ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REINGENIERÍA DE LA RED DE DATOS CORPORATIVA DE LA ADMINISTRACIÓN ZONAL SUR ELOY ALFARO DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO

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

CHRISTIAN VINICIO BARREIRO PÉREZ
christianbarreirop@gmail.com

ANDRÉS EDWIN HERRERA VELA
and.herr@hotmail.com

DIRECTOR: ING. WILLAMS FERNANDO FLORES CIFUENTES
fflores@fie-epn.net

Quito, Septiembre 2012

DECLARACIÓN

Nosotros, **Christian Vinicio Barreiro Pérez** y **Andrés Edwin Herrera Vela** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada 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 correspondientes 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.

_____	_____
Christian Barreiro	**Andrés Herrera**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por **Christian Vinicio Barreiro Pérez** y **Andrés Edwin Herrera Vela,** bajo mi supervisión.

_____

Ing. Fernando Flores

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a todas aquellas personas que han formado parte de mi vida dándome ánimos, motivación y fuerza para enfrentar los retos como el presente.

En forma especial agradezco a mi familia, a mi padre Ángel, mi madre Elisa y mi hermana Nelly, cuyas enseñanzas y soporte han sido un pilar fundamental en todo momento.

A mi compañero de tesis Andrés, cuyo apoyo y trabajo constante han permitido la culminación del presente proyecto.

A mis tíos y tías Jorge, Olger, Silvia y Carmen, cuya guía ha sido parte esencial en el desarrollo y culminación de esta etapa universitaria.

Al Ingeniero Fernando Flores por haber guiado el presente proyecto, compartiendo su conocimiento y experiencia, con el objeto de culminarlo satisfactoriamente.

Al ingeniero Mario Veloz, la Ingeniera Elisabeth Aguirre y a los miembros de la Administración Zonal Eloy Alfaro por su apoyo y su predisposición a compartir la información necesaria para la consecución del presente proyecto.

A mis amigos que me han acompañado a lo largo de la época universitaria, existiendo siempre en ellos aquellas palabras de aliento y alegría que permitían afrontar los diferentes retos que se presentaban a lo largo de la carrera universitaria.

Christian

AGRADECIMIENTO

A todas aquellas personas que siempre han estado pendientes en este trayecto de mi vida, muchas cosas han sucedido en este periodo, pero ellos me han dado su apoyo.

A mi mami Blanca y a mi papi José, que han estado ahí empujándome para continuar a pesar de las dificultades.

A mis hermanas Cathy y Andrea, a mis sobrinas Alisson, Emily y Camila por todo el apoyo que he recibido de su parte.

A mi compañero de tesis y amigo Christian por estar siempre con esa candidez y paciencia a cada una de mis cuestiones.

A mi primo Galo por su ayuda en este proyecto con algunos datos.

A mi abuelita Custodia y a toda mi familia, tíos, tías, primos, primas, etc. por estar ahí pendientes de todo.

A mis amigos Iván, Pao, César, David, Francisco, Israel, José y todos quienes han aportado para llevar a cabo este proyecto.

Al Ing. Fernando Flores por su tiempo y disponibilidad ante nuestras cuestiones.

Al Ing. Mario Veloz, a la Ing. Elizabeth Aguirre, David del departamento de Obras Públicas y al personal de la AZEA que nos brindaron su apoyo y consejo, así como su amistad para sacar este proyecto adelante.

A todos gracias por su buena energía.

Andrés

DEDICATORIA

Dedico este trabajo a mi familia, cuyo apoyo me ha permitido enfrentar las diferentes pruebas encontradas a lo largo del camino.

A mi padre Ángel, por su continua muestra de trabajo y cariño.

A mi madre Elisa por su incansable amor y fuerza.

A mi hermana Nelly por su muestra de amor y sencillez.

Christian

DEDICATORIA

A todos quienes he tenido la suerte de conocer y me han regalado un poco de su amistad, de su alegría y candidez. Sobre todo a quienes me han contagiado con su espíritu.

A mi familia, a mi mami Blanca, a mi papi José, a mis hermanas Cathy y Andrea, a mis sobrinas Alisson, Emily y Camila, a mi primo Galo, a mi abuelita Custodia, y demás familiares.

A mis amigos y conocidos que siempre me han dado una mano en los mejores y peores momentos.

A todos ellos va dedicado este trabajo.

Andrés

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

RESUMEN

La Administración Zonal Eloy Alfaro es parte del Municipio del Distrito Metropolitano de Quito y como tal brinda sus servicios en miras de mejorar la calidad de vida de los ciudadanos sujetos a su jurisdicción. El presente proyecto se enfoca en el rediseño de la red de datos actual, sustentándose en una base teórica, un estudio de la situación actual, un análisis de requerimientos, un rediseño, un análisis de las opciones tecnológicas disponibles para la elección de la más adecuada y por último la definición de conclusiones del proyecto desarrollado.

El primer capítulo enmarca la introducción teórica a los conceptos a ser usados durante el desarrollo del proyecto. Se presentan los fundamentos de redes de voz y datos, tratando temas como: elementos de la red, normas de cableado estructurado, topologías en redes LAN, estándares de videoconferencia, telefonía IP y streaming de video entre otros.

El segundo capítulo define la situación actual en la que se encuentra la red de datos de la Administración Zonal Eloy Alfaro. Se realiza un recuento de la información pertinente a las instalaciones, equipamiento, sistema de cableado, manejo de servicios y datos de los usuarios. También se presenta un estudio del tráfico que atraviesa los enlaces de datos que permiten la comunicación de la Administración hacia el exterior, definiendo de esta manera los requerimientos para el rediseño.

El tercer capítulo presenta el rediseño de la red multi-servicios con el objeto de soportar los servicios actualmente provistos y los que deberán implementarse. En la red pasiva se definen las características de los componentes del sistema de cableado estructurado, en cuanto a los equipos de conectividad, se definirá aquellos que pueden ser reusados y las características de los equipos necesarios para el rediseño.

También se especifica el procedimiento a seguir en la transición hacia la implementación de la nueva red mediante un plan de migración que busca el minimizar el impacto sobre los servicios provistos a la comunidad. Como último punto se define un plan de contingencia que mostrará los procesos a seguirse ante posibles eventos que provoquen discontinuidad del servicio en la red actual.

El capítulo cuatro presenta los costos de la implementación tanto en la red pasiva como activa, del mismo modo se presenta un prototipo a ser implementado para corroborar la factibilidad del diseño presentado, junto a las pruebas a ser realizadas sobre el mismo y los resultados obtenidos.

PRESENTACIÓN

El Municipio del Distrito Metropolitano de Quito cumple la tarea legislativa para la aprobación de ordenanzas, resoluciones y acuerdos en el Distrito Metropolitano de Quito. El Concejo está conformado por 15 concejales cada uno encargado de diferentes comisiones. Es un órgano de gobierno que actúa como facilitador de los esfuerzos de la comunidad en la planificación, ejecución, generación, distribución y uso de los servicios que hacen posible la realización de sus aspiraciones sociales.

Con el objeto de mejorar la administración de la ciudad, el Municipio de Quito a sectorizado a la ciudad enmarcándolas bajo lo que se conoce como Administraciones Zonales, tal es el caso de la Administración Zonal Eloy Alfaro, que sirve a cerca de 650.000 habitantes.

Debido al continuo crecimiento poblacional, la Administración Zonal Eloy Alfaro busca aprovechar al máximo las nuevas alternativas que brindan las tecnologías de información y comunicación para mejorar sus procesos internos y servir a la comunidad de mejor manera.

Acorde a la necesidad de contar con el soporte para los nuevos servicios a implementarse con el transcurso del tiempo, así como con el incremento de la cantidad de funcionarios que la conforman, la Administración Zonal Eloy Alfaro debe disponer de una red multi-servicios que respalde estos procesos y permita un crecimiento continuo. Actualmente este crecimiento se veía limitado por una serie de problemas en la red de datos que incluso llevaban a la falta de continuidad en las operaciones a causa de fallas en los equipos de red.

La Administración Zonal Eloy Alfaro debe avanzar en la búsqueda e incorporación de nuevos niveles de modernización para incrementar la productividad, planificación y administración. Esto se logrará mediante la adopción de tecnologías modernas y apropiadas para mejorar su servicio a la comunidad.

De acuerdo a lo enunciado anteriormente, la Administración Zonal Eloy Alfaro debe contar con una red multi-servicios que garantice la continuidad de la conexión entre los distintos departamentos en forma segura y que permita acceder a los servicios requeridos por los mismos en forma eficaz.

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

1.1 FUNDAMENTOS DE REDES DE DATOS [PW1] [P2]

Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se han diseñado específicamente para la transmisión de información mediante el intercambio de datos.

Los avances de la tecnología permiten consolidar las redes de teléfono tradicional, radio, televisión y de datos en una única plataforma: una plataforma definida como una red convergente. El flujo de voz, vídeo y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas.

En una red convergente existen varios puntos de contacto y dispositivos pero una sola infraestructura de red común.

1.1.1 CLASIFICACIÓN DE LAS REDES

Las redes de datos se pueden clasificar de acuerdo a una gran variedad de criterios: por la tecnología de transmisión, por el medio de transmisión, por su cobertura, entre otros.

1.1.1.1 Por la tecnología de transmisión [F1]

De acuerdo a la tecnología de transmisión se tiene redes punto a punto y redes de difusión.

En las redes punto a punto, existen varias conexiones entre pares de máquinas y la información podría atravesar máquinas intermedias hasta llegar a su destino.

En las redes de difusión existe solo un medio compartido al cual están conectadas todas las máquinas, los datos son recibidos por todos quienes comparten el canal

pero puede ser procesado exclusivamente por el destinatario, este puede ser un destinatario único (*Unicast*), un grupo (*Multicast*), o pueden ser todos (*Broadcast*).

1.1.1.2 Por el medio de Transmisión [L3] [F1]

De acuerdo al medio de transmisión, existen redes por medio guiado y por medio no guiado.

Las redes por medio guiado, usan algún tipo de cable para conectar los diferentes dispositivos, estos cables pueden ser: trenzado, coaxial, fibra óptica, entre otros, mismos que permiten el transporte y la distribución de las señales.

Las redes por medio no guiado, usan para su conexión señales de radio, microondas, infrarrojo, entre otras, que permiten la comunicación de las distintas estaciones de trabajo.

1.1.1.3 Por la cobertura [L5] [F1]

De acuerdo al área de cobertura o alcance se puede tener: (Personal Area Network, *PAN), (Local Area Network, LAN),* (Metropolitan Area Network, *MAN), (Wide Area Network, WAN)* e internet.

Las redes *PAN* pueden tener un alcance de hasta 1 m. Las redes *LAN* pueden tener un alcance de 10 m a 1 Km, con la existencia de 10 a 1000 nodos. Las redes *MAN* pueden tener un alcance de 1 Km a 10 Km, con la existencia entre 100 a 1000 nodos. Las redes *WAN* pueden tener un alcance de 10 Km a 10.000 Km y la existencia de 1000 a 1 millón de nodos. Internet es la red más grande ya que tiene un alcance mundial, con más de 100 millones de nodos.

1.1.2 ARQUITECTURA DE RED [P2]

El término arquitectura de red, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados, que pueden trasladar los mensajes en toda esa infraestructura.

1.1.2.1 Características de las arquitecturas

Debido a que Internet evoluciona, al igual que las redes en general, se descubre que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

1.1.2.1.1 Tolerancia a fallas

Una red tolerante a fallas, es la que limita el impacto de una falla de software o hardware y puede recuperarse rápidamente al producirse dicha falla. Estas redes dependen de enlaces o rutas redundantes. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente y transparente para los usuarios en cada extremo.

1.1.2.1.2 Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio. Esto depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red.

1.1.2.1.3 Calidad de Servicio

Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no son necesarios para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad. Los nuevos requerimientos para admitir esta calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas de red.

1.1.2.1.4 Seguridad

Las expectativas de privacidad y seguridad que se originan del uso de redes para intercambiar información empresarial crítica y confidencial requieren ser suplidas, debido a la rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales, aumentando la necesidad de incorporar seguridad en la arquitectura de red.

1.2 REDES LAN

1.2.1 ARQUITECTURA POR CAPAS

Toda comunicación, está regida por reglas predeterminadas denominadas protocolos. Para la comunicación exitosa entre los hosts de una red se requiere de la interacción de gran cantidad de protocolos específicos para cada conversación.

Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Estos protocolos se implementan en el software y hardware de cada host y dispositivo de red.

Los protocolos se muestran como una jerarquía en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores.

1.2.2 PROTOCOLOS DE RED

Los protocolos de red son el conjunto de normas y reglas destinados a permitir la adecuada comunicación entre los dispositivos de red.

El conjunto de protocolos de red describen procesos como:

- El formato o estructura del mensaje.
- El método por el cual los dispositivos de red comparten información sobre rutas con otras redes.

- Cómo y cuándo se pasan los mensajes de error y del sistema entre dispositivos.
- El inicio y terminación de las sesiones de transferencia de datos.

Los protocolos individuales de un conjunto de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva.

1.2.3 MODELO DE REFERENCIA OSI [L3] [P3]

Inicialmente, el modelo OSI (*Open System Interconnection*) fue diseñado por la Organización Internacional para la Estandarización (*International Organization for Standardization, ISO*) con el propósito de proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos.

El modelo OSI está constituido por siete capas para proporcionar una amplia lista de funciones y servicios que pueden producirse en cada capa.

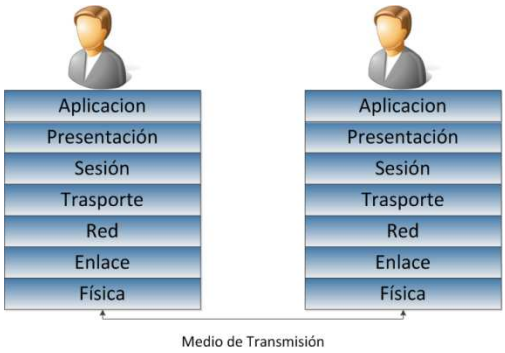


Figura 1.1 Capas Modelo OSI

1.2.3.1 Capa Física

Tiene por función la transmisión de bits a través de un canal de comunicación definiendo las características funcionales, mecánicas y eléctricas de las interfaces a usarse. Su unidad de información es el bit.

1.2.3.2 Capa Enlace

Establece un enlace lógico entre los nodos adyacentes. Sus funciones son: organización de las tramas, control de errores y control de flujo. Su unidad de información es la trama.

1.2.3.3 Capa Red

Se encarga de la entrega de paquetes desde el origen hasta el destino mediante el enrutamiento, a través de redes heterogéneas. Su unidad de información es el paquete.

1.2.3.4 Capa de Transporte

Su función básica consiste en aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasarlas a la capa de red y asegurarse de que las unidades lleguen correctamente al otro extremo, ya que es una conexión de extremo a extremo.

1.2.3.5 Capa Sesión

Permite manejar múltiples peticiones de conexiones mediante sesiones, además establece puntos de referencia en caso de interrupción y de esta manera puede continuar con transmisiones.

1.2.3.6 Capa de Presentación

Se encarga de la sintaxis y la semántica de la información transmitida con el fin de que las computadoras con diferentes presentaciones se puedan comunicar.

1.2.3.7 Capa de Aplicación [PW2]

Proporciona los medios para la conectividad extremo a extremo entre usuarios de red, además de ofrecer la interfaz entre la estación y el usuario, permitiendo la comprensión de los datos.

1.2.4 ARQUITECTURA TCP/IP

La arquitectura TCP/IP es una familia de protocolos. Define cuatro capas que deben tener lugar para que las comunicaciones sean exitosas.

1.2.4.1 Capa Host-Red

El modelo TCP/IP puntualiza que el host tiene que conectarse a la red mediante un mismo protocolo para que se puedan intercambiar paquetes IP. No define un protocolo específico.

1.2.4.2 Capa Internet

Permite que los host intercambien paquetes dentro de cualquier red y que los mismos viajen a sus destinos en forma independiente. Se define el formato del paquete y protocolo llamado IP (*Internet Protocol*).

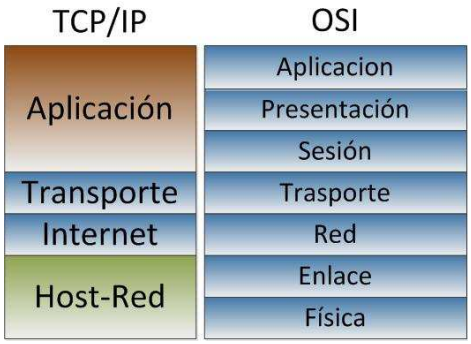


Figura 1.2 Modelo de capas

1.2.4.3 Capa Transporte

Se define para permitir que las entidades iguales tanto en el host origen como en el final puedan llevar a cabo una conversación. Se tienen dos protocolos: TCP (*Transfer Control Protocol*), que es orientado a conexión y confiable, y UDP (*User Datagram Protocol*), que es no orientado a conexión y no confiable.

1.2.4.4 Capa Aplicación

Define los protocolos que usan las aplicaciones para intercambiar información. Contiene los protocolos de nivel más alto.

1.2.5 TOPOLOGÍAS LAN [F1] [T2]

Las topologías de red cada día se han vuelto más complejas, adaptándose a las necesidades de cada organización. La topología básicamente es la forma en que los elementos de red se encuentran conectados. Las topologías más conocidas son: bus, anillo y estrella; existen otras que son combinaciones de las mencionadas anteriormente.

1.2.5.1 Topología en bus

Todos los elementos de red están conectados a un mismo medio de transmisión compartido. En este tipo de topología existe la necesidad de un mecanismo que controle el acceso al medio. Es asociado con la tecnología Ethernet.

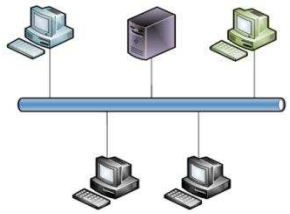


Figura 1.3 Topología en bus

1.2.5.2 Topología en anillo

Todas las máquinas pertenecientes a la red se encuentran formando un anillo de comunicación, donde cada elemento tiene contacto con el dispositivo a la derecha y a la izquierda de él. Es asociado con tecnologías *Token Ring* y *FDDI* (*Fiber Distributed Data Interface*). La implementación de éste tipo de topología es costosa, sin embargo presenta gran confiabilidad y tolerancia a fallos.

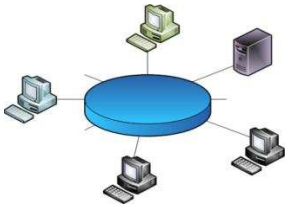


Figura 1.4 Topología en anillo

1.2.5.3 Topología estrella

Un elemento de red central recibe las conexiones de todos los elementos de red que lo rodean, de modo que todo el tráfico de red pasa a través del elemento central. Su desventaja radica en que si el elemento central falla, el resto de elementos conectados quedarán sin conectividad.

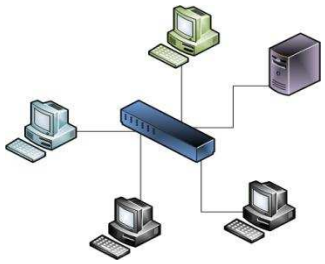


Figura 1.5 Topología estrella

1.2.6 TECNOLOGÍAS LAN

Las tecnologías LAN son métodos usados para permitir la conexión entre los elementos que conforman la red. En la actualidad la tecnología más utilizada, para implementar redes de datos, es IEEE 802.3 conocida como Ethernet.

1.2.6.1 Estándar IEEE 802.3: Ethernet [F1] [PW3] [T1] [T2] [T3]

Ethernet es una tecnología LAN que fue estandarizada por la IEEE (*Institute of Electrical and Electronics Engineers*), bajo el grupo de trabajo IEEE 802.3. Se basa en el método de acceso CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Desde sus inicios fue desarrollada con el propósito de evitar las colisiones que se presentan en un medio de transmisión compartido.

El estándar IEEE 802.3 ha tenido un desarrollo continuo, definiendo diferentes capas físicas lo que le permite tener flexibilidad con respecto a la velocidad de transmisión, dependiendo del medio de físico y el tipo de transmisión que puede ser banda base o banda ancha. En la figura 1.6 se puede apreciar los parámetros para identificar los estándares de IEEE 802.3.

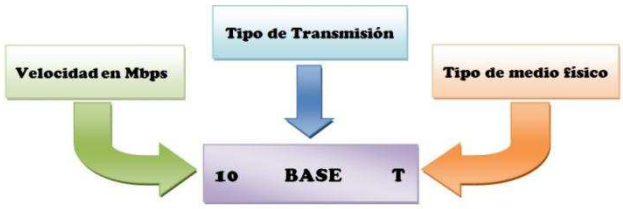


Figura 1.6 Parámetros para identificadores de capa física en IEEE 802.3

CSMA/CD es el mecanismo utilizado en IEEE 802.3 para evitar que existan colisiones en la red y así aumentar el rendimiento de la misma.

Su funcionamiento se da al momento que una máquina quiere transmitir, para ello escucha el medio, si está libre entonces envía la información, pero si se encuentra ocupado la estación seguirá escuchando hasta que el medio se libere, para poder transmitir.

Si el canal está libre y dos estaciones envían información al mismo tiempo se producirá una colisión, las máquinas involucradas emitirán una señal de *jamming* para indicar al resto de estaciones que ha ocurrido una colisión.

Después de la colisión las estaciones involucradas esperan un tiempo aleatorio para intentar volver a trasmitir por el medio compartido.

A pesar de los mecanismos de acceso al medio y las altas velocidades de transmisión que se fueron desarrollando, el compartir un mismo medio no permitía incrementar el rendimiento en las redes de área local, por lo cual se optó por implementar un esquema de conmutación, y de esta forma eliminar las colisiones, así también la información que se envía solo se dirige al destinatario y no a todas las estaciones que comparten el medio.

Se han definido varios estándares por parte del grupo de trabajo de la IEEE 802.3, en la actualidad varios de ellos han sido utilizados a nivel comercial por la velocidad de transmisión que ofrecen y la compatibilidad que existe entre los mismos. En la tabla 1.1 se muestra las características de los estándares IEEE 802.3 que se utilizan mayormente a nivel empresarial y/o comercial.

Estándar	Descripción	Distancia máxima [m]	Medio de transmisión
802.3i	10 Base-T (Ethernet)	100	UTP cat 3, cat 5, cat 5e
802.3u	100 Base-T (Fast Ethernet)	100	STP o UTP cat 5, cat 5e
802.3ab	1000 Base-T (Gigabit Ethernet)	100	UTP cat 6, cat 6a
802.3z	1000 Base-X (Gigabit Ethernet)	25 275 – 550 550 – 5000	STP F.O. Multimodo F.O. Monomodo

Tabla 1.1 Algunos estándares IEEE 802.3 en redes LAN

1.2.6.2 VLAN [P3] [PW4]

Una VLAN es una red LAN virtual que permite agrupar en segmentos varios dispositivos de redes conmutadas, de forma lógica, permitiéndoles actuar de manera independiente dentro de la misma red física.

El propósito de la segmentación de la red es incrementar el rendimiento de la misma, también permite la implementación de políticas de acceso y seguridad para grupos particulares de usuarios, además se usa para estructurar geográficamente la red.

1.2.6.2.1 Tipo de VLAN [PW5]

Se han definido diversos tipos de VLAN, según criterios de conmutación y de acuerdo al nivel en el que se lleve a cabo:

- VLAN de nivel 1: Define una red virtual según los puertos de conexión del conmutador. También se la denomina VLAN basada en puerto.
- VLAN de nivel 2: Define una red virtual según las direcciones MAC de las máquinas. También se la denomina VLAN basada en la dirección MAC.
- VLAN de nivel 3: Existen dos tipos de VLAN de nivel 3.
    - VLAN basada en la dirección de red: Esta conecta subredes según la dirección IP de origen de la información.

- VLAN basada en protocolo: Permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Porque se pueden agrupar todos los equipos que utilizan el mismo protocolo.

1.3 REDES WLAN

1.3.1 FUNDAMENTOS DE REDES INALÁMBRICAS [PW6] [P3]

Una red de área local inalámbrica o WLAN (*Wireless Local Area Network*) utiliza ondas electromagnéticas para enlazar los equipos conectados a la red, en lugar de medios físicos como cables.

Característica	LAN inalámbrica 802.11	Redes LAN Ethernet 802.3
Capa física	Radiofrecuencia (RF)	Cable
Acceso de medios	Prevención de colisión	Detección de colisiones
Disponibilidad	Cualquiera con una radio NIC en el rango de un punto de acceso	Se requiere conexión por cable
Interferencia en la señal	Sí	Irrelevante
Regulación	Regulación adicional a cargo de las autoridades locales	El estándar IEEE dictamina

Tabla 1.2 Comparación entre LAN y WLAN [P2]

Una WLAN proporciona al usuario gran movilidad sin perder conectividad. Es de fácil instalación y permite el ahorro por la supresión del medio de transmisión cableado. Aun así sus prestaciones son menores en lo referente a la velocidad de transmisión. En las redes WLAN, los dispositivos clientes se conectan a un Access Point.

1.3.2 ESTÁNDARES DE LAS WLAN

Las redes LAN inalámbricas 802.11 pertenecen a un estándar de la IEEE que define cómo se utiliza la radiofrecuencia en las bandas sin licencia de frecuencia médica, científica e industrial para la capa física y la subcapa MAC de enlaces inalámbricos.

Las tasas de datos de los diferentes estándares de LAN inalámbrica están afectadas por la técnica de modulación. Las dos técnicas de modulación más usadas son: Espectro de dispersión de secuencia directa (DSSS) y Multiplexación

por división de frecuencias ortogonales (OFDM). Cuando un estándar utilice OFDM, tendrá tasas de datos más veloces. Además, el DSSS es más simple que el OFDM, de modo que su implementación es más económica.

1.3.2.1 Estándar IEEE 802.11a

El IEEE 802.11a adoptó la técnica de modulación OFDM y utiliza la banda de 5 GHz. Los dispositivos 802.11a tienen menos probabilidades de interferencia que los dispositivos que operan en la banda de 2.4 GHz porque existen menos dispositivos comerciales que utilizan la banda de 5 GHz. Además, las frecuencias más altas permiten la utilización de antenas más pequeñas.

Existen algunas desventajas importantes al utilizar la banda de 5 GHz. La primera es que, a frecuencia de radio más alta, mayor es el índice de absorción por parte de obstáculos como paredes, y esto ocasiona un rendimiento pobre del 802.11a. El segundo es que esta banda de frecuencia alta tiene un rango más acotado que el 802.11b o el 802.11g.

1.3.2.2 Estándar IEEE 802.11b y Estándar IEEE 802.11g

El estándar IEEE 802.11b especificó las tasas de datos de 1; 2; 5.5 y 11 Mb/s en la banda de 2.4 GHz ISM (*Industrial, Scientific and Medical*) que utiliza DSSS (*Direct-Sequence Spread Spectrum*).

El estándar IEEE 802.11b especificó las tasas de datos superiores en esa banda mediante la técnica de modulación OFDM. IEEE 802.11g también especifica la utilización de DSSS para la compatibilidad retrospectiva de los sistemas IEEE 802.11b. El DSSS admite tasas de datos de 1; 2; 5.5 y 11 Mb/s, como también las tasas de datos OFDM de 6; 9; 12; 18; 24; 48 y 54 Mb/s.

Los dispositivos en la banda de 2.4 GHz tendrán mejor alcance que aquellos en la banda de 5 GHz. Además, las transmisiones en esta banda no se obstruyen fácilmente como en 802.11a.

Hay una desventaja importante al utilizar la banda de 2.4 GHz. Muchos dispositivos de clientes también utilizan la banda de 2.4 GHz y provocan que los dispositivos 802.11b y g tiendan a tener interferencia.

1.3.2.3 Estándar IEEE802.11n

El estándar IEEE 802.11n fue pensado para mejorar las tasas de datos y el alcance de la WLAN sin requerir energía adicional o asignación de la banda RF. 802.11n utiliza la tecnología de entrada múltiple/salida múltiple (MIMO), divide un stream rápido de tasa de datos en múltiples streams de menor tasa y los transmite simultáneamente por las radios y antenas disponibles. Esto permite una tasa de datos teórica máxima de 248 Mb/s por medio de dos streams.

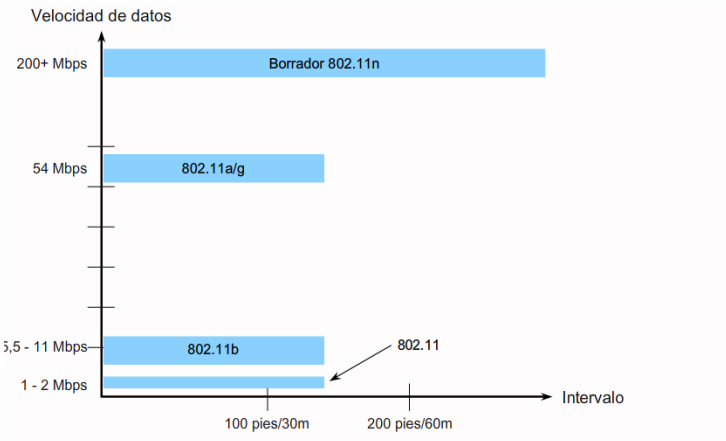


Figura 1.7 Estándares de WLANs [P3]

1.4 REDES WAN [F2] [T1]

La necesidad de conectar redes LAN alejadas geográficamente, que permitan a sus usuarios interactuar, permite el surgimiento de las redes WAN. Este tipo de redes ayuda a organizaciones a interconectarse por medio de un canal de telecomunicaciones, sea éste alquilado o implementado por las mismas empresas, haciendo posible la compartición de información.

1.4.1 TECNOLOGÍAS WAN

Las tecnologías WAN permiten realizar la conmutación en los nodos, por los que tiene que a travesar la información, antes de llegar a su destino. Ésta conmutación puede ser mediante las técnicas de circuitos, mensajes o paquetes.

Conmutación de circuitos: Tiene tres fases para cumplir su objetivo, establecimiento de la comunicación, transmisión de los datos y terminación de la comunicación. Este tipo de conmutación necesita de un enlace dedicado entre los extremos. Usado mayormente en telefonía.

Conmutación de mensajes: Fue establecida para mejorar la conmutación de circuitos, sin embargo los nodos intermedios para este caso necesitan tener mejores características de hardware para recibir y almacenar los mensajes, y luego reenviarlos a su destino.

Conmutación de paquetes: La información es dividida en paquetes variables o de igual tamaño y luego enviados a través de la red, cada uno encaminado de forma independiente. Este tipo de conmutación es el más utilizado en redes WAN, pudiéndose implementar con Frame Relay, ATM, MPLS entre otros.

1.4.2 FRAME RELAY

Frame Relay trabaja en la capa de enlace de datos del modelo ISO/OSI, mediante un conjunto de protocolos. Esta tecnología permite conmutaciones orientadas a conexión a través de una red pública, usando circuitos virtuales. Los circuitos virtuales pueden ser permanentes PVC *(Permanent Virtual Circuit*) o conmutados SVC *(Switched Virtual Circuit*).

1.4.3 ATM, *ASYNCHRONOUS TRANSFER MODE*

ATM es una tecnología orientada a conexión. Tiene una transferencia de información no sincrónica, estableciendo para aquel propósito paquetes, denominados celdas, de longitud fija que puedan ser enrutados de manera individual, y que permitan la transmisión de cualquier tipo de información. ATM trabaja con conexiones virtuales definiendo a VC (*Virtual Channel*) y VP (*Virtual Path*). Un VP es un camino entre dos routers *ATM* y puede contener varios VC, quienes a su vez establecen los enlaces para la transmisión de datos.

1.4.4 MPLS, *MULTIPROTOCOL LABEL SWITCHING* [F3]

MPLS trabaja entre la capa de enlace de datos y la capa de red del modelo ISO/OSI, mediante una etiqueta añadida antes del encabezado IP. Mejora la transferencia de información haciendo que la conmutación sea más rápida, añade calidad de servicio permitiendo una clasificación más simple para determinar el siguiente salto, ingeniería de tráfico para optimizar el balanceo de carga en la red, VPNs (*Virtual Private Network*) que ayudan con el establecimiento de túneles seguros. Además tiene soporte multi-protocolos.

1.5FUNDAMENTOS DE CABLEADO ESTRUCTURADO [PW7]

Los sistemas de cableado en las redes de información actuales deben permitir la interconexión de los distintos equipos tomando en cuenta su heterogeneidad y deben contemplar la integración de los diferentes servicios que hacen uso de la red para cubrir las necesidades de los usuarios durante la vida útil del edificio sin necesidad de realizar más tendido de cables.

El cableado estructurado es un método para crear un sistema de cableado organizado que permita la comprensión por parte de los instaladores, los administradores de la red y en general por cualquier persona que esté encargado de la manipulación del sistema de cableado.

Los sistemas de cableado estructurado se instalan de acuerdo a normas para cableado definidas en estándares, los cuales definen a su vez características de los cables, los elementos que serán usados para la interconexión, la administración y comprobación del cableado entre otros, con miras a implementar un cableado de calidad.

1.5.1 ESTÁNDARES DE CABLEADO ESTRUCTURADO [P1] [PW8]

La mayoría de los estándares en la industria de telecomunicaciones son voluntarios y basados en consensos. Las dos principales organizaciones que desarrollan estándares para esta industria son la IEEE que se enfoca en las

aplicaciones Ethernet y la TIA (*Telecommunications Industry Association*), que se enfoca en la red pasiva para soportar las aplicaciones como Ethernet.

La TIA se encuentra acreditada por la ANSI (*American National Standards Institute*) para desarrollar estándares de la industria para una gran variedad de productos de telecomunicaciones.

Los estándares son documentos que deben ser constantemente revisados para reflejar las necesidades del mercado emergente. La ANSI define un máximo de 5 años de vida para los estándares, después de los cuales deben ser revisados y posteriormente reafirmados o retirados. A continuación se encuentran listados los estándares comúnmente utilizados en la industria.

- TIA/EIA-568-C: El estándar de cableado para edificios comerciales brinda a los usuarios y diseñadores de red más soluciones compatibles con las normas: se incluyen nuevas opciones de medios de comunicación junto con su adecuada instalación y los procedimientos de prueba. Sin embargo, además de las actualizaciones técnicas, 568-C refleja una nueva estructura organizativa que se ha diseñado para simplificar y agilizar los procesos de las futuras normas de reducción de información duplicada, y el establecimiento de una base común para los futuros documentos. También admite un entorno de múltiples proveedores y productos.
    - TIA/EIA-568-C.0: Cableado de Telecomunicaciones genérico para instalaciones de cliente. Se especifican los requerimientos mínimos para el cableado genéricos de telecomunicaciones tales como la arquitectura de cables, que aplicaciones debe soportar el cableado, que distancias y otros requerimientos en general incluyendo la estructura de los sistemas de cableado, topologías, instalación, rendimiento y pruebas.
    - TIA/EIA-568-C.1: Estándar de cableado de telecomunicaciones para edificios comerciales. Se especifican los requerimientos para el cableado de telecomunicaciones dentro y entre edificios comerciales (orientados a oficinas). Este estándar define términos, requerimientos de cableado, distancias, terminales de

telecomunicaciones, configuraciones de los conectores, topologías físicas entre otros.

