/4 | PROCS OK: 70 processes with STATE = RSZDT |
| R1_Internet | PING | OK | 02-08-2015 13:58:05 | 0d 1h 14m 57s | 1/4 | PING OK - Packet loss = 0%, RTA = 45.26 ms |
| | Verificar Interfaz | OK | 02-08-2015 14:02:39 | 0d 0h 2m 18s | 1/1 | Serial1/0:UP, Serial1/1:UP:2 UP: OK |
| R2_SERV | Router-servidores interfaz serial 1/0 | OK | 02-08-2015 13:52:56 | 0d 1h 40m 8s | 1/3 | PING OK - Packet loss = 0%, RTA = 22.72 ms |
| | Verificar Interfaz | OK | 02-08-2015 14:02:26 | 0d 0h 1m 54s | 1/1 | Serial1/1:UP, Serial1/0:UP:2 UP: OK |
| | interfaz serial 1/1 | OK | 02-08-2015 14:00:01 | 0d 1h 13m 1s | 1/3 | PING OK - Packet loss = 0%, RTA = 23.64 ms |
| R3_INTRANET | Nombre Equipo | OK | 02-08-2015 13:54:36 | 0d 1h 18m 26s | 1/3 | SNMP OK - Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(15)T9, RELEASE SOFTW (fc5) |
| | Router-servidores interfaz serial 1/0 | OK | 02-08-2015 13:56:32 | 0d 1h 16m 30s | 1/3 | PING OK - Packet loss = 0%, RTA = 24.01 ms |
| | Verificar Interfaz | OK | 02-08-2015 14:02:42 | 0d 0h 2m 20s | 1/1 | Serial1/1:UP, Serial1/0:UP:2 UP: OK |
| | interfaz serial 1/1 | OK | 02-08-2015 13:53:44 | 0d 1h 19m 18s | 1/3 | PING OK - Packet loss = 0%, RTA = 23.81 ms |
| Server_DNS | Nombre Equipo | OK | 02-08-2015 13:59:59 | 0d 0h 33m 3s | 1/3 | SNMP OK - "Linux dns 3.11.0-18-generic #32-Ubuntu SMP Tue Feb 18 21:11:14 UTC 2014 x86_64" |

**Figura 4.40** Mapa de servicios monitoreados

Se puede verificar el estado de los servicios para el router R1_INTERNET, como se indica en la figura 4.41.


**Host Information**
Last Updated: Sun Feb 8 16:48:48 ECT 2015
Updated every 90 seconds
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as *nagiosadmin*

View Status Detail For This Host
View Alert History For This Host
View Trends For This Host
View Alert Histogram For This Host
View Availability Report For This Host
View Notifications For This Host

Host
**Router de borde AZNEE**
**(R1_Internet)**

Member of
**Routers**

172.20.5.14

**Host State Information**

| | |
|---|---|
| **Host Status:** | UP (for 0d 0h 45m 56s) |
| **Status Information:** | PING OK - Packet loss = 0%, RTA = 45.48 ms |
| **Performance Data:** | rta=45.484001ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0 |
| **Current Attempt:** | 1/10 (HARD state) |
| **Last Check Time:** | 02-08-2015 16:46:02 |
| **Check Type:** | ACTIVE |
| **Check Latency / Duration:** | 0.087 / 4.061 seconds |
| **Next Scheduled Active Check:** | 02-08-2015 16:51:12 |
| **Last State Change:** | 02-08-2015 16:02:52 |
| **Last Notification:** | 02-08-2015 16:02:52 (notification 0) |
| **Is This Host Flapping?** | NO (0.00% state change) |
| **In Scheduled Downtime?** | NO |
| **Last Update:** | 02-08-2015 16:48:42 ( 0d 0h 0m 6s ago) |

| | |
|---|---|
| **Active Checks:** | ENABLED |
| **Passive Checks:** | ENABLED |
| **Obsessing:** | ENABLED |
| **Notifications:** | ENABLED |
| **Event Handler:** | ENABLED |
| **Flap Detection:** | ENABLED |

**Figura 4.41** Comprobación de servicios para el router R1_INTERNET

Verificación del estado de los servicios para el router R2_SERV indicado en la figura 4.42.

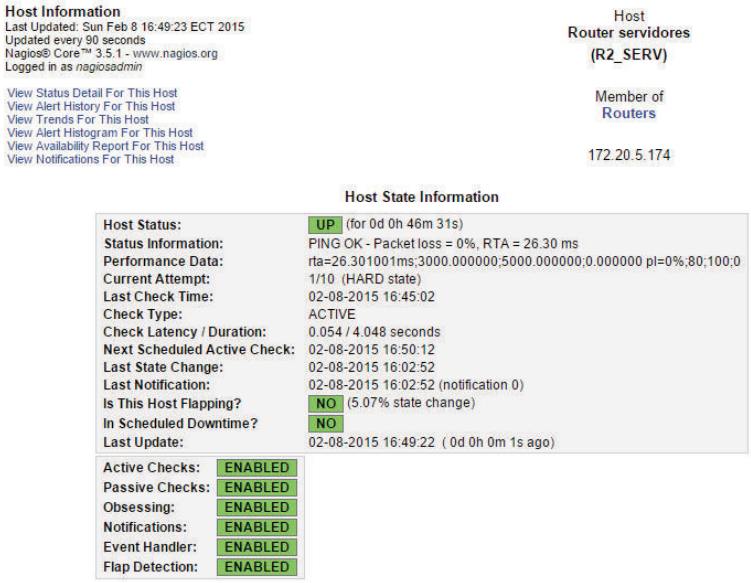



**Figura 4.42** Comprobación de servicios para el router R2_SERV

Verificación del estado de los servicios para el router R3_INTRANET indicado en la figura 4.43.

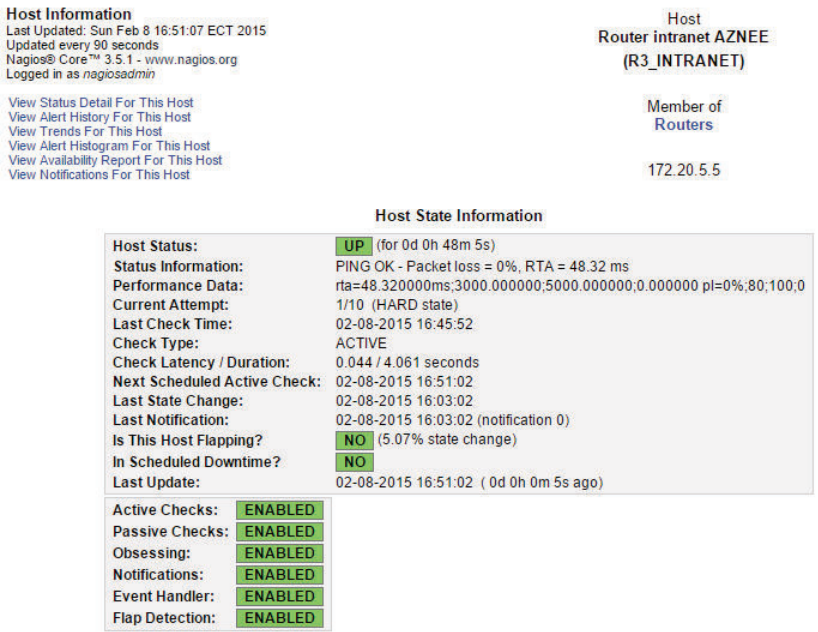



**Figura 4.43** Comprobación de servicios para el router R3_INTRANET

En la figura 4.44 se muestra el estado de los servicios del servidor Nagios.

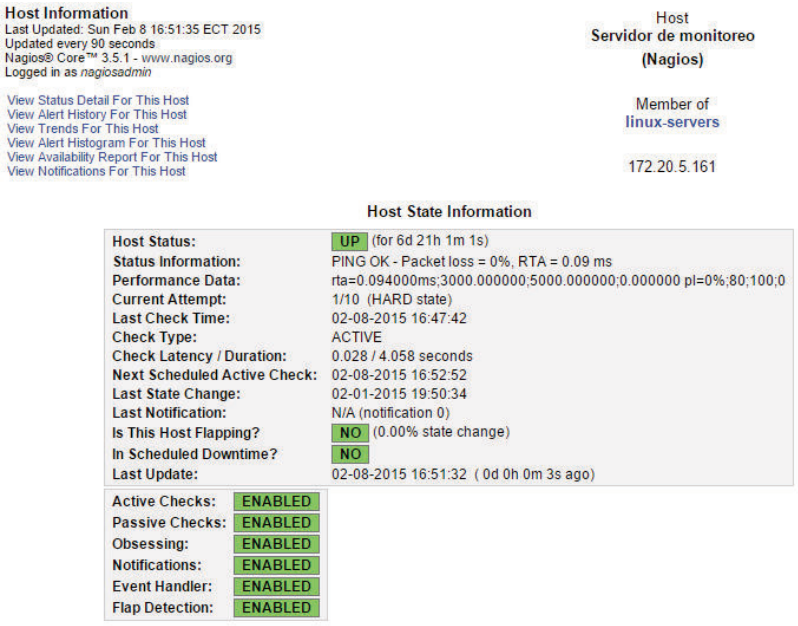



**Figura 4.44** Comprobación de servicios para el servidor Nagios

En la figura 4.45 se muestra el estado de los servicios del servidor de telefonía IP.

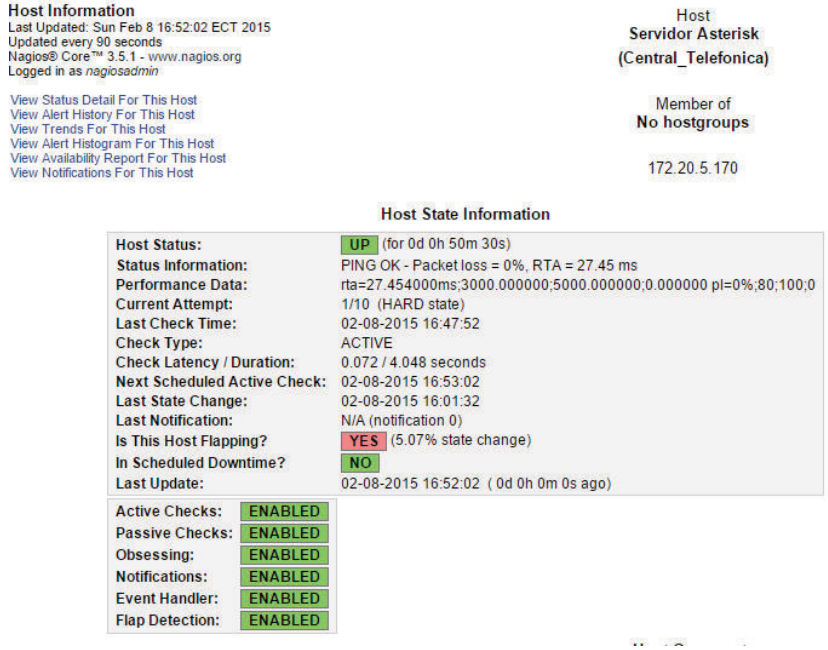



**Figura 4.45** Comprobación de servicios para el servidor de telefonía IP

En la figura 4.46 se muestra el estado de los servicios del servidor Zentyal

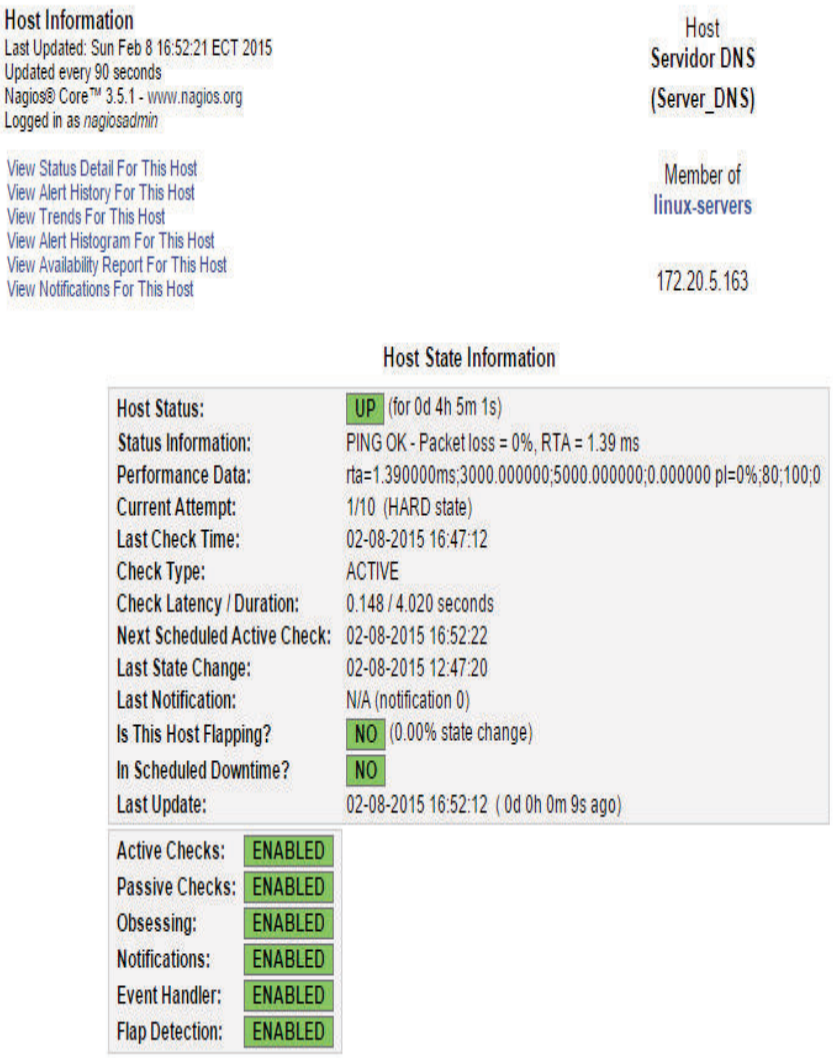



**Figura 4.46** Comprobación de servicios para el servidor Zentyal

### 4.4.6 SERVIDOR DE TELEFONÍA IP

Para comprobar este servicio se realizó la configuración de los softphone con las extensiones 1402 y 1403 bajo el protocolo SIP (Session Initiation Protocol).

En la figura 4.47 se puede observar la realización de una llamada mientras que en la figura 4.48 se muestra el establecimiento de la llamada en el servidor Asterisk.


**Figura 4.47** Realización de la llamada

```
me,i)=Diana Tupiza") in new stack
    -- Executing [s@macro-dial-one:41] Set("SIP/1402-0000001d", "CONNECTEDLINE(n
m)=1401") in new stack
    -- Executing [s@macro-dial-one:42] Set("SIP/1402-0000001d", "D_OPTIONS=TtrI"
 in new stack
    -- Executing [s@macro-dial-one:43] Macro("SIP/1402-0000001d", "dialout-one-p
redial-hook,") in new stack
    -- Executing [s@macro-dialout-one-predial-hook:1] MacroExit("SIP/1402-000000
d", "") in new stack
    -- Executing [s@macro-dial-one:44] Dial("SIP/1402-0000001d", "SIP/1401,15,Tt
rI") in new stack
  == Using SIP VIDEO TOS bits 136
  == Using SIP VIDEO CoS mark 6
  == Using SIP RTP TOS bits 184
  == Using SIP RTP CoS mark 5
       > [INSERT INTO cel (eventtype,eventtime,cid_name,cid_num,cid_ani,cid_rdni
s,cid_dnid,exten,context,channame,appname,appdata,amaflags,accountcode,uniqueid,
linkedid,peer,userdeftype,userfield) VALUES ('CHAN_START',{ts '2015-01-31 17:57:
05'},'Diana Tupiza','1401','','','','s','from-internal','SIP/1401-0000001e','','
',3,'','1422745025.30','1422745024.29','','','')]
    -- Called SIP/1401
    -- Connected line update to SIP/1402-0000001d prevented.
    -- SIP/1401-0000001e is ringing
    -- SIP/1401-0000001e is ringing
localhost*CLI> _
```

**Figura 4.48** Establecimiento de la llamada en el servidor Asterisk.

Se realizó de una llamada desde el smartphone, con la utilización de la aplicación ZOIPER. En la figura 4.49 se puede verificar la conexión.