- TIA/EIA-568-C.2: Estándar de componentes de cableado de cobre. Especifica los requerimientos mínimos para varios componentes, modelos de rendimiento de transmisión y procedimientos de medida requeridos para la verificación del cableado de par trenzado de cobre. Este estándar también define los instrumentos de medición de campo, incluyendo procesos de medición de referencia para todos los parámetros definidos dentro del mismo. Los sistemas de cableado de 4 pares y el cableado balanceado multipar están cubiertos dentro de este estándar.
- TIA/EIA-568-C.3: Estándar de componentes del cableado de Fibra Óptica. Especifica los requerimientos de rendimiento mínimos para los componentes de un sistema de cableado de fibra óptica, definido para su uso por los fabricantes. Presenta una lista de definiciones, abreviaciones, acrónimos, y unidades de medida.
- TIA/EIA-568-C.4: Estándar de Componentes de sistemas de cable coaxial de banda ancha. Especifica los requerimientos de rendimiento mínimos para componentes de sistemas de cableado de banda ancha de 75-Ohm, incluyendo la transmisión, mecánica, y los requerimientos de compatibilidad. Incluye los procedimientos de instalación y los terminales de conexión así como los procedimientos de las pruebas de campo.

- TIA/EIA-569-C: Este estándar define los recorridos, el espacio y las prácticas de construcción para el soporte de los medios de comunicación y equipos dentro de los edificios. Se incluye los recorridos de accesos al servicio inalámbrico, cuartos de ingreso, recorridos en edificios, cuartos de distribución, espacios de acceso y provisión de servicios, recorridos de entradas de servicios y ubicación de los equipos.
- TIA/EIA-606-B: Estándar de administración para la Infraestructura de telecomunicaciones, especifica cuatro clases de administración basadas en la complejidad del sistema de cableado que se está siendo administrado.

Se incluye la asignación de identificadores a los componentes de la infraestructura, especificación de los elementos de información que conforman los registros para cada identificador, especificación de las relaciones entre los registros para acceder a la información contenida, especificación de reportes presentando la información de grupos de registros y la especificación de los requisitos gráficos y simbólicos.

- TIA/EIA-607-B: Los estándares sobre requisitos de conexión a tierra y conexión de telecomunicaciones para edificios comerciales. Este estándar provee los principios básicos, componentes y diseños de las uniones y puestas a tierra de telecomunicaciones que deben ser seguidas para asegurar que los sistemas de puesta a tierra dentro del edificio tengan un potencial eléctrico.

1.5.1.1 Subsistemas del Cableado Estructurado [P1] [T1]

Hay siete subsistemas relacionados con el sistema de cableado estructurado, cada subsistema realiza funciones determinadas para proveer servicios de datos y voz en toda la planta de cables:

- Punto de demarcación: Es el punto en el que el cableado externo del proveedor de servicios se conecta con el cableado *backbone* dentro del edificio. Representa el límite entre la responsabilidad del proveedor de servicios y la responsabilidad del cliente.
- Sala de equipamiento: Es el centro de la red de voz y datos. La sala de equipamiento es esencialmente una gran sala de telecomunicaciones que puede albergar el marco de distribución, servidores de red, routers, switches, PBX telefónico, protección secundaria de voltaje, receptores satelitales, moduladores y equipos de Internet de alta velocidad, entre otros.
- Sala de telecomunicaciones: Albergan el equipo del sistema de cableado de telecomunicaciones para un área particular de la LAN. Esto incluye las terminaciones mecánicas y dispositivos de conexión cruzada para sistemas de cableado *backbone* y horizontal.

- Cableado *backbone*, también conocido como cableado vertical: Cableado que interconecta a la sala de equipamiento, sala de telecomunicaciones y entradas de servicios.
- Cableado de distribución, también conocido como cableado horizontal: Cableado que se extiende desde el closet de telecomunicaciones hasta el área de trabajo LAN.
- Área de trabajo: Es el área a la que una sala de comunicaciones en particular presta servicios. Un área de trabajo por lo general ocupa un piso o una parte de un piso de un edificio.
- Administración: Los dispositivos de administración de cables son utilizados para tender cables a lo largo de un trayecto ordenado e impecable y para garantizar que se mantenga un radio mínimo de acodamiento. La administración de cables también simplifica el agregado de cables y las modificaciones al sistema de cableado.

1.5.1.2 Categorías de Cable [PW9] [T2]

El cable de par trenzado es actualmente el tipo de cable más común en redes de área local y se originó como solución para conectar redes de comunicaciones reutilizando el cableado existente de redes telefónicas. Cada cable de este tipo está compuesto por una serie de pares de cables trenzados. Los pares se trenzan para reducir la diafonía (interferencia o *crosstalk* entre pares adyacentes).

Categoría	Ancho de Banda (Velocidad)
Cat 3	16 MHz (10 Mbps)
Cat 4	20 MHz (16 Mbps)
Cat 5	100 MHz (100 Mbps)
Cat 5e	100 MHz, puede llegar a 125 MHz (250Mbps)
Cat 6	250 MHz (600 Mbps)
Cat 7	600 MHz

Tabla 1.3 Categorías de cable UTP

Las normativas de cableado estructurado clasifican los diferentes tipos de cable de pares trenzados en categorías de acuerdo con sus características para la transmisión de datos, las cuales vienen fijadas fundamentalmente por la densidad de trenzado del cable (número de vueltas por metro) y los materiales utilizados en

el recubrimiento aislante. La característica principal de un cable desde el punto de vista de transmisión de datos es su atenuación.

1.6 EQUIPOS DE CONECTIVIDAD

1.6.1 HUB

En un hub, los datos que llegan a uno de sus puertos, se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos. Los dispositivos conectados al hub reciben todo el tráfico que se transporta a través del mismo. Cuántos más dispositivos están conectados al hub, mayores son las probabilidades de que existan colisiones.

Los hubs por lo general se utilizaban en las redes Ethernet 10BASE-T o 100BASE-T, aunque hay otras arquitecturas de red que también los utilizan.

1.6.2 SWITCH

Los switches aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red y utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están enviando de un computador a otro de la red.

En la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos que es el procedimiento mediante el cual una trama se recibe en un medio de entrada y luego se transmite a un medio de salida. El segundo es el mantenimiento de operaciones de conmutación cuando los switches crean y mantienen tablas de conmutación y buscan lazos.

Los switches operan a velocidades mucho más altas que los hubs y pueden admitir nuevas funcionalidades como, por ejemplo, las LAN virtuales.

1.6.3 ROUTER

Los routers son los responsables de encaminarlos paquetes de datos desde su origen hasta su destino en la red LAN, y de proveer conectividad a la WAN. Dentro de un entorno de LAN, brinda servicios locales de resolución de direcciones, tal como ARP, y puede segmentar la red utilizando una estructura de subred. Para brindar estos servicios, el router debe conectarse a la LAN y a la WAN.

1.6.4 FIREWALL [PW10]

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. En general un firewall dispone de o más interfaces de red en la que se establecen reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT (*Network Address Translation*).

1.7 MODELO CLIENTE SERVIDOR [P2]

Un cliente comienza el intercambio de información solicitando los datos requeridos al servidor, que responde enviando uno o más flujos de datos al cliente. Los protocolos de capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio puede requerir de información adicional, como la autenticación del usuario y la identificación de un archivo de datos a transferir.

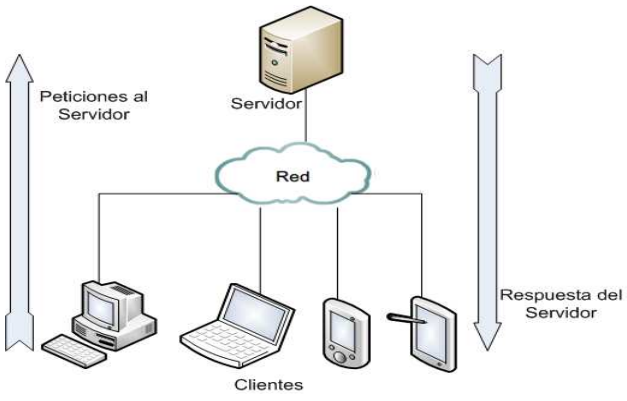


Figura 1.8 Modelo Cliente Servidor

Los servidores generalmente tienen múltiples clientes que solicitan información al mismo tiempo. Estas solicitudes individuales del cliente pueden manejarse en forma simultánea y separada para que la red sea exitosa.

1.8 SERVICIOS EN LA INTRANET

1.8.1 DNS, *DOMAIN NAME SERVER* [PW11]

1.8.1.1 Definición

Domain Name System o DNS es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir o resolver nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS.
- Los Servidores DNS: Contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
- Zonas de autoridad: Son porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio

y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

1.8.1.2 Tipos de Servidores DNS

Se definen tres tipos de servidores básicos:

1.8.1.2.1 Servidores Maestros

Son autorizados para un dominio, pueden iniciar transferencias de zona a servidores de nombre esclavos, brinda servicio a todas las peticiones cliente y permite realizar búsquedas en caché para otros dominios.

1.8.1.2.2 Servidores Esclavos

También son autorizados para un dominio, recuperan información de un servidor maestro mediante una transferencia de zona, sirve a todas las peticiones cliente y permite realizar búsquedas en caché para otros dominios.

1.8.1.2.3Servidores Caché

No tienen información para un dominio, sirven a todas las peticiones cliente y permiten realizar búsquedas en caché para todos los dominios (pero no son autorizados).

1.8.1.3 Consultas DNS [PW12]

Cuando un servidor DNS recibe una consulta, primero comprueba si puede responder la consulta con autoridad en función de la información de registro de recursos contenida en una zona configurada localmente en el servidor. Si el nombre consultado coincide con un registro de recursos correspondiente en la información de zona local, el servidor responde con autoridad y usa esta información para resolver el nombre consultado.

Si no existe ninguna información de zona para el nombre consultado, a continuación el servidor comprueba si puede resolver el nombre mediante la

información almacenada en la caché local de consultas anteriores. Si aquí se encuentra una coincidencia, el servidor responde con esta información. De nuevo, si el servidor preferido puede responder al cliente solicitante con una respuesta coincidente de su caché, finaliza la consulta.

Si el nombre consultado no encuentra una respuesta coincidente en su servidor preferido, ya sea en su caché o en su información de zona, el proceso de consulta puede continuar y se usa la recursividad para resolver completamente el nombre. Esto implica la asistencia de otros servidores DNS para ayudar a resolver el nombre.

1.8.1.4 Aplicaciones DNS

1.8.1.4.1 Bind, Berkeley Internet Name Domain [PW13] [PW14]

El nombre BIND proviene de "Berkeley Internet Name Domain", ya que el software se originó en la década de 1980 en la Universidad de California en Berkeley.

BIND es el software DNS más usado en Internet. Proporciona una plataforma sólida y estable, sobre la cual las organizaciones pueden crear sistemas distribuidos de computación, sabiendo que esos sistemas son totalmente compatibles con las normas publicadas DNS. La distribución de software BIND contiene tres partes:

- Un servidor de nombres de dominios: Este es un programa llamado "*named*", y significa "demonio de nombre". Responde a las preguntas que se envían a la misma, siguiendo las normas especificadas en el protocolo DNS.
- Un Sistema de Nombres de Dominio: Es una colección de componentes de software que un programador puede añadir, lo que dará al software mayor capacidad de resolver los nombres.
- Herramientas de software para servidores de pruebas: Estas son las herramientas que se usan para realizar pruebas y comprobar que la configuración del servidor es correcta.

1.8.2 DHCP, *DYNAMIC HOST CONFIGURATION PROTOCOL* [P4]

1.8.2.1 Definición

DHCP asigna direcciones IP y otra información de configuración de la red de manera dinámica. Como los clientes de escritorio por lo general conforman la mayoría de los nodos de red, DHCP es una herramienta muy útil puesto que ahorra tiempo a los administradores de red.

1.8.2.2 Funcionamiento de DHCP

La asignación de direcciones IP a los clientes es la tarea más fundamental que realiza un servidor de DHCP. Incluye tres mecanismos diferentes para la asignación de direcciones a fin de proporcionar flexibilidad al momento de establecer direcciones IP:

- Asignación manual: El administrador establece una dirección IP asignada previamente al cliente y DHCP sólo comunica la dirección IP al dispositivo.
- Asignación automática: DHCP asigna automáticamente una dirección IP estática permanente a un dispositivo; la dirección es seleccionada de un conjunto de direcciones disponibles. No hay arrendamiento y la dirección se asigna permanentemente al dispositivo.
- Asignación dinámica: DHCP asigna automáticamente una dirección IP dinámica, o arrendada, tomada de un grupo de direcciones IP por un período limitado seleccionado por el servidor o hasta que el cliente informe al servidor de DHCP que ya no necesita la dirección.

1.8.2.3 Aplicaciones DHCP

La mayoría de las distribuciones en Linux usan el servidor DHCP del *Internet Software Consortium*, mismo que mantiene un programa demonio denominado dhcpd.

El archivo de configuración del servidor se denomina dhcpd.conf y se encuentra ubicado por lo general en la carpeta /etc/.

1.8.3 PROXY [PW15]

1.8.3.1 Definición

Un proxy es un programa o dispositivo que realiza una tarea de acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo.

En general un servidor proxy ayuda en los siguientes aspectos:

- Control: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- Ahorro: Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- Velocidad: Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- Filtrado: El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- Modificación: Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- Anonimato: Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

1.8.3.2 Aplicaciones Proxy

1.8.3.2.1 Squid [PW16]

Squid es un proxy cache Web para el apoyo a HTTP, HTTPS, FTP, reduce el ancho de banda y mejora los tiempos de respuesta al almacenar en cache y reutilizar las páginas web solicitadas con mayor frecuencia.

Squid tiene varios controles de acceso a más que se ejecuta la mayoría de los sistemas disponibles, incluyendo Windows y está licenciado bajo la GNU GPL.

1.8.4 CORREO ELECTRÓNICO [PW17]

1.8.4.1 Definición

El correo electrónico permite a los usuarios el intercambio de mensajes escritos en forma digital sin importar la distancia a la que se encuentren.

La arquitectura de un sistema de correo está basado en la arquitectura tipo cliente/servidor. El sistema de correo, está organizado por tres entes participantes de la comunicación que son:

- MTA (*Mail Transfer Agent*): Como servidor que implementa el protocolo SMTP (*Simple Mail Transfer Protocol*) cuya función es transmitir el correo de un sitio a otro.
- MUA (*Mail User Agent*): Como cliente, implementa los protocolos POP3 e IMAP, el cual permite leer y crear mensajes de correo.
- MDA (*Mail Delivery Agent*): Se encarga de tomar el mensaje y dirigirlo al buzón de usuario apropiado; por lo general la mayoría de los sistemas de correo integran MDA en MTA.

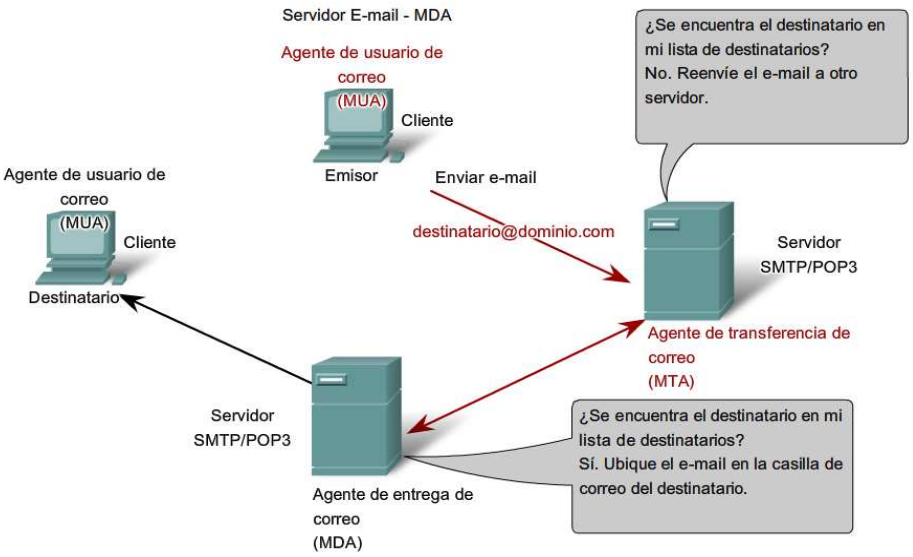


Figura 1.9 Proceso de entrega de correo electrónico [P2]

1.8.4.2 Protocolos usados en Correo Electrónico

1.8.4.2.1 SMTP*, Simple Mail Transfer Protocol* [PW18] [PW19]

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesador automático de la respuesta, mientras que el texto permite que un humano interprete la respuesta.

En el conjunto de protocolos TCP/IP, el SMTP va por encima de TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

1.8.4.2.2 POP3, Post Office Protocol [PW20] [PW21]

POP3 está diseñado para recibir correo, permite a los usuarios con conexiones intermitentes o muy lentas descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados. Un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

1.8.4.2.3 IMAP, Internet Message Access Protocol [PW21] [PW22]

Es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. IMAP tiene varias ventajas sobre POP, por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP3.

1.8.4.3 Aplicaciones de Correo Electrónico

1.8.4.3.1 SquirrelMail

SquirrelMail es una aplicación webmail, puede ser instalada en la mayoría de servidores web siempre y cuando éste soporte PHP y el servidor web tenga acceso a un servidor IMAP y a otro SMTP.

SquirrelMail sigue el estándar HTML 4.0 para su presentación, haciéndolo compatible con la mayoría de servidores web. SquirrelMail está diseñado para trabajar con plugins, lo cual hace más llevadera la tarea de agregar nuevas características entorno al núcleo de la aplicación.

Licenciada bajo la GNU General Public License, SquirrelMail es software libre. Actualmente está disponible en más de 40 lenguajes.

1.8.4.3.2 Zimbra [PW23]

Zimbra es una solución para correo electrónico y calendario de código abierto para empresas, proveedores de servicios, instituciones académicas y gubernamentales, ofrece un grupo de software moderno e innovador que entre sus principales características se tiene:

- Flexibilidad: es posible la personalización de Zimbra fácilmente según las necesidades de la organización,
- Libertad: utiliza el cliente web de Zimbra junto con otros programas tradicionales, como plataforma mixta,
- Durabilidad: es un servidor de correo electrónico y calendario extraordinariamente fiable y ampliable,
- Bajo mantenimiento: su gestión es completamente sencilla.

1.9 SERVICIOS EN TIEMPO REAL [P6]

Los servicios se ofrecen a través de un proveedor que centraliza la información en su servidor, para que sea accesible por sus clientes, esta información que pueden ofrecer puede estar previamente almacenada (un objeto de una página web,

vídeo o audio pregrabados, etc.) o generarse en tiempo real (comunicación de voz, videoconferencia, etc.).

1.9.1 TELEFONÍA IP

1.9.1.1 Definición [PW24]

La Telefonía IP es una solución tecnológica que sirve para transmitir comunicaciones de voz sobre una red de datos basada en el estándar IP. Con la solución de Telefonía IP, la organización reduce costos integrando sus aplicaciones de voz y datos sobre una única plataforma de red.

1.9.1.2 Características

- Convergencia de redes: Integración de las redes de voz y datos.
- Escalabilidad y flexibilidad: Permiten desarrollar mayores servicios sobre las redes implantadas.
- Compatibilidad con los sistemas tradicionales.
- Confidencialidad en las comunicaciones.
- Apertura real en las comunicaciones: Permitiendo interoperabilidad y libre dirección por uso de estándares abiertos.

1.9.1.3 Beneficios

- Ahorro en los costos operacionales: Costos de implementación y costos de gestión.
- Reduce desembolso de Capital: Una sola infraestructura convergente, un solo cableado.
- Ahorro en llamadas entre locales.
- Administración Centralizada.
- Los equipos de Telefonía IP pueden ser conectados desde cualquier punto de la red de la empresa manteniendo su mismo número y las mismas características sin necesidad de ser reconfigurados.

1.9.1.4 Recomendación H.323 [PW25] [PW26] [PW27]

H.323 es una recomendación del ITU-T (*International Telecommunication Union*), que especifica cómo las terminales (PC), equipos y servicios multimedia se comunican sobre redes que no proporcionan una calidad de servicio garantizada.

La recomendación describe los componentes de un sistema H.323, estos son:

- Terminales: Son puntos finales de la comunicación, proporcionan comunicación en tiempo real bidireccional. Para permitir que cualquier terminal ínter opere, se define que todos deben tener soporte para voz y códec G.711.Todos los terminales deben soportar H.245, el cual es usado para negociar el uso del canal y las capacidades.
- Gateways: Son dispositivos que implementan cuando se necesita la comunicación entre distintas redes. Proporcionan servicios como la traducción entre formatos de transmisión y entre procedimientos de comunicación.
- Gatekeepers: Son los elementos que actúan como punto central de todas las llamadas dentro de una zona y proporcionan servicios a los terminales registrados y control de llamadas. Proporciona dos grandes funciones de control de llamada que son la traducción de direcciones desde alias de la red H.323 a direcciones IP y gestionan el ancho de banda.
- MCU (*Multipoint Control Unit*): Controla conferencias entre tres o más extremos. Se compone de un MC (Multipoint Controller) que gestiona las negociaciones H.245 entre todos los terminales para determinar las capacidades comunes para el procesado de audio y video, y un MP (Multipoint Processor) que se encarga de procesar el audio y video.

La recomendación H.323 incluye estándares tales como el H.225.0 *Packet and Synchronization*, el H.245 *Control*, los H.261 y H.263 *Video Codecs*, los G.711, G.722, G.728, G.729 y G.723 *Audio Codecs* y la serie T.120 de protocolos de comunicaciones multimedia mostrados en la figura 1.10.

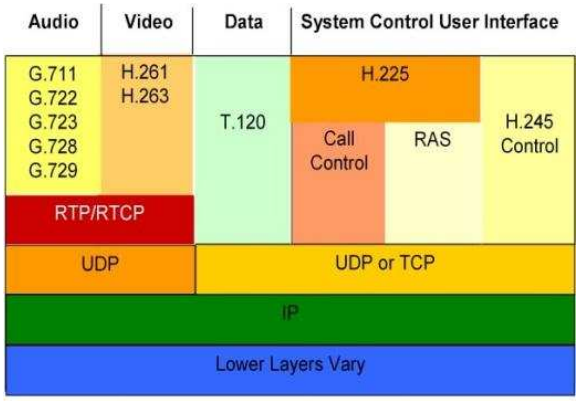


Figura 1.10 Estándares y protocolos de la recomendación H.323

1.9.1.5 SIP, *Session Initiation Protocol* [PW28]

SIP es un protocolo desarrollado por el grupo de trabajo MMUSIC (*Multiparty Multimedia SessIon Control*) del IETF (*Internet Engineering Task Force*) con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como: video, voz, mensajería instantánea, juegos en línea y realidad virtual.

Este protocolo hereda de ciertas funcionalidades de los protocolos HTTP (*Hyper Text Transport Protocol*) utilizados para navegar sobre el WEB y SMTP (*Simple Mail Transport Protocol*), utilizados para transmitir mensajes electrónicos. SIP se apoya sobre un modelo transaccional cliente/servidor.

El protocolo SIP es solo un protocolo de señalización. Una vez la sesión establecida, los participantes de la sesión intercambian directamente su tráfico audio/video a través del protocolo RTP (*Real-Time Transport Protocol*). Por otra parte, SIP no es un protocolo de reservación de recursos, y en consecuencia, no puede asegurar la calidad de servicio.

Una red basada en señalización SIP tiene al menos cinco tipos de entidades lógicas. Cada entidad tiene una función determinada y participa en las conversaciones SIP como cliente (inicia solicitudes), como servidor (responde a solicitudes) o de ambas formas.

- El Agente Usuario (*User Agent*) o “UA”: Se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un UE (*User Equipment*) una PC, un teléfono IP o una estación móvil UMTS (*Universal Mobile Telecommunications System*). La RFC 3261 define el Agente de Usuario como una aplicación, que contiene dos elementos: un Agente de Usuario cliente y un Agente de Usuario servidor, tal como se detalla a continuación:
    - Agente de Usuario Cliente (UAC): una aplicación cliente que inicia solicitudes SIP hacia la red IP.
    - Agente de Usuario Servidor (UAS): una aplicación que al recibir una solicitud SIP de la red IP se pone en contacto con el usuario y devuelve la respuesta que este desee.
- El Servidor Proxy (Proxy Server): Su función principal es conseguir que la solicitud del cliente se remita a la entidad más cercana al usuario de destino, también se emplean para verificar las políticas (esto es, comprobar si el usuario está autorizado a efectuar una llamada). El proxy interpreta, y si fuese preciso, reescribe partes del mensaje de solicitud antes de reenviarlo.
- El Servidor de Re direccionamiento (Redirect Server): se trata de un servidor quien acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el número del destinatario en el mensaje SIP recibido, en un número de reenvió de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el redirect server devuelve el nuevo número (número de reenvió) al cliente de origen quien se encarga de establecer una llamada hacia este nuevo destino.
- El Servidor Registrador: se trata de un servidor quien acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al servidor la dirección donde es localizable (dirección IP). El servidor registrador actualiza entonces una base de datos de localización.

- Agente de Usuario Inverso, B2BUA (*Back-to-Back User Agent*): Los B2BUA se emplean en aquellas funciones donde es preciso controlar el saldo remanente del usuario o el tiempo que le queda de conversación, como es el caso de los locutorios y de los sistemas de llamadas pre pagadas.

1.9.2 PROTOCOLOS DE TRANSPORTE EN TIEMPO REAL [L2]

Al transmitir datos que no necesitan llegar en tiempo real, la latencia no es un factor muy importante, siempre y cuando los paquetes lleguen al destino. Al transmitir audio, video o cualquier sesión multimedia esta situación no debe producirse, pues en este tipo de comunicación la temporización es muy importante para comprender el contenido del mismo.

El protocolo encargado de la temporización y del reordenado de este tipo de paquetes es RTP, éste sin embargo, confía en que los paquetes llegarán en un tiempo adecuado para que el destino pueda reordenarlos.

La utilización de paquetes UDP unido a la creación de buffer de compensación que almacena los paquetes entrantes para corregir el *jitter* y a la utilización de equipos con QoS, permiten mantener controlada la latencia de red y hacer que la transmisión de datos multimedia sea lo suficientemente fluida para humanos, sin los cortes producidos por paquetes que llegan fuera de tiempo.

RTP (*Real-time Transport Protocol*) y RTCP (*Real-time Transport Control Protocol*), son protocolos destinados al transporte de flujos multimedia. Mientras RTP se encarga del transporte propiamente dicho, RTCP utiliza RTP para ofrecer calidad de servicio y otras funciones relacionadas con conferencias y sesiones multimedia.

1.9.3 VIDEOCONFERENCIA

1.9.3.1 Definición [PW29]

Videoconferencia es la comunicación simultánea bidireccional de audio y vídeo, permitiendo mantener reuniones con grupos de personas situadas en lugares alejados entre sí. Adicionalmente, pueden ofrecerse facilidades telemáticas o de

otro tipo como el intercambio de gráficos, imágenes fijas, transmisión de ficheros desde el ordenador, etc.

El núcleo tecnológico usado en un sistema de videoconferencia es la compresión digital de los flujos de audio y vídeo en tiempo real. Su implementación proporciona importantes beneficios, como el trabajo colaborativo entre personas geográficamente distantes y una mayor integración entre grupos de trabajo.

1.9.3.2 Clasificación de las videoconferencias [PW30]

1.9.3.2.1 Videoconferencia punto a punto

Es la conexión directa entre dos sitios, su gestión se realiza mediante la negociación bilateral entre los dos sitios. No es necesario contar con ningún equipo adicional para realizar videoconferencias de este tipo.

1.9.3.2.2 Videoconferencia Multipunto

En este tipo de videoconferencias intervienen más de dos sitios. La comunicación se establece mediante un equipo MCU (*Multipoint Control Unit*) que es el encargado de repartir las señales de audio y video de todos a todos.

Existen dos tipos de videoconferencia multipunto dependiendo de la configuración de la MCU para la distribución del audio y video que recibe. Se tiene tipo presentación y tipo discusión.

1.9.3.2.3 Videoconferencias tipo presentación

En este tipo de videoconferencia multipunto, la MCU escoge automáticamente el ponente principal, el cual proviene del sitio que emite la señal de audio de forma continua. Si otro sitio desea ser el ponente principal, únicamente tiene que comenzar a emitir audio.

1.9.3.2.4 Videoconferencias tipo discusión

La MCU recibe las señales de audio y video de todos los sitios pertenecientes a la videoconferencia, mezcla todas las señales y la resultante es enviada a cada uno

de los participantes. De esta forma cada sitio puede ver y escuchar simultáneamente todos los sitios.

1.9.3.3 Tecnologías de Videoconferencia

1.9.3.3.1 Recomendación H.320 [P7]

H.320 es una recomendación del ITU-T (*International Telecommunication Union*), que establece los requisitos técnicos para sistemas y equipos terminales de videoconferencia en banda estrecha.

1.9.3.4 Elementos del sistema de videoconferencia [PW31] [T3]

- Sala de videoconferencia: Es el lugar físico donde se encuentra ubicado los equipos que se usa para realizar la videoconferencia, además de los participantes de la misma. Cualquier espacio puede adecuarse para una videoconferencia dependiendo del tipo de videoconferencia que se desee.
- Códec: Es el encargado de codificar-decodificar las señales de audio y video, comprimir y multiplexar para transformarlas en señal digital.
- Sistema de audio: Permite recibir y distribuir la señal de audio. Además éste sistema regula las características acústicas de la sala, está conformado por micrófonos, parlantes, amplificadores, mezcladoras y ecualización de la sala.
- Sistema de video: Permite enviar, recibir y observar la imagen en los sitios pertenecientes a la videoconferencia. Además permite observar cualquier información visual como videos, diapositivas, etc., está conformado por: cámaras, proyector y pantallas.

1.9.3.5 Software para videoconferencia Openmeetings

Openmeetings es un software que permite realizar conferencias a través de internet mediante el uso de un navegador web, utiliza la licencia Eclipse Public License, siendo software libre.

Es utilizado para presentaciones, la formación en línea, conferencias web, pizarra de dibujo, colaboración y edición de documentos, intercambio de escritorio del

usuario. El producto se basa en el marco RIA de OpenLaszlo[1] y el servidor de video Red5, que a su vez se basa en componentes de código abierto. La comunicación tiene lugar en las salas de reunión en las que se establecen la seguridad y los modos de calidad de vídeo. La base de datos recomendada es MySQL[2].

Para su funcionamiento utiliza tecnología Flash para lo que utiliza el servidor RED5 que es una aplicación que pretende ser una alternativa libre al Flash Media Server de Adobe.

Características

- Permite la difusión de Video y Audio
- Se puede visualizar el escritorio de cualquier participante
- Disponible en 19 idiomas
- Pizarra virtual con capacidades de dibujo, escritura, edición, cortar y pegar, redimensionamiento de imágenes e inserción símbolos
- Conferencias mientras se dibuja
- Importación de documentos
- Envío de invitaciones y links directos dentro de la conferencia
- Sistema de moderadores
- Cuartos públicos y privados para conferencias
- El servidor se puede ejecutar tanto en Windows como en Linux y los clientes únicamente necesitan un navegador y el Flash Player por lo que se puede participar en una sesión desde prácticamente cualquier plataforma.

1.10 STREAMING DE AUDIO Y VIDEO [PW32]

El streaming es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga. Un sistema de video streaming puede ser representado mediante siete bloques, tal como muestran en la figura 1.11.

[1]OpenLaszlo, una plataforma de código abierto, ofrecida bajo la Licencia Pública Común (*Common Public License o CPL*), para el desarrollo y la entrega de aplicaciones de Internet enriquecidas.
[2]MySQL, sistema de gestión de bases de datos relacional, multi-hilo y multiusuario.

Los datos de video y audio en bruto son pre-comprimidos por compresión de video y de audio y luego guardados en dispositivos de almacenamiento. A pedido del cliente, el servidor de streaming recupera datos de audio/video del almacenamiento donde el módulo de control de QoS (*Quality of Service*) y la capa de aplicación adapta los flujos de bits al estado de la red y los requerimientos de QoS. Posteriormente, los protocolos de transporte convierten los flujos de bits comprimidos en paquetes y los envían sobre la red.

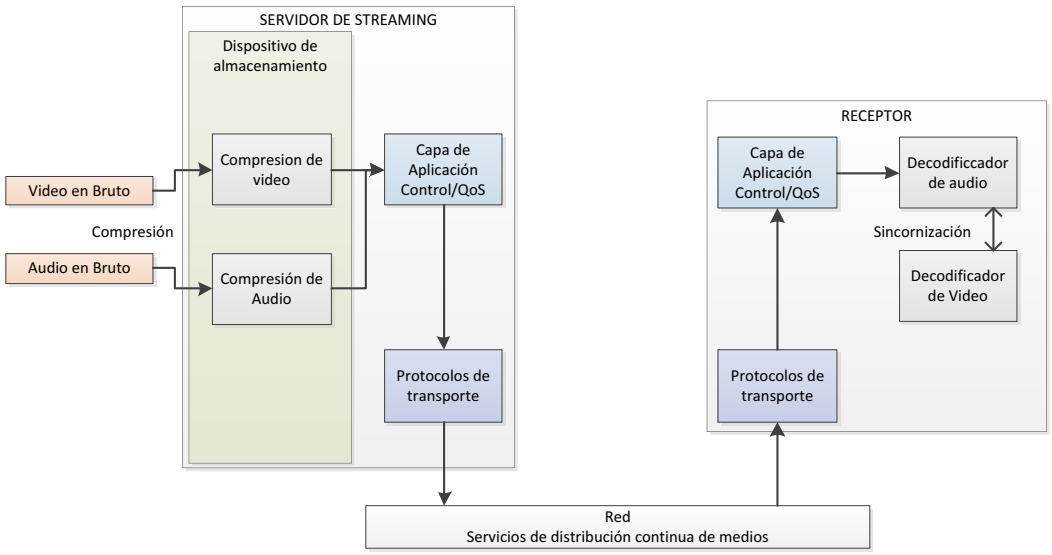


Figura 1.11 Sistema de video streaming

Durante el proceso de transmisión de los datos puede ocurrir que existan paquetes descartados o que los mismos presenten demoras significativas debido a la congestión. Para conseguir una sincronización entre el audio y el video se requieren mecanismos de sincronización de medios.