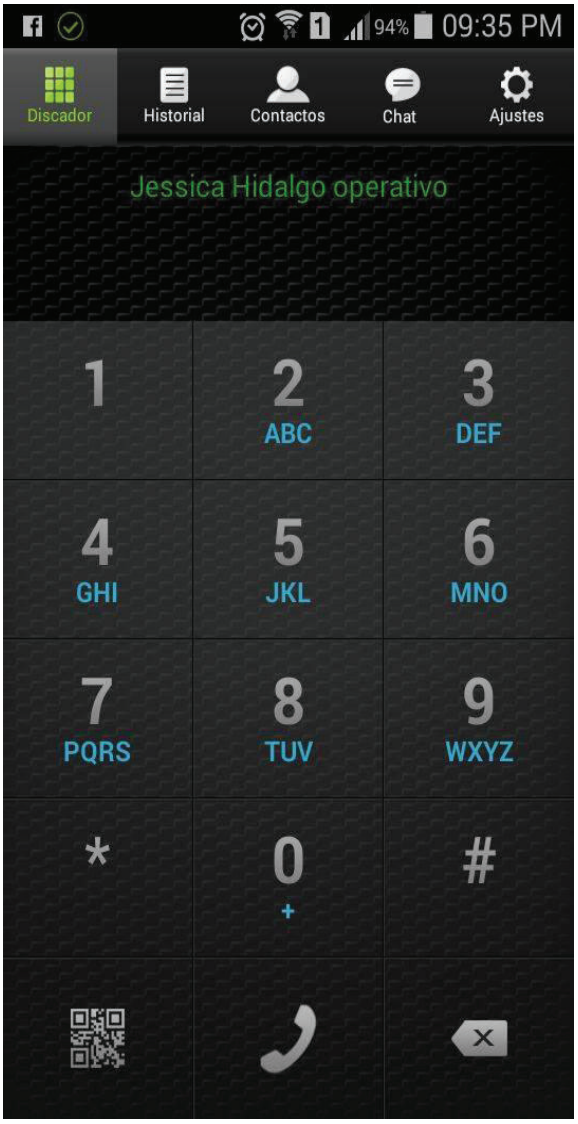



**Figura 4.49** Realización de la llamada con un smartphone

### 4.4.7 SEGURIDAD

Las configuraciones de seguridad se las realizaron a cada uno de los servidores mediante la herramienta de IPTABLES, mencionada anteriormente en donde se verificó el estado de los puertos y se procedió a utilizar la herramienta nmap[69] obteniendo los resultados de las figuras 4.50, 4.51 y 4.52:

[69] NMAP: Mapeador de Redes

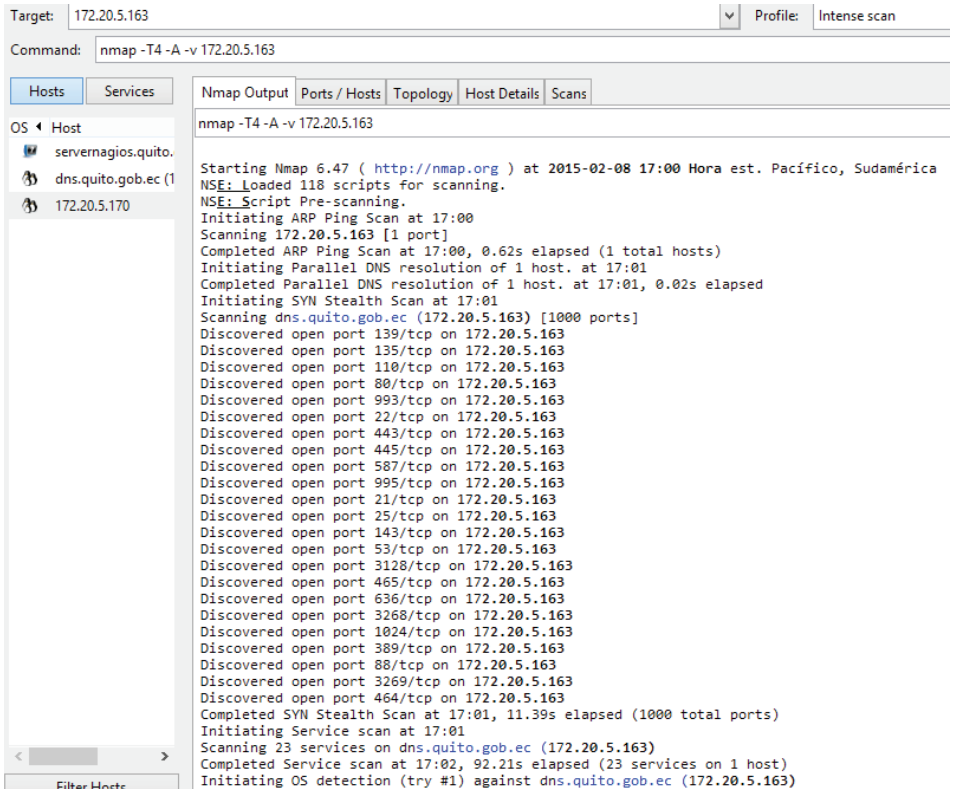



**Figura 4.50** Puertos abiertos en el Servidor Zentyal

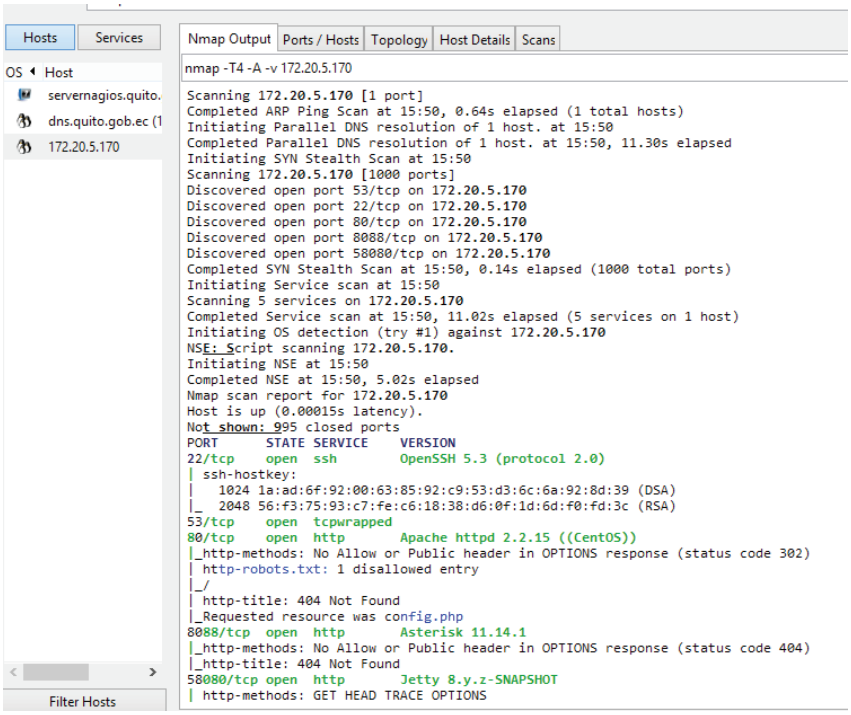



**Figura 4.51** Puertos abiertos en el Servidor Asterisk

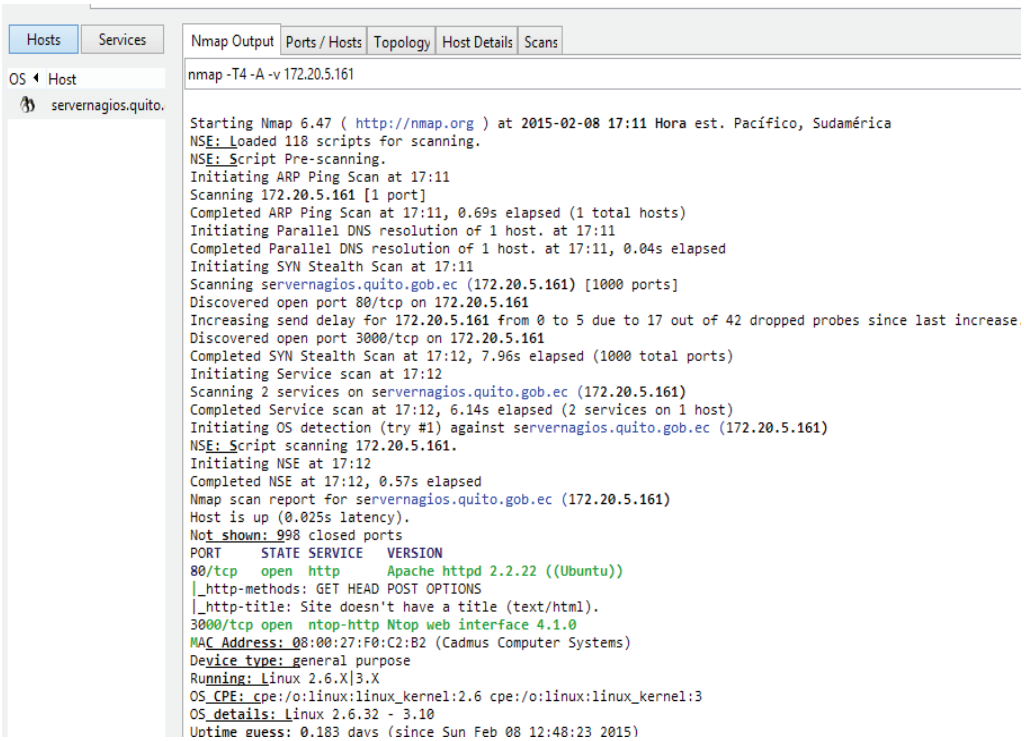



**Figura 4.52** Puertos abiertos en el Servidor de Monitoreo Nagios

### 4.4.8 PRUEBAS DE CONECTIVIDAD

Las pruebas de conectividad se realizaron a cada uno de los servidores y usuarios como se indica en el Anexo N. Para las puebas de conectividad se utilizó el protocolo ICMP como indica la figura 4. 53

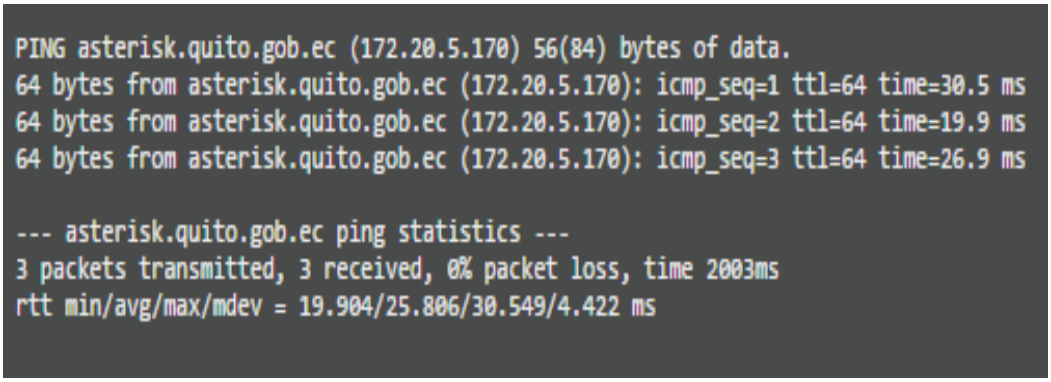



**Figura 4.53** Ping desde servidor Zentyal a Asterisk

## 4.5 ANÁLISIS DE RESULTADOS

Por medio de las pruebas realizadas al prototipo implementado se puede concluir que el rediseño planteado en el capítulo 3 para la red multiservicios cumple con todos los servicios de voz, datos y sobre todo seguridad. De estas pruebas podemos determinar lo siguiente:

- Los servidores fueron configurados para manejar el tráfico generado por los usuarios, brindando servicios de: DNS, correo, monitoreo de red y telefonía IP.
- Los servicios implementados en el servidor Zentyal cumplen un correcto funcionamiento, tanto en DNS, FTP y correo.
- El sistema de detección de intrusos forma una parte primordial en este diseño ya que permitió el análisis el tráfico que circula por la red.
- El servidor de monitoreo Nagios por medio de la configuración de SNMP, permitió gestionar la red de una manera más específica, para determinar de manera oportunidad los inconvenientes, mediante las notificaciones de alertas enviadas al correo del administrador de la red para que evalué cada situación y la resuelva de la manera más pertinente.
- La zona WIFI por falta de recursos físicos se la configuró de la manera señalada, se probó la conectividad con la red y con los servicios, sobre todo la comprobación de la telefonía IP desde un celular Smartphone.
- Mediante la herramienta de Iptables y el análisis de seguridad realizado se procedió al cierre de puertos para evitar el acceso no autorizado a nuestros servidores.

# CAPITULO V

# EVALUACIÓN ECONÓMICA DEL PROYECTO

En este capítulo se determinará la viabilidad del rediseño realizando una evaluación económica del proyecto, mediante indicadores de costo - eficiencia. Se seleccionarán los equipos adecuados según los requerimientos establecidos, las cotizaciones respectivas se encuentran en el Anexo O.

## 5.1 COSTO DE INVERSIÓN

El costo de inversión está compuesto por los costos de la red pasiva, de la red activa y los costos nominales que se detallarán los literales 5.1.1, 5.1.2 y 5.1.3.

### 5.1.1 ACTIVOS FIJOS DE LA RED PASIVA

#### 5.1.1.1 Sistema de cableado estructurado

En la tabla 5.1 se detalla el costo de los elementos del cableado estructurado en dos marcas diferentes.

**Tabla 5.1** Detalle de costos de cableado estructurado

| ELEMENTOS | CANTIDAD | PROPUESTA N° 1 LEVITON | PROPUESTA N° 2 QUEST |
|---|---|---|---|
| Cable categoría 6 tipo CMR (305m/rollo) | 30 | $ 6.954,00 | $ 5.673,00 |
| Jacks categoría 6 color negro | 380 | $ 1.755,60 | $ 1.463,00 |
| Faceplate de 1 posición | 190 | $ 256,50 | $ 218,50 |
| Patch panel de 24 puertos | 10 | $ 273,50 | $ 320,00 |
| Caja para toma 40x40mm | 190 | $ 288,80 | $ 171,00 |
| Patch cord de 1 m azul categoría 6 | 380 | $ 1.577,00 | $ 1.140,00 |
| Patch cord de 2 m blanco categoría 6 | 190 | $ 974,70 | $ 807,50 |
| Organizador horizontal 80x80 | 10 | $ 145,00 | $ 115,00 |
| Organizador vertical 80x80 | 4 | $ 189,24 | $ 160,00 |
| Multitoma horizontal de 4 tomas dobles | 4 | $ 127,76 | $ 116,80 |

| | | | |
|---|---|---|---|
| Rack de 42 UR cerrado con puerta de malla (2200X800X1000) | 2 | $ 2.156,84 | $ 1.598,00 |
| Bandeja de fibra óptica deslizable,Cassettes portafusion 12 hilos | 3 | $ 234,96 | $ 207,00 |
| Adaptadores duplex LC multimodo OM3 | 12 | $ 45,00 | $ 30,00 |
| Pigtail LC OM3 de 1 metro | 24 | $ 88,32 | $ 76,80 |
| Patch cord de F.O. LC/LC OM3 de 2m | 12 | $ 193,68 | $ 175,80 |
| Cable de fibra óptica de 6 hilos OM3 para interiores | 70 | $ 182,00 | $ 203,00 |
| Canaleta de superficie 32x12 | 94 | $ 231,24 | $ 281,06 |
| Unión 32x12 | 30 | $ 11,70 | $ 19,50 |
| Fin de canaleta 32x12 | 30 | $ 11,70 | $ 19,50 |
| Ángulo interno 32x12 | 30 | $ 15,00 | $ 21,00 |
| Ángulo externo 32x12 | 30 | $ 15,00 | $ 21,00 |
| Ángulo plano 32x12 | 30 | $ 15,00 | $ 127,50 |
| | **SUBTOTAL** | $ 8.912,54 | $ 7.069,96 |
| | **IVA 12%** | $ 1.069,50 | $ 848,40 |
| | **TOTAL** | **$ 9.982,04** | **$ 7.918,36** |

### 5.1.2 ACTIVOS FIJOS DE LA RED ACTIVA

El costo de la red activa contempla los equipos de conectividad como son: routers, switches, además de equipos terminales como teléfonos IP, servidores y el sistema de alimentación ininterrumpida UPS[70].