1.10.1 COMPRESIÓN DE VIDEO

La compresión de video se obtiene mediante la explotación de semejanzas o redundancias que existen en una señal de video típica. Tomando en cuenta que un video es una secuencia de cuadros o imágenes, cada cuadro puede ser codificado como una imagen separada, sin embargo, considerado que los cuadros vecinos son muy similares, se puede alcanzar una mayor compresión explotando la semejanza de cuadros sucesivos.

Un sistema de compresión de video está compuesto de un codificador y un decodificador que interpretan de la misma forma las ráfagas de bits comprimidos. El codificador toma el video original y lo comprime en una secuencia de bits, la que es enviada al decodificador para que produzca el video reconstruido.

1.10.2 ESTÁNDARES DE COMPRESIÓN DE VIDEO

Los estándares de compresión de video brindan un gran número de beneficios entre los que destacan el aseguramiento de la interoperabilidad y la comunicación entre codificadores y decodificadores realizados por personas o compañías diferentes.

Calidad	Estándar	Sin compresión [Mbps]	Con Compresión [Mbps]
HDTV 1920x1080/60	--	2000	--
	MPEG-2	--	25 a 34
ITU-R digital TV	ITU-R 601	166	--
	MPEG-2	--	3 a 6
TV broadcast	MPEG-2	--	2 a 4
VCR	MPEG-1	--	1,2
Videoconferencia	H.261	--	0,1

Tabla 1.4 Algunos estándares de codificación de video [PW33]

Los estándares no especifican ni el codificador ni el decodificador. Lo que si se describe es la sintaxis para la secuencia de bits, y el proceso de decodificación.

1.10.3 SERVIDORES DE STREAMING

Para poder ofrecer servicios de calidad, los servidores de streaming deben procesar datos multimedia con ciertas restricciones temporales para prevenir fallas. También deberán soportar comandos que permitan: parar, poner en pausa, adelantar o retroceder el video y entregar el audio y video sincronizados.

Un servidor típico de streaming consta de:

- Comunicador: Involucra la capa de aplicación y los protocolos de transporte implementados en el servidor.

- Sistema Operativo: Además de los servicios típico el SO deberá soportar aplicaciones en tiempo real.
- Sistema de almacenamiento: Deberá soportar almacenamiento y retiro continuo de medios.

1.10.4 PROTOCOLOS PARA VIDEO STREAMING

Los protocolos son diseñados y estandarizados para la comunicación entre los clientes y los servidores de streaming. Se clasifican en tres categorías: Protocolos de capa de red, protocolos de transporte y protocolos de control de sesión.

1.10.4.1 Real Time Messaging Protocol, *RTMP* [PW34] [PW35]

RTMP es un protocolo de alto rendimiento para transmisión de Audio, Vídeo y Datos, desarrollado por Adobe para trabajar entre plataformas con Tecnología *Adobe Flash.* RTMP se encuentra basado en TCP, mantiene conexiones persistentes y permite una comunicación de baja latencia.

Para mantener el flujo constante y transmitir la mayor cantidad de información posible, divide el flujo en fragmentos y su tamaño es negociado dinámicamente entre el cliente y el servidor. El tamaño por defecto del fragmento de audio es de 64 bytes y de 128 bytes para video y la mayoría de otros contenidos. Los fragmentos de distintos flujos pueden ser intercalados y multiplexados a través de una sola conexión.

RTMP define varios canales virtuales por los cuales los paquetes pueden ser enviados y recibidos, estos canales operan en forma independiente.

RTMP está actualmente disponible como una especificación abierta para crear productos y tecnologías que permiten la distribución de vídeo, audio y datos en los formatos abiertos: AMF, SWF, FLV y F4V compatibles con Adobe Flash Player.

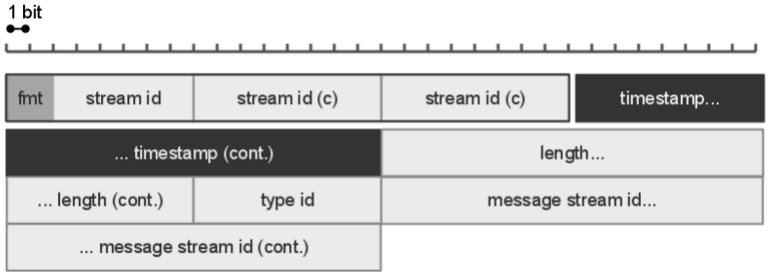


Figura 1.12 Diagrama de un paquete RTMP

1.10.5 APLICACIONES PARA STREAMING DE VIDEO

1.10.5.1 Red5 Open Source Flash Server [PW37] [PW38]

Red5 Media Server ofrece un servidor de streaming de vídeo de gran alcance y multi-usuario similar a la solución de Adobe flash Player y otras tecnologías de cliente emocionantes. Basado en Java y algunos de los marcos de código abierto más poderosos, Red5 se erige como una solución sólida para los negocios de todos tamaños, incluyendo la empresa.

Entre sus principales características se tiene:

- El servidor puede detectar automáticamente la velocidad de conexión entre el cliente y proporcionar automáticamente la mejor visualización del video,
- Capacidad de reproducción parte de un video sin necesidad de la transferencia completa del archivo,
- Transmisión de señales en tiempo real,
- Grabación de contenido en formato FLV,
- Facilidad de implementar pantallas compartidas,
- Análisis y reportes de datos en tiempo real,
- Protección de derechos de autor, pues no se transmiten los archivos físicos, sino que se envía el contenido en streaming.

1.11 SEGURIDAD EN LA RED [L4] [PW39]

La seguridad en la red comprende la protección de equipos conectados a la red y de los datos que estos almacenan y comparten, junto con el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto de la red.

Partiendo de que una amenaza es una potencial violación de seguridad, la cual se da cuando hay una circunstancia, capacidad, acción, o evento que puede incumplir con la seguridad y causar daño. Un ataque a un sistema de seguridad es un intento deliberado para evadir los servicios de seguridad y violar las políticas de seguridad de un sistema.

Una clasificación útil es dividir los ataques en términos de pasivos y activos. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

En los ataques activos el atacante altera las comunicaciones. Pueden subdividirse en cuatro categorías: suplantación de identidad, donde el intruso se hace pasar por una entidad diferente; re actuación, donde uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no autorizado; modificación de mensajes, donde el intruso varía los datos transmitidos y degradación fraudulenta del servicio, donde el intruso intenta impedir que los entes dialogantes puedan realizar correctamente su función, mediante destrucción o retardo de mensajes o la introducción de mensajes falsos con el fin de congestionar la red.

Para hacer frente a las amenazas de seguridad, se definen una serie de servicios que realzan la seguridad de los sistemas de proceso de datos y de transferencia de información. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

- Confidencialidad: Requiere que la información sea accesible únicamente por las entidades autorizadas.
- Autentificación: Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa.
- Integridad: Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y re actuación de los mensajes transmitidos.
- No repudio: Requiere que ni el emisor ni el receptor del mensaje puedan negar la transmisión.
- Control de acceso: Requiere que el acceso a la información sea controlado por el sistema destino.

1.11.1 MECANISMOS DE SEGURIDAD [L1] [P5]

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

- Intercambio de autentificación: Corrobora que una entidad, ya sea origen o destino de la información, es la deseada,
- Cifrado: Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados,
- Integridad de datos: Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir. Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados,
- Firma digital: Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía al receptor junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad,
- Control de acceso: Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red.

1.11.2 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad son reglas que son electrónicamente programadas o guardadas dentro de los equipos de seguridad para controlar los privilegios de accesibilidad a ciertas áreas. También las políticas de seguridad son escritas en regulaciones verbales por la organización que las define.

Una política de seguridad debe cumplir los siguientes objetivos:

- Informar a los usuarios, al personal y a los gerentes acerca de los requisitos obligatorios para proteger los bienes de tecnología e información.
- Especificar los mecanismos a través de los cuales se pueden cumplir estos requisitos.
- Proporcionar una línea de base a partir de la que se pueda adquirir, configurar y auditar redes y sistemas informáticos para que cumplan la política.

1.11.3 INGENIERÍA SOCIAL

La ingeniería social se aprovecha de las vulnerabilidades personales que pueden ser descubiertas por agresores talentosos. Puede incluir apelaciones al ego de un empleado, o bien puede tratarse de una persona simulada o un documento falsificado que logra que una persona proporcione información confidencial.

La suplantación de identidad es un tipo de ataque de ingeniería social que involucra el uso de correo electrónico u otros tipos de mensajes para intentar engañar a otras personas, de modo que brinden información confidencial.

Los ataques de suplantación de identidad pueden prevenirse educando a los usuarios e implementando pautas de información cuando se reciben correos electrónicos sospechosos. Los administradores también pueden bloquear el acceso a determinados sitios Web y configurar filtros que bloqueen el correo electrónico sospechoso.

1.11.4 FIREWALL Y LISTAS DE ACCESO [PW10] [PW40]

Un elemento clave para la seguridad de la red es un firewall, mismo que mitiga los riesgos a la infraestructura de la red contra los ataques a nivel de capa de red y aplicación a más de virus y gusanos informáticos.

Con el objeto de filtrar el tráfico en la red se crean las listas de control de acceso que permiten definir qué paquetes serán entregados o bloqueados en las interfaces de los equipos de control.

Las listas de control de acceso o ACL's (*Access Control Lists*) son una colección secuencial de condiciones que permiten o deniegan, que se aplican a un paquete IP, los equipos como los ruteadores o firewalls prueban cada paquete con las condiciones definidas en las listas, una a la vez, siendo la primera coincidencia la que determinará la decisión a tomar. Debido a ello, el orden de las condiciones es esencial para un correcto filtrado.

Es posible definir dos grupos de ACL's:

- ACL's Estándar: controlan el tráfico al comparar la dirección IP de origen con las direcciones IP configuradas en la lista.
- ACL's Extendidas: controlan el tráfico al comprar la dirección IP de origen y destino con las direcciones IP configuradas en la lista. Las ACL's extendidas pueden ser más específicas al filtrar el tráfico mediante criterios como protocolos o número de puerto.

El comportamiento de un firewall puede ser enmarcado en dos políticas básicas que cambiarán radicalmente la seguridad de la red, estas son:

- Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.

- Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.

1.12 ADMINISTRACIÓN DE LA RED

Las administración de las redes de comunicaciones tiene una gran importancia puesto que define un conjunto de normas para mantener funcionando adecuadamente a una red compleja, a mas que maximiza la eficiencia y productividad y permite al administrador de la red conocer las necesidades de la misma.

Tomando en cuenta que mientras más grandes son las redes, estas tienden a implementar sistemas más complejos, más aplicaciones y usuarios. En base a esto, dos factores comienzan a evidenciarse:

- La red, sus recursos asociados y
- Las aplicaciones distribuidas que comienzan a hacerse indispensables.

Muchos dispositivos pueden fallar, inutilizando toda la red o una porción de ella, o la carga sobre la red puede ir degradando el desempeño hasta niveles inaceptables.

Para dar respuesta a estas necesidades han surgido aplicaciones estándar que permiten administrar las redes, cubriendo servicios, protocolos y bases de información de gestión, tal es el caso de un sistema de gestión de red que puede definirse como una colección de herramientas para el monitoreo y control de redes el cual es integrado en el siguiente sentido:

- Una interfaz simple para el operador y amigable colección de comandos que permita ejecutar la mayoría o todas las tareas de gestión de red.
- Proveer una visión de la red en su totalidad.

1.12.1 SNMP, *SIMPLE NETWORK MANAGEMENT PROTOCOL*

SNMP es un protocolo que permite que una entidad gestora tenga acceso a información sobre el estado de cualquier dispositivo de la red. Este acceso se realiza mediante la lectura/escritura de variables que reciben el nombre de objetos gestionados y que se organizan siguiendo la notación de sintaxis abstracta ASN.1 (*Abstract Syntax Notation One*) en una base de datos denominada MIB (*Management Information Base*). Una aplicación Agente es la responsable de completar y actualizar la información de la MIB, facilitar la información requerida por la entidad gestora e informar a la misma de eventuales anomalías mediante el uso de menajes denominados Traps.

El SNMP se ha convertido en un estándar de gestión de red dominante y la mayoría de los equipos de interconexión (routers, switches, hubs, bridges) dispositivos de encaminamiento, estaciones de trabajo y PC ofrecen paquetes de agentes SNMP para ser gestionados.

1.13 PLAN DE CONTINGENCIA [PW41]

1.13.1 INTRODUCCIÓN

Las tecnologías de información son vulnerables a una variedad de interrupciones, comprendidas entre leves y severas. Algunas vulnerabilidades pueden ser minimizadas o eliminadas a través de soluciones técnicas, organizativas u operacionales como parte del esfuerzo para mitigar riesgos de la organización, sin embrago es imposible eliminar todos los riesgos. Un plan de contingencia es diseñado para mitigar estos riesgos

Es de suma importancia que los servicios provistos por estos sistemas sean capaces de operar efectivamente sin interrupciones excesivas. La planeación de contingencia aporta a este requisito, al establecer planes completos, procedimientos y medidas que pueden permitir la recuperación rápida de un sistema.

1.13.2 PLANEACIÓN DE CONTINGENCIA Y MANEJO DE PROCESOS DE RIESGO

El manejo de riesgos enmarca una gran cantidad de actividades para identificar, controlar, y mitigar los riesgos en un sistema de información.

En este ámbito se definen dos funciones principales. Primero, se debe identificar las amenazas y vulnerabilidades, para que controles apropiados puedan ser puestos en marcha con el objetivo de prevenir o limitar los incidentes. Estos controles de seguridad pueden ser clasificados en tres:

- Naturales.- por ejemplo huracanes, fuego o inundaciones.
- Humanos.- por ejemplo error de los operadores, implante de códigos maliciosos o ataques terroristas.
- Ambientales.- por ejemplo fallas en los equipos por cambios de temperatura.

Segundo, la administración de los riesgos debe identificar, los riesgos residuales para los cuales los planes de contingencia deben ser puestos en marcha.

Para determinar los riesgos en un sistema durante una interrupción es necesaria una valoración. Estos riesgos deben ser valorados y clasificados acorde a un nivel de amenaza, por ejemplo Alto, Medio o Bajo.

Debido a que los riesgos varían en transcurso del tiempo y nuevos riesgos pueden reemplazar a viejos tal como evoluciona el sistema, el proceso de administración de riesgos debe ser creciente y dinámico.

1.13.3 TIPOS DE PLANES

Los planes de contingencia tienen una gran cantidad de alcances y actividades diseñadas para mantener y recuperar los servicios críticos de las tecnologías de información después de una emergencia. Una organización debe usar un conjunto de planes para preparar adecuadamente la respuesta, recuperación y continuidad

de actividades para interrupciones que afecten a las tecnologías de información de la organización.

Plan	Propósito	Alcance
Continuidad de Negocios	Provee los procedimientos para mantener las operaciones de negocios esenciales mientras se recupera de una interrupción significante.	Enfocado en los procesos de negocio. Solo toma las *TIC*[3] que soportan esos procesos.
Recuperación de Negocios	Provee procedimientos para recuperar las operaciones de negocios inmediatamente después de un desastre.	Enfocado en los procesos de negocio. No toma en cuenta las *TIC*.
Continuidad de Operaciones	Proporciona los procedimientos y capacidades para mantener una organización de funciones esenciales y estratégicas en un lugar alternativo para un máximo de 30 días	Enfocado en un subconjunto de misiones organizativas que son identificadas como las más críticas. No toma en cuenta los recursos de tecnologías de Información.
Continuidad de Soporte / Plan de Contingencia	Provee procedimientos y capacidades para recuperar una aplicación principal o el sistema de apoyo general.	Enfocado en los procesos de negocio y las *TIC* basándose únicamente en su apoyo a los procesos de negocio.
Comunicaciones de crisis	Proporciona los procedimientos para la difusión de informes sobre la situación del personal y el público.	Enfocado en la comunicación con el personal y el público. No en las *TICs*.
Respuesta a un incidente cibernético	Proporciona estrategias para detectar, responder a, y limitar consecuencias de incidentes cibernéticos maliciosos.	Se centra en las respuestas de seguridad de la información a los incidentes que afectan a los sistemas y / o redes.
Recuperación de Desastre	Proporciona procedimientos detallados para facilitar la recuperación de las capacidades en un sitio alternativo	A menudo centrada en las *TIC*, se limitan a grandes trastornos con efectos a largo plazo
Ocupación de Emergencia	Proporciona procedimientos coordinados para minimizar la pérdida de vidas, lesiones y la protección de daños a la propiedad en respuesta a una amenaza física	Se centra en el personal y la propiedad particular para la instalación específica, no de procesos de negocio o de TIC basada en la funcionalidad del sistema

Tabla 1.5 Tipos de planes de contingencia

[3] TIC, *Tecnologías de la información y la comunicación.*

1.13.4 CONTROLES PREVENTIVOS

En algunos casos, los impactos definidos en la tabla 1.5 pueden ser mitigados o eliminados a través de medidas preventivas. Cuando es factible y rentable, los métodos de prevención son preferibles a las acciones que sean necesarias para recuperar el sistema después de una interrupción. Para el caso presente se pueden listar los siguientes:

- Adecuado dimensionamiento de los UPS para proporcionar un respaldo de energía a corto plazo para todos los componentes de la red.
- Generadores de gasolina o diesel para proveer un respaldo de energía a largo plazo.
- Sistemas de aire acondicionado con adecuada capacidad.
- Sistema de supresión de incendios.
- Detectores de humo.
- Sensores de agua en el techo y piso del cuarto de equipos.
- Interruptor maestro para apagar los equipos.
- Respaldo de información frecuente.

1.13.4.1 Estrategias de recuperación

1.13.4.1.1 Métodos de respaldo de información

La información de los equipos de red debe ser respaldada regularmente, deben definirse políticas de frecuencia de información basadas en la información crítica y cuando nueva información es configurada en los equipos. Acorde a ello es necesario mantener un servidor de respaldo para los equipos de red, este usará el protocolo TFTP para copiar la configuración de los equipos de red al servidor.

1.13.4.1.2 Reemplazo de Equipos

Si los equipos de conectividad sufren daños o son destruidos, es necesario obtener el hardware y software necesario en forma inmediata, para ello se dispone de tres tipos de estrategias que son:

- Acuerdos con los Fabricantes.- contempla la definición de varios SLA (*Service Level Agreements*) con los fabricantes.
- Inventario de Equipos.- contempla la compra de equipos y su almacenamiento para su uso en caso de un fallo de un equipo similar.
- Equipos existentes compatibles.- contempla el uso de equipos que están siendo usados pero en casos de fallas pueden ser reutilizados en otros puntos.

De acuerdo a las características de los equipos en la AZEA, se define el uso de la estrategia de inventario de equipos, misma que se encuentra respaldada con el recuento de equipos disponibles y usados mostrados en el anexo I.

1.13.4.1.3 Mantenimiento del Plan

Con el objeto de ser efectivo, el plan debe mantenerse siempre listo y reflejar en forma precisa los requerimientos, procedimientos, estructura organizacional y políticas. Debido a que la red sufre cambios frecuentes por las necesidades cambiantes del negocio, nuevas tecnologías o nuevas políticas internas o externas. Por tal motivo es esencial que el plan de contingencia sea revisado y actualizado al menos una vez al año o cuando se implementen grandes cambios en la red. El plan se evaluará en los siguientes aspectos:

- Requerimientos Operacionales.
- Requerimientos de Seguridad.
- Hardware, software y otros equipos.
- Nombre e información de contacto de los miembros del plan de contingencia.

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL, REQUERIMIENTOS

2.1 INTRODUCCIÓN

En el presente capítulo se definirá la situación actual en la que se encuentra la Administración Zonal Eloy Alfaro. Se definirán las características en la red de datos y telefonía, con base en esta información se determinarán los requerimientos necesarios del rediseño de la nueva red que incluya soporte a telefonía y video.

A continuación se mencionan algunas características propias de la Administración Zonal Eloy Alfaro.

2.1.1 ANTECEDENTES [P8]

La Administración Zonal Eloy Alfaro fue creada en 1994 y regentaba 10 parroquias, años más tarde, tomando en consideración la gran extensión y el gran número de habitantes del sur, y con el fin de dar un mejor servicio a la comunidad, mediante Resolución Nº- 048 del 12 de junio del 2001, se subdivide al sur en dos zonas: Quitumbe y Eloy Alfaro.

La Administración Zonal Eloy Alfaro tiene una extensión de 58.005,9 hectáreas, cobija a 465 barrios y una población cercana a los 650.000 habitantes, (450 000 permanente y 200 000 flotantes) en su gran mayoría, fruto del alto índice de migración de provincias hacia la capital en busca de mejores oportunidades para su familia.

Están bajo su administración las parroquias de: La Magdalena, Chimbacalle, La Argelia, Chilibulo, San Bartolo, La Mena, Ferroviaria, Solanda y la parroquia rural de Lloa. En la figura 2.1 se muestran las parroquias que administra la AZEA.

Características De La Zona:

- La Zona Eloy Alfaro es la más densamente poblada.
- Es la Zona con mayor consolidación.
- Es la Zona con mayor atención a los servicios básicos prioritarios.

La Zona Eloy Alfaro, se encuentra dividida en nueve (9) parroquias, ocho (8) urbanas y una (1) rural, tiene asentamientos milenarios como Chilibulo y La Magdalena.

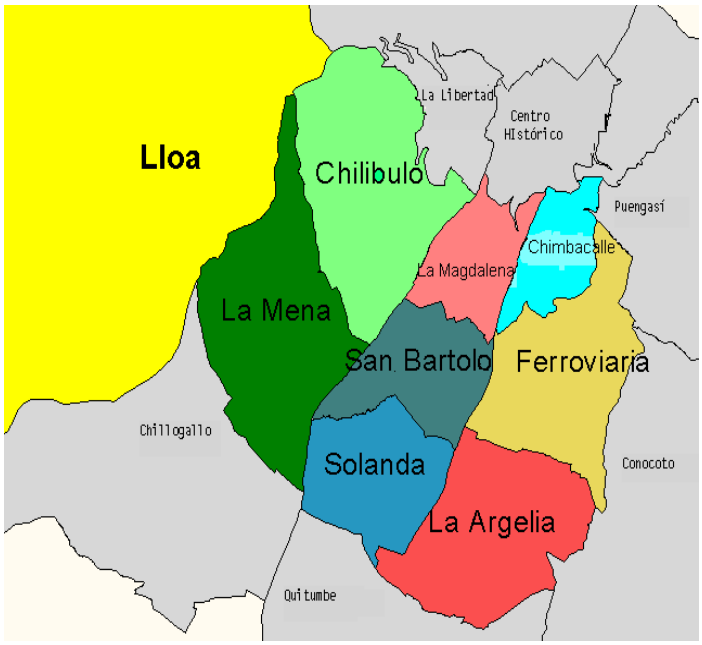


Figura 2.1 Parroquias que conforman la zona Eloy Alfaro en el distrito [P8]

2.1.2 UBICACIÓN [P8]

La Zona Municipal Eloy Alfaro se encuentra geográficamente en el Centro Sur de Quito, a una altura de 2.450msnm. La Zona Eloy Alfaro, debido a su posición geográfica se encuentra ubicada en:

- Noreste: Latitud Sur 0°, 14', 32''; Longitud Oeste 78°, 29', 50''
- Noroeste: Latitud Sur 0°, 16', 5''; Longitud Oeste 78°, 33', 41''
- Suroeste: Latitud Sur 0°, 16', 42''; Longitud Oeste 78°, 33', 8''
- Sureste: Latitud Sur 0°, 17', 20'' ; Longitud Oeste 78°, 31', 14''

2.1.3 VISIÓN [P8]

“La Administración Zonal Eloy Alfaro, moderna, participativa y tolerante, con barrios verdes y seguros, lugar para trabajar y recrearse, con habitantes saludables y orgullosos y orgullosas de vivir en el Distrito Metropolitano de Quito.”

2.1.4 MISIÓN [P8]

“Administrar eficientemente los recursos en la planificación y ejecución de proyectos comunitarios, que mejoren el entorno y la calidad de vida de su gente, asegurando el desarrollo sustentable de la Zona Eloy Alfaro.”

2.1.5 ORGANIGRAMA [PW42]

La estructura organizacional de la AZEA se encuentra divida en tres niveles, a la cabeza de los cuales se encuentra el Administrador Zonal, cargo presidido por el Ing. César Andrade, a continuación de este se presentan los niveles directivos, de asesoría y operativos, los que cuentan en cada nivel con distintas direcciones y jefaturas acorde a lo mostrado en la figura 2.2.

2.2 INFRAESTRUCTURA FÍSICA

La Administración Zonal Sur Eloy Alfaro cuenta con tres zonas plenamente definidas, al occidente se tiene la Plaza Cívica Eloy Alfaro en la cual se realizan constantemente eventos de interés público.

En la parte central están ubicados los dos edificios sobre los que se brindan los distintos servicios a la comunidad, para su diferenciación se los ha denominado edificio principal y edificio secundario conforme las dimensiones físicas y concurrencia de público.

En la parte oriental se tienen los parqueaderos usados por el personal de la AZEA y el público en general.

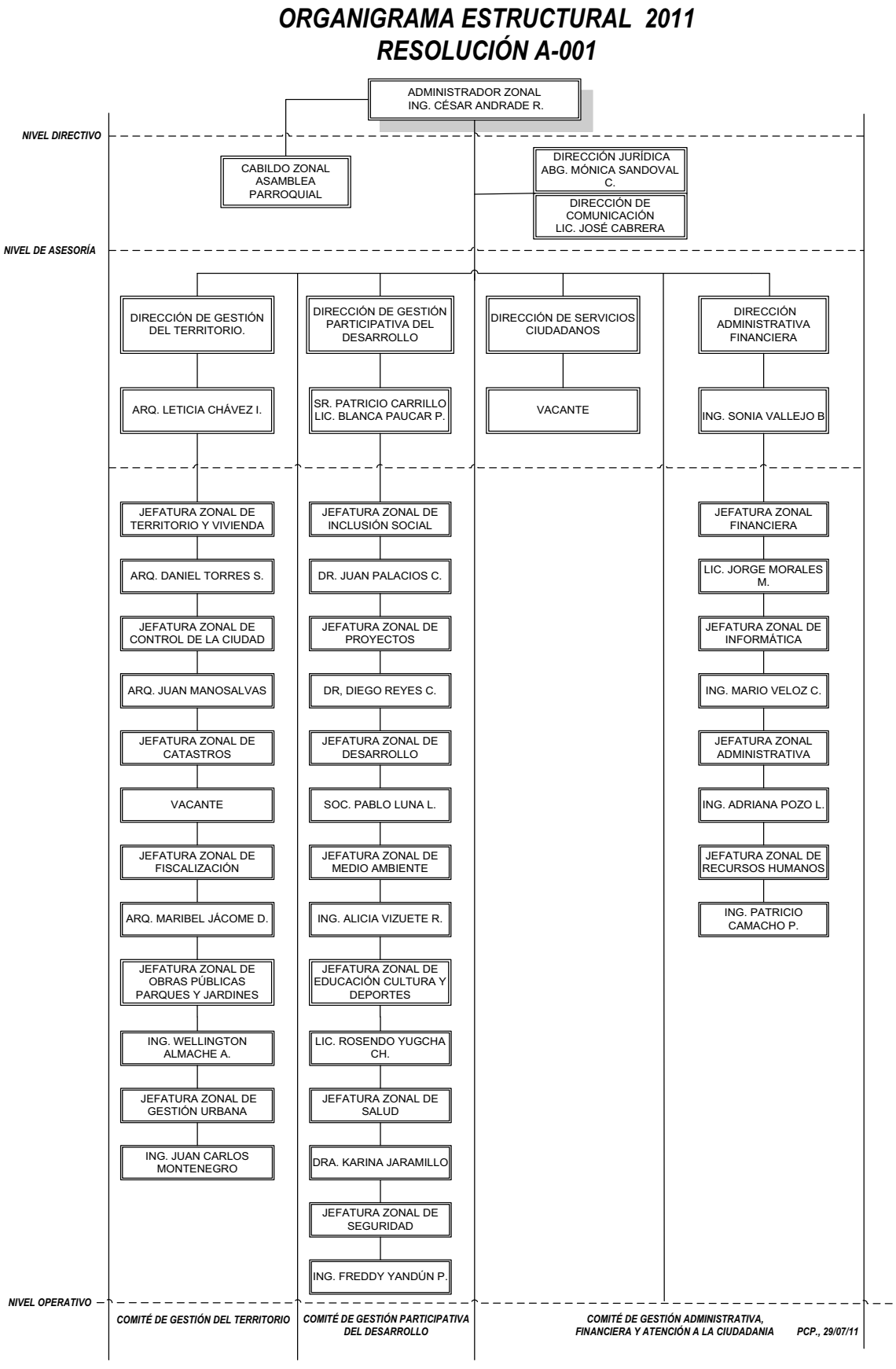


Figura 2.2 Organigrama estructural de la Administración Zonal Eloy Alfaro [PW41]

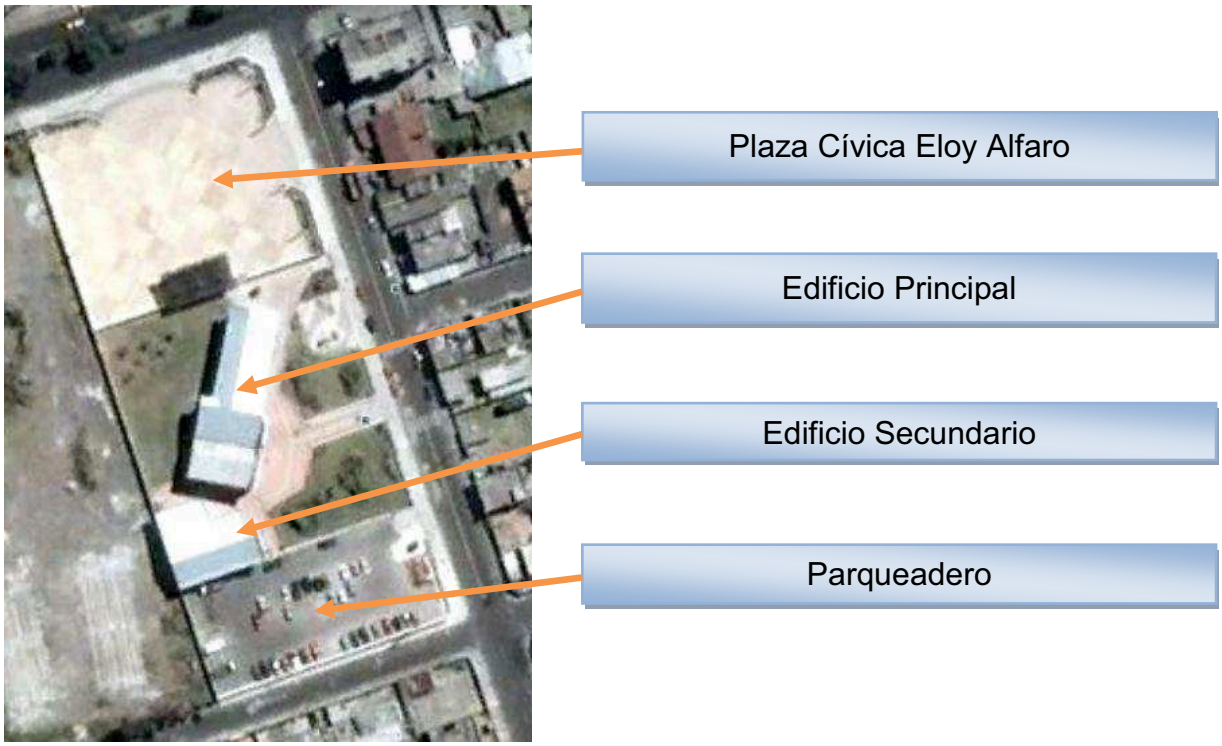


Figura 2.3 Instalaciones físicas de la AZEA

2.2.1 EDIFICIO PRINCIPAL

El edificio principal fue construido con el objeto de convertirse en las instalaciones del cuartel Pichincha, defiendo las características estructurales para este fin. Posteriormente el Ilustre Municipio de Quito tomó el control de esta infraestructura y la readecuo con el propósito de ubicaren este lugar a las instalaciones de la AZEA, respondiendo así al crecimiento poblacional y las necesidades de esta zona de Quito.

Figura 2.4 Edificio principal, Administración Zonal Eloy Alfaro

El edificio principal está constituido por hormigón armado y sus paredes fueron levantadas con la utilización de bloques. Tiene un área de 1563 m^2 distribuidos en tres plantas como se muestra en la tabla 2.1.

Edificio Principal	
Piso	Área [m^2]
Planta Baja	577
Primer Piso	465
Segundo Piso	521
Total:	1563

Tabla 2.1 Área de las plantas del edificio principal de la AZEA

En la planta baja de este edificio se encuentran los departamentos que tienen mayor concurrencia por parte de los usuarios.

2.2.2 EDIFICIO SECUNDARIO

El edifico secundario de la AZEA se encuentra a 10 metros del edificio principal, su estructura está constituida de hormigón armado y paredes de bloque. Cuenta con dos plantas, cada una de las cuales tiene un área aproximada de 290 metros cuadrados.

2.3 DESCRIPCIÓN DEL SISTEMA DE COMUNICACIÓN DE DATOS

La AZEA cuenta con una infraestructura de telecomunicaciones que maneja los servicios de datos y de voz en forma independiente, existiendo un sistema de cableado para cada uno, sin embargo los dos usan las mismas rutas y canaletas para guiarse a lo largo de los edificios.

Los cables son guiados casi en su totalidad usando canaletas plásticas y metálicas a través de los distintos departamentos que conforman la AZEA y que son mostrados en el anexo A, esto se debe a que durante la construcción de los dos edificios, no se tomó en cuenta la instalación de tuberías para guiar los cables correspondientes al sistema de comunicación.

Figura 2.5 Edificio secundario, Administración Zonal Eloy Alfaro

Con el paso del tiempo, el sistema de comunicaciones ha ido creciendo sin tener en cuenta las normas ni recomendaciones de cableado estructurado aplicables al caso, por ello la red actual tiene un bajo desempeño y la tarea de detección de fallas se ha complicado.

En la red de datos se cuenta con equipos que en su mayoría son de marca 3Com, de los cuales apenas un 14% de los equipos en uso tiene capacidad administrativa.

El sistema de voz se maneja mediante una central PBX marca Panasonic, modelo KX-TDA 200 que maneja 69 extensiones internas analógicas.

La red de datos maneja distintos servicios propios de la AZEA, teniendo una gran participación aquellos que utilizan la conexión WAN para alcanzar a los servidores de la Administración General del Ilustre Municipio de Quito ubicados en la calle Venezuela y Espejo en el centro de Quito.

Entre los principales servicios se tienen: internet, correo electrónico, compartición de recursos, consultas, entre otros.

2.3.1 RED LAN

La AZEA cuenta con una red distribuida en dos edificios denominados principal y secundario conforme sus dimensiones, están constituidos en base a hormigón

armado y usan biombos y mamparas modulares para la división entre las distintas áreas de trabajo dentro de ellos.

Cuenta con una red de datos puramente cableada que hace uso de cable UTP Cat 5 y Cat 5e para guiar las señales de los distintos equipos de red, existiendo 4 racks que almacenan los principales equipos. A esto se le suma la existencia de equipos de conectividad que se han añadido fuera de los racks con el propósito de brindar nuevos puntos de red.

La red de datos mantiene una topología física en estrella, contando con los equipos de núcleo y servidores en el segundo piso del edificio principal. Los equipos de la red *LAN* mantienen la configuración de fábrica, siendo definida solamente la dirección administrativa en los equipos que lo permiten, pudiendo así ser reemplazados en forma rápida en caso de un desperfecto.

Se cuenta con 37 equipos de conectividad, mismos que se distribuyen de la siguiente manera:

- 32 switches.
- 3 routers.
- 2 hubs.

Estos equipos se encuentran instalados en racks, bajo escritorios o empotrados en las paredes. La información del piso y el departamento en el que se encuentran se muestra en el anexo I y para la ubicación específica puede referir a los planos en el anexo B.

El control, mantenimiento de todos los equipos informáticos y de redes se encuentra a cargo de la Jefatura Zonal de Informática, que cuenta con dos funcionarios especialistas en sistemas y la participación de jóvenes estudiantes de bachillerato y universitarios en calidad de pasantes. Sobre los dos funcionarios recae la responsabilidad de brindar atención inmediata ante posibles fallos en la red de datos, software y hardware de los equipos terminales y servicios.

2.3.1.1 Diagrama de la red de datos actual

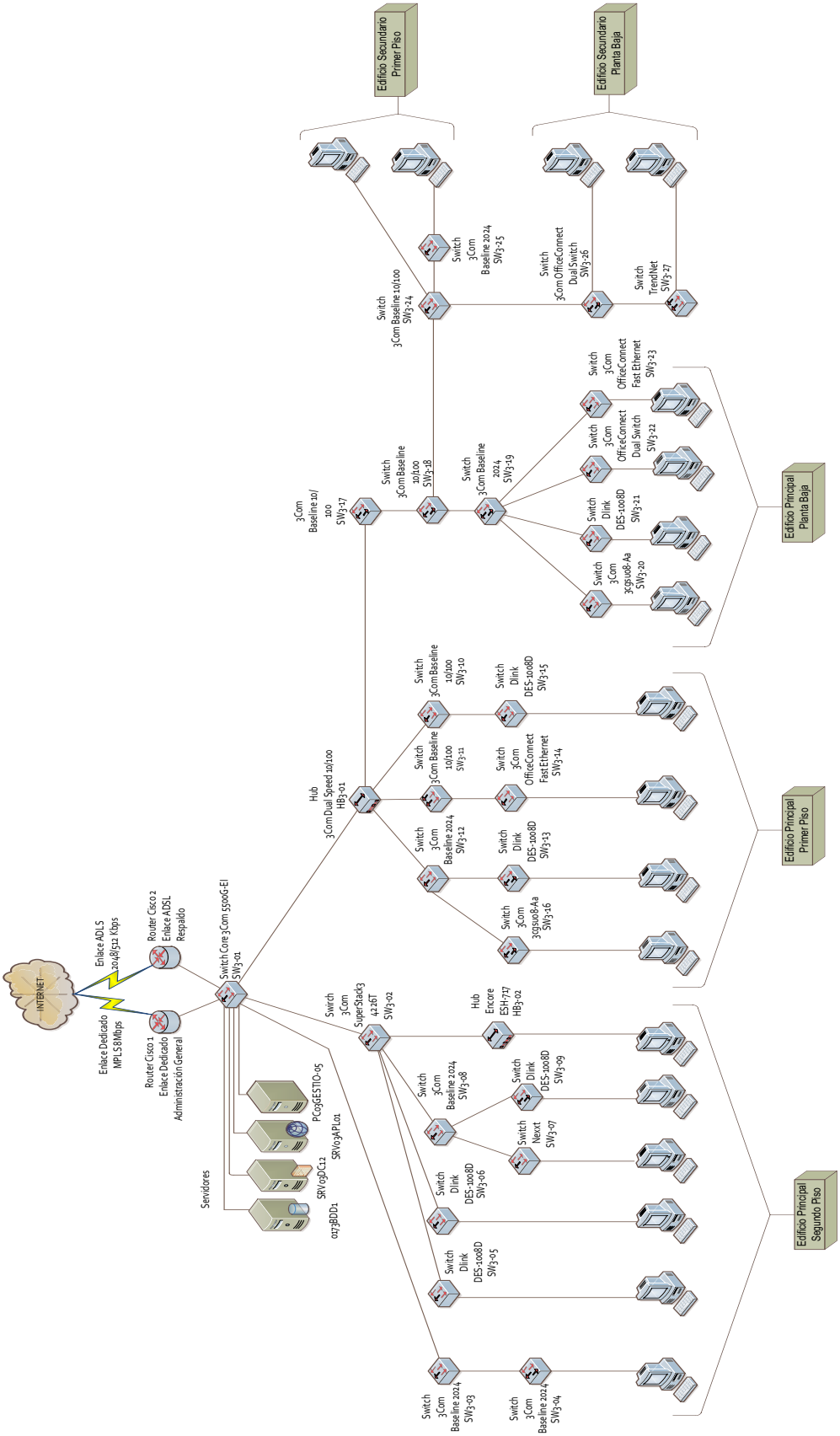


Figura 2.6 Diagrama de red de la AZEA en la actualidad

2.3.1.2 Sistema de Cableado Estructurado

Tomando en cuenta la instalación y distribución del cableado actuales a través de las instalaciones de la AZEA, se pueden enunciar las siguientes observaciones:

- En varios puntos existe una mala instalación de los cables, estos se encuentran fuera de las canaletas, presentando un riesgo de seguridad debido a que pueden ser manipulados por personas no autorizadas tal como se muestra en la figura 2.7, contraviniendo con el estándar TIA/EIA 568-C.1.

Figura 2.7 Cables de red expuestos en el cableado actual

- Algunos cables son guiados a través de agujeros en las paredes sin contar con el enrutamiento apropiado y sin protección alguna, incumpliendo el estándar TIA/EIA 569-C tal y como se aprecia en la figura 2.8.

Figura 2.8 Cables guiados fuera del edificio principal

- Algunos cables son guiados por la parte externa del edificio sin protección debido a que no se dispone de un ducto o tubería que permita la conexión entre equipos de diferentes pisos, exponiendo directamente al cableado a las condiciones climáticas entre otros riesgos, incumpliendo la norma TIA/EIA 569-C, tal como se muestra en la figura 2.8.

- En varias zonas la curvatura de los cables son mayores a las referidas en las normas de cableado estructurado incumpliendo con el estándar TIA/EIA 568-C.0, como se muestra en la figura 2.9.

Figura 2.9 Cables de red con curvaturas incorrectas

- La mayoría de los cables y los puntos de red no cuenta con una etiqueta en absoluto, y los que disponen de ella no bastan para permitir una buena administración y corrección de fallos ante posibles eventualidades, esto se ve reflejado en la figura 2.7 e incumple el estándar TIA/EAI 606-B.
- Algunas canaletas que guían a los cables de datos pasan muy cerca de los cables de alimentación eléctrica, lo cual puede inducir interferencia sobre los cables de datos, incumpliéndose la sugerencia definida en el estándar TIA/EIA 568-C.0, esto se muestra en la figura 2.10.

Figura 2.10 Equipos cerca de cables de alimentación eléctrica

- No se tiene una correcta instalación de los dispositivos de red, como es el caso del switch de núcleo que no está ubicado en el rack, sino sobre un escritorio, lo cual conlleva un entorpecimiento en la administración de esta

clase de dispositivos, incumpliéndose lo dicho en el estándar TIA/EIA 568-C.1, como se puede apreciar en la figura 2.11.

Figura 2.11 Ubicación del switch de núcleo

- El cuarto de equipos que se encuentra ubicado en la segunda planta del edificio principal no cuenta con un espacio independiente pues comparte el espacio físico con el departamento de Proyectos, dispone de un espacio físico de aproximadamente 3x3 metros en los cuales se encuentra instalado un rack y dos escritorios sobre los que se encuentran los servidores de réplica, turnos y el switch de núcleo y el sistema de puesta a tierra en el mismo es deficiente. La figura 2.12 ilustra lo descrito previamente. Esta instalación incumple las normas de cableado estructurado TIA/EIA 568-C.1, TIA/EIA-569-C, TIA/EIA 607-B.

Figura 2.12 Cuarto de equipos

- El cuarto de equipos no presenta las características mínimas de seguridad y protección de equipos, por lo que es importante, definir un espacio físico

adecuado para este fin en el rediseño acorde al estándar TIA/EIA-569-C, como puede ser apreciado en la figura 2.12.

- Las tomas eléctricas destinadas para los equipos de red en los racks también son usadas para alimentar dispositivos que no tienen relación al manejo de la red, incumpliendo la norma TIA/EIA-568-C.1.

Figura 2.13 Utilización de las tomas eléctricas del rack en otros fines

Los planos que muestran el sistema de cableado de la red de datos actual se muestra en el anexo B y la tabla 2.2 muestra el número de puntos de red actuales así como el número de racks y los cuartos de telecomunicaciones y sala de equipos.

Edificio	Planta	Puntos Actuales		Numero de Racks	Cuarto de Telecomunicaciones	Sala de Equipos
		Datos	Voz			
Principal	Segunda	50	20	1	✓	✓
	Primera	78	31	1	✓	✗
	Baja	55	17	2	✓	✗
Total		183	68	4		
Secundario	Primera	28	10	-	✗	✗
	Baja	18	11	-	✗	✗
Total		46	21	-		
Total AZEA		**229**	**89**	**4**		

Tabla 2.2 Distribución de puntos de red, cuartos de telecomunicaciones y sala de equipos en la AZEA

Los cuartos de telecomunicaciones así como la sala de equipos no disponen de un espacio exclusivo para los mismos pues se encuentran instalados en departamentos donde se encuentran funcionarios de la AZEA realizando sus labores cotidianas, es así que la tabla 2.3 muestra los departamentos en los que se encuentran dichos espacios en el edificio principal.

Planta	Cuarto de Telecomunicaciones	Ubicación (Departamento)	Sala de Equipos	Ubicación (Departamento)
Segunda	✓	Jefatura de Proyectos	✓	Jefatura de Proyectos
Primera	✓	Obras Públicas	✗	--
Baja	✓	Recaudacion	✗	--

Tabla 2.3 Ubicación de los cuartos de telecomunicaciones y sala de equipos

2.3.1.3 Edificio Principal

2.3.1.3.1 Descripción Física

El edificio principal cuenta con tres plantas, en las que se distribuyen los departamentos listados en la tabla 2.4.Se encuentra construido en base a hormigón armado y en su estructura no se contempla las instalaciones de red ni telefonía, tan solo se planificó los puntos correspondientes a la instalación eléctrica, debido a ello se usan canaletas y se han realizado orificios en las paredes para distribuir los cables necesarios con la finalidad de brindar conectividad a los distintos equipos de la AZEA.

Los departamentos pertenecientes al mismo piso se encuentran separados mediante el uso de biombos y mamparas modulares, sobre los cuales se encuentran instaladas canaletas para la distribución de los puntos de red, telefonía y tomacorrientes.

2.3.1.3.2 Red Cableada

La red cableada de datos usa cable UTP categoría 5 y 5e, así como cable categoría 3 para la interconexión de los teléfonos y la PBX, estos son manejados en forma analógica.

El sistema de comunicación de datos cuenta con alrededor de 200 puntos que aumentan y disminuyen frecuentemente debido la adición de switches de acceso, o con la readecuación de espacios.

Tanto el cableado de datos como el de voz se encuentran instalados con la ayuda de canaletas a lo largo del edificio y en ciertas zonas los cables se encuentran expuestos.

Piso	Departamentos
Planta baja	Rentas, Gestión urbana y control, Avalúos y Catastros, Balcón de Servicios, Escuela de Formación Ciudadana, Secretaría General, Jefatura zonal de Coordinación Parroquial, Coordinación Zonal de territorio, Comunicación Social, Secretaría de Coordinación, Recaudación.
Primer Piso	Coordinación de Gestión y Control Zonal, Jefatura Zonal , Control de la Cuidad, Fiscalización, Talento Humano, Obras Públicas, Jefatura Zonal de Territorio y Vivienda, Jefatura Zonal de Seguridad Ciudadana, Jefatura Zonal de Educación, Cultura, Deporte y Recreación, Subprocuraduría Zonal, Coordinación de Desarrollo Zonal, Jefatura Zonal de Salud, Jefatura Zonal De Medio Ambiente, Jefatura Zonal de obras Públicas, Parques, y Jardines, Gerencia de Espacio, Coordinación de Gestión y Control Zonal.
Segundo Piso	Jefatura Zonal de Informática, Jefatura de Proyectos, Jefatura Zonal Administrativa, Jefatura Zonal de talento Humano, Jefatura Zonal Financiera, Coordinación Zonal de Administración y Servicios.

Tabla 2.4 Departamentos en edificio principal de la AZEA

2.3.1.3.3 Planta Baja

En esta planta se encuentra los departamentos en los que se brindan los servicios más concurridos por parte de la población del Sur de Quito, debido a ello es indispensable garantizar un alto nivel de continuidad de operaciones en esta planta.

Esta planta dispone de un rack abierto de 24 unidades ubicado en una pequeña área del departamento de Recaudación junto a los equipos de respaldo de energía eléctrica UPS. En este rack se encuentran instalados dos switches marca 3Com de 24 puertos y no cuentan con un etiquetado que permita administrarlos. El personal del departamento de Recaudación tiene libre acceso al rack, a más que usa los tomacorrientes destinados a los equipos de red para otros fines.

La planta baja también cuenta con un rack abierto de pared de 8 unidades ubicado en el departamento de Archivo, en el que se encuentra instalado solamente un switch marca 3Com de 24 puertos. El personal de este departamento tiene libre acceso a este rack, constituyéndose en un riesgo de seguridad.

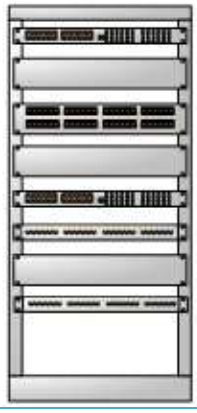
<table>
<tr><td colspan="2">Rack principal</td></tr>
<tr><td> 
</td><td>  </td></tr>
<tr><td colspan="2">Rack secundario</td></tr>
<tr><td> 
</td><td>  </td></tr>
</table>

Tabla 2.5 Diagrama de rack, planta baja, edificio principal

A los equipos instalados en los racks se le suman aquellos que están distribuidos en los distintos departamentos y que fueron añadidos debido a la necesidad de nuevos puntos de red, estos equipos se encuentran listados en la tabla 2.6.

Equipos fuera de rack				
Equipo	Marca	Modelo	Número de Puertos	Ubicación
Switch	3Com	Office Connect Dual Switch	16	Jefatura Zonal de Coordinación Parroquial
Switch	D-Link	Des1008-D	8	Secretaría General
Switch	3Com	3cgsu08-Aa	8	Balcón de Servicios
Switch	3Com	Office Connect Fast Ethernet	16	Comunicación Social

Tabla 2.6 Equipos de conectividad instalados fuera del rack en la planta baja, edificio principal

Los equipos fuera de rack son equipos que no disponen de ningún tipo de protección física ante el acceso y manipulación por parte de personal no

autorizado, sumándose su mala instalación física pues la mayoría se encuentran bajo algún escritorio o empotrados en una pared.

La tabla 2.7 muestra un recuento de los equipos terminales acorde a los distintos departamentos de la planta baja, en total se tienen 43 equipos terminales entre computadoras, laptops e impresoras de red.

Equipos terminales					
Departamento		Computador de Escritorio	Computador Portátil	Impresoras de red	Total de Dispositivos
1	Jefatura Zonal de Avalúos y Catastros	8	-	1	9
2	Comunicación Social	3	-	-	3
3	Coordinación Zonal de Territorio	-	1	-	1
4	Gestión Urbana	4	-	-	4
5	Información (Balcón de servicios)	2	-	-	2
6	Recaudación	5	-	-	5
7	Rentas	7	-	-	7
8	Secretaria General	3	-	-	3
9	Escuela de Formación Ciudadana	3	-	-	3
10	Jefatura Zonal de Coordinación Parroquial	6	-	-	6
11	Archivo	-	-	-	-
TOTAL		41	1	1	43

Tabla 2.7 Dispositivos terminales en la planta baja, edificio principal

2.3.1.3.4 Primer Piso

Los distintos puntos de red del primer piso son guiados a través de canaletas plásticas y metálicas instaladas en las paredes y modulares divisorios que convergen en un rack de 24 unidades ubicado en el departamento de Obras

Públicas. En el rack se encuentran instalados 3 switches marca 3Com de 24 Puertos y un Hub marca 3Com de 24 puertos. Este Rack no cuenta con ninguna protección ante el acceso no autorizado puesto que solo lo cubre un cartel.

Equipos fuera de rack				
Equipo	Marca	Modelo	Número de Puertos	Ubicación
Switch	D-Link	Des1008-D	8	Jefatura de Obras Públicas
Switch	D-Link	Des1008-D	8	Subprocuraduría Zonal
Switch	3Com	3cgsu08-Aa	8	Jefatura Zonal de Fiscalización
Switch	3Com	Office Connect Fast Ethernet	16	Jefatura Zonal de Seguridad Ciudadana

Tabla 2.8 Equipos de conectividad fuera del rack en el primer piso, edificio principal

En este piso se encuentra instalada la central telefónica analógica Panasonic, debido a ello se tiene una gran cantidad de cables de par trenzado que converge en este punto. Los cables pertenecientes al sistema telefónico no disponen de una adecuada organización, existiendo una gran cantidad de cables sueltos y ninguna etiqueta que permita la identificación de los mismos.

Diagrama de rack	
 Switch 3COM Baseline 10/100 Organizador Patch Panel Organizador Switch 3COM Baseline 10/100 Switch 3COM Baseline 2024 Patch Panel Organizador 3COM Dual Speed Hub	

Tabla 2.9 Diagrama de rack, primer piso, edificio principal

El cableado usado tanto en el rack como en la conexión con los equipos terminales es de categoría 5 y 5e, no cuenta con un etiquetado apropiado puesto que solo algunos cables tienen una etiqueta que describe en forma explícita su destino, haciendo sumamente difícil la administración de la red.

Dispositivos terminales					
Departamento		Computador de Escritorio	Computador Portátil	Impresoras de red	Total de Dispositivos
1	Jefatura Zonal de Control de la Ciudad	9	-	-	9
2	Coordinación de Gestión y Control	2	-	-	2
3	Coordinación de Desarrollo Zonal	1	1	-	2
4	Jefatura Zonal de Educación, Cultura, Deportes y Recreación	5	1	-	6
5	Jefatura Zonal de Fiscalización	10	-	1	11
6	Gerencia de Espacio Público (EMMOP)	1	-	-	1
7	Gestión Urbana	7	-	-	7
8	Jefatura Zonal de Medio Ambiente	4	-	1	5
9	Jefatura Zonal de Territorio y Vivienda	4	-	-	4
10	Jefatura Zonal de Obras Públicas, Parques y Jardines	9	-	-	9
11	Jefatura Zonal de Salud	7	-	-	7
12	Jefatura Zonal de Seguridad Ciudadana	6	-	-	6
13	Subprocuraduría Zonal	6	-	1	7
TOTAL		71	2	3	76

Tabla 2.10 Dispositivos terminales en el primer piso, edificio principal

En la tabla 2.9 se detallan los componentes del rack del primer piso y en la tabla 2.10 se listan los dispositivos terminales del primer piso, teniendo un total de 76 dispositivos.

2.3.1.3.5 Segundo Piso

En este piso se encuentran ubicados los servidores junto a un rack de 24 unidades compartiendo el espacio físico destinado al departamento de proyectos. En el rack se tienen instalados los equipos que brindan conectividad hacia la red WAN, contándose con un router Cisco series 800, que se enlaza hacia la Administración General del Ilustre Municipio de Quito haciendo uso de un enlace E2 (8Mbps) bajo el protocolo MPLS (*Multi-Protocol Label Switching*) mediante fibra óptica. La fibra óptica es guiada en forma aérea a través de los postes de energía eléctrica hasta el techo del edificio principal, como se muestra en la figura 2.14, donde ingresa hasta el llegar al rack correspondiente a este piso.

La AZEA cuenta con un enlace de respaldo a más del enlace de fibra óptica, este enlace utiliza un router de la misma serie, que se conecta mediante tecnología ADSL (*Asymmetric Digital Subscriber Line*) a una línea telefónica para brindar un enlace de respaldo ante un fallo en el enlace principal. La capacidad del enlace de respaldo es de 2048 Kbps de bajada por 512 Kbps de subida.

Figura 2.14 Ruta de la Fibra Óptica hasta la AZEA

En el rack se dispone de los elementos mostrados en la tabla 2.11, resaltando que el switch de la parte superior no se encuentra instalado en el rack, solo está sobrepuesto en la parte superior.

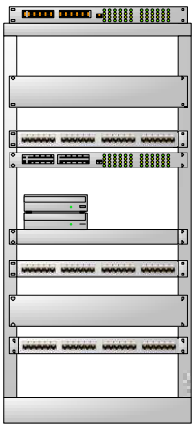
Diagrama de rack	
 Switch 3COM Baseline 2024 Organizador Patch Panel Switch 3COM Baseline 4226T Router CISCO Series 800 Router CISCO Series 800 Bandeja Fibra Optica Patch Panel Organizador Patch Panel	

Tabla 2.11 Diagrama de rack del segundo piso, edificio principal

El switch de núcleo de la AZEA es de marca 3COM, modelo 5500G-EI de 24 puertos, que no se encuentra instalado en el rack sino colocado sobre una mesa como lo muestra la figura 2.15, existiendo un gran desorden en cuanto a los cables que interconectan al resto de equipos pertenecientes al rack.

Figura 2.15 Switch de Núcleo 3Com 5500G-EI

El switch de núcleo tiene un cableado que cuenta con ciertas etiquetas que mencionan en forma explícita la proveniencia de los cables, pero debido al constante cambio en las conexiones provocadas principalmente por fallos en la red, algunos no corresponden a su etiqueta.

A más de los equipos instalados en el rack, se cuenta con equipos de red distribuidos a lo largo del piso, mismos que se muestran en la tabla 2.12.

Equipos de conectividad fuera de rack				
Equipo	Marca	Modelo	Número de Puertos	Ubicación
Switch	3Com	Baseline 2024	24	Jefatura Zonal de Informática
Switch	D-Link	Des1008-D	8	Jefatura Zonal de Financiero
Hub	3Com	3cgsu08-Aa	8	Jefatura Zonal de Financiero
Switch	D-Link	Des1008-D	8	Jefatura Zonal Administrativo
Switch	Nexxt	--	8	Jefatura Zonal de Talento Humano
Switch	D-Link	Des1008-D	8	Secretaría del Administrador
Switch	3Com	Baseline 2024	24	Coordinación Zonal de Administración y Servicios
Switch	3Com	Super Stack 4 5500G	24	Jefatura de Proyectos

Tabla 2.12 Equipos de conectividad fuera del rack en el segundo piso, edificio principal

En este piso se tiene un total de 47 equipos terminales, entre computadores de escritorio, computadores portátiles e impresoras de red, su distribución en los distintos departamentos se encuentra detallada en la tabla 2.13.

Dispositivos terminales					
Departamento		Computador de Escritorio	Computador Portátil	Impresoras de red	Total de Dispositivos
1	Administrador y Secretaría	3	1	1	5
2	Jefatura Zonal Administrativo	8	1	2	11
3	Auditorio	-	1	-	1
4	Coordinación Zonal de Administración y Servicios	2	2	1	5
5	Jefatura Zonal de Financiero	10	-	1	11
6	Jefatura Zonal de Informática	7	-	2	9
7	Jefatura de Proyectos	1	-	-	1
8	Jefatura Zonal de Talento Humano	4	-	-	4
TOTAL		35	5	7	47

Tabla 2.13 Dispositivos terminales en el segundo piso, edificio principal

2.3.1.4 Edificio Secundario

2.3.1.4.1 Descripción Física

El edificio secundario de la AZEA está construido a base de hormigón armado y cuenta con dos plantas donde se encuentran los departamentos detallados en la tabla 2.14.

Piso	Departamentos
Planta baja	Centro de Equidad y Justicia (Psicología, Trabajo Social, Área Legal y Coordinación), Comisarías de Laderas
Primer Piso	Comisaria de Salud y Ambiente, Comisaría Sur este, Comisaría Sur Oeste, Dispensario Médico.

Tabla 2.14 Distribución de los departamentos por piso, Edificio Secundario

Al igual que en el edificio principal, los departamentos pertenecientes a la misma planta se encuentran separados mediante el uso de biombos y mamparas modulares, sobre los que se encuentran instaladas canaletas para la distribución de los puntos de red, telefonía y tomacorrientes.

2.3.1.4.2 Red Cableada

El edificio secundario no cuenta con racks destinados a alojar a equipos de red, por ello estos se encuentran empotrados en las paredes. Para enlazar la red entre los dos edificios se usa un cable UTP categoría 5e que está guiado en forma subterránea a través de un tubo de PVC (*Polyvinylchloride*), este cable une un switch ubicado en el rack del departamento de Recaudación en la planta baja del edificio principal con un switch ubicado en el primer piso del edificio secundario.

2.3.1.4.3 Planta Baja

Esta planta cuenta con dos switches no administrables de 8 y 16 puertos, empotrados en las paredes en la ubicación correspondiente mostrada en la tabla 2.15.

Equipos de conectividad				
Equipo	Marca	Modelo	Número de Puertos	Ubicación
Switch	TRENDnet	TEG-S8	8	Comisarías de Laderas
Switch	3Com	Office Connect Dual Switch	16	Coordinación, Centro de Equidad y Justicia

Tabla 2.15 Equipos de conectividad en la planta baja, edificio secundario

En esta planta se tiene un total de 14 equipos terminales, tal como se muestra en la tabla 2.16.

Dispositivos terminales					
Departamento		Computador de Escritorio	Computador Portátil	Impresoras de red	Total de Dispositivos
1	Centro de Equidad y Justicia	7	1	1	9
2	Comisaria de Laderas	5	-	-	5
TOTAL		12	1	1	14

Tabla 2.16 Dispositivos terminales en la planta baja, edificio secundario

2.3.1.4.4 Primer Piso

En esta planta se cuenta con dos switches marca 3Com de 24 puertos, mostrados en la tabla 2.17.

Edificio Secundario, Primer Piso				
Equipo	Marca	Modelo	Número de Puertos	Ubicación
Switch	3Com	Baseline 2024	24	Comisaría Sur Oeste
Switch	3Com	Baseline 10/100	24	Comisaría Sur Oeste

Tabla 2.17 Equipos de conectividad en el primer piso, edificio secundario

Los switches se encuentran ubicados bajo los escritorios y no cuentan con ninguna protección física, a ello se le suma que el personal tiene libre acceso a ellos y los cables se encuentran disperso en el piso.

En el primer piso se cuenta con 27 dispositivos terminales, sin que se tenga computadores portátiles, la información detallada del número de equipos terminales y su respectivo departamento se muestra en la tabla 2.18.

Dispositivos terminales					
Departamento		Computador de Escritorio	Computador Portátil	Impresoras de red	Total de Dispositivos
1	Comisaria Salud y Ambiente	7	-	1	8
2	Comisaria Sur Este	7	-	-	7
3	Comisaria Sur Oeste	7	-	-	7
4	Dispensario Médico	3	-	-	3
5	Despacho 1	1	-	-	1
6	Despacho 2	1	-	-	1
TOTAL		26	-	1	27

Tabla 2.18 Dispositivos terminales en el primer piso, edificio secundario

2.4 EQUIPOS DE INTERCONEXIÓN

La AZEA dispone de varios equipos de interconexión que en su mayoría no han sido implementados acorde a una correcta planificación y se encuentran ubicados sin cumplir las normas de cableado estructurado.

2.4.1 EQUIPOS DISPONIBLES

En la tabla 2.19 se muestran los equipos disponibles en la AZEA, indicando si se encuentran en uso o en reserva, y de esta forma poder definir equipos que servirían de respaldo ante un posible fallo en la red.

2.4.2 CARACTERÍSTICAS DE LOSEQUIPOS DISPONIBLES

2.4.2.1 Switch de Núcleo, 3Com 5500G-EI de 24 Puertos

El switch de núcleo usado en la AZEA de marca 3Com modelo 5500G-EI de 24 puertos, es un switch administrable de capa 3.

Equipos en Uso			
Dispositivo	Marca	Modelo	Capacidad Administrativa
Router	Cisco	Series 800, 871	✓
Router	Cisco	Series 800, 877-m	✓
Hub	3Com	Dual Speed Hub	✗
Hub	3Com	Dual Speed Hub	✗
Switch	3Com	Super Stack 4 5500G	✓
Switch	3Com	Baseline 2024	✗
Switch	3Com	Super Stack 3 4226T	✓
Switch	3Com	Baseline 2024	✗
Switch	DLink	Des-1008d	✗
Switch	DLink	Des-1008d	✗
Switch	Nexxt	---	✗
Switch	3Com	Baseline 2024	✗
Switch	DLink	Des-1008d	✗
Switch	3Com	Baseline 10/100	✗
Switch	3Com	Baseline 10/100	✗
Switch	3Com	Baseline 2024	✗
Switch	DLink	Des-1008d	✗
Switch	3Com	Office Connect Fast Ethernet	✗
Switch	DLink	Des-1008d	✗
Switch	3Com	3cgsu08-Aa	✗
Switch	3Com	Baseline10/100	✗
Switch	3Com	Baseline10/100	✗
Switch	3Com	Baseline 10/100	✗
Switch	3Com	3cgsu08-Aa	✗
Switch	DLink	Des-1008d	✗
Switch	3Com	Office Connect Dual Switch	✗
Switch	3Com	Office Connect Fast Ethernet	✗
Switch	3Com	Baseline 10/100	✗
Switch	3Com	Baseline 2024	✗
Switch	3Com	Office Connect Dual Switch	✗
Switch	TRENDnet	TEG-S8	✗
Equipos en Reserva			
Router	Cisco	1841	✓
Switch	3Com	Super Stack 3 4226T	✓
Switch	3Com	Super Stack 4 5500G	✓
Switch	3Com	Baseline 2024	✗
Switch	3Com	Office Connect Fast Ethernet	✗
Switch	3Com	Office Connect Fast Ethernet	✗

Tabla 2.19 Equipos de conectividad disponibles en la AZEA

Entre sus principales características se tiene:

- Dispone de 24 puertosRJ-45 blindados que trabajan a 10BASE-T/100BASE-TX/1000BASE-T, sumados a 4 puertos de uso dual 10/100/1000BASE-T o 1000BASE-X SFP (*Small Form Factor Pluggable*).
- Cuenta con una ranura para módulo de expansión en su parte posterior.

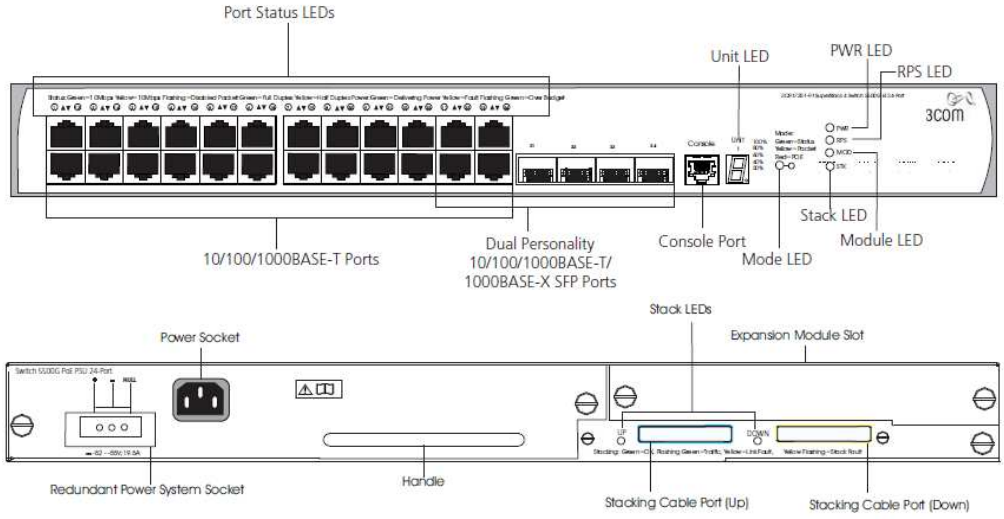


Figura 2.16 Vista frontal y posterior del switch 3Com 5500G-EI

- Soporta los siguientes estándares Ethernet:
  IEEE 802.1D (STP), IEEE 802.1p (CoS), IEEE 802.1Q (VLANs), IEEE 802.1s (MSTP), IEEE 802.1v (Protocol VLANs), IEEE 802.1w (RSTP), IEEE 802.1X (Security), IEEE 802.3 (Ethernet), IEEE 802.3ab (1000BASE-T), IEEE 802.3ad (Link Aggregation)IEEE 802.3af (Power over Ethernet, IEEE 802.3ah (Ethernet in First Mile over Point to Point Fiber — EFMF), IEEE 802.3i (10BASE-T), IEEE 802.3u (100BASE-TX/-FX),IEEE 802.3x (Flow Control),IEEE 802.3z (1000BASE-X).
- Es un switch apilable haciendo uso de la tecnología *XRN* (*eXpandable Resilient Networking*), permitiendo la apilación de hasta 8 unidades para proveer un máximo de 448 puertos usando switches de 56 puertos.
- Cuenta con una ranura para una fuente de poder redundante de -48 V DC.
- Su capacidad máxima de conmutación es de 12.8 Gbps, y 9.5 Mpps (*Million packets per second*) de tasa de envío.

- Capacidad de ruteo mediante protocolos RIP (*Routing Information Protocol*) v1, v2 y OSPF (*Open Shortest Path First*).
- Dispone de un puerto de consola que permite conectar un terminal y llevar a cabo la administración remota o local fuera de banda.

2.4.2.2 Switch 3Com Baseline 4226T

Los switches Baseline 4226T que dispone la AZEA son utilizado como switches de acceso, a pesar de tener la capacidad de definir configuraciones acordes a las necesidades de la empresa, los switches se encuentran funcionando con la configuración de fábrica.