#### 5.1.2.1 Equipos de conectividad

En la tabla 5.2 se muestra el costo de los equipos de conectividad.

**Tabla 5.2** Costo de los equipos de conectividad

| ELEMENTOS | CANTIDAD | PROVEEDOR N° 1 | PROVEEDOR N° 2 |
|---|---|---|---|
| Switches Acceso-Cisco Catalyst 3560 Series | 10 | $ 23.500,00 | $ 13.220,00 |

[70] UPS: Uninterruptible Power Supply, Sistema de alimentación ininterrumpida

| | | | |
|---|---|---|---|
| Switches Core y distribución-Cisco 3750 Series | 6 | $ 9.396,00 | $ 10.782,00 |
| Routers Principales - CISCO 2811 | 2 | $ 2.656,00 | $ 2.238,00 |
| Router Inalámbrico - Cisco Router Wireless | 2 | $ 336,00 | $ 260,00 |
| | **SUBTOTAL** | $ 35.238,00 | $ 26.000,00 |
| | **IVA** | $ 4.228,56 | $ 3.120,00 |
| | **TOTAL** | **$ 39.466,56** | **$ 29.120,00** |

### 5.1.2.2 Equipos terminales

En la tabla 5.3 se muestra los costos de los teléfonos IP y servidores que se ajustan a los requerimientos de la AZNEE.

**Tabla 5.3** Costo de equipos terminales

| ELEMENTOS | CANTIDAD | PROPUESTA N° 1 | | PROPUESTA N° 2 | |
|---|---|---|---|---|---|
| Servidor , 16GB de RAM, 5TB de disco | 2 | $ 10.146,00 | **HP ProLiant DL380e** | $ 17.108,00 | **HP ProLiant ML350p** |
| Teléfonos IP | 40 | $ 5.796,00 | **CIS SPA303G** | $ 6.678,00 | **CIS SPA512G** |
| | **SUBTOTAL** | $ 15.742,00 | | $ 23.606,00 | |
| | **IVA** | $ 1.889,04 | | $ 2.832,72 | |
| | **TOTAL** | **$ 17.631,04** | | **$ 26.438,72** | |

Cada servidor debe contar con un sistema de alimentación ininterrumpida, mismo que permitirá tener los servicios siempre activos, logrando respaldar y administrar la información del sistema a cada instante.

### 5.1.2.3 Sistema de alimentación ininterrumpida

El propósito del sistema de alimentación ininterrumpida es proporcionar una fuente de energía que permanezca con tensión estable y continua independientemente de los cambios que puedan presentarse en la red eléctrica.

Es importante que los servidores sean apagados adecuadamente debido a que si sufren cortes de energía inesperados pueden presentarse daños en los diferentes componentes de los equipo, como por ejemplo las tarjetas de red pueden quemarse por el cambio brusco de tensión.

En la figura 5.1 se presenta el cálculo de la capacidad del UPS que debe tener el cuarto de equipos de la AZNEE.

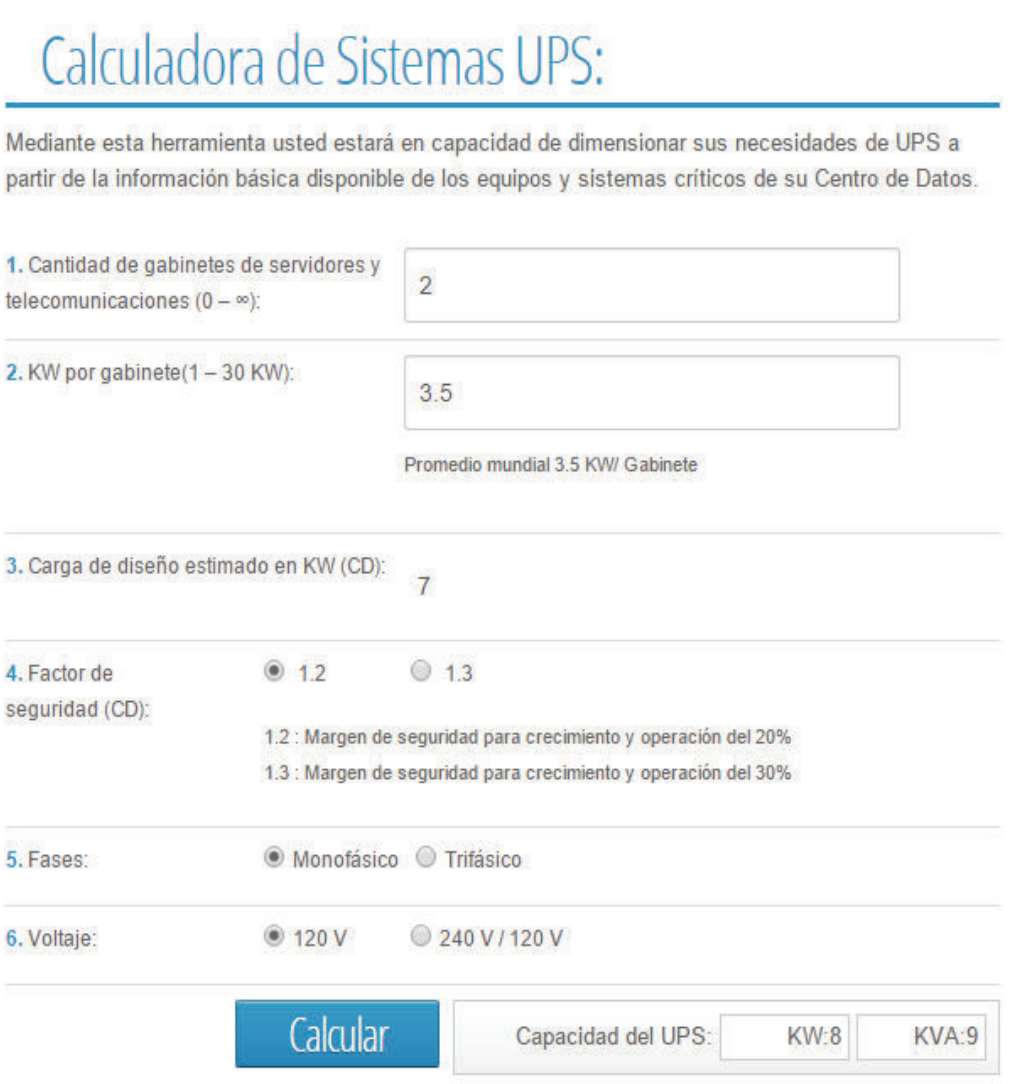



**Figura 5.1** Cálculo de capacidad de UPS para el cuarto de equipos.
Fuente http://www.datacenterconsultores.com/sistema-ups

En la tabla 5.4 se muestran los costos del sistema de alimentación ininterrumpida.

**Tabla 5.4** Costo del Sistema de alimentación ininterrumpida

| ELEMENTOS | CANTIDAD | PROPUESTA N° 1 | PROPUESTA N° 2 |
|---|---|---|---|
| UPS SUA2200 de 2.2KVA | 5 | $ 4.725,00 | $ 5.675,00 |
| Ups Netion 10 KVA On Line | 1 | $ 5.480,00 | $ 5.650,00 |
| | **SUBTOTAL** | $ 10.205,00 | $ 11.325,00 |
| | **IVA** | $ 1.224,60 | $ 1.359,00 |
| | **TOTAL** | **$ 11.429,60** | **$ 12.684,00** |

### 5.1.2.4 Servicio de internet

En la tabla 5.6 se detalla el costo de contratación del servicio, y en la tabla 5.5 se encuentran las características del servicio que ofrece cada proveedor de internet.