Función	Característica
Direcciones	Se admiten hasta 8000. Hasta 64 entradas permanentes.
Negociación Automática	Se admiten en todos los puertos. MDI/MDI-X automático.
Modos de envío	Store and Forward.
Modos dúplex	Half dúplex y full dúplex en todos los puertos 10/100. Full dúplex en los puertos 1000BASE-T.
Control de Flujo	Se admiten todos los puertos en modo full dúplex.
Detección automática inteligente	Se admiten en todos los puertos. Smart auto-sensing permite negociar de forma automática los puertos que se van a supervisar, detectar un porcentaje de errores alto en un enlace, o un problema de la interconexión física a otro puerto. Y reaccionar de forma adecuada.
Asignación de prioridades de tráfico	Se admite (IEEE 802.1D): 2 colas por puerto.
Puertos Ethernet y Fast Ethernet	Negociación automática de puertos 10BASE-T/100BASE-TX.

Tabla 2.20 Características de la familia de switches 4200

Los switches 3Com Baseline 4226T son dispositivos apilables de 10/100/1000 Mbps compuestos de 24 puertos RJ-45 blindados que trabajan a 10BASE-T/100BASE-TX y 2 Puertos 10/100/1000 BASE-T.

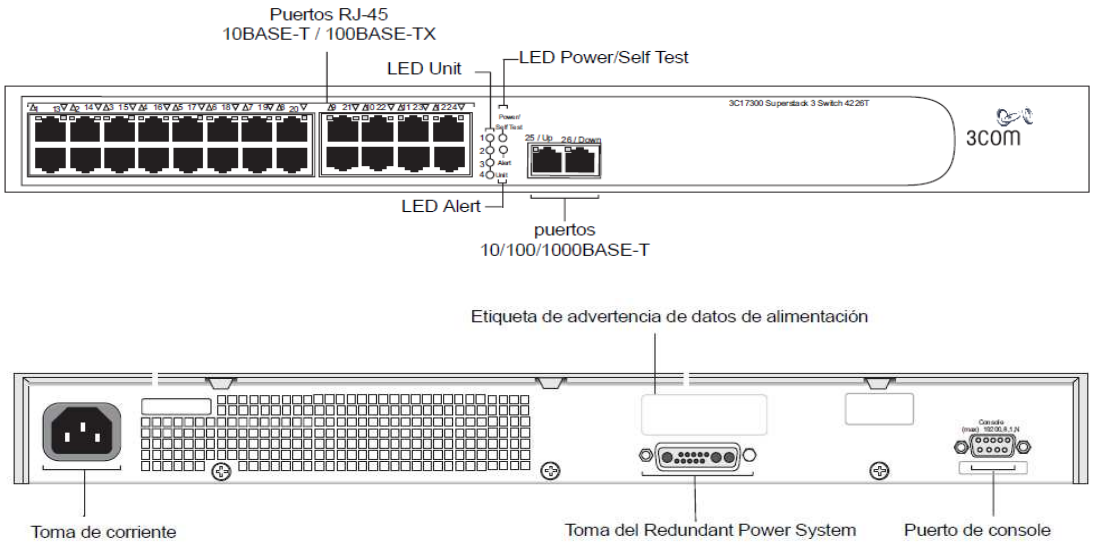


Figura 2.17 Vista frontal y posterior del switch 3Com 4226T

La tabla 2.20 muestra las principales características de la familia de switches 3Com 4200.

2.4.2.3 Switch 3Com Baseline 2024

El Switch 3Com Baseline Switch2024 es un dispositivo no administrable, versátil y de uso simple.

El switch tiene en su panel delantero 24 puertos RJ-45 blindados, de negociación automática de 10/100 Mb/s. Cada puerto determina automáticamente la velocidad y el modo dúplex del equipo conectado y brinda una conexión conmutada adecuada. Además, los puertos admiten la detección MDI/MDI-X automática.

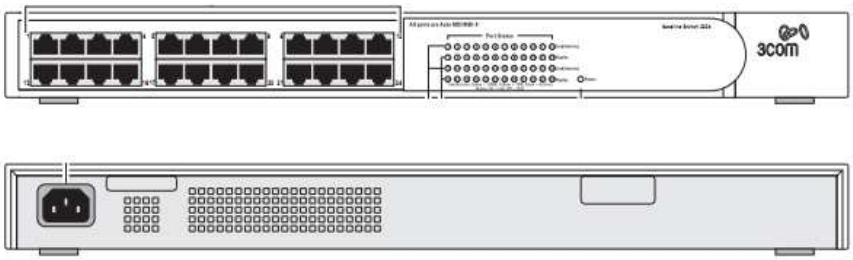


Figura 2.18 Vista frontal y posterior de Switch 3Com Baseline2024

2.4.2.4 Switch 3Com Office Connect Dual Speed/Office Connect Fast Ethernet

Los Switches 3Com Office Connect Dual Speed y Office Connect Fast Ethernet son dispositivos no administrables que permiten conexiones dedicadas de alta velocidad de 10BASE-T ó 100BASE-TX, disponen de 16 puertos RJ-45 blindados. La tabla 2.21muestra las principales características de este tipo de dispositivos.

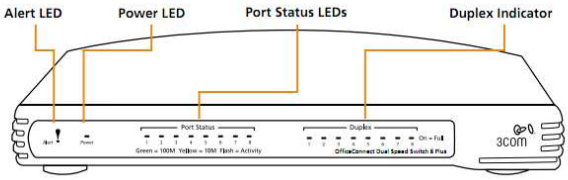


Figura 2.19 Vista frontal de Switch 3Com Office Connect Dual Speed

Función	
10/100 puertos con auto detección	16
Memoria en Buffer	1M
Puertos bidireccionales o semi-duplex con auto negociación	Todos
Soporte de direcciones MAC	2048
Método de envió	Store and Forward

Tabla 2.21 Características del Switch 3Com Office Connect Dual Speed

2.4.2.5 Switch 3com Gigabit 3cgsu08-Aa

El Switch 3ComGigabit 3cgsu08-Aa está diseñado para pequeñas oficinas y sucursales remotas que necesitan un alto rendimiento de red para intercambiar voluminosos archivos de datos e imágenes, así como acceder a la información en tiempo real, o conectarse a servidores o a una red troncal de alta velocidad.

Las principales características se encuentran listadas en la tabla 2.22 y su vista frontal y posterior se representa en la imagen 2.20.

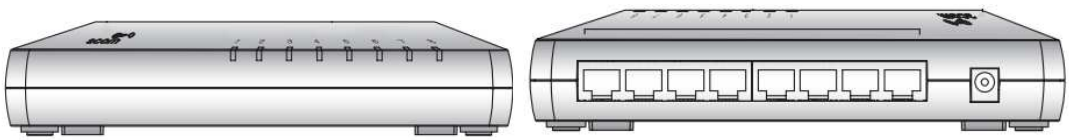


Figura 2.20 Vista frontal y posterior del switch 3com Gigabit 3cgsu08-Aa

Función	Especificación
Número Total de puertos	8 Ethernet 10/100/1000 con detección automática.
Interfaces con los medios	8 RJ-45 10BASE-T/100BASE-TX/1000BASE-TX.
Características de conmutación Ethernet	Store-and-forward; auto-negociación full-/half-duplex; priorización de tráfico 802.1p (asignación de colas de prioridad)

Tabla 2.22 Características del switch3com Gigabit 3cgsu08-Aa

2.4.2.6 Switch D-Link Des1008-D

El switch D-Link Des1008-D provee de 8 puertos con capacidad de negociar las velocidades de red entre 10BASE-T y 100BASE-TX, como también el modo de operación en Half o Full Duplex.

Su arquitectura de Parallel Switching para el modo de operación Store and Forward, permite la transferencia de datos en forma directa entre las distintas puertas, con Full Error Checking, eliminando en el tráfico de la red el envío de paquetes incompletos, fragmentados o con errores de CRC, salvaguardando de esta forma la integridad de los datos.

Figura 2.21 Switch D-Link Des1008-D

2.4.2.7 Switch Nexxt

El switch Nexxt es un dispositivo que provee 8 puertos RJ-45 con capacidad de negociar las velocidades de red entre 10BASE-T y 100BASE-TX.

Figura 2.22 Switch Nexxt de 8 puertos

2.4.2.8 Switch TRENDnet TEG-S8

El switch TRENDnetTEG-S8 es un dispositivo que provee 8 puertos RJ-45 que pueden funcionar a velocidades de 10/100/1000 Mbps. Tiene capacidad dúplex y negociación automática, usa Store and Forward como método de envío.

Figura 2.23 Switch TRENDnet TEG-S8

2.4.2.9 Hub Super Stack II Dual Speed Hub 50

El hub Super Stack II Dual Speed Hub 50 es un repetidor de 24 puertosRJ-45 blindados y que pueden trabajar a 10/100Mbps con auto-sensing.

Este hub también dispone de dos ranuras para módulos de expansión que se pueden equipar con módulos de gestión, o módulos 3Com 10Mbps o 100Mbpspara proporcionar tipos de conexión de red adicionales.

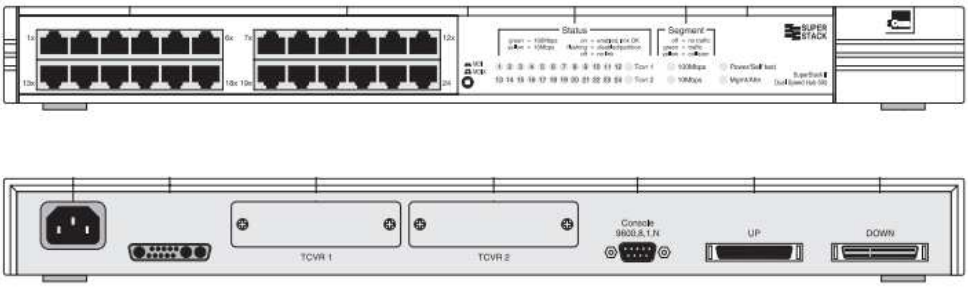


Figura 2.24 Vista frontal y posterior del Super Stack II Dual Speed Hub 50

2.4.2.10 Encore 16-Port Mini Hub ESH-717 [PW43]

El hub Encore es un repetidor que dispone de 16 puertosRJ-45 blindados que trabajan a 10BASE-T, un puerto UTP RJ-45 para la conexión entre Hubs y un puerto BNC (*Bayonet-Neill-Concelma*) para trabajar con 10BASE-2 que es una variante de Ethernet que usa cable coaxial fino. La figura 2.25 muestra la vista superior de este dispositivo.

Figura 2.25 Encore 16-Port Mini Hub ESH-717

2.5 ESTUDIO DE SERVIDORES

La AZEA dispone de cuatro servidores, ubicados en el segundo piso del edificio principal junto al rack instalado en el departamento de la Jefatura de Proyectos. Los servidores se encuentran colocados bajo un escritorio y no cuentan con protección ante su manipulación por parte de personal no autorizado.

Figura 2.26 Ubicación de los servidores de la AZEA

Nombre	Marca	Procesador	RAM	Disco Duro [GB]	Sistema Operativo	Puerto en SW de Núcleo
SRV03APL01	HP Proliant ML370GS	Intel Xeon 2 GHz	2 GB	C: 48.8 G: 156	Windows Server 2003 R2	8
0173BDD1	HP Proliant ML350	Intel Xeon 2 GHz	1 GB	C: 19.5 D: 48.7	Windows Server 2003 R2	9
PC03GESTIO-05	Clon	Intel Core i3 3 GHz	4 GB	C: 195 F: 270	Windows 7 Ultimate x86	10
SRV03DC12	IBM SYSTEM X 3200 M2	Intel Xeon 2.83 GHz	2 GB	C: 250	Windows Server 2003 R2	7

Tabla 2.23 Servidores de la AZEA

Todos los servidores se conectan al switch de núcleo 3Com 5500G-EI con el uso de cable UTP Cat 5e, el switch se encuentra ubicado sobre un escritorio que aloja en su parte inferior a los servidores, como se aprecia en la figura 2.26. La tabla 2.23 resume las principales características de los servidores.

2.5.1 SERVIDOR SRV003DC12

Dado que la AZEA maneja servicios que dependen de la Administración General del Ilustre Municipio de Quito se manejan parámetros que son definidos en dicha entidad, debido a ello, el servidor mencionado es usado como un servidor de réplica, que mantiene la configuración necesaria en cuanto a direccionamiento IP, servicios propios del IMQ[4], *DNS*. También se mantiene en este servidor una réplica de la configuración del servidor *Active Directory*.

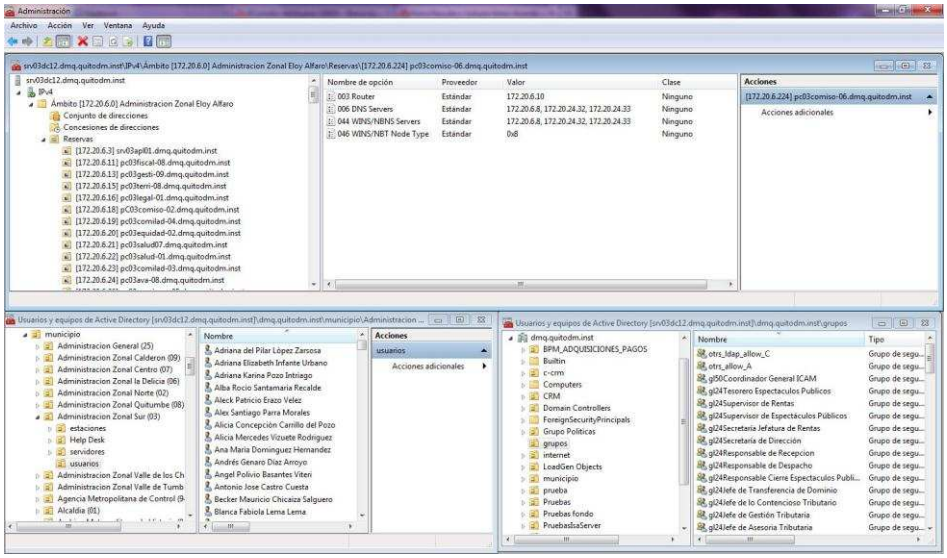


Figura 2.27 Consola de administración de Active Directory

Servidor Réplica SRV03DC12	
Dirección IP	172.20.6.8
Mascara	255.255.255.0
DNS	172.20.24.32

Tabla 2.24 Configuración de la interfaz de red del servidor SRV03DC12

[4] IMQ, *Ilustre Municipio de Quito*

2.5.2 SERVIDOR DE TURNOS PC03GESTIO-05

Para mantener el orden en los módulos que prestan servicios en la AZEA, se ha implementado un servidor que se encarga de la asignación de turnos para los departamentos de Despacho y Recepción, Avaluó y Catastro, Recaudación, Certificados y Tasas, Gestión Urbana, Línea de Fabrica, Transferencias de Dominio y Patente.

El programa implementado en este servidor se denomina SIPSE, que son las siglas de Sistemas Informáticos Para Salas de Espera, en la siguiente figura se muestra su interfaz de configuración.

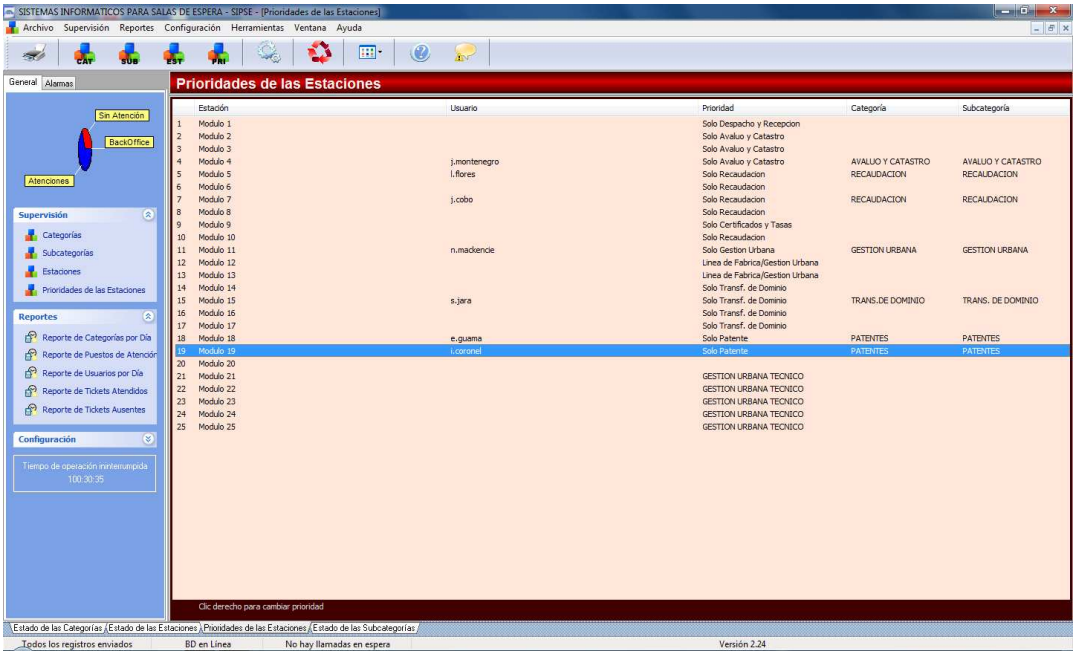


Figura 2.28 Interfaz de administración del sistema de turnos

La configuración de la interfaz de red del servidor de turnos es mostrada en la tabla 2.28.

Servidor de Tickets PC03GESTIO-05	
Dirección IP	172.20.6.192
Mascara	255.255.255.0
Gateway	172.20.6.10
DNS	172.20.6.8

Tabla 2.25 Configuración de la interfaz de red del servidor de Turnos

2.5.3 SERVIDOR SRV03APL01

Este servidor se usa para alojar el programa GDOC (Gestión Documental de Requerimientos) que permite realizar consultas, ingresos y seguimientos de los trámites que se desarrollan en el Ilustre Municipio de Quito. Además este servidor mantiene instaladores de programas usualmente requeridos, como el antivirus, AutoCAD entre otros.

Figura 2.29 Sistema de gestión documental GDOC

Servidor SRV03APL01	
Dirección IP	172.20.6.3
Mascara	255.255.255.0
Gateway	172.20.6.10
DNS	172.20.6.8

Tabla 2.26 Configuración de la interfaz de red del servidor de SRV03APL01.

2.5.4 SERVIDOR 0173BDD1

Este servidor actualmente solo se lo usa para mantener respaldos de los programas comúnmente usados, a más de la información pertinente a ciertos usuarios.

Servidor 0173BDD1	
Dirección IP	172.20.6.2
Mascara	255.255.255.0
Gateway	172.20.6.10
DNS	172.20.6.8

Tabla 2.27 Configuración de la interfaz de red del servidor de 0173BDD1

2.6 SISTEMAS Y APLICACIONES.

2.6.1 BPM, *BUSINESS PROCESS MANAGER*

Es un sistema también conocido como Tramifácil, este sistema permite a los usuarios atender a la ciudadanía mediante la obtención de permisos de construcción, licencias de construcción, licencias de funcionamiento, permisos de funcionamiento, registros de planos, inspecciones, anulaciones, declaraciones, renovaciones y solicitudes.

Este sistema actualmente lo utilizan en toda la AZEA, sobre todo en los departamentos de Gestión Urbana, Rentas, Salud y Subprocuraduría, en el que se ha vuelto una herramienta indispensable para la atención al público y la realización de trámites.

Funciona mediante Microsoft Internet Explorer 6 o superior. Su comunicación con la Administración General se da a través del proxy que se encuentra configurado en los computadores de la AZEA, este a su vez tiene configurado el puerto por defecto (puerto 80).

Los datos técnicos a cerca de este sistema, no fueron proporcionados, ya que es información sensible para el IMQ.

2.6.2 EASYTELLER [PW44]

Es un sistema cuyo objetivo es la obtención de certificados de no adeudar al municipio, además ayuda en la recaudación de impuestos y tasas, este sistema se encuentra disponible en los departamentos de Recaudación y Tesorería.

Funciona mediante Microsoft Internet Explorer 6 o superior. Su comunicación con la Administración General se da a través del proxy que se encuentra configurado en la AZEA.

Los datos técnicos a cerca de este sistema, no fueron proporcionados, ya que es información sensible para el IMQ.

2.6.3 RUMBA

También conocido como Rehosting, es una aplicación muy utilizada dentro de la AZEA ya que se conecta con la Administración General permitiendo conocer la información de los ciudadanos y siendo usada en los departamentos de Tesorería y Financiero para la obtención de partidas presupuestarias y para cálculos de presupuestos. En los departamentos de Comisarias se lo usa como consulta para tener datos del predio urbano. En Avalúos y Catastros, así como en Rentas permite realizar los trámites de transferencia de dominio.

Los datos técnicos a cerca de este sistema, no fueron proporcionados, ya que es información sensible para el IMQ.

2.6.4 OCS, MICROSOFT OFFICE COMMUNICATION SERVER [PW45] [PW46]

Es una plataforma de comunicaciones, que permite a los usuarios compartición de archivos, chat, compartición del escritorio y comunicaciones de voz y video.

El OCS está disponible en cada computador de la AZEA, y solo está habilitada la función de chat, los usuarios que dispone de una máquina podrán acceder a esta plataforma, logrando un mejor desempeño, ya que no tienen la necesidad de abandonar sus puestos de trabajo para poder comunicarse.

El cliente OCS hace peticiones de comunicación al puerto 5061 y recibe las respuestas al rango de puertos: 1024-65535. Para que el cliente se conecte necesita la IP del host remoto y las credenciales de usuario, y de esta forma es aceptado el acceso.

2.6.5 LINCE Y SIARH, *SISTEMA INTEGRADO DE ADMINISTRACION DE RECURSOS HUMANOS*

Estos sistemas son utilizados en el departamento de Recursos Humanos. Ambos sistemas permiten registrar el ingreso y salida del personal, es decir que lleva el control de asistencia, así como la nómina de los empleados.

En la puerta de acceso al personal, se encuentran los dispositivos que obtienen la información de los empleados, mediante control biométrico, esta información es almacenada a una base de datos ORACLE ubicada en un computador del departamento de Recurso Humanos.

Los datos técnicos a cerca de este sistema, no fueron proporcionados, por ser información sensible para el IMQ.

2.6.6 ICUS, *INFORME DE COMPATIBILIDAD DE USO DE SUELO*

El ICUS es un sistema integrado de gestión territorial usado en el departamento de Territorio y Vivienda. Este permite realizar consultas a cerca de predios, así como ver claves catastrales de acuerdo a la información proporcionada por el ciudadano.

Los datos técnicos a cerca de este sistema, no fueron proporcionados, ya que es información sensible para el IMQ.

2.6.7 ANTIVIRUS

En el IMQ se utiliza una red de datos con clientes Microsoft Windows, por tal motivo la necesidad de tener un antivirus es primordial. La Administración General para la protección de sus equipos clientes ha decidido utilizar la plataforma ESET Smart Security Business Edition. La plataforma ha sido distribuida a todas las administraciones y se han proporcionado los instaladores, licencia, configuraciones de clientes y manuales correspondientes.

En la AZEA toda la información necesaria para la instalación y correcto funcionamiento del antivirus se encuentra en el servidor SRV03APL01. Cada

equipo cliente, así como servidores tienen instalados el antivirus ESET, el cual se conecta a la Administración General por medio de la dirección 172.20.47.8 y puerto 2221 para obtener e instalar las actualizaciones correspondientes, cada 60 minutos.

2.6.8 CORREO ELECTRÓNICO [PW47]

El servicio de correo electrónico en la AZEA es proporcionado por el servidor de SRV003DC12 y los clientes son manejados a través de la aplicación Microsoft Office Outlook 2007. Este servicio ha permitido que los funcionarios de la AZEA puedan enviar y recibir correos electrónicos dentro de la misma red, además admite la transferencia de correos entre los usuarios en distintas administraciones dentro del Municipio de Quito

El servicio está habilitado para todos los usuarios en la AZEA y se puede acceder al mismo presentado las credenciales correctas. Además Microsoft Office Outlook 2007 tiene configurado para la transferencia de mensajería, los protocolos POP3 y SMTP.

2.6.9 INTERNET

En la AZEA el servicio de internet es proporcionado al 90% de usuarios, este servicio es muy importante ya que la mayoría de empleados que usan internet necesitan ingresar o consultar información en páginas estatales, descargar software, así como actualizaciones del sistema operativo o del software instalado en cada computador.

Dependiendo del cargo que ocupen dentro de la administración, los usuarios tienen acceso controlado a este servicio mediante el servidor proxy, ubicado en la Administración General. El control que se proporciona se lo hace mediante la dirección IP configurada en cada computador y por la dirección IP y el puerto del servidor proxy, mostrado en la tabla 2.26, configurado en los navegadores web. Los navegadores web que se encuentran instalados en los computadores de la AZEA son: Internet Explorer, Mozilla Firefox y Google Chrome.

El control de contenido al que no tienen acceso los empleados, está dirigido principalmente a redes sociales, videos online, audio online, descarga de audio y/o video, chat, servidores de descarga y contenido que implique un alto consumo de los recursos de red y que no tengan relación con las funciones que los empleados deben cumplir.

2.6.10 DNS

El servicio DNS en la AZEA es manejado por el servidor SRV003DC12. Si el DNS local no logra resolver el nombre o la dirección, enviará aquella consulta a los servidores DNS ubicados en la Administración General y estos a su vez si no logran resolver la consulta la reenviarán a servidores DNS externos pre configurado.

La información de los servidores DNS, no fue proporcionada, ya que es información sensible para el IMDQ.

2.6.11 DHCP

El servicio de DHCP se encuentra configurado en el servidor réplica. Este servicio permite a la AZEA una asignación dinámica de direcciones IP a los dispositivos de red como computadores.

En la AZEA el rango de direcciones usado para asignación dinámica va desde 172.20.6.1 a 172.20.6.254, exceptuando la dirección del default-gateway: 172.20.6.10 y las direcciones de los servidores: tabla 2.22, tabla 2.23, tabla 2.24 y tabla 2.25.

Cabe mencionar que la AZEA ya ha ocupado casi en su totalidad el rango de direcciones disponibles en la dirección de red 172.20.6.0 con máscara de red 255.255.255.0.

2.6.12 PROXY

El servicio Proxy se encuentra configurado en un servidor remoto y se lo alcanza a través del enlace *WAN*, este servicio proporciona a la red de la AZEA los

parámetros de configuración necesarios para acceder a los servicios de la Administración General, mediante un navegador web, así también permite el acceso a internet. Los parámetros de configuración se muestran en la tabla 2.28.

Este servicio ha sido implementado para controlar el uso de internet, mediante la configuración manual en cada navegador de las estaciones de trabajo. Si los usuarios desean acceder a internet, al ingresar la dirección de un sitio web en un navegador, la petición es dirigida por el proxy, el cual en base a su lista de reglas permite o no el acceso, si la dirección es permitida, el usuario podrá ingresar en el sitio web, caso contrario el proxy devuelve el mensaje del servidor indicando que no es permitido el acceso a la página web ingresada.

Dirección IP	Puerto
172.20.24.3	80

Tabla 2.28 Parámetros de configuración del Servidor Proxy

La información del servidor proxy, no fue proporcionada por tratarse de información sensible para el IMQ.

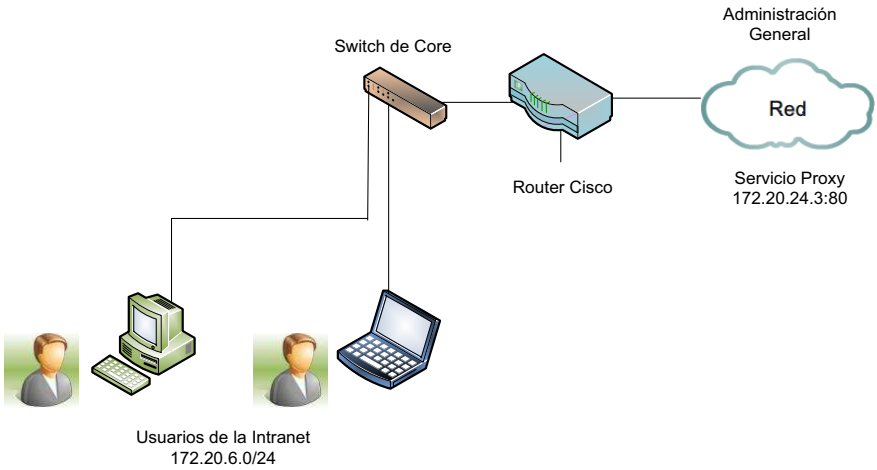


Figura 2.30 Esquema de funcionamiento del Proxy

2.7 RED DE VOZ

El servicio de telefonía de la AZEA cuenta con una central PBX de tipo propietario marca Panasonic modelo KX-TDA 200 hibrida, instalada en el primer piso junto al

rack del departamento de Obras Públicas y hace uso de la PSTN para llamadas externas a través de la infraestructura de la Corporación Nacional de Telecomunicaciones.

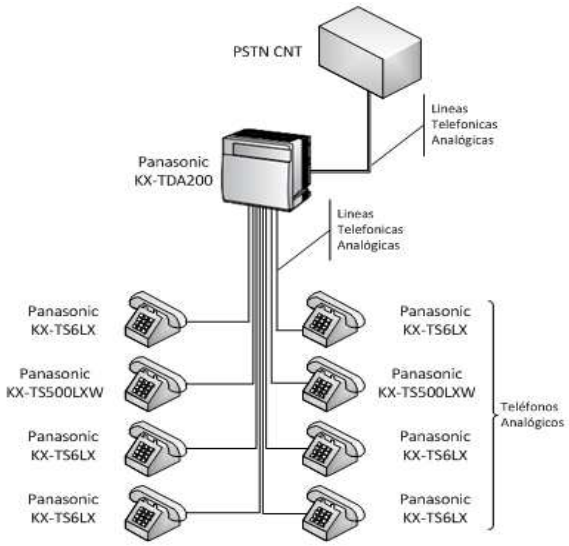


Figura 2.31 Esquema de red telefónica

2.7.1 DESCRIPCIÓN DEL SISTEMA DE TELEFONÍA PANASONIC KX-TDA200 [PW48]

El sistema profesional híbrido KX-TDA200 permite su expansión con la instalación de tarjetas adicionales y añadiendo teléfonos. Todas las ranuras de expansión son universales por lo que cualquier tarjeta universal puede ser conectada en cualquier ranura.

El software del sistema y la información de la base de datos local se encuentran almacenados permanentemente en una tarjeta SD.

El sistema cuenta con interfaces RS-232 y USB para su programación, a más de ello brinda la opción de programarlo a través de internet con la utilización de un modem.

Figura 2.32 Sistema Panasonic KX-TDA200

En términos de capacidad de sistema, el KX-TDA200 puede ofrecer hasta 192 puertos con 128 teléfonos inalámbricos.

2.7.1.1 Tarjetas Universales instaladas en el sistema telefónico

EL sistema telefónico de la AZEA cuenta con 9 tarjetas universales instaladas para su central telefónica, siete de ellas están dedicadas a las extensiones internas y las dos restantes son usadas para la conexión hacia la PSTN, su detalle se muestra en la tabla 2.29.

Figura 2.33 Centralita Telefónica Panasonic KX TDA-200

Slot	Tarjeta	Función
1	LCOT 16	Tarjeta de 16 líneas troncales analógicas
2	LCOT 8	Tarjeta de 8 líneas troncales analógicas
3	SLC 8	Tarjeta de 8 extensiones unilínea.
4	SLC 16	Tarjeta de 16 extensiones unilínea.
5	DHLC 8	Tarjeta Híbrida para 8 extensiones digitales y/o analógicas.
6	SLC 16	Tarjeta de 16 extensiones unilínea.
7	SLC 16	Tarjeta de 16 extensiones unilínea.
8	SLC 16	Tarjeta de 16 extensiones unilínea.
9	SLC 16	Tarjeta de 16 extensiones unilínea.
10	--	--

Tabla 2.29 Tarjetas Instaladas en la PBX Panasonic KX-TDA200

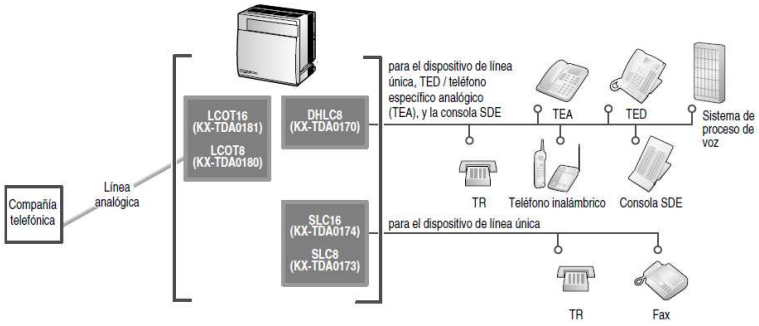


Figura 2.34 Tarjetas universales para la PBX Panasonic KX-TDA200

2.7.2 USUARIOS ACTUALES

Actualmente en el sistema se encuentran conectadas 69 extensiones telefónicas para servicios internos de la AZEA, las que se encuentran distribuidas en los dos edificios que la conforman.

Debido al crecimiento y cambio continuo de funcionarios y espacios físicos, el sistema de numeración no mantiene un orden general, y existen puntos de voz que no se encuentran en funcionamiento debido a que el cableado se encuentra en mal estado.

La central telefónica maneja 6 troncales telefónicas conectadas hacia la red de telefonía pública de la Corporación Nacional de Telecomunicaciones, adicionando 2 líneas directas que son usadas para el envío y recepción de faxes y para el departamento de comunicación social.

Extensión Telefónica	Ubicación
1xx	Edificio Principal, Planta Baja
2xx	Edificio Principal, Primer Piso
3xx	Edificio Principal, Segundo Piso
4xx	Edificio Secundario

Tabla 2.30 Asignación de extensiones telefónicas por piso

A los distintos usuarios se les ha asignado extensiones de tres dígitos, siendo el primer digito el identificador del piso o edificio al que pertenecen, tal como se muestra en la tabla 2.30.

Para la comunicación interna el marcado se lo hace en forma directa, mientras que para realizar llamadas a números fuera de la AZEA se requiere un código de salida.

La distribución de las extensiones se muestra en el anexo D. Todos los teléfonos son analógicos o convencionales, a excepción del teléfono usado por el administrador zonal que se encuentra ligado a los servidores de telefonía de la administración general del IMQ.

La infraestructura telefónica actual de la AZEA tiene un tiempo de vida aproximado de 10 años, a lo largo de este tiempo se han suplido las necesidades debidas al crecimiento de usuarios mediante la adición de tarjetas de expansión llegando a utilizar casi en totalidad la capacidad de expansión de la PBX.

2.8 CONEXIÓN HACIA OTRAS DEPENDENCIAS

La AZEA cuenta con un enlace dedicado *MPLS* a través de fibra óptica, cuya capacidad es 8 Mbps (E2) para su comunicación con la Administración General. Esta conexión es usada para el tráfico de los servicios propios del IMQ, así como del tráfico hacia internet.

También se ha contemplado una posible falla del enlace, para ello se dispone de un enlace de respaldo ADSL de 2048 kbps de bajada por 512 kbps de subida.

2.9 DIRECCIONAMIENTO IP

La AZEA mantiene alrededor de 200 usuarios que comparten un solo dominio de broadcast bajo un solo esquema de red.

La red se implementa usando las direcciones disponibles en la red 172.20.6.0, con máscara de red 255.255.255.0. Este direccionamiento brinda la posibilidad de usar 254 direcciones para los dispositivos de red como los computadores, impresoras de red, routers, switches, etc.

Actualmente se tiene problemas en la asignación de direcciones IP pues no se ha administrado en forma correcta la asociación entre los usuarios y sus respectivas direcciones, provocando una inconsistencia en la tabla y la posterior dificultad en la asignación de direcciones a nuevos usuarios.

El anexo C muestra las direcciones IP asignadas a los equipos de la AZEA.

2.10 DESCRIPCIÓN DE LA SEGURIDAD EN LA RED

Teniendo en consideración que el edificio que aloja las instalaciones no fue construido para brindar los servicios que presta actualmente, se pueden identificar graves falencias en cuanto a la seguridad física. A ello se le suma la inexistencia de políticas de seguridad.

Uno de los mayores problemas que tiene la AZEA es la falta de espacios físicos destinados a alojar a los equipos de red en los que se mantenga un correcto control acceso y climatización. Los racks están instalados compartiendo el espacio con oficinas y por ende se encuentran vulnerables a la manipulación e incluso robo por parte de personas no autorizadas. A esto se le suma el uso de las fuentes de alimentación eléctrica en otros fines como es el caso de conexión de cafeteras u otros dispositivos ajenos al sistema de telecomunicaciones.

No existen políticas de seguridad definidas por el departamento de informática de la AZEA, aumentando los riesgos de sufrir algún percance debido a acceso no autorizado.

Las contraseñas de acceso a los computadores que manejan los usuarios son muy simples y no contemplan cambio periódico, convirtiéndose en un gran riesgo puesto que a más de permitir el acceso a los computadores, estas sirven para la autenticación de diversos servicios como el correo electrónico.

Los equipos de red como el switch de núcleo se encuentran configurados con los parámetros por defecto del fabricante, permitiendo que usuarios no autorizados puedan accederlos y realizar cambios en su configuración.

Los puertos de los equipos de red administrables no están deshabilitados como medida de prevención ante el acceso no autorizado.

Los dispositivos de red permiten realizar conexiones usando el protocolo Telnet, lo cual implica enviar texto no cifrado y por ende constituye una falencia en la seguridad de la red.

2.11 ESTUDIO DEL TRÁFICO

Para la recopilación de información sobre el tráfico que atraviesa principalmente los enlaces de la AZEA, se usó la herramienta Colasoft Capsa 6.9 Enterprise Edition que dispone de una serie de herramientas para obtener el tráfico de una red IP y analizarlo. Los datos de tráfico fueron recolectados en el periodo de Julio a Septiembre de 2011.

Con el uso de Colasoft se monitorizó un puerto en el switch de núcleo (3Com 5500G) por el cual el tráfico a registrarse era duplicado usando la característica de Port Mirroring endicho switch.

También se recopiló información con la herramienta PRTG Network monitor, durante la semana comprendida entre el 10 y 14 de octubre del 2011, valiéndose para ello de SNMP (*Simple Network Management Protocol*) en el switch de núcleo.

Los puertos monitorizados corresponden al enlace WAN entre la AZEA y la Administración General del Distrito Metropolitano de Quito, al enlace de respaldo y el puerto del servidor local que brinda los servicios de DHCP, DNS y Proxy.

2.11.1 ENLACE WAN

El enlace WAN que dispone la AZEA es un enlace simétrico dedicado, que tiene una capacidad de 8192 kbps. Por el atraviesa el tráfico correspondiente a internet y a los distintos servicios propios de la AZEA.

En la figura 2.35 se puede apreciar la tendencia del tráfico a lo largo de los días de la semana comprendida entre el 22 y 26 de agosto del 2011, observándose un claro patrón de repetición.

Se aprecia claramente dos zonas en las que se tiene una gran cantidad de tráfico que atraviesa la red, la primera zona corresponde al tráfico de actualización del servidor de réplica, mismo que maneja los servicios de DNS, DHCP y Proxy, esta actualización se inicia a las 3:00 AM y finaliza a las 3:30 AM en promedio.

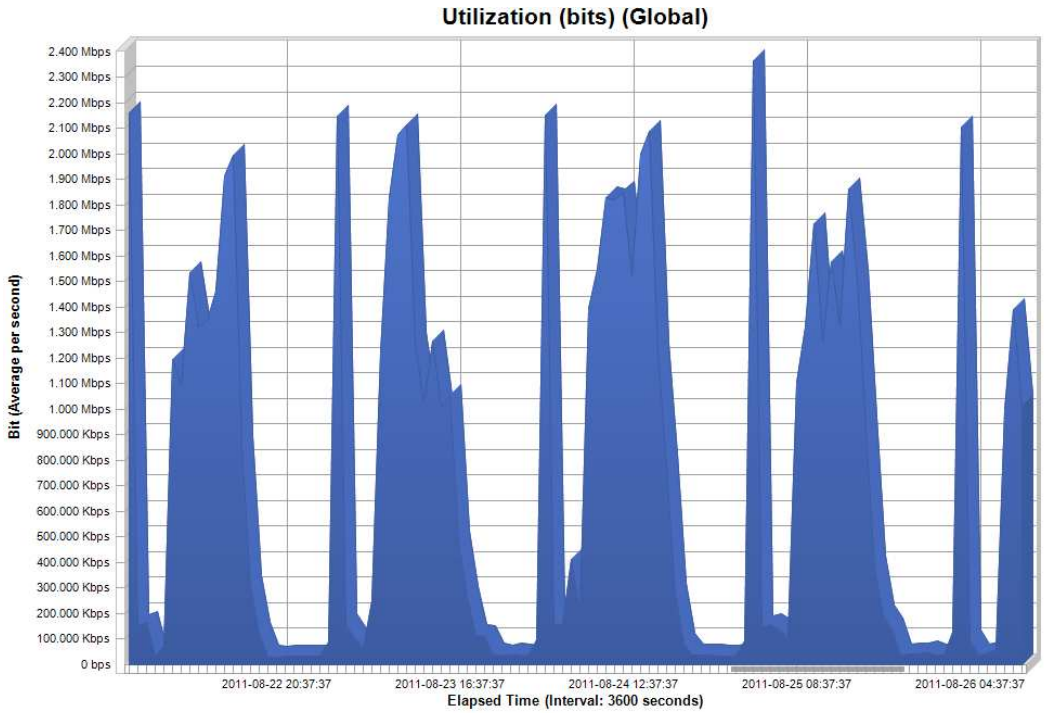


Figura 2.35 Utilización del enlace WAN en una semana

La segunda zona corresponde al tráfico perteneciente al uso de los diferentes equipos y servicios de red que empieza desde las 8:00 AM y finaliza a las 7:00 PM en promedio, esto debido a que el horario de atención al público es de 8:00 AM a 4:00 PM y algunos funcionarios continúan trabajando fuera de este horario.

En la figura 2.36 se puede notar la utilización del enlace WAN con un intervalo de 1 hora, en base a ella se puede definir que el enlace WAN no llega a saturarse pero existen picos en los que la utilización llega casi al 100%. En promedio su uso se encuentra por debajo de los 5 Mbps correspondiendo a un 62% del mismo.

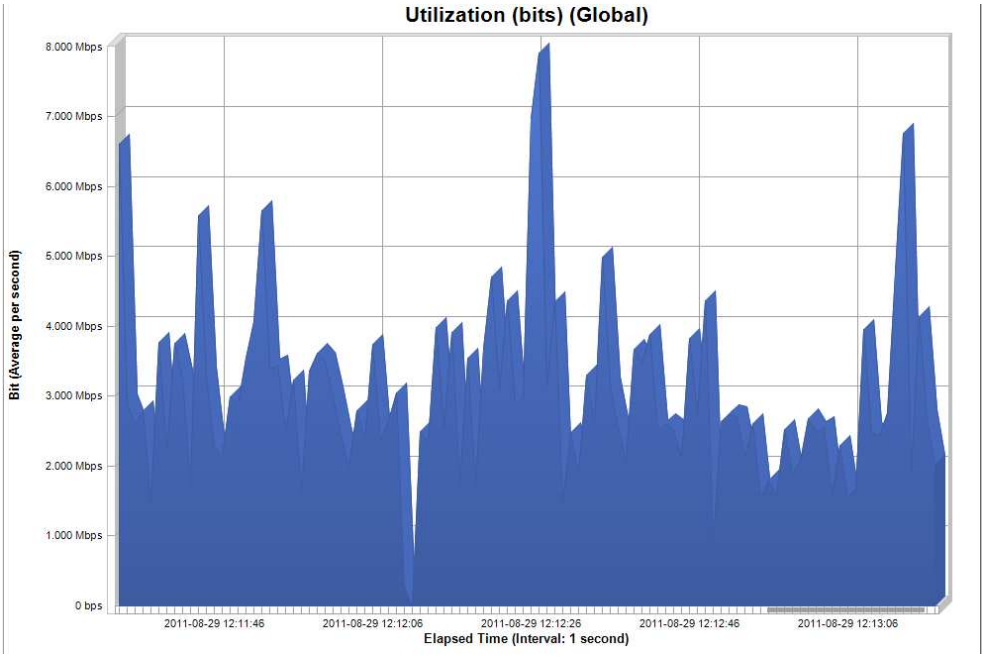


Figura 2.36 Tráfico en el enlace WAN en un día

Capacidad	Velocidad Máxima	Porcentaje	Uso Promedio	Porcentaje
8124 kbps	7911 kbps	97.38%	4997	61.51%

Tabla 2.31 Utilización del enlace WAN

2.11.2 ENLACE DE RESPALDO

El enlace de respaldo de la AZEA corresponde a un enlace ADSL (*Asymmetric Digital Subscriber Line*) de 2048kbps de velocidad de bajada por 512 kbps de subida.

Este enlace se monitoreó usando Colasoft, obteniendo como resultado que el tráfico que lo atravesaba fue prácticamente nulo, indicando que el enlace WAN de 8 Mbps es el que se usa para todo el tráfico.

También se utilizó la herramienta PRTG Network Monitor sobre el enlace para obtener una gráfica en el tiempo. En la figura 2.37 se aprecia el uso del enlace de respaldo y claramente se define una actividad muy baja, siendo el promedio de velocidad de 1Kbps.

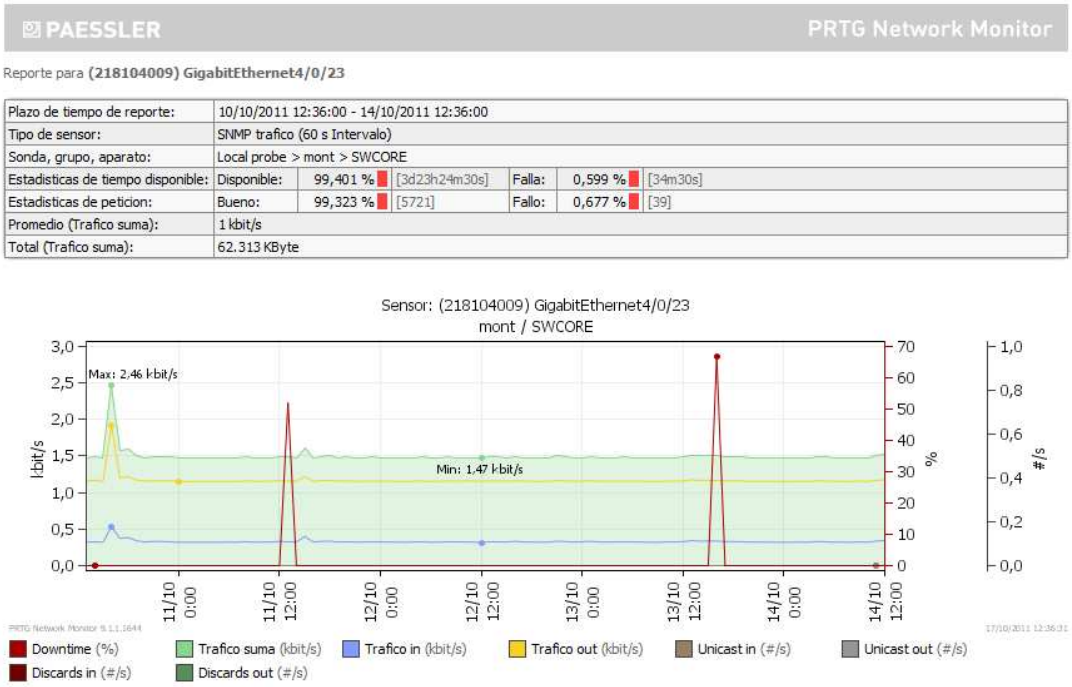


Figura 2.37 Tráfico del enlace de respaldo

2.11.3 PROTOCOLOS

Para obtener la información correspondiente a los protocolos dentro de la red, se usó las herramientas que ofrece Colasoft. Se monitorizó el tráfico de los servidores así como el de los equipos clientes. En la figura 2.36 se muestra el porcentaje de utilización de los protocolos en el tiempo comprendido entre Julio y Septiembre.

Como se puede apreciar en la figura 2.38, los protocolos más usados son: HTTP (*Hypertext Transfer Protocol*), CIFS (*Common Information File System*), entre otros. HTTP es el protocolo más utilizado debido a que una gran cantidad de servicios que presta la AZEA son gestionados mediante una interfaz web como es el caso del Tramifácil VPM, Teller, entre otros, a esto se le suma las consultas a internet en las páginas permitidas por el servidor proxy.

Dentro de los protocolos referidos como otros se encuentran aquellas conexiones entre los servidores de actualizaciones de definiciones de virus, tráfico DHCP, consultas a los servidores DNS, entre otros.

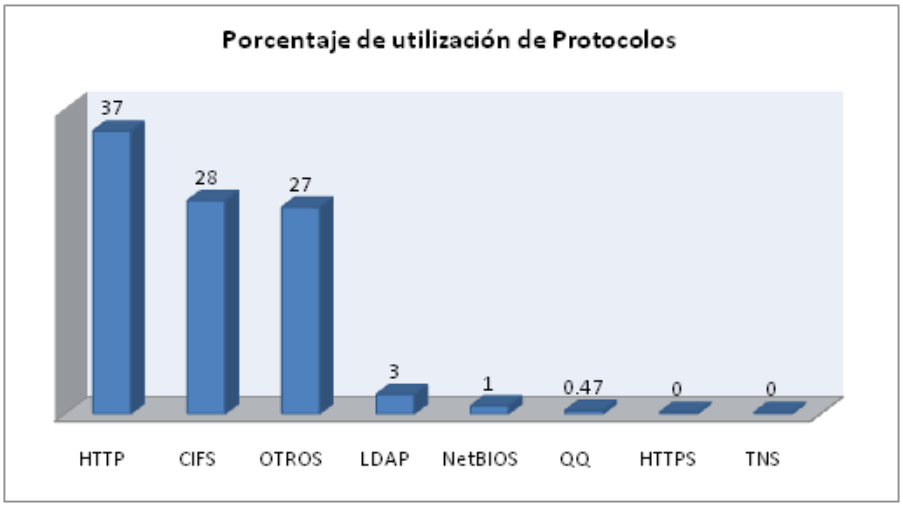


Figura 2.38 Porcentaje de utilización de los protocolos en AZEA

2.12 RESULTADOS DEL ANÁLISIS DE LA SITUACIÓN ACTUAL

Con los resultados del análisis de los elementos pasivos y activos de la red de la AZEA, se definirá el estado actual de la red enfocada en los siguientes aspectos:

- Rendimiento
- Escalabilidad
- Disponibilidad
- Administración
- Seguridad

2.12.1 RENDIMIENTO

Los elementos de la red de datos de la AZEA de mayor demanda son los servidores, en especial el servidor proxy, que se le adjudica un tráfico de entrada del 21.58% y uno de salida de 4.71% en base a todo el tráfico de la red. Este servidor no se encuentra en la AZEA por lo que es necesario que todo el tráfico entre este y el resto de dispositivos atraviese el enlace WAN.

El servidor local de mayor ocupación es el de réplica (SRV03DC12), al que se adjudica un tráfico de entrada de 3.07% y salida de 15.38%.

El servidor de tickets tiene una demanda sumamente baja a lo largo del día de trabajo, su capacidad de procesamiento se mantiene como media en 2% y la memoria RAM se usa en un 50%. La memoria se encuentra subutilizada pues a pesar que el servidor tenga instalada una capacidad total de 4GB para gestionarla se utiliza un sistema operativo Windows 7 a 32 bits, limitando a 3GB la memoria RAM.

El servidor SRV03APLI01 que es usado como servidor respaldo de archivos tiene una ocupación baja, en promedio la capacidad de procesamiento usada es de 5% y memoria en un 45%.

Los servidores de SRV03APLI01 y 0173BDD1 se encuentran funcionando con un margen de espacio libre en los discos duros muy bajo, debido a que fueron destinados a almacenar respaldos, pero no se hizo un correcto seguimiento de los datos que contienen, hasta el punto de saturarlos de información.

El switch de núcleo de la red (3Com 5500G), ha fallado algunas veces, debiéndose principalmente a fallas en el cableado subyacente, a esto se le suma que el equipo de conectividad enlazado a este switch y que deriva la conexión hacia toda la administración excepto el segundo piso del edificio principal es un Hub, afectando considerablemente el desempeño de la red.

El rendimiento también se ve afectado por el uso de Hubs de 8 puertos que solo funcionan a 10 Mbps, reduciendo el rendimiento de los equipos conectados.

La central telefónica Panasonic solo dispone de un Slot universal adicional para su extensión, limitando su futuro crecimiento.

El enlace WAN, por el cual atraviesa todo el tráfico destinado hacia internet o hacia la Administración General, es usado en un 61.51% en promedio, llegando en puntos de mayor demanda a 99.38 %.

2.12.2 ESCALABILIDAD

Los principales problemas identificados están relacionados con el cableado y los equipos de conectividad.

El cableado en la red no está basado en estándares, afectando en gran medida la confiabilidad, a eso se le suma la falta de puntos de conectividad en los equipos, lo cual ha provocado la adición de equipos no planificados.

Los equipos de conectividad no se encuentran organizados acorde a un modelo de planificación, esto se debe principalmente a la adición de switches de acceso para brindar conectividad a nuevas estaciones de trabajo en forma desordenada, mismos que son conectados a cualquier puerto libre de un switch o hub cercano, a ello se le suma la falta de documentación en los cambio que ha sufrido la red.

Los cambios en la red tales como la adición de switches y/o cables no son administrados en forma centralizada, pues la persona encargada del mantenimiento general de la infraestructura puede hacerlos sin que exista una autorización previa por parte de la dirección de informática.

2.12.3 DISPONIBILIDAD

La red de la AZEA se ve afectada constantemente por problemas debidos a fallas en los equipos de conectividad y fallas en los cables UTP, a esto se le suma las fallas en la energía eléctrica.

A pesar que la AZEA dispone de un UPS ante un fallo en la energía eléctrica, este no se encuentra instalado y funcionando para que pueda dar soporte ante un eventual corte de energía en forma imprevista.

Durante el periodo de recopilación de datos el enlace WAN no ha sufrido fallas, siendo el principal problema los equipos de conectividad internos. La mayoría de equipos que dispone la AZEA no son administrables, haciendo muy difícil poder implementar configuraciones destinadas a mejorar la disponibilidad.

Uno de los principales problemas es generado por la manipulación indebida, esto se da por la inexistencia de políticas de seguridad en cuanto al acceso físico y por la mala instalación de los cables UTP en las canaletas, permitiendo que personal no autorizado tenga acceso a ellos.

2.12.4 ADMINISTRACIÓN

La AZEA no cuenta con un plan de administración interno de la red, a esto se le suma que la mayoría de switches no son administrables y los que tienen esta característica no son usados para recopilar información del estado de la red.

Dentro de los inconvenientes en la administración se tiene el incumplimiento en cuanto a las normas ANSI/EAI/TIA, siendo el etiquetado de cables y equipos el mayor problema pues impide el localizar averías en forma rápida.

Otro inconveniente es la falta de un registro actualizado que permita conocer los activos locales y remotos de la red. No se tiene una herramienta de administración de red que permita conocer el estado de los distintos componentes de la red.

2.12.5 SEGURIDAD

La AZEA se enfrenta a varias amenazas internas, siendo una de las principales el acceso por parte de personal no autorizado a servidores y equipos críticos de conectividad, ya que los equipos no cuentan con un espacio físico exclusivo para alojarlos.

La información que circula a través de red lo hace en texto plano, lo que en conjunto con el acceso a puntos de red puede permitir la utilización de herramientas de sniffing.

Se tiene configurado un servidor proxy que limita las páginas a las que pueden acceder los usuarios de la red, excluyendo especialmente aquellas que permiten descargas de archivos y video streaming.

No existen lineamientos de seguridad en cuanto a la asignación de contraseñas y su cambio periódico.

2.13 REQUERIMIENTOS PARA EL REDISEÑO

Tomando en cuenta las necesidades actuales de la AZEA, se definen los siguientes requerimientos para el diseño de su nueva red de datos:

- Transmisión de audio y video en tiempo real para suplir las necesidades de telefonía, videoconferencia y streaming de video.
- Brindar el servicio de telefonía IP a los jefes de los distintos departamentos y a los miembros del personal que necesitan tener acceso a este servicio con el fin de acelerar los diferentes procesos que son llevados en la AZEA al eliminar la necesidad de desplazarse físicamente para comunicar un mensaje.
- Brindar el servicio de videoconferencia sobre el auditorio, teniendo como fuentes de señal las oficinas de los principales jefes de los departamentos de la AZEA y los diferentes centros de desarrollo comunitario con el fin de mantener reuniones y dictar clases sin la necesidad de desplazarse físicamente.
- Brindar el servicio de streaming de video a través de una máquina que genere la señal y permita que los dispositivos clientes accedan a dicha señal para presentarla a los ciudadanos que esperan ser atendidos en las instalaciones de la AZEA.
- Definir políticas de seguridad en los dispositivos de red para atenuar los riesgos a los que se encuentra expuesta con el fin de aumentar la continuidad del servicio que se presta a los ciudadanos.
- Definir una configuración de los servidores de correo, DNS, Proxy y DHCP que provean a la red de las configuraciones acordes a las características de la red de la AZEA disminuyendo al máximo posible los problemas que puedan presentarse debido a configuraciones incorrectas en los equipos terminales.

2.13.1 ANÁLISIS DE REQUERIMIENTOS

Del estudio anterior se puede definir que es necesario el definir una red que permita optimizar el funcionamiento de los equipos existentes, haciendo uso de las características que brindan los mismos.

A continuación se definen los requerimientos para el rediseño de la red para la integración de voz, datos y video teniendo en cuenta un crecimiento en 5 años.

2.13.1.1 Infraestructura de Cableado Estructurado

Acorde al estudio de la situación actual es necesario definir un nuevo sistema de cableado estructurado pues el sistema actual no permite una administración correcta del sistema. El cable de red no ha sido instalado siguiendo los normas sugeridas por los estándares ANSI/EIA-TIA, a esto se le suma la falta casi total de etiquetas, el enrutamiento de los mismos fuera de las canaletas.

Para la nueva infraestructura de cableado estructurado se requiere:

- Correcta identificación de cables mediante el uso de etiquetas para la documentación y administración de la red.
- Correcta instalación de los equipos de red en los racks, así como la organización e identificación de los cables en los mismos.
- Cumplir las normas enunciadas en las normas de cableado estructurado ANSI/EIA-TIA.
- Mejorar la seguridad física en cuanto al acceso de los cuartos de equipos y telecomunicaciones destinando espacios exclusivos para este fin.
- Mejorar condiciones de climatización dentro de los cuartos de equipos y telecomunicaciones evitando inconvenientes debidos al sobrecalentamiento y acumulación de polvo.
- Mejorar el sistema de respaldo de energía ante un posible fallo en la red eléctrica pues aunque existen los equipos destinados a este fin, estos no se encuentran instalados para suplir esta falencia.

2.13.1.2 Estructura de la red LAN

En cuanto a la red LAN de la AZEA se requiere:

- Incrementar la disponibilidad, ya que la red deberá soportar más servicios de red que los que actualmente maneja.
- Características de administración y gestión de los equipos activos facilitando la tarea de monitorear, detectar y corregir fallos en la red.
- Definir las características de los nuevos servidores destinados a alojar los servicios a implementarse.
- Definir políticas de administración y seguridad.

2.13.1.3 Requerimientos para la integración de voz, datos y video

Debido a que el servicio de telefonía y video pasarán a formar parte del tráfico de la red de datos se requiere el dimensionamiento de una red capaz de soportarlos, teniendo en cuenta los siguientes requerimientos.

2.13.1.3.1 Funciones del sistema de telefonía IP

El sistema de telefonía IP debe reemplazar al sistema de telefonía analógico que se tiene en funcionamiento, acorde a la cantidad de usuarios existentes en la administración y tomando en cuenta el crecimiento futuro se requiere un aproximado de 80 extensiones.

La migración hacia el sistema de telefonía IP haya su razón de ser en la centralización de la administración de la red que en conjunto con la facilidad de configuración y adición de nuevos usuarios permite un crecimiento más dinámico y ordenado de la red, a ello se le suma la poca capacidad de expansión que dispone la central telefónica actual y el desorden existente en el cableado de la red telefónica analógica actual.

2.13.1.3.2 Funciones de streaming de video

El video y audio de la señal generada a través de un servidor de *streaming* debe ser recuperada por los equipos que la requieran, tomando en cuenta que la señal será reproducida en al menos 20, monitores alrededor de la AZEA.

Este servicio es ofrecido acorde a la necesidad de presentar la información correspondiente a los procesos necesarios a seguir para acceder a los diferentes servicios ofrecidos en la AZEA a más de presentar las distintas campañas e iniciativas que son propulsadas dentro de la administración con el fin de incentivar la participación de todos los ciudadanos a formar parte de las mismas.

2.13.1.3.3 Funciones de Videoconferencia

Se requiere un servidor de videoconferencia que permita la interacción entre el Auditorio de la AZEA y los 3 Centros de Desarrollo Comunitario, para la futura implementación de clases virtuales.

Este servicio es ofrecido acorde a la necesidad de realizar reuniones entre los agentes directivos de los diferentes centros de desarrollo comunitario y el administrador zonal o los representantes de sus intereses, sin la necesidad el desplazamiento y pérdida de tiempo involucrado en dicho proceso al ser realizado en forma personal. A esto se suma un futuro plan de impartir clases virtuales de diferente índole desde la AZEA a los diferentes CDC’s con el objeto de mejorar la calidad de vida de los ciudadanos que se hallan bajo esta administración.

CAPÍTULO 3

DISEÑO DE LA RED Y PLANES DE MIGRACIÓN Y CONTINGENCIA

3.1 SISTEMA DE CABLEADO ESTRUCTURADO

3.1.1 INTRODUCCIÓN

La infraestructura actual con la que cuenta la Administración Zonal Sur Eloy Alfaro no cumple con los estándares de cableado estructurado requeridos para garantizar un correcto desempeño de la red de datos, debido a esto se presenta el siguiente diseño enfocado en dar soporte a los servicios requeridos que serán implementados en lo posterior.

La AZEA cuenta con dos edificios en los que se encuentran distribuidos los distintos departamentos que la conforman.

El edificio principal cuenta con tres pisos que albergan alrededor de 150 usuarios de la red de datos.

3.1.2 DISTRIBUCIÓN DE LOS PUNTOS DE CABLEADO POR ÁREAS

Conforme a las características físicas de sus instalaciones, se han agrupado los distintos departamentos del edificio principal, por pisos y se ha conformado un solo grupo con los usuarios del edificio secundario, existiendo una densidad promedio de 48 usuarios actuales por área.

A continuación se presenta un resumen de las áreas en las que se debe brindar acceso a la red, estas se encuentran divididas de acuerdo a los pisos y a los edificios:

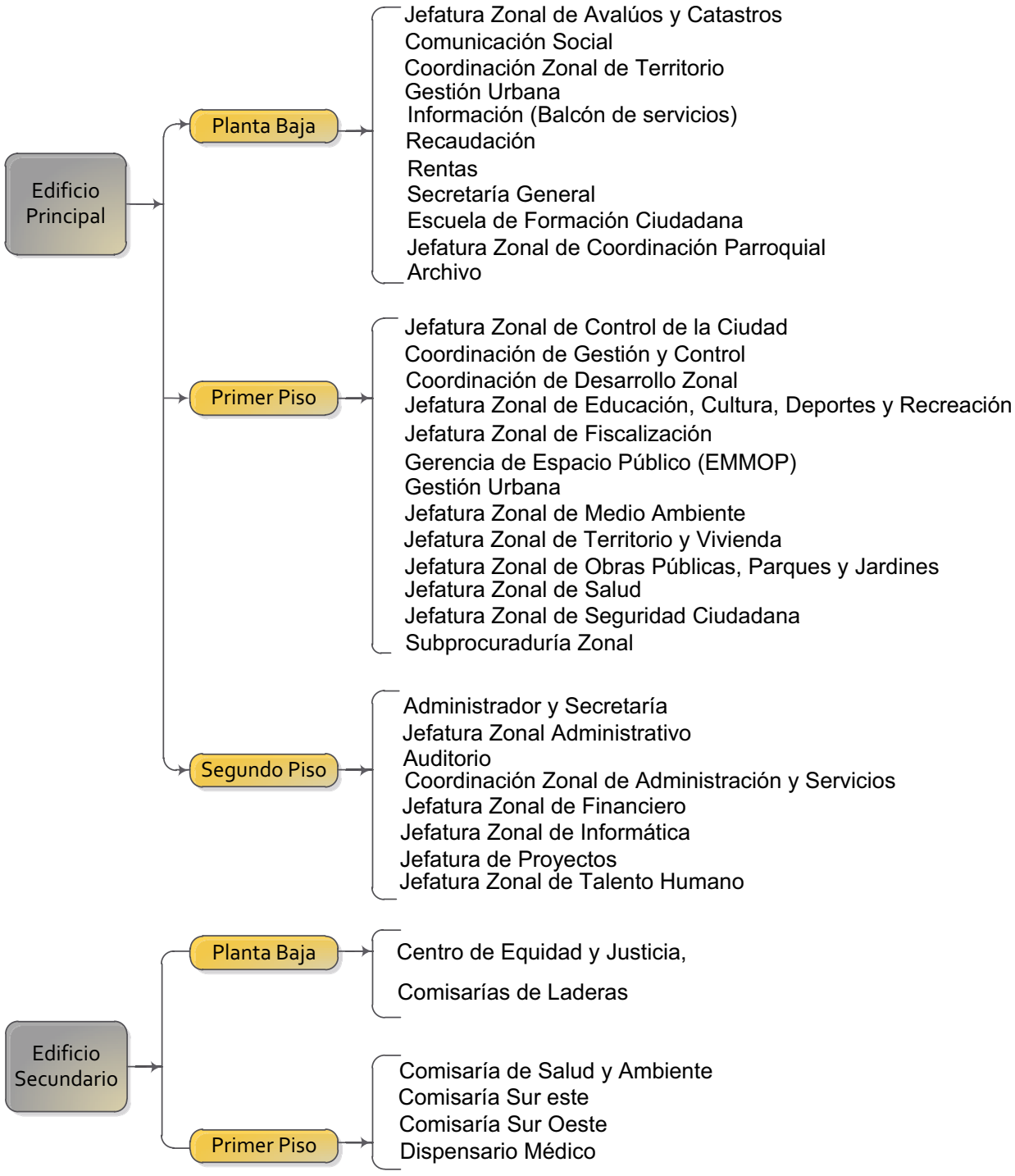


Figura 3.1 Áreas de la AZEA.

3.1.2.1 Edificio Principal

Para empezar el rediseño de la red es necesario definir el número de usuarios actuales y definir una tendencia de crecimiento a futuro, para ello se consultó a los funcionarios del departamento de Recursos Humanos acerca del personal existente desde Diciembre del año 2008, hasta Noviembre del 2011. Estos datos son mostrados en la figura 3.2.

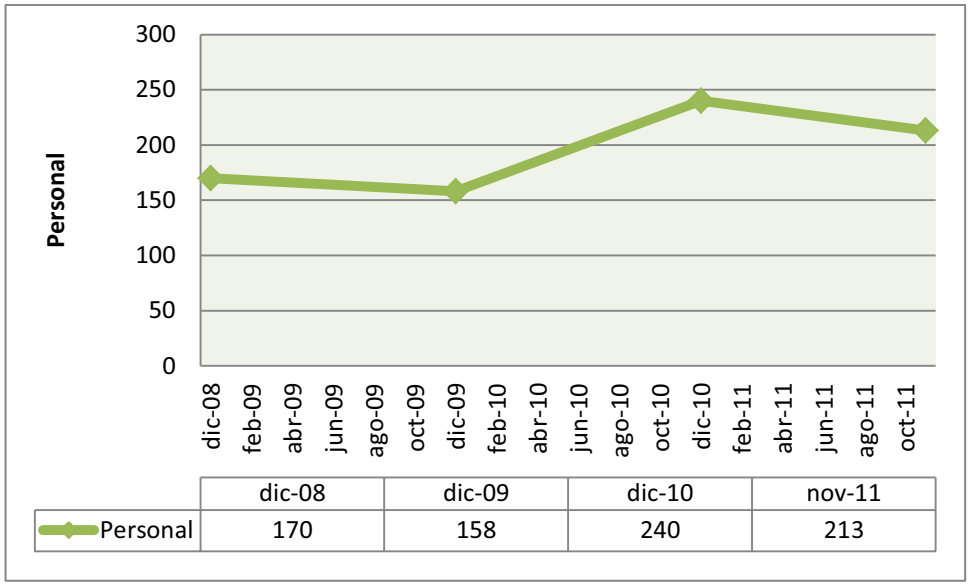


Figura 3.2 Personal de la AZEA desde el año 2008

Acorde a los datos proporcionados por el personal de la AZEA, a noviembre del 2011 existían 213 personas trabajando activamente, y de ellas alrededor de 170 usuarios utilizan la red de datos, sumándose a los equipos de impresión en red que suman 13 y 15 usuarios adicionales contemplados en los eventos a ser realizados en el auditorio, se tiene un máximo de 198 usuarios en la red actual.