**Tabla 5.5** Características del servicio

| CLARO | NETLIFE |
|---|---|
| IP Dinámica | IP Dinámica |
| Conexión permanente las 24 horas. | Disponibilidad 98% |
| La compartición de estos planes es 2:1 | Compartición 2:1 |
| Navegación ilimitada | Soporte presencial 5x8 |
| Todos los planes están sujetos a facilidades técnicas y de cobertura. | Puerto 25 protegido |
| Conexión de alta velocidad con soporte técnico permanente y alta calidad de servicio. | Soporte telefónico 7x24 |

**Tabla 5.6** Costo del servicio de internet

| ELEMENTOS | PROPUESTA N° 1 CLARO | PROPUESTA N° 2 NETLIFE |
|---|---|---|
| Costo Mensual del Servicio de Internet 3 Mbps | $ 59,50 | $ 35,86 |
| **SUBTOTAL** | $ 59,50 | $ 35,86 |
| **IVA** | $ 7,14 | $ 4,30 |
| **TOTAL** | **$ 66,64** | **$ 40,16** |

### 5.1.3 COSTOS NOMINALES

#### 5.1.3.1 Configuración e instalación

Para este rediseño se necesitará realizar configuraciones a los equipos de conectividad y servidores. En la tabla 5.7 se detalla los costos para estos requerimientos.

**Tabla 5.7** Costos del servicio de configuración e instalación

| ELEMENTOS | COTIZACIÓN |
|---|---|
| Instalación de los Puntos de Red. | $ 5.050,00 |
| Certificación de los Puntos de Red. | $ 845,00 |
| Costo de Configuración de Routers y Switches | $ 650,00 |
| Costo de Configuración de Servidores | $ 650,00 |
| Costo de instalación internet | $ 100,00 |
| Costo por Retirar Cableado antiguo | $ 200,00 |
| **TOTAL** | **$ 7.495,00** |

## 5.2 COSTOS DE OPERACIÓN

Para este rediseño se necesitará realizar el mantenimiento anual de los equipos de conectividad y servidores, además se considera el pago de $700 mensuales a los encargados del área de TICs (tres personas). En la tabla 5.8 se detallan estos costos.

**Tabla 5.8** Costos de operación

| ELEMENTOS | COSTOS |
|---|---|
| Costos de mantenimiento y configuración | $ 400,00 |
| Nómina | $ 8400,00 |
| **TOTAL** | **$ 8800,00** |

## 5.3 COSTO TOTAL DEL PROYECTO

En la tabla 5.9 se presenta el costo total del proyecto, con los valores de las dos propuestas especificadas anteriormente.

**Tabla 5.9** Costo total del proyecto

| ELEMENTOS | PROPUESTA N° 1 | PROPUESTA N° 2 |
|---|---|---|
| Activos Fijos | $ 78549,41 | $ 76227,71 |
| Activos Nominales | $ 7495 | $ 7495 |
| **TOTAL** | **$ 86044,41** | **$ 83722,72** |

## 5.4 ANÁLISIS ECONÓMICO DEL PROYECTO

Para evaluar la eficiencia del proyecto se realizará la comparación del Índice Costo-Eficiencia de las dos propuestas presentadas.

A continuación, se realizará el cálculo para 5 años del costo de operación de cada propuesta para determinar los flujos de inversión que se necesitarán para este proyecto. En las tablas 5.1 y 5.11 se presentan los costos de operación.

**Tabla 5.10** Costo de operación Propuesta N° 1

| PERÍODO | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| **1. COSTOS DE OPERACIÓN** | $- 86.444,41 | **$ -8.400,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** |
| | | | | | | |
| **1.1 Costo de Inversión** | $ -86.444,41 | | $ - | $ - | $ - | $ - |
| 1.1.1 Activos Fijos | $ -78.549,41 | | $ - | $ - | $ - | $ - |
| 1.1.2 Activos Nominales | $ - 7.895,00 | | | | | |
| | | | | | | |
| **1.2 Otros Gastos** | | **$ -8.400,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** |
| 1.2.1 Mantenimiento | | | $ -400,00 | $ -400,00 | $ -400,00 | $ -400,00 |
| 1.2.2 Otros (Nómina) | | $ -8.400,00 | $ -8.400,00 | $ -8.400,00 | $ -8.400,00 | $ -8.400,00 |
| | | | | | | |
| **TOTAL COSTOS DE OPERACIÓN** | **$ -86.444,41** | **$ -8.400,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** |

**Tabla 5.11** Costo de operación Propuesta N° 2

| PERÍODO | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| **1. COSTOS DE ÓPERACIÓN** | $ -84.122,72 | **$ -8.400,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** |
| | | | | | | |
| **1.1 Costo de Inversión** | $ -84.122,72 | | $ - | $ - | $ - | $ - |
| 1.1.1 Activos Fijos | $ -76.227,72 | | $ - | $ - | $ - | $ - |
| 1.1.2 Activos Nominales | $ -7.895,00 | | | | | |
| | | | | | | |
| **1.2 Otros Gastos** | | **$ -8.400,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** |
| 1.2.1 Mantenimiento | | | $ -400,00 | $ -400,00 | $ -400,00 | $ -400,00 |
| 1.2.2 Otros (Nómina) | | $ -8.400,00 | $ -8.400,00 | $ -8.400,00 | $ -8.400,00 | $ -8.400,00 |
| | | | | | | |
| **TOTAL COSTOS DE OPERACIÓN** | **$ - 84.122,72** | **$ -8.400,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** | **$ -8.800,00** |

A continuación en la tabla 5.12 se realizará el cálculo para 5 años del valor actual neto VAN[71] para dos escenarios.

**Tabla 5.12** Cálculo del VAN

| AÑO | COSTO DE OPERACIÓN PROPUESTA N° 1 | COSTO DE OPERACIÓN PROPUESTA N° 2 | FACTOR DE DESCUENTO | FLUJO ACTUALIZADO PROPUESTA N°1 | FLUJO ACTUALIZADO PROPUESTA N°2 |
|---|---|---|---|---|---|
| **0** | -86444,41 | -84122,72 | $\frac{1}{(1+0.2)^n}$ | -86444,41 | -84122,72 |
| **1** | 8400 | 8400 | | 7000 | 7000 |
| **2** | 8800 | 8800 | | 6111,11 | 6111,11 |
| **3** | 8800 | 8800 | | 5092,59 | 5092,59 |
| **4** | 8800 | 8800 | | 4243,83 | 4243,83 |
| **5** | 8800 | 8800 | | 3536,52 | 3536,52 |
| **VAN** | | | | **-60460,36** | **-58138,67** |

Para establecer la eficiencia del proyecto se utilizó la siguiente fórmula:

$$ICE = \frac{VAC\ (Inversión\ )}{Población\ Beneficiada}$$

[71] VAN: Valor Actual Neto

**Dónde:**

**ICE:** Índice Costo Eficiencia

**VAC**: Valor Actual de Costos a Precios Social

**Población beneficiada:** 150 usuarios

En la tabla 5.13 se muestran los resultados del ICE[72] y del VAN para las dos propuestas.

**Tabla 5.13** Resultados Índice Costo Eficiencia y VAN

| | Índice Costo Eficiencia | Valor Actual Neto |
|---|---|---|
| **Propuesta N° 1** | $ 576,30 | -60460,36 |
| **Propuesta N° 2** | $ 560.81 | -58138,67 |

El análisis se realizó comparando las propuestas detalladas anteriormente, la propuesta #1 ofrece mayor garantía, además de experiencia técnica en su personal y la propuesta #2 ofrece calidad aceptable, garantía de los equipos y cuenta con personal idóneo para realizar las configuraciones que se realizarán para implementar los servicios.

Como se puede observar los índices de costo - eficiencia varían de $ 576,30 por usuario beneficiado en la primera propuesta y $ 560.81 por usuario beneficiado para la segunda propuesta.

Debe notarse que en Valor Actual Neto presenta signo negativo, debido a que en el presente proyecto no se generan ingresos, aun así, la propuesta N°2 muestra un valor más cercano a cero, por lo cual se debe elegir la propuesta mencionada.

Como se apreciar en la tabla 5.12 el ICE de la propuesta Nº2 es menor, por lo tanto, se concluye que es la más eficiente en función de costos para el presente proyecto.