Tomando en cuenta que el crecimiento de usuarios en el edificio principal se ve limitado por el espacio físico disponible, debido a que las áreas provistas con el uso de divisiones modulares han sido ocupadas casi en su totalidad, es imposible el mantener el crecimiento de usuarios mostrado en el intervalo de tiempo total señalado en la gráfica, que corresponde a un 25.3%, por lo que el crecimiento será decidido en función de la cantidad de usuarios que pueden ser instalados en los diferentes espacios de las instalaciones de la AZEA.

Acorde a los datos presentados anteriormente, se ha definido un crecimiento promedio del 17% a 10 años en cuanto al número de puntos de red, sustentándose en la información proporcionada y las características físicas del edificio.

El resumen del crecimiento a presentarse en los distintos pisos de los edificios de la AZEA es presentado en la tabla 3.1, el detalle de los puntos de red así como teléfonos analógicos existentes y proyectados para el rediseño se presentan en el anexo E.

Puntos de Acceso de Telecomunicaciones							
Edificio Principal							
Planta	Área [m^2]	Actual			Rediseño		
		Datos	Voz	Total	Datos	Voz	Total
Planta Baja	577	55	17	72	66	21	87
Primer Piso	465	78	31	109	88	34	122
Segundo Piso	521	50	20	70	61	20	81
TOTAL:	1563	251			290		
Edificio Secundario							
Planta	Área [m^2]	Actual			Rediseño		
		Datos	Voz	Total	Datos	Voz	Total
Planta Baja	290	18	11	29	20	10	30
Primer Piso	290	28	10	38	40	12	52
TOTAL:	580	67			82		

Tabla 3.1 Resumen de puntos de datos y voz actuales y futuros por pisos

De acuerdo a las proyecciones presentadas en la tabla 3.1, es necesaria la instalación de 372 puntos de red para cubrir la demanda de conectividad futura de los usuarios y equipos de la AZEA.

3.1.3 ASIGNACIÓN DE GRUPOS DE USUARIOS

Con la finalidad de mejorar la administración y proporcionar los servicios de red es importante definir grupos de usuarios acorde a las características comunes de los servicios de red que cada grupo requiere.

En base a las características presentes en la distribución de los departamentos, es posible agrupar a los diferentes departamentos según el piso al que

pertenecen, esto se debe a que se mantiene una distribución organizacional acorde a la similitud de funciones por piso.

Es así que se definen 4 grupos de usuarios, relacionados por el piso o edificio de pertenencia:

- Grupo 1: Comprenderá la planta baja del edificio principal.
- Grupo 2: Comprenderá el primer piso del edificio principal.
- Grupo 3: Comprenderá el segundo piso del edificio principal.
- Grupo 4: Comprenderá todo el edificio secundario.

3.1.4 REDISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO

El sistema de cableado actual presenta grandes falencias en cuanto a seguridad y administración como se evidenció en el capítulo anterior, a esto se suma la inexistencia de una red de cableado que permita brindar el servicio de telefonía IP, por lo que es necesario definir un nuevo esquema de cableado que se ajuste a los requerimientos de la red multi-servicios. Los planos que muestran la distribución de los puntos de red así como la ubicación de los elementos de conectividad pueden hallarse en el anexo B.

3.1.4.1 Áreas de Trabajo

Para establecer las áreas de trabajo de la AZEA, se hace referencia a los departamentos existentes en cada planta de los dos edificios. Tomando en cuenta que la norma TIA/EIA 569-A define que un área de trabajo es aquella donde los usuarios interactúan con los equipos de telecomunicación.

Dentro de cada departamento existen divisiones modulares que dividen el área de trabajo de cada usuario, estas áreas en conjunto con las posibles nuevas áreas a ser creadas serán tomadas en cuenta para la definición de los puntos de datos y voz.

De acuerdo a las necesidades de cada usuario, se destinarán como mínimo una salida de datos en cada área de trabajo. En la instalación de puntos de red

adicionales se tomará en cuenta los lugares donde se tenga necesidad de salidas extras debido a la existencia de otros equipos de red, como impresoras de red y telefonía IP, por lo tanto deberá aumentar el número de puntos, ya que deben existir al menos dos salidas de voz por cada departamento, aumentando su cantidad dependiendo del número de usuarios.

Cada área de trabajo contará con la conexión necesaria mediante el uso de canaletas plásticas, *face-plates* que contengan un número de salidas acorde al área con sus respectivos jacks RJ-45. Los pares trenzados utilizarán el estándar T568B, como se muestra en la figura 3.3.

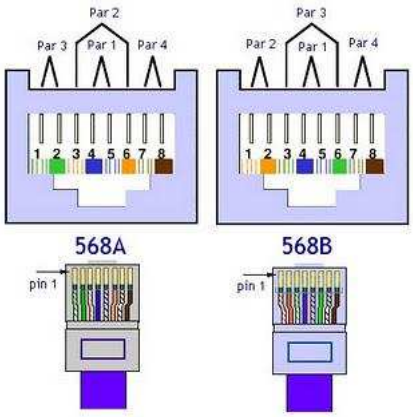


Figura 3.3 Estándar T568B [PW49]

3.1.4.2 Cuarto de Equipos

El cuarto de equipos se mantendrá en el segundo piso del edificio principal, ya que este punto brinda ciertas características adecuadas que son recomendadas por la norma EIA/TIA 569-A, como:

- Altura Mínima de 3 metros.
- No se tienen tuberías de agua alrededor o sobre el cuarto.

Sin embargo estas características deben complementarse con ciertas medidas destinadas a mejorar este espacio, como:

- Mejorar el acceso físico para que sólo personal autorizado pueda manipular los equipos.
- Mejorar el respaldo de energía.

- Mejorar la climatización.
- Mejorar la distribución y organización de los cables de datos.

El cuarto de equipos también es definido como punto de demarcación para los enlaces contratados a la CNT, pues hasta este punto llegan los enlaces de fibra óptica y el cable telefónico usado para el enlace *ADSL*.

3.1.4.3 Cuartos de Telecomunicaciones

Tomando en cuenta que la norma EIA/TIA 568-C recomienda que la distancia máxima desde los cuartos de telecomunicaciones hasta la estación de trabajo no debe superar los 100 metros, incluidos los *patch cords* y la norma TIA/EIA 569-C que sugiere la existencia de un cuarto de telecomunicaciones por piso o por edificio, se define asignar un cuarto de telecomunicaciones por cada piso del edificio principal y uno para el edificio secundario tal como se muestra en la tabla 3.2.

Edificio	Área	Ubicación del cuarto de Telecomunicaciones	Puntos de Red y Datos	Área del piso a cubrir [m^2]
Principal	Planta Baja	Departamento de Recaudación	87	577
	Primer Piso	Departamento Obras Públicas	122	465
	Segundo Piso	Departamento de Proyectos	81	521
Secundario	Primer Piso	Comisaría Sur Oeste	82	580

Tabla 3.2 Ubicación de las Salas de Equipos en cada una de las áreas

El cuarto de equipos y los cuartos de telecomunicaciones se distribuirán según se muestra en las figuras 3.4 y 3.5.

3.1.4.4 Puesta a Tierra [PW50] [PW51] [PW52] [PW53] [PW54]

Tomando en cuenta que la puesta a tierra da una vía directa al voltaje que puede estar presente en el chasis de los equipos, es de gran importancia el definir dicha

vía acorde al estándar TIA/EAI-607-B, con el fin de evitar posibles daños a los equipos y al personal humano que trabaja con ellos.

Como punto inicial es necesario en mencionar que el estándar TIA/EIA-607-B define que los racks o gabinetes que sean usados en la instalación deben ser eléctricamente continuos, a mas que es necesario el aterrizar los equipos a tierra sin importar que cuenten en su cable de poder con el terminal de conexión a tierra, a ello se suma el uso de conductores, empalmes y conectores certificados.

Como parte general del sistema de puesta a tierra en la AZEA se tienen los elementos mostrados en la figura 3.4.

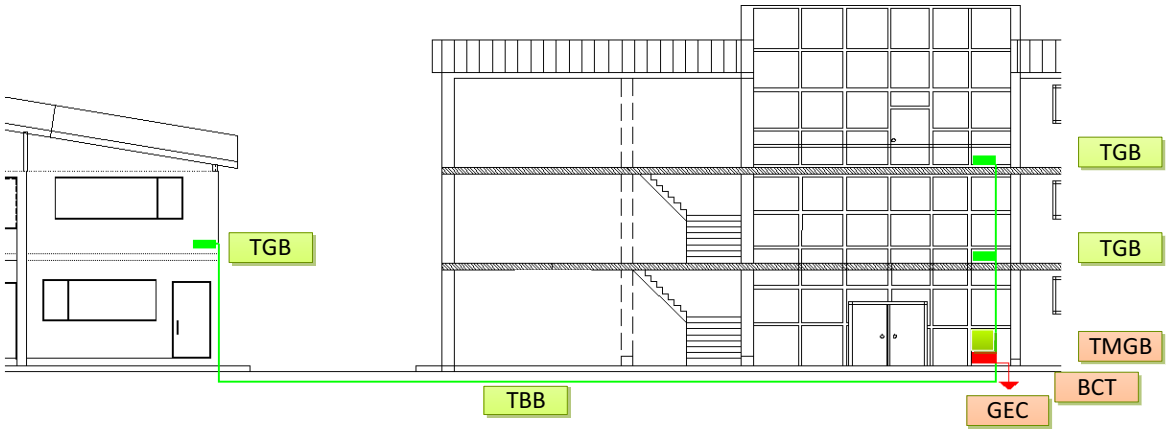


Figura 3.4 Esquema general de puesta a tierra

Componentes:

- TMGB (*Telecommunications main grounding busbar*), es una barra de cobre con perforaciones roscadas, debe tener como mínimo 6 mm de espesor, 100 mm de ancho y el largo adecuado para la conexión de los cables provenientes de las 3 TGB.
- TGB (*telecommunications grounding busbars*), se encuentran ubicadas en la cuarto de equipos y en cuarto sala de telecomunicaciones, en estas barras se conectaran las conexiones a tierra de los equipos mediante un conductor denominado TEBC. Debe tratarse de una barra de cobre con perforaciones roscadas y perforaciones necesarias para alojar a todos los cables que lleguen desde los equipos de conectividad cercanos.

- TBB (*telecommunications bonding busbars*), es un conductor que une a la TMGB con las distintas TGB. Es un conductor cuyo diámetro mínimo es 6 AWG para distancias de hasta 4 metros, y debe incrementarse su tamaño en 2 kcmil por pie lineal, debiéndose instalar un conductor de diámetro 4/0 AWG para unir el TGB del cuarto de telecomunicaciones del edificio secundario con el TMGB ubicado en el edición principal acorde a la distancia que los separa. Este conductor no debe tener empalmes en ningún punto de su recorrido.
- BCT (*Bonding Conductor for Telecommunications*), es un conductor que debe tener al menos el mismo tamaño del TBB y que une a la TMGB con la puesta a tierra general del edificio, teniéndose para ello un conductor de diámetro 4/0 AWG para el presente caso.
- GEC (*Grounding Electrode Conductor*), es el conductor usado para unir el electrodo de puesta a tierra a BCT.
- RGB (*Rack Grounding Busbar*), se trata de una barra que se sitúa en los racks o gabinetes. Esta barra dispone de una serie de perforaciones roscadas que permitirán la conexión de los cables provenientes de los equipos de conectividad, esto puede verse en la figura 3.5.

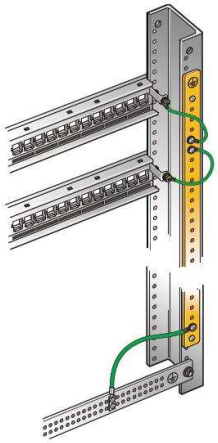


Figura 3.5 Barra de tierra vertical en un rack

- TEBC (*Telecommunications Equipment Bonding Conductor*), es un conductor que conecta el TMGB o TGB a los RGB en los racks, debe existir una separación mínima de 50 mm a los cables de poder.

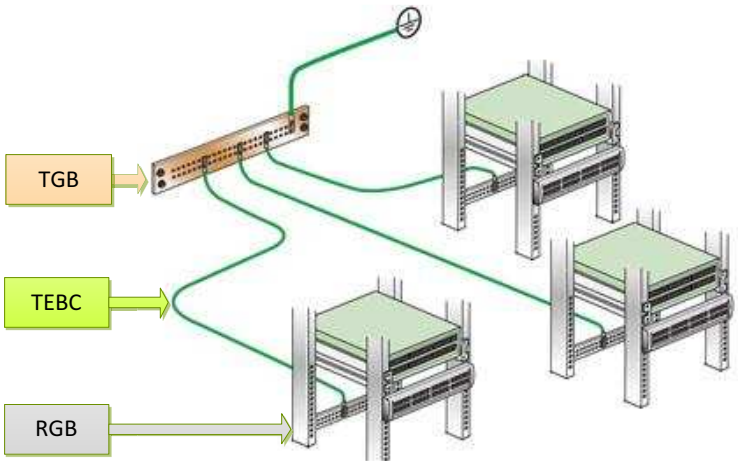


Figura 3.6 Conexión de los racks a la puesta a tierra

Finalmente todos los equipos de conectividad deben conectarse a tierra mediante un conductor de un calibre mínimo 12 AWG.

3.1.4.5 Cableado Horizontal

El cableado existente en la AZEA no cumple con las normas internacionales y se encuentra deteriorado por la mala instalación y administración del mismo, lo que impide su reutilización para el nuevo sistema. Debido a ello es necesario la definición de un sistema de cableado nuevo.

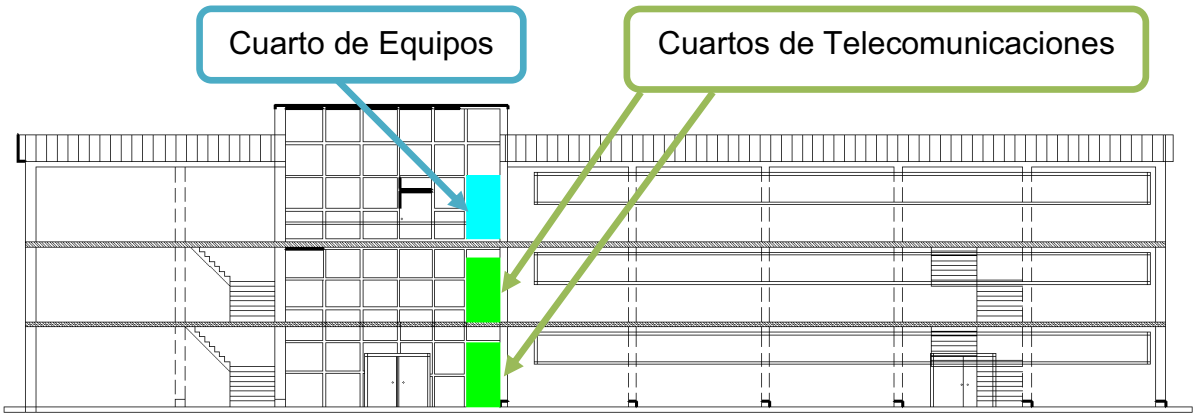


Figura 3.7 Cuartos de Telecomunicaciones, Edificio Principal

Con el objeto de soportar los servicios requeridos por la AZEA a implementarse, se recomienda el uso de cable UTP Cat 6 para la conexión desde las áreas de trabajo hasta los distintos switches de acceso. Esta elección está basada en las

características del ancho de banda necesario para que los distintos servicios que serán prestados funcionen con normalidad.

Figura 3.8 Cuarto de Telecomunicaciones, Edificio Secundario

3.1.4.5.1 Categoría a Utilizar

Con base a las nuevas tecnologías de red y a la utilización de servicios multimedia que demandan de una buena capacidad del medio de transmisión, se define que el cable a ser utilizado será UTP Cat 6. Cabe resaltar que este tipo de cable está reemplazando al cable UTP Cat 5e que puede soportar velocidades de hasta 100 Mbps. Con base en estos puntos, se usará cable UTP Cat 6 así como *jacks* y *plugs* RJ-45, y demás accesorios que cumplan con ésta categoría.

3.1.4.5.2 Rutas de Cableado

En el edificio principal, el cableado usará canaletas pegadas a la pared o a los biombos modulares para su distribución. También será necesario el uso de tubería *Conduit* en sitios donde se tenga que atravesar paredes, pues actualmente los cables son guiados por las paredes sin protección.

En el edificio secundario se aprovechará la facilidad del techo falso, que permitirá la instalación de escalerillas y canaletas con sus respectivos accesorios.

3.1.4.6 Cableado Vertical (*Backbone*)

El cableado vertical utilizará una topología jerárquica en forma de estrella y tendrá 2 niveles jerárquicos de interconexión, con el fin de evitar la degradación

de la señal producida por sistemas pasivos y para simplificar la administración de la red de cableado.

3.1.4.6.1 Categoría a Utilizar

El medio de transmisión a usarcé en este subsistema será cable UTP Cat 6a, para trabajar a velocidades de 1Gbps de acuerdo al estándar 802.3ab.

Las distancias a cubrirse para la conexión de los diferentes dispositivos no sobrepasan los 100 metros como se muestra en la figura 3.6, debido a ello es factible el uso de cable UTP Cat 6a.

3.1.4.6.2 Rutas de Backbone

Debido a la existencia de dos edificios que conforman la AZEA, el *backbone* comprenderá dos tipos de rutas, una interna y otra externa.

En el edificio principal se usarán tuberías *Conduit* de 3 pulgadas, cuya capacidad máxima es de 20 cables UTP Cat 6a con un diámetro de 7.9 mm. Esta tubería guiará 8 cables UTP destinados al *backbone* (4 usados y 4 de respaldo), acorde a la cantidad de cables utilizados, se usa un 40% de la capacidad máxima de la tubería.

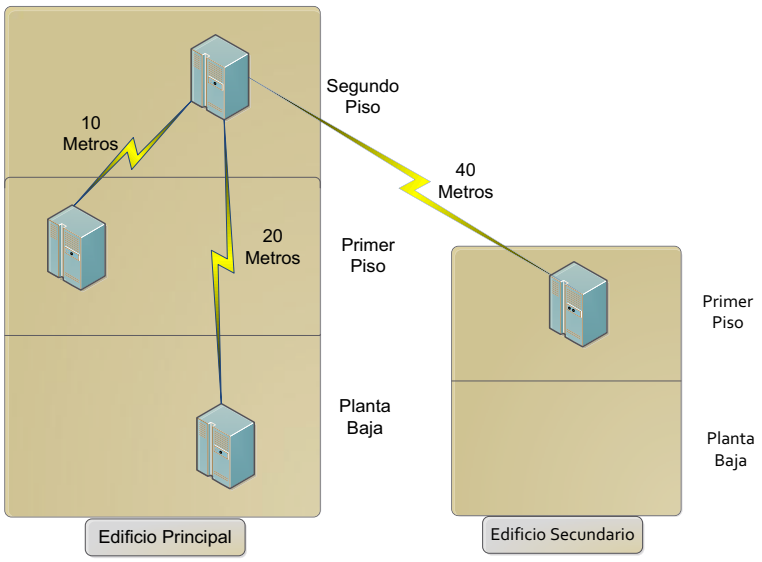


Figura 3.9 Distancias desde el cuarto de equipos a los racks

La interconexión entre el edificio principal y el secundario demanda de una tubería subterránea que se acople a la tubería antes mencionada y permita transportar 2 cables UTP Cat 6a, como se muestra en la figura 3.10. Con este objeto se define una tubería de 1 1/2 pulgada, cuya capacidad máxima de es 6 cables UTP Cat 6a y acorde a la cantidad de cables utilizados, se usa un 33.3% de la capacidad total.

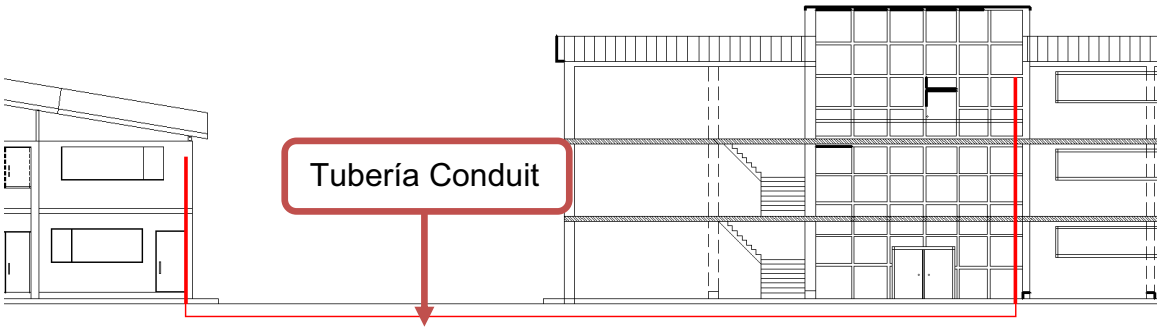


Figura 3.10 Ruta de conexión entre edificios

3.1.4.7 Dimensionamiento de elementos para rutas de cableado

Para seleccionar adecuadamente las dimensiones de las rutas, es necesario tomar en cuenta la sección del medio de transmisión que se va a transportar. El cable UTP categoría 6 tiene un diámetro promedio de 6.1 mm y respecto al número de cables que se van a colocar se definirá el tamaño de la tubería.

La tabla 3.3 muestra la cantidad máxima de cables de 6.1 mm que se pueden colocar en el interior de una tubería *Conduit*, según la norma EIA/TIA 569A.

Tubería Conduit		Número máximo de cables UTP con diámetro de 6.1 [mm]
Medida [Pulgadas]	Diámetro interno [mm]	
½	15.7	0
¾	20.8	3
1	26.7	6
1 ¼	35	10
1 ½	40.9	15
2	52.6	20
2 ½	62.7	30
3	80	40

Tabla 3.3 Capacidad de tuberías *Conduit* para cable *UTP* de 6.1 mm

Para el uso de escalerillas y canaletas, se debe usar máximo el 40% de su capacidad al momento de la instalación, para que con las adiciones futuras se pueda llegar a utilizar como máximo el 60% de la capacidad.

La información concerniente al número de cables UTP que pueden ser guiados a través de las escalerillas y canaletas es mostrada en la tabla 3.4.

Ducto	Medidas		Área		Número de cables UTP de 6.1 [mm]	
	Ancho [mm]	Alto [mm]	[mm^2]	[pulg^2]	40%	60%
Escalerilla	300	100	30000	46.50	397	596
	150	100	15000	23.25	199	298
Canaleta	13	7	91	0.14	1	2
	20	12	240	0.37	3	5
	30	12	360	0.56	5	7
	40	25	1000	1.55	13	20
	60	40	2400	3.72	32	48
	100	45	4500	6.98	60	89

Tabla 3.4 Capacidad de escalerillas y canaletas para cable *UTP* de 6.1 mm

3.1.4.8 Cálculo del número de rollos de cable

Para el cálculo del número total de rollos de cable UTP a utilizarse en el nuevo diseño, se puede usar una estimación en base a la fórmula estandarizada. A continuación de mostrará el procedimiento a seguir tomando como ejemplo el segundo piso del edificio principal.

1. Obtener un promedio en base a la distancia del punto de red más lejano y del punto de red más cercano.

$$d_{med} = \frac{d_{máx} + d_{mín}}{2}$$

$$d_{med} = \frac{49.2 + 2.8}{2}$$

$$d_{med} = 26\ [m]$$

2. Ajustar la distancia promedio, aumentando un 10% de margen de holgura.

$$d_{ajd} = d_{med} + 10\% = 26 + 2.6 = 28.6\ [m]$$

3. Obtener el número de corridas por rollo de cable *UTP,* mediante la relación entre la longitud estándar de un rollo para la distancia promedio ajustada y redondear este resultado hacia el número entero menor.

$$\#\ corridas = \frac{L_{rollo}}{d_{adj}} = \frac{305}{28.6} = 10.66$$

$$\#\ corridas = 10$$

4. Calculo del número total de rollos con la división del número de puntos de red para el número de corridas y aproximación al número entero superior.

$$\#\ rollos = \frac{\#_{puntos}}{\#_{corridas}} = \frac{81}{10} = 8.1$$

$$\#\ rollos = 9$$

El número total de rollos de cable UTP Cat 6 obtenidos en base a los cálculos antes mencionados se muestra en la tabla 3.5.

Edificio	Planta	$d_{mín}\ [m]$	$d_{máx}\ [m]$	$d_{med}\ [m]$	$d_{ajd}\ [m]$	# Corridas	# rollos
Principal	Planta Baja	2.97	51.31	27.14	29.85	10	9
	Primer Piso	2.78	57.51	30.15	33.17	9	14
	Segundo Piso	2.8	49.2	26	28.6	10	9
Secundario	Planta Baja	1.43	35.13	18.28	20.11	15	2
	Primer Piso	3.35	30.8	17.1	17.25	17	3
Total de Cable							37

Tabla 3.5 Rollos de cable UTP Cat 6 a ser usados

3.1.4.9 Área de los cuartos de telecomunicaciones

Para definir el área de los distintos cuartos de comunicaciones se puede tomar en cuenta el área utilizable y el número de equipos a los que se va a servir. En base a estas recomendaciones hechas por el estándar se pueden definir qué los cuartos de telecomunicaciones deberán tener las siguientes áreas.

Espacio Utilizable [m^2]	Número de equipos por Espacio Utilizable	Tamaño recomendado para el cuarto de Telecomunicaciones [m^2]
500	50	3 x 2.2
800	80	3 x 2.8
1000	100	3 x 3.4

Tabla 3.6 Espacio físico del cuarto de telecomunicaciones

Edificio	Área	Área Recomendada
Principal	Planta Baja	3 x 2.8
Principal	Primer Piso	3 x 3.4
Principal	Segundo Piso	3 x 2.8
Secundario	Primer Piso	3 x 2.8

Tabla 3.7 Áreas recomendadas para los cuartos de telecomunicaciones de la AZEA

3.1.4.10 Etiquetado

Basándose en el estándar EIA/TIA 606, se propone un etiquetado que identifique a cada uno de los subsistemas del cableado. Se colocará etiquetas en cada extremo del cable, en los *face-plates* y *patch panels* de los cuartos de telecomunicaciones instalados en la AZEA.

Las etiquetas deberán mantener el formato mostrado a continuación, esta se compondrá de tres partes principales:

- Identificación del punto dentro de la AZEA.
- Identificación del punto dentro del Rack
- Identificación del punto según el servicio que brinda (Voz o Datos).

E1-PB-01-04-D

Dónde:

- E1-PB: Identifica a la ubicación del punto de red en la AZEA, para ello se usa un campo destinado a identificar al edificio y otro destinado a identificar el piso. El edificio principal es denotado mediante el identificador E1 y el

secundario con E2, y los distintos pisos según la información mostrada en la tabla 3.8.

- 01-04: Identifica la ubicación del punto dentro del rack, el primer valor identifica el número de *patch panel* al que pertenece y el segundo número define su ubicación dentro del *patch panel*.
- D: Identifica el tipo de servicio que presta el cable, pudiendo ser D de Datos o V de voz.

Edificio	Área	Identificador
Principal	Planta Baja	E1-PB
Principal	Primer Piso	E1-PP
Principal	Segundo Piso	E1-SP
Secundario	Planta Baja	E2-PB
Secundario	Primer Piso	E2-PP

Tabla 3.8 Etiquetado de las áreas de la AZEA

3.2 DIMENSIONAMIENTO DEL TRÁFICO

La nueva infraestructura de comunicaciones debe brindar servicios adicionales a los que actualmente se manejan en la misma, para ello es necesario asegurar que los nuevos servicios dispongan de un ancho de banda apropiado.

Con el objeto de garantizar el correcto desempeño de la red, deben tomarse en cuenta los servicios actuales, entre los que se encuentran el servicio Web, correo electrónico, descarga de archivos y actualizaciones del antivirus, a los que se sumarán los nuevos servicios como son la videoconferencia y el streaming de video.

3.2.1 ANCHO DE BANDA PARA SERVICIO WEB

Para calcular el ancho de banda para cada aplicación, es necesario conocer el tamaño promedio de la información a ser transmitida, para el caso del servicio Web, se tiene como peso promedio 965 KB[5] para una página Web.

[5] Dato obtenido de http://www.extremetech.com/computing/110099-the-web-in-2011-html5-dominates-flash-trouble-for-data-capped-mobile-surfers, a diciembre del 2011

También se define el acceso promedio a 15 páginas Web en una hora, esto debido a los requerimientos del personal.

Por tal motivo, para el servicio Web será necesario asegurar el ancho de banda siguiente:

$$AB_{Web} = \frac{965\ KBytes}{página} * \frac{8\ bits}{1\ byte} * \frac{15\ páginas}{1\ hora} * \frac{1\ hora}{3600\ segundos}$$

$$AB_{Web} = 32{,}2\ kbps$$

Tomando en cuenta una simultaneidad del 20% sobre este servicio, y considerando que se tienen un total de 275 equipos que pueden acceder al mismo, se define un uso de 55 equipos en forma simultánea, teniendo:

$$AB_{Web\_Total} = 32{,}2\ kbps * 55 = 1769{,}2\ kbps$$

3.2.2 ANCHO DE BANDA PARA SERVICIO DE CORREO

Siendo el correo electrónico una de las principales formas de comunicación que se tienen en la AZEA, es muy importante garantizar que este servicio sea soportado adecuadamente.

Tomando en cuenta que el tamaño promedio de un correo electrónico es de 75 KB[6] y que cada usuario recupera cinco correos electrónicos por hora, con una simultaneidad del 10% de usuarios se tiene:

$$AB_{email} = \frac{75\ KBytes}{mail} * \frac{8\ bits}{1\ byte} * \frac{15\ mail}{1\ hora} * \frac{1\ hora}{3600\ segundos}$$

$$AB_{email} = 2{,}5\ kbps$$

$$AB_{email\_Total} = 2{,}5\ kbps * 28 = 70\ kbps$$

[6] Dato obtenido de http://email.about.com/od/emailstatistics/f/What_is_the_Average_Size_of_an_Email_Message.htm, actualizado a enero del 2012

3.2.3 ANCHO DE BANDA PARA LA TRANSFERENCIA DE ARCHIVOS

Para la transferencia de archivos se considera que los archivos descargados desde internet tienen en promedio 1MB, y se deben descargar máximo en 30 segundos pues este servicio solo es accedido en forma restringida. A este servicio tienen acceso solo los jefes de los departamentos y el personal de la Jefatura Zonal de Informática, acorde a ello la cantidad de usuarios se limita a 40.

$$AB_{Trans} = \frac{1024\ KBytes}{archivo} * \frac{8\ bits}{1\ byte} * \frac{1\ archivo}{30\ segundos}$$

$$AB_{Trans} = 273{,}1\ kbps$$

Tomando en cuenta una simultaneidad del 15% sobre este servicio, y considerando que se tienen un total de 40 usuarios que pueden acceder a dicho servicio, se define el uso de 6 usuarios en forma simultánea, teniendo:

$$AB_{Trans\_Total} = 273{,}1\ kbps * 6 = 1638{,}6\ kbps$$

3.2.4 ANCHO DE BANDA PARA STREAMING DE VIDEO

El ancho de banda definido para el streaming de video se encuentra en función de las características del video a ser reproducido, en especial de las dimensiones y de la tasa de bits.

De acuerdo a las características del servidor de streaming RED5, es posible distribuir videos en formato MP4, la cual se presenta en la tabla 3.9 que define el ancho de banda recomendado en base al uso de un códec MP4 a 30 cuadros por segundo.

Dado que los videos a ser reproducidos en la AZEA son en su mayoría de 360p (640x360) de resolución, se requerirá un ancho de banda de al menos 728 kbps por cliente que reproduzca el video.

Protocolo de Streaming	Códec de Video	Resolución	Bitrate del Video	Códec de Audio	Tasa de Muestreo	Stereo Audio Bitrate
RTMP Flash Streaming	H.264 Main Profile	720p (1280x720)	2,000 kbps	AAC-LC	44.1khz	128kbps
RTMP Flash Streaming	H.264 Main Profile	480p (854x480)	1,000 kbps	AAC-LC	44.1khz	128kbps
RTMP Flash Streaming	H.264 Main Profile	360p (640x360)	600 kbps	AAC-LC	44.1khz	128 kbps
RTMP Flash Streaming	H.264 Baseline Profile	240p (426x240)	250 kbps	AAC-LC	44.1khz	128 kbps

Tabla 3.9 Tasas de bits recomendadas para audio y video [PW55]

Según las necesidades de los funcionarios de la AZEA, se estima que se tendrán 30 clientes en forma simultánea, lo que define el uso del ancho de banda mostrado a continuación:

$$AB_{Stream} = \frac{728\ Kbits}{segundo} * 30$$

$$AB_{Stream} = 21{,}33\ Mbps$$

Este servicio será interno, y su tráfico no afectará al del enlace WAN, ya que el objeto es disponer de los videos institucionales a cualquier momento para su reproducción interna en la intranet.

3.2.5 ANCHO DE BANDA PARA LA VIDEOCONFERENCIA [T5]

El servicio de videoconferencia será utilizado en forma esporádica, por lo que su tráfico no afectará en forma continua al desempeño de la red.

La videoconferencia será llevada a cabo dentro de la AZEA y permitirá la comunicación con los dos centros de desarrollo comunitario que están bajo la administración de la AZEA. De acuerdo a esto, se define la participación de dos usuarios por dependencia, teniendo un promedio de 6 usuarios.

Todos los usuarios de la videoconferencia compartirán audio y video en forma simultánea, también interactuarán a través de las distintas herramientas de *Openmeetings*, lo que aumentará el ancho de banda requerido para el servicio.

En base a las características de *OpenMeetings*, se define un consumo promedio de 100 kbps solamente en sesiones con audio y video por usuario, mientras que en una sesión en la que también se incluya la compartición del escritorio, se consume en promedio 350 kbps por usuario.

Acorde al consumo de ancho de banda con el uso del escritorio compartido, se tiene un consumo de total de red de:

$$AB_{Videoconf} = \frac{350\ Kbits}{segundo} * 6$$

$$AB_{Videoconf} = 2100\text{Kbits}$$

Debido a que el tráfico que atravesará el enlace WAN solamente será de los dos centros de desarrollo comunitario, su valor será el siguiente:

$$AB_{VideoconfWAN} = \frac{350\ Kbits}{segundo} * 4$$

$$AB_{VideoconfWAN} = 1400\text{Kbits}$$

3.2.6 ANCHO DE BANDA PARA ACTUALIZACIONES DEL ANTIVIRUS

La AZEA utiliza el antivirus NOD32 de ESET, para las actualizaciones se maneja un servidor de actualizaciones, mismo que recupera las actualizaciones desde internet diariamente y las entrega a los dispositivos terminales.

Las actualizaciones diarias este antivirus tienen un tamaño promedio de 4 Mbytes[7], y se las realiza durante la noche, sin que se vea afectado el desempeño de la red durante horas laborables.

Debido a que la descarga de las actualizaciones puede realizarse durante un tiempo prolongado sin que se comprometa la seguridad de la red, se define un tiempo de media hora como máximo para la descarga diaria de actualizaciones:

$$AB_{Antivirus} = \frac{4096\ KBytes}{actualización} * \frac{8\ bits}{1\ byte} * \frac{1\ actualización}{30\ minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{Antivirus} = 18{,}2\ kbps$$

3.2.7 DIMENSIONAMIENTO DEL ENLACE *WAN*

El enlace WAN de la AZEA debe soportar adecuadamente los servicios requeridos, a más de definir una capacidad extra para un futuro crecimiento.

Los servicios que circularán a través del enlace WAN son:

- Acceso Web
- Descarga de Archivos
- Actualización de Antivirus
- Videoconferencia
- Servicios propios de la AZEA

Con respecto a los cálculos previamente presentados, se define el siguiente consumo de ancho de banda mostrado en la tabla 3.10.

Para los servicios presentados, es necesario garantizar un ancho de banda de al menos 5920,0 kbps. Actualmente la AZEA cuenta con un enlace WAN que dispone de un ancho de banda de 8192 kbps, lo que es suficiente para soportar los servicios a ser implementados.

[7] Dato obtenido de ESET, http://www.eset.com/us/business/whyeset/compare/, febrero del 2012

Servicio	Ancho de Banda
Acceso Web	1769,2 kbps
Correo Electrónico	70 kbps
Descarga de Archivos	1638,6 kbps
Actualización de Antivirus	18,2 kbps
Video Conferencia	1400 kbps
Servicios propios de la AZEA	1024 kbps
Total	5920,0 kbps

Tabla 3.10 Ancho de banda del enlace WAN

3.3 DISEÑO DE LA RED ACTIVA

El nuevo diseño combina la red de datos, voz y video en una misma infraestructura. La red de datos propuesta basará su distribución de equipos en un modelo jerárquico, permitiendo que la red sea mucho más fácil de administrar, flexible y escalable.

3.3.1 ELEMENTOS ACTIVOS DE LA RED

Los elementos activos de la red son los terminales del usuario, los equipos de conectividad y los servidores, todos ellos se conectarán usando la tecnología *Ethernet* y usará una topología en estrella. Debido a la heterogeneidad de velocidades de los dispositivos en la red de la AZEA, se debe permitir que los dispositivos de baja velocidad puedan comunicarse con el resto a velocidades acordes a sus características.

3.3.1.1 Dispositivos Terminales

Los dispositivos terminales que se comunicarán en la red multi-servicios serán computadores de escritorio, computadores portátiles, teléfonos IP e impresoras IP.

Los computadores de escritorio y algunos computadores portátiles así como las impresoras de red se conectarán directamente a los puntos de red de datos mediante cables *patch cord* UTP Cat 6, con una distancia máximo de 5 metros entre el dispositivo y el *face-plate.* Todos estos dispositivos deberán contar con una NIC que les permita trabajar a velocidades de 10/100 o 10/100/1000 Mbps.

Las características de hardware y software de estos equipos son propios de sus funciones.

Los teléfonos IP se conectarán a los puntos de red de voz, con el uso de cable UTP Cat 6 y que no superará los 5 metros de longitud.

3.3.1.2 Equipos de Conectividad

Los equipos de conectividad en el nuevo diseño de la red son switches y routers de la AZEA, a ellos se le suman los equipos de los proveedores de los enlaces *WAN*.

Los switches se clasificarán en switches de núcleo, switches de distribución y switches de acceso, teniendo cada uno de estos las características propias de sus funciones. Estos equipos estarán instalados en los racks de los cuartos de equipos o telecomunicaciones con respecto al área de servicio. Usarán tecnología *Fast Ethernet* y *Gigabit Ethernet* para la conexión a los equipos terminales o hacia otros equipos del mismo tipo.

Para permitir la comunicación entre la central telefónica o servidor de telefonía IP con la PSTN se usarán tarjetas *PCI*.

3.3.1.3 Servidores

Los servidores serán redimensionados de acuerdo a los servicios a ser implementados, esto obedece a que los servidores actuales se encuentran saturados de información y no presentan las características de hardware necesarias para sostener los nuevos servicios a implementarse.

Los servidores se ubicarán en el cuarto de equipos situado en el segundo piso del edificio principal, junto a la Jefatura Zonal de Informática, sitio que es usado actualmente para el mismo objetivo, pero que no cuenta con las características físicas necesarias para cumplir esta función.

Los servidores deberán disponer de las características de hardware acordes a los servicios que prestarán, y dispondrán de los sistemas operativos Windows Server, CentOS o Ubuntu. Deberán contar con tarjetas de red que soporten la tecnología Gigabit Ethernet y se conectarán al switch de la DMZ mediante cables UTP Cat 6a.

3.3.2 CONECTIVIDAD

La red multi-servicios estará definida en tres niveles, correspondientes a núcleo, distribución y acceso.

3.3.2.1 Núcleo de la Red

El nivel de núcleo comprende un switch multicapa que cumplirá la función del enrutamiento de paquetes entre las *VLAN's* IEEE 802.3Q, por lo que deberá ser capaz de trabajar en capa 3 para manejar direcciones IP, también deberá soportar uno o más protocolos de ruteo como RIPv2 y el soporte de *sub netting*.

Los servidores se encuentran en esta capa, y se conectarán al switch de núcleo mediante cables UTP Cat 6 a velocidades de 1000 Mbps usando IEEE 802.3ab.

De acuerdo al crecimiento de las redes y el uso de fibra óptica como nuevo medio de transmisión el switch deberá tener la capacidad de soportar al menos 2 puertos de fibra DFP-GBIC.

Debido a que estos dispositivos manejarán una gran cantidad de información pues son el punto por el que atraviesa todo el tráfico hacia la red WAN, deben tener características adecuados para este requerimiento, tales como un nivel de *throughput* alto y nivel de disponibilidad elevado. Con el objeto de brindar alta disponibilidad, se define un switch que tenga doble fuente de poder.

3.3.2.2 Capa de Distribución

En la capa de distribución es necesario disponer de dispositivos que permitan el manejo de voz y datos mediante la diferenciación de *VLAN's*. Estos equipos se

conectarán utilizando el estándar IEEE 802.3ad para la agregación de enlaces al switch de núcleo.

En esta capa se implementará el control y filtrados de paquetes mediante el uso de Listas de Acceso o ACL's, por ello los switches deberán ser capaces de manejar estas características.

3.3.2.3 Capa de Acceso

En esta capa se encuentran los switches que brindarán conectividad a los dispositivos terminales con velocidades de 10/100Mbps que son suficientes para las necesidades de los usuarios. Con la finalidad de evitar problemas en cuanto a la velocidad y tipo de cable UTP a usarse, se requerirá que los switches dispongan de puertos con *Auto-sense* y MDI/MDI-X.

Debido a la necesidad de una conmutación rápida debida a los servicios, se recomienda que los switches trabajen usando el método de conmutación *fragment free,* lo que permite bajar el tiempo de latencia de procesamiento.

La conexión de los switches de acceso con los de distribución se realizará utilizando cables UTP Cat 6a a 1000 Mbps.

Los switches que serán usados para la conexión de los teléfonos IP dispondrán de PoE (*Power over Ethernet*), para facilitar el uso de teléfonos en sitios en los que no se tenga acceso a tomacorrientes.

3.3.3 DISEÑO LÓGICO DE LA RED

Acorde a los nuevos servicios que se prestará en la red y el número de usuarios se definirá un direccionamiento IP para todos los dispositivos terminales, servidores y equipos de conectividad.

3.3.3.1 Direccionamiento IP

La AZEA deberá contar con un total de 372 puntos de telecomunicaciones, los cuales se dividen en 275 puntos para datos y 97 para voz. La AZEA siendo parte

del IMQ tiene dependencia de los campos de direcciones asignados por el mismo para la correcta compartición de recursos. La tabla 3.11 muestra los campos de direcciones asignados a la AZEA.

Campo de Direcciones	Máscara de Red	Número de host disponibles
172.20.6.0	255.255.255.0	254
172.20.127.0	255.255.255.0	254

Tabla 3.11 Direcciones IP establecidas por el IMQ para la AZEA

Partiendo de los campos de direcciones asignadas a la AZEA, se plantea el direccionamiento IP mostrado en la tabla 3.12 como una alternativa a ser usado para el presente diseño.

Las estaciones de trabajo tendrán asignada una dirección IP estática que será entregada por un servidor *DHCP*. También se dispondrá de una subred para la administración de los equipos de red como switches en una VLAN independiente.

Área	Número de Hosts	Subred/Mascara
Edificio Principal, Planta Baja	66	172.20.127.0/25
Edificio Principal, Primer Piso	88	172.20.127.128/25
Edificio Principal, Segundo Piso	81	172.20.6.0/25
Edificio Secundario	60	172.20.6.128/26
Servidores	5	172.20.6.224/28
Telefonía IP	117	192.168.10.0/24

Tabla 3.12 Direccionamiento IP propuesto para el rediseño

Los teléfonos IP mantendrán una dirección IP estática configurada en cada uno de ellos.

3.3.3.2 Diseño de *VLAN's*

Con el objeto de optimizar el uso de direcciones IP, mantener la confidencialidad de la información y disminuir la cantidad de tráfico broadcast, es necesaria la creación de redes LAN virtuales. Estas redes virtuales serán creadas en el switch

de núcleo y se compartirán hacia el resto de switches que trabajen con esta información mediante un protocolo de enlace troncal.

Los switches mantendrán una configuración que relacione los puertos con la *VLAN* correspondiente, existiendo grupos de puertos asignados a *VLAN's* independientes. Mediante esta asignación se busca tener una fácil administración y configuración de los equipos.

Las *VLAN's* creadas guardan relación con el grupo de direcciones IP designadas por la Administración General del Distrito Metropolitano de Quito, existiendo dos campos de direcciones IP para manejar los distintos equipos pertenecientes a ella.

Nombre VLAN	Subred/Máscara	Direcciones IP		Gateway
		Inicial	Final	
AZ_ADM	172.20.6.192/27	172.20.6.193	172.20.6.221	172.20.6.222
AZ_PPB	172.20.127.0/25	172.20.127.1	172.20.127.125	172.20.127.126
AZ_PPP	172.20.127.128/25	172.20.127.129	172.20.127.253	172.20.127.254
AZ_PSP	172.20.6.0/25	172.20.6.1	172.20.6.125	172.20.6.126
AZ_SE	172.20.6.128/26	172.20.6.129	17.20.6.189	172.20.6.190
AZ_SRV	172.20.6.224/28	172.20.6.225	172.20.6.237	172.20.6.238
AZ_VOZ	192.168.10.0/24	192.168.10.1	192.168.10.253	192.168.10.254

Tabla 3.13 VLAN's propuestas para el rediseño

3.3.3.2.1 Enrutamiento entre VLAN's

El switch de núcleo se encargará del enrutamiento entre las *VLAN's,* puesto que los switches de distribución pasarán las tramas con la etiqueta correspondiente mediante enlaces configurados como troncales hacia el switch de núcleo, mismo que podrá enrutar la trama conforme su tabla de VLAN's.

3.3.4 DIMENSIONAMIENTO DE EQUIPOS DE LA RED LAN

3.3.4.1 Servidores [PW56] [PW57] [PW58]

Los servidores a ser implementados en la AZEA operarán con el uso de software libre o software propietario según sea el servicio a ofrecerse. En el caso de los servidores de software libre se recomienda trabajar con Red Hat o CentOS Linux.

Los requerimientos mínimos y recomendados de los sistemas operativos Ubuntu Server, CentOS y Windows Server se muestran en las tablas 3.14, 3.15 y 3.16.

Linux Ubuntu Server 11.04	
Arquitecturas	x86, AMD64
Procesador	300 MHz x86 o superior
Random Access Memory	128 MiB[8]
Disco Duro	1 GB de espacio libre

Tabla 3.14 Requerimientos mínimos de Ubuntu Server 11.04

Linux CentOS 5	
Arquitecturas	Intel x86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP). AMD64(Athlon 64, etc.) e Intel EM64T (64 bit)
Procesador	Pentium 3 500 MHz o superior
Random Access Memory	512 MB
Disco Duro	2 GB de espacio libre

Tabla 3.15 Requerimientos mínimos de CentOS 5

Windows Server 2008 R2		
Arquitecturas	x86, AMD64	
Característica	Mínimo	Recomendado
Procesador	1 GHz (x86) 1.4 GHz (x64)	2 GHz o superior
Random Access Memory	512 MB	6 GB (32 bits) 32 GB (64 bits)
Disco Duro	10 GB de espacio libre	50 GB o más

Tabla 3.16 Requerimientos mínimos de Windows Server 2008 R2

Acorde a las características enunciadas sobre los requerimientos de los sistemas operativos presentados, es posible definir las características básicas para el correcto desempeño del sistema operativo, pero también se debe tomar en cuenta los servicios a ser soportados por cada uno de ellos antes de definir sus características.

[8] MiB, contracción de megabyte binario, 1 MiB = 2^{20} bytes = 1.048.576 bytes

3.3.4.1.1 Servidor DNS y DHCP

Para su implementación se recomienda el uso de un servidor *BIND,* sobre un sistema operativo Linux para servidores como CentOS o Red Hat, La última versión estable es la 9.8.1, lanzada el 31 de agosto del 2011.

El servidor *DHCP* asignará las direcciones IP a los equipos terminales de la AZEA y se implementará sobre un servidor Linux con CentOS 6.2, pues esta distribución cuenta con un servidor *DHCP* por defecto denominado *dhcpd*.

3.3.4.1.2 Servidor Correo Electrónico [PW59]

En el presente rediseño se recomienda el uso de Zimbra, mismo que para su correcto funcionamiento es recomendado disponer de la siguiente configuración:

- CPU Intel/AMD de 32 bits a 2.0GHz o superior,
- Mínimo 2 GB de RAM,
- 10 GB de disco duro para actualizaciones, logs y software, con RAID para redundancia de datos,
- Espacio de disco adicional para el almacenamiento de los buzones de correo y las bases de datos.

Se recomienda el uso de una CPU de doble núcleo o superior, y preferiblemente doble CPU.

3.3.4.1.3 Servidor Telefonía IP [PW60]

En el presente diseño se considera el uso de un servidor de telefonía IP con ayuda de Elastix, para el que se definen las siguientes características mínimas:

- Procesador Intel Pentium 4 2.4Ghz o superior,
- 4Gb de memoria RAM,
- 80 Gb de espacio libre disponible en el disco duro,
- Unidad de CD-ROM para la instalación,
- Al menos tres interfaces PCI para la conexión de tarjetas de expansión.

3.3.4.1.4 Servidor Proxy [PW61]

Para su implementación se puede optar por *Squid*, cuya última versión disponible es la 3.1.15, liberada el 28 de agosto del 2011. Se recomienda su implementación sobre un sistema operativo Linux, en su distribución CentOS.

Para el correcto desempeño de *Squid*, se debe asegurar los siguientes parámetros en el equipo:

- Tiempo de búsqueda en disco (velocidad del disco),
- Cantidad de memoria del sistema,
- Rendimiento del disco sostenido,
- Capacidad del CPU.

3.3.4.1.5 Servidor de Streaming de Video y Video Conferencia [PW62]

El servidor de streaming y de video conferencia hará uso de software libre, para ello se implementará un servidor de streaming de video con Red5 y videoconferencia con *Openmeetings*.

Los requerimientos en cuanto a hardware de Red5 en su versión 0.9.1 son los siguientes:

- Procesador Dual-core / Quad-core o superior,
- 2 – 4 GB de memoria RAM disponible,
- Tarjeta de red a 1Gbps,
- 200 MB de espacio disponible en el disco duro.

En el servicio de videoconferencia proporcionado por OpenMeetings se recomienda disponer de un equipo con las siguientes características:

- Procesador Dual-core / Quad-core o superior,
- 4 GB de memoria RAM disponible,
- Auricular/Micrófono Logitech Clear Chat PC Wireless o compatibles.

3.3.4.1.6 Hardware recomendado para la implementación de servidores

En base a las características de los diferentes servicios y sus requerimientos, se presenta la tabla 3.17 que muestra las características básicas de los servidores.

Los servidores deben ser equipos robustos que garanticen la continuidad de las operaciones de la AZEA, por lo que a más de las características mencionadas anteriormente, es primordial contemplar aspectos como un buen sistema de ventilación, uso de arreglos de discos para disminuir el riesgo de pérdida de información, entre otros.

En el mercado existen fabricantes de equipos especializados para este trabajo, por lo que se recomienda utilizar equipos de este tipo y no adaptar computadoras de escritorio para este fin.

Hardware recomendado para los servidores					
Nombre	Servicios	CPU	RAM	Sistema Operativo	Disco Duro
Streaming	Streaming / Videoconferencia	2 GHz Dual Core o superior	4 GB	Ubuntu 11.04	500 GB
Mail	Correo Electrónico	2 GHz Dual Core o superior	4 GB	CentOS 5	500 GB
Telefonía	Telefonía IP	2 GHz Dual Core o superior	4 GB	Elastix	500 GB
DDP	DNS/DHCP/PROXY	2 GHz Dual Core o superior	4 GB	CentOS 6	500 GB
Active Directory	Autenticación	2 GHz Dual Core o superior	4 GB	Windows Server 2008 R2	500 GB

Tabla 3.17 Características de hardware para los servidores

3.3.4.2 Switches

3.3.4.2.1 Dimensionamiento de los switches de la capa de acceso

La cantidad de switches de acceso necesarios está en función del número de dispositivos terminales a ser configurados en la red. Los switches de acceso serán instalados en los racks de los cuartos de telecomunicaciones

pertenecientes a cada piso en el caso del edificio principal y en el rack ubicado en el segundo piso del edificio secundario, esto obedece a la cantidad de usuarios que se tiene por piso y a la disponibilidad previa de racks en los pisos. En la tabla 3.19 se muestra la cantidad de switches necesarios para cada piso.

Edificio	Piso	Puntos Datos	Puntos de Voz	Puntos Totales
Principal	Planta Baja	66	21	87
	Primer Piso	88	34	122
	Segundo Piso	61	20	81
Secundario	Planta Baja	20	10	82
	Primer Piso	40	12	

Tabla 3.18 Puntos de red necesarios

Edificio	Piso	Puntos Datos Requeridos	Puntos de Voz Requeridos	Número De Switches	Número de Puertos por Switch	Número de Puertos Provistos
Principal	Planta Baja	66	--	3	24	72
		--	21	1	24 PoE	24
	Primer Piso	88	--	4	24	96
		--	34	2	24 PoE	48
	Segundo Piso	61	--	3	24	72
		--	20	1	24 PoE	24
Secundario	Planta Baja y Primer Piso	60	--	3	24	72
		--	12	1	24 PoE	24

Tabla 3.19 Equipos necesarios para la capa de acceso

Dado la cantidad de usuarios por piso, es necesaria la instalación de 13 switches de 24 puertos y 5 switches de 24 puertos que dispongan POE para los teléfonos IP. Los equipos mencionados deben trabajar a velocidades de 10/100/1000 Mbps en sus puertos.

3.3.4.2.2 Dimensionamiento de los switches de la capa de distribución

En la capa de distribución se dispondrá de 4 switches que tengan al menos 12 puertos cuya velocidad de transmisión sea de 10/100/1000 Mbps.

Características Recomendadas Switch de Acceso	
Velocidad de backplane mínimo	8.8 Gbps
Throughput	6.6 Mbps
Número de Puertos Ethernet 10/100	24
Número de Puertos Ethernet 10/100/1000	2
Estándares Soportados:	IEEE 802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.1p, IEEE802.1q, IEEE802.1w, IEEE802.1s
De montaje en Rack	
Soporte POE[9]	
Soporte para ruteo Estático	
Interfaz de administración GUI basada en Web	
Soporte SNMP v1, v2 y v3.	

Tabla 3.20 Características Switches de Acceso

3.3.4.2.3 Dimensionamiento de los switches de la capa de núcleo

En la capa de núcleo se requerirá de 3 switches, un switch principal y un switch redundante para el manejo del tráfico en la intranet, a ellos se les suma un switch para la zona desmilitarizada, que conectará a los distintos servidores a la red de datos.

Estos switches deben cumplir con los siguientes parámetros para proveer un servicio acorde a las necesidades de la red:

- Soporte al estándar IEEE 802.1q, permite el uso de varias redes virtuales en una misma red física.
- Soporte al estándar IEEE 802.3ab, permite alcanzar velocidades de 1000 Mbps sobre un cable de par trenzado no blindado.
- Soporte al estándar IEEE 802.3af, permite agregar enlaces para obtener un mayor ancho de banda disponible.
- Soporte al estándar IEEE 802.3x permite la transmisión y recepción en forma simultánea.
- Soporte al estándar IEEE 802.1d y 802.1w para evitar que se formen lazos en la red.

[9] En los switches destinados a Voz IP.

- Soporte al estándar IEEE 802.1p que permite priorizar el tráfico, diferenciando y dando un trato adecuado al tráfico de voz, video y datos.
- Deben permitir el uso de los protocolos de enrutamiento como *RIP* versión 2, OSFP o EIGRP, a más de manejar rutas estáticas.
- Interfaz de administración Web para acceso remoto.

Características Recomendadas Switch de Núcleo	
Velocidad de backplane mínimo	24 Gbps
Throughput	17.9 Mbps
Número de Puertos Ethernet 10/100/1000 mínimo	12
Estándares Soportados:	IEEE 802.3u IEEE802.3ab IEEE802.3x IEEE802.1p IEEE802.1d IEEE802.1q IEEE802.1w IEEE802.1s IEEE802.3z IEEE802.3af IEEE802.1q
De montaje en Rack	
Deberá soportar listas de control de acceso (ACL),	
Enrutamiento IPv4 estático y dinámico RIPv1 y RIPv2 con Capacidad de ampliación a otros protocolos como OSPF.	
Al menos dos fuentes que funcionen de manera redundante	
Interfaz de administración GUI basada en Web	
Soporte SNMP v1, v2 y v3.	

Tabla 3.21 Características Switches de Núcleo

3.3.4.2.4 Dimensionamiento de la velocidad de backplane y throughput [T1]

Para asegurar un correcto funcionamiento de los switches es necesario tener en cuenta la cantidad de información que éste deberá ser capaz de procesar, para ello es necesario el cálculo del *backplane* y *throughput*.

Para calcular la velocidad del backplane se toma en cuenta el número de puertos del switch, su capacidad y modo de transmisión. Debido a que se usarán puertos full dúplex, la capacidad por puerto debe ser duplicada, teniéndose la expresión:

$$Vbackplane = \#puertos * capacidad * 2$$

Tomando como ejemplo un switch de capa de acceso de 24 puertos en el que cada uno de sus puertos trabaja a 100 Mbps, y dispone dos puertos de *uplink* a 1000 Mbps, el cálculo sería el siguiente:

$$Vbackplane = (24 * 100 + 2 * 1000) * 2\ [Mbps]$$

$$Vbackplane = 8.8\ [Gbps]$$

El *throughput* se obtiene mediante la relación entre la capacidad total de los puertos y la longitud de los paquetes que el switch debe procesar.

$$Throughput = \frac{\#\ puertos\ x\ capacidad}{longitud\ paquete}$$

La longitud de los paquetes puede variar entre 64 y 1518 bytes. Acorde a los datos recopilados en la AZEA la distribución de tamaño de los paquetes es la mostrada en la figura 3.11.

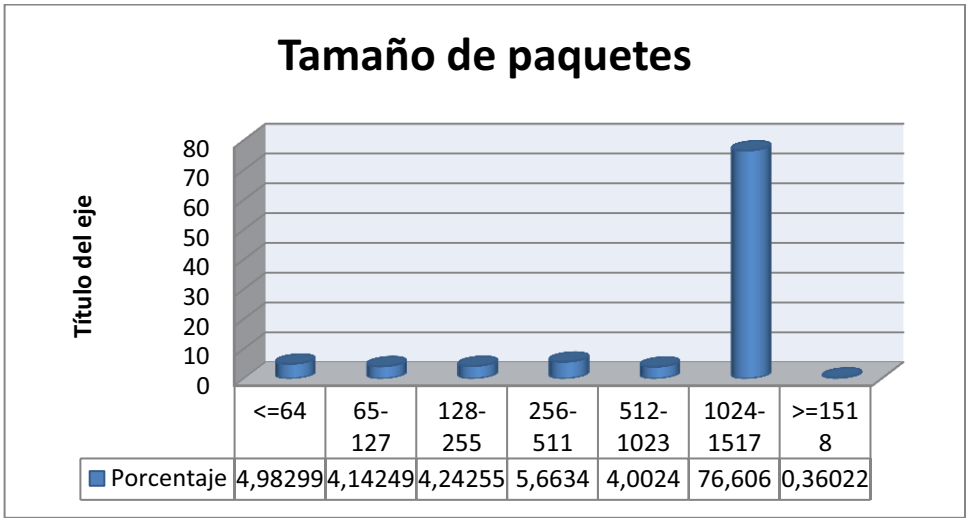


Figura 3.11 Tamaño de paquetes

El peor escenario es cuando los paquetes procesados tienen una longitud pequeña, para el cálculo se tomará una longitud de 64 bytes sumada a 20 bytes que el switch no procesa, pero que también se transmiten a través del cable, 12 bytes de *GAP* (una pausa obligatoria de 96 tiempos de bit entre cada trama), 7 bytes de preámbulo y 1 byte de inicio de trama.

$$Throughput = \frac{24\ x\ 100\ \frac{Mbit}{s} + 2\ x\ 1000\ \frac{Mbit}{s}}{\frac{(64+20)\ byte}{1\ paquete} \times \frac{8\ bit}{1\ byte}} = 6.6\ Mpps$$

De la misma forma se realiza el cálculo para cada uno de los switches a ser usados, obteniéndose los resultados resumidos en la tabla 3.22.

Switch	Número de Switches	Puertos 10/100	Puertos 10/100/1000	Velocidad *backplane* [Gbps]	*Throughput [Mpps]*
Núcleo	2	--	12	24	17.9
Distribución	4	--	12	24	17.9
Acceso	18	24	2	8.8	6.6
DMZ	1	--	12	24	17.9

Tabla 3.22 Velocidades de backplane y throughput requeridas

Todos los equipos de red serán instalados en racks, reutilizando 2 racks de 24 unidades que actualmente se dispone en la AZEA sumando 2 racks de 42 unidades que deberán ser adquiridos.

3.3.5 DISEÑO DE LA RED DE ÁREA LOCAL INALÁMBRICA

La red inalámbrica brindará movilidad a los usuarios propios de la AZEA que ocupen el auditorio ubicado en el segundo piso del edificio principal, y permitirá la asociación y acceso a la red por parte de los equipos invitados que utilicen esta sala, así también estará presente en el departamento del Sr. Administrador, con el fin de tener este servicio para reuniones que se den en este despacho. La red inalámbrica brindará los mismos servicios que la red cableada, debido a ello se deberá tomar en cuenta medidas de seguridad pertinentes para disminuir los riesgos.

	Etiqueta	Tipo	Número de Puertos 10/100/1000 Mbps	Power Over Ethernet
1	FIREWALL	Firewall	8	✗
2	SWCR03-01	Switch de Núcleo	12	✗
3	SWCR03-02		12	✗
4	SWDZ03-01		12	✗
5	SWBK03-01	Switch de Distribución	12	✗
6	SWBK03-02		12	✗

7	SWBK03-03		12	✗
8	SWBK03-04		12	✗
9	SWAC03-01	Switch de Acceso	24	✗
10	SWAC03-02		24	✗
11	SWAC03-03		24	✗
12	SWAV03-04		24	✓
13	SWAC03-05		24	✗
14	SWAC03-06		24	✗
15	SWAC03-07		24	✗
16	SWAC03-08		24	✗
17	SWAV03-09		24	✓
18	SWAV03-10		24	✓
19	SWAC03-11		24	✗
20	SWAC03-12		24	✗
21	SWAC03-13		24	✗
22	SWAV03-14		24	✓
23	SWAC03-15		24	✗
24	SWAC03-16		24	✗
25	SWAC03-17		24	✗
26	SWAV03-18		24	✓

Tabla 3.23 Switches requeridos en el rediseño

La figura 3.12 muestra el área de cobertura a la que debe servir el dispositivo inalámbrico que generará la señal.

La red inalámbrica mantendrá en promedio 10 equipos terminales propios de la AZEA, y se tiene una estimación de 20 equipos adicionales que usarán esta red, acorde a ello, se define un direccionamiento y un SSID para esta red.

3.3.5.1 Tipo de aplicaciones Soportadas [PW63]

Las aplicaciones soportadas sobre la red inalámbrica corresponden a las mismas que serán brindadas por la red cableada, entre las que se pueden mencionar como principales al acceso Web, correo electrónico y transferencia de archivos.

Dado que las dimensiones del auditorio corresponden a 10 metros de ancho por 16 metros de largo, se puede garantizar una velocidad de acceso suficiente para soportar las aplicaciones de la red multi-servicios.

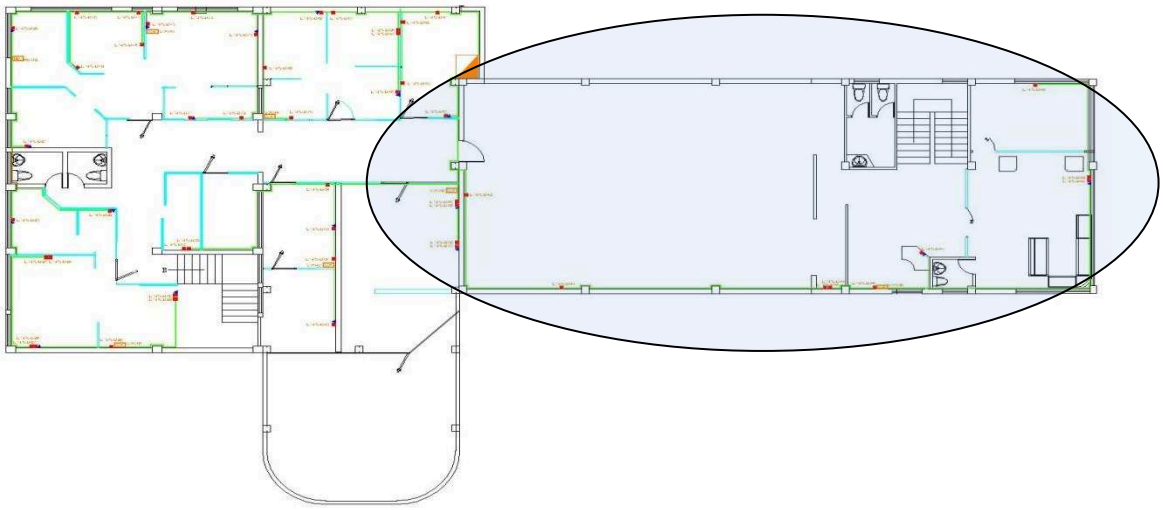


Figura 3.12 Cobertura de la red inalámbrica de la AZEA

3.3.5.2 Conexión de la WLAN con la red cableada

Para la conexión del equipo que brindará acceso inalámbrico se dispondrá de un punto de red dedicado a este fin, ubicado en la parte superior del auditorio. Como medida adicional se debe conectar este puerto a un switch que permita el uso de *Power Over Ethernet* PoE.

3.3.5.3 Velocidad de operación

Actualmente el estándar IEEE 802.11g es el más usado en redes inalámbricas, pero el estándar IEEE 802.11n lo reemplazará ya que permite alcanzar una mayor velocidad haciendo uso de varias antenas.

Los estándares IEEE802.11a y el IEEE802.11b no son comúnmente usados, y por lo tanto no serán empleados en el presente diseño, de esta manera el estándar a seguir será el IEEE 802.11n, pero debido a la existencia de muchos dispositivos terminales que no pueden manejar este estándar, también soportará el estándar IEEE 802.11g.

El estándar IEEE 803.11g puede tener las velocidades hipotéticas mostradas en la tabla 3.24, mismas que son suficientes en el caso del auditorio en el que el rango no supera los 20 metros.

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

Tabla 3.24 Velocidades vs distancias en 802.11g [PW63]

3.3.5.4 Identificador de la red SSID y seguridad de acceso

Acorde al uso de una correcta política de seguridad, el SSID de una red inalámbrica no debe reflejar su procedencia, así que se usará un identificador que no esté relacionado con la AZEA en forma explícita, por ello se utilizará el identificador *wafelz.*

SSID: wafelz

Debido a que la información de la red inalámbrica es transmitida por el espacio libre, cualquier persona podría intentar recuperar la información que es trasmitida y/o modificarla. Por ello es necesario usar mecanismos de seguridad para proteger la información.

Con el objeto de proteger la información que viaja en un medio propenso a ataques, se puede cifrar mediante una palabra clave, justamente esa es la forma en la que trabaja el protocolo de seguridad *WEP* (*Wireless Equivalent Privacy*). En la actualidad existe una serie de aplicaciones que permiten obtener esta palabra clave y vulnerar este protocolo de seguridad, convirtiéndolo en protocolo inseguro.

Por esta falla en el protocolo de seguridad *WEP* se desarrolló WPA (*Wi-Fi Protected Access*), que en base a TKIP (*Temporal Key Integrity Protocol*), realiza el cambio de la clave constantemente, evitando que una clave sea válida por más de un periodo de tiempo definido, lo cual robustece la seguridad ante ataques.

Actualmente se cuenta con el protocolo de seguridad WPA2 que hace uso del algoritmo CCMP (*Counter Mode with Cipher Block Chaining Message*) en lugar de TKIP.

Para la distribución de las claves de autenticación se definen dos métodos:

- Personal: la autenticación la realiza el punto de acceso, y es usada en redes caseras y pequeñas oficinas.
- Enterprise: este método define el uso de un servidor *RADIUS* (*Remote Authentication Dial-In User Server*) para autenticar a los usuarios.

En base a las características presentadas, se recomienda el uso de WPA2 Enterprise, ya que presenta las características de seguridad necesarias para el nuevo diseño.

3.3.5.5 Recomendación para la selección del Access Point

El Access Point a ser utilizado para brindar acceso al auditorio debe tener ciertas características mínimas que garanticen su correcto desempeño, estas características se encuentran mostradas en la tabla 3.25.

3.3.6 DIAGRAMA DE RED

La figura 3.13 muestra el diagrama de la red diseñada para la AZEA, mostrando los elementos que la conforman. En el mismo se pueden apreciar los niveles de acceso, distribución y núcleo.

3.3.7 RACKS

De acuerdo a las características de los espacios disponibles en la AZEA y a los equipos a ser instalados, se define el uso de 5 racks, distribuidos de la siguiente manera:

- 1 rack de piso de 42 unidades (73.5 pulgadas) para el cuarto de equipos ubicado en el segundo piso del edificio principal, junto a la Jefatura Zonal

de Informática y que mantendrá los equipos correspondientes a este piso