[72] ICE : Índice Costo - Eficiencia

# CAPÍTULO VI

## 6.1. CONCLUSIONES

- El presente proyecto nace de la necesidad de la Administración Zonal Norte Eugenio Espejo de mejorar la infraestructura de conectividad existente, puesto que en la actualidad se encuentra trabajando con cableado categoría 5e que tiene un ancho de banda de 100 MHz, mismo que no permite brindar un servicio adecuado a los usuarios. Se plantea la migración del sistema a categoría 6, el cual posee un ancho de banda de 250 MHz, y de esta forma proporcionar una relación señal a ruido más alta, lo que da como resultado una mayor fiabilidad para las aplicaciones actuales y mayores velocidades para aplicaciones futuras. Se debe tener en cuenta que un sistema de cableado estructurado deberá tener un tiempo de vida útil mínimo de 15 años, por lo que se debe elegir una categoría que soporte las futuras aplicaciones asegurando así el retorno de la inversión.

- Para que la AZNEE se encuentre alineado con el resto de instituciones del estado, es preciso implementar un sistema de cableado estructurado apegado a la norma ANSI/TIA 568.C “Alambrado de telecomunicaciones para edificios comerciales”, esto permitirá que todas las infracciones existentes, como son: switches colocados en cascadas fuera de cuartos de telecomunicaciones, puntos de red sin identificar, rutas de cables improvisadas, entre otras se reformen y sean implementadas de acuerdo al estándar, como se lo describe en el presente proyecto. Esto dará como resultado que el tiempo de respuesta ante movimientos o cambios de los puntos de red sean de aproximadamente 10 minutos, presentando un mejoramiento en los tiempos de respuestas del 300%, ya que al momento la identificación de un punto de red tomaría alrededor de 30 minutos por la desorganización existente.
- Mediante la utilización de NTOP como herramienta de análisis de tráfico, se pudo determinar aspectos importantes como: el día pico (lunes), horas

pico (10:00-12:00) y las aplicaciones (proxy, DHCP, http) que consumen recursos en la red, corroborando así los resultados obtenidos en la encuesta realizada al personal de la institución. Con la información obtenida y la proyección del 5% de crecimiento de los usuarios de la red, se procedió al cálculo del ancho de banda que se debería contratar en el enlace de datos para brindar un servicio de excelente calidad, lo que arrojó como resultado la necesidad de incrementar el enlace a 3Mbps puesto que se encuentran trabajando al momento apenas con 1 Mbps.

- La tendencia del mercado está orientada hacia los servicios IP, es por esto, que se presenta una solución de telefonía IP basada en software libre; se eligió Asterisk por ser una central telefónica de fácil configuración la misma que permite disminuir los costos en las llamadas, manejar n números de extensiones, registrar las llamadas establecidas y su duración, establecer categorías de acceso a los servicios por ejemplo, que usuarios podrán realizar llamadas a celulares o llamadas internacionales, capturar llamadas dentro un grupo que pertenezca a un mismo departamento, etc. Otra de las ventajas de la telefonía IP radica en la movilidad, los usuarios podrán configurar su extensión en un softphone que puede ser instalado en un equipo con sistema operativo android, en este proyecto se utilizó la versión gratis de Zoiper, esto es viable gracias a que se realizó un estudio de la cobertura de la red inalámbrica, y con los cambios sugeridos se asegura que en toda la AZNEE se tendrán señal inalámbrica.

- La característica principal de una red de área local es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo. El propósito de utilizar VLAN's es agrupar usuarios con características en común y asociarlos en una subred lógica sin importar su ubicación. Cada una de estas redes virtuales serán configuradas en los switches de acceso y su información se transmitirá a través de enlaces troncales al resto de la red. Las VLAN's que se asignaron para el presente rediseño permitirán proporcionar seguridad, debido a que se configuró cierta cantidad de puertos para cada VLAN, y

controlar la administración de las direcciones IP, ya que por cada departamento se asignó un bloque de direcciones IPs, y sobre todo mejorar el rendimiento al tener una red mejor organizada, estandarizada y administrada.

- La utilización de una red de prueba o también llamada Honeynet permite emular los servicios de una red de producción y simular ataques sin presentar un riesgo para el normal funcionamiento de la red existente; se procedió a implementar la honeynet con las copias de seguridad de los servidores de la AZNEE, las cuales se obtuvieron mediante la utilización del programa Clonezilla. La determinación de las interfaces de red y las direcciones IP tanto de los honeypots como del servidor de administración deben ser colocadas adecuadamente, de lo contrario no se obtendrá el filtrado de paquetes, y por ende no se podrá determinar las instrucciones a la red de prueba.

- En la actualidad el desarrollo de las empresas se basa en el manejo de la información y en cómo protegerla de los ataques de intrusos, con este fin se utiliza el hacking ético, que es un conjunto de herramientas que permiten desde un ambiente controlado realizar ataques a los sistemas y determinar las vulnerabilidades existentes para posteriormente tomar medidas para mitigarlas. En la AZNEE se consideró necesario realizar algunas de las técnicas de hacking ético, como son: footprinting, scanning, enumeration, puertas traseras e ingeniería social, las mismas que permitieron recopilar información relevante para proponer políticas de seguridad y precautelar la integridad de la información que manejada la institución.

- Entre las principales vulnerabilidades encontradas se destacan los puertos que se encuentran innecesariamente abiertos, mismos que funcionan como un agujero en la seguridad, por ejemplo, el puerto 23/tcp que está ligado al servicio Telnet y que permite conectarse de forma remota a los servidores no encripta las contraseñas, por lo cual se convierte en un blanco fácil para

ataques por sniffing. En total se encontraron siete puertos de alto riesgo (puertos:23,80,135,3389,59000,1521,5432) y cuatro puertos de riesgo moderado (puertos:21,139,445,5555). Además se encontraron subdominios pertenecientes a www.quito.gob.ec que no son visibles para el público en general pero que se encuentran en los registros de DNS y que pueden ser explotados mediante ataques de dominio, y esto debido a que son creados para un objetivo específico y posteriormente no son borrados quedando con información que puede ser útil para los intrusos.

- Una de las técnicas más utilizadas y que pasan por desapercibidas es la de ingeniería social, la cual se aprovecha de un cargo o de afinidad de los individuos para obtener información sensible y de esta forma tener acceso a los sistemas sin la necesidad de forzar o utilizar técnicas de intrusión. Por lo que se vuelve indispensable definir una política que establezca los lineamientos con los que un funcionario proporciona información de la red a terceros, ya que será responsabilidad de cada uno precautelar la información de cada departamento de la AZNEE.

- Para análisis económico se utilizó el método costo – eficiencia, que nos permitió comparar el costo y el efecto que se tendrá con dos propuestas para el mismo proyecto. La primera ofrece una mayor garantía en la marca de los elementos del cableado estructurado, ya que es una marca reconocida a nivel. La segunda ofrece una buena calidad y garantía de los equipos, cuenta con personal idóneo para las configuraciones que se realizarán para implementar los servicios. Como se puede observar los índices de costo-efectividad varía de $ 576,30 por usuario beneficiado para la nueva red multiservicios y $ 560.81 usuario beneficiado para la segunda propuesta. Como se puede apreciar el índice costo eficiencia de la propuesta Nº2 es menor, por lo tanto, se concluye que es la más eficiente en función de los costos para el presente proyecto.

- El prototipo de la red rediseñada se basó en la utilización de máquinas virtuales y el emulador GNS3, los que permitieron crear una red virtual con

los servicios que la AZNEE utiliza; con dicho fin se utilizó software libre para emular los servicios requeridos, por ejemplo para la implementación de los servidores de correos, FTP, DNS Y DHCP se manejó el servidor Zentyal, el cual presenta una interfaz gráfica que facilitó las configuraciones. La versión gratuita es idónea para empresas con baja cantidad de usuarios, para redes con mayor número de personas se debe adquirir una licencia y de esa manera acceder a todas las funcionalidades del software.

Uno de los mayores problemas enfrentados en la implementación del prototipo fueron las limitaciones de las máquinas físicas, puesto que debieron manejar varias interfaces de red y varias máquinas virtuales, lo que sobrellevo a problemas de falta de memoria y lentitud en el procesamiento, por lo que a largo de las pruebas se debió realiza mejoras en los componentes como aumento de memorias RAM; todo esto debido a que para realizar un prototipo con equipos reales se necesitaría de una inversión considerable.

## 6.2. RECOMENDACIONES

- Una de las principales recomendaciones que se plantean es la realización de un cableado estructurado que cumpla normas internacionales, para de esta manera asegurar el correcto funcionamiento de la red de datos y prestar un servicio óptimo a los usuarios de la AZNEE.

- Se recomienda tener información actualizada de la estructura de la red, topologías, direccionamiento, información de usuarios, correos, documentación de cambios, para tener un menor tiempo de respuesta frente alguna eventualidad.

- En la parte de seguridad, mediante el análisis previo realizado, se procedió a generar un conjunto de políticas de seguridad para garantizar la seguridad de los equipos y la integridad de la información manejada por los mismos, que deberían ser implementados para proteger los equipos informáticos.

- Mantener a los equipos informáticos con las últimas actualizaciones de seguridad disponibles, logrando con ello tener un nivel elevado de protección a la información.

- Se recomienda cambiar las credenciales de acceso en periodos de 3 a 6 meses para evitar inconvenientes. Adicionalmente, se sugiere que las claves se las almacene en un gestor de contraseñas.

- Se considera necesario mantener un cronograma activo para la gestión de backups y respaldos de información, éstos pueden almacenarse en cintas magnéticas, cds o algún dispositivo electrónico de almacenamiento masivo de información.

- Monitorear los servidores constantemente para evitar cualquier pérdida de información o problemas de disponibilidad que puedan afectar el trabajo de los usuarios en la red.

- No se debe actualizar los servidores de aplicaciones a menos que sea íntegramente necesario para el buen funcionamiento de los servicios que mantiene. Se debe considerar que una actualización innecesaria podría afectar de sobremanera el buen funcionamiento de los servicios y aplicaciones disponibles.

- Se considera necesario tener un control documentado de cambios y ampliaciones que se realicen a la red, ya que en caso de no encontrarse el administrador de infraestructura, en base a la documentación, se pueda dar una solución rápida y confiable por parte de otra persona del área de informática, ante algún problema que se presente.

# REFERENCIAS BIBLIOGRÁFICAS


## LIBROS

[2] TANENBAUM, A. S. (2003). REDES DE COMPUTADORAS (Cuarta Edición ed.). México: PEARSON EDUCACIÓN,ISB 970-26-0162-2.

[6] Stallings, W. (2000). Comunicaciones y Redes de Computadoras (6ta edición ed.). PRENTICE HALL, 9.ISB 8420541109.

[15] TORI CARLOS. (2008). HACKING ÉTICO (Primera Edición ed.). ROSARIO: ISBN 978-987-05-4364-0.

## PUBLICACIONES (PAPERS, REVISTAS, ETC)

[9] Cisco Networking Academy CCNA Exploration v4.0. (2008). Conmutación y conexión inalámbrica de LAN.

[13] Programa de la Academia de Networking de Cisco CCNA 1 v3.1. (2003). Suplemento sobre el cableado estructurado. PANDUIT.

## FOLLETOS

[3] Vinueza, M., & Hidalgo, P. (2010). REDES DE ÁREA LOCAL.
[10] HIDALGO, P. (2011). Redes de Área Extendida.
[11] SINCHE, S. (2011). Redes de Área Extendida.

## PÁGINAS WEB

[1] Scrib. (s.f.). FUNDAMENTOS DE REDES. Recuperado el 11 de Marzo de 2013, de http://es.scribd.com/doc/5881631/FUNDAMENTOS-DE-REDES

[4] XIMENA, L. (12 de Marzo de 2013). CISCO PRIMER CAPITULO. Obtenido de http://laurapita.blogspot.com/2009/03/arquitectura-de-red.html

[5] Kioskea. (09 de Diciembre de 2012). TCP/IP. Recuperado el 15 de Marzo de 2013, de http://es.kioskea.net/contents/internet/tcpip.php3

[7] Llamas, J. M. (s.f.). Curso de Redes de Área Local. Recuperado el 19 de Marzo de 2013, de http://thales.cica.es/rd/Recursos/rd99/ed99-0432-01/seccion/ieee.html

[8] CISCO. (s.f.). Red LAN Inalámbrica. Recuperado el 19 de Marzo de 2013, de http://www.cisco.com/web/LA/soluciones/la/wireless_lan/index.html

[14] TIA. (2009). Evolution of estructured cabling. Recuperado el 21 de Marzo de 2013, de http://guimi.net/monograficos/G-Cableado_estructurado

**TESIS**

[1] Pinto E., “Rediseño de la red de comunicaciones de la Cooperativa de Ahorro y Crédito Mushuc Runa para manejar aplicaciones de voz y datos con calidad de servicio”, Ing. tesis, Quito, Ecuador, Marzo 2012.

[2] Barreriro C., Herrera A., “Reingeniería de la red de datos corporativo de la Administración Zonal Sur Eloy Alfaro del Municipio del Distrito Metropolitano de Quito”, Ing. tesis, Quito, Ecuador, Septiembre 2012.

[3] Jácome G., Quiroga L., “Diseño de una red multiservicios para el centro de Rehabilitación Médico N°3 y la Dirección Provincial MIES-INFA en Portoviejo”, Ing. tesis, Quito, Ecuador, Septiembre 2013.

[4] Andrango C., “Rediseño de la red multiservicios de la Dirección Provincial de Pichincha del Instituto de la Niñez y la Familia MIES-INFA”, Ing tesis, Quito, Ecuador, Abril 2014.

# ANEXOS

## ANEXO A - PROYECTO MANUAL ORGÁNICO MDMQ 2014

EL Proyecto manual orgánico MDMQ 2014 para este proyecto de titulación puede ser encontrado en el cd del proyecto.

## ANEXO B- DIAGRAMAS DE LA AZNEE ACTUALES

Los diagramas de la AZNEE utilizadas para este proyecto de titulación pueden ser encontrados en el cd del proyecto.

## ANEXO C - DIRECCIONAMIENTO IP ACTUAL

El archivo del direccionamiento IP actual de la AZNEE puede ser encontrado en el cd del proyecto.

## ANEXO D – DIRECTORIO TELEFÓNICO DE LA AZNEE

El directorio telefónico con el que cuenta la AZNNE AZNEE puede ser encontrado en el cd del proyecto.

## ANEXO E – FORMATO DE ENCUESTA

El formato de la encueta utilizada en este proyecto de titulación puede ser encontrado en el cd del proyecto.

## ANEXO F - CONFIGURACIÓN DE LA HONEYNET

Las configuraciones para la Honeynet utilizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.

## ANEXO G - CÁLCULO DE ESCALERILLA

El cálculo para las escalerillas utilizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.

## ANEXO H - MECANISMO PARA BLOQUEO DE PUERTOS

Los mecanismos para el bloqueo de puertos utilizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.

## ANEXO I - CONFIGURACIONES DE ROUTERS Y SWITCHES

Las configuraciones de routers y switches utilizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.

## ANEXO J - ARCHIVO DE CONFIGURACIÓN DE FTP

El archivo de configuración del servicio de FTP utilizado para este proyecto de titulación puede ser encontrado en el cd del proyecto.

## ANEXO K - ARCHIVO DE CONFIGURACIÓN DE NAGIOS

El archivo de configuración del servidor NAGIOS utilizado para este proyecto de titulación puede ser encontrado en el cd del proyecto.

## ANEXO L - DATASHET 3CXPhoneSystem

La hoja de datos para el softphone 3CXPhoneSystem utilizada para este proyecto de titulación puede ser encontrada en el cd del proyecto.

## ANEXO M - MANUAL DE ZOIPER

El manual de Zoiper utilizado para este proyecto de titulación puede ser encontrado en el cd del proyecto.

## ANEXO N - PRUEBAS DE CONECTIVIDAD

Las pruebas de conectividad realizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.

## ANEXO O – COTIZACIONES

Las cotizaciones utilizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.

## ANEXO P – SIGLAS

Las siglas utilizadas para este proyecto de titulación pueden ser encontradas en el cd del proyecto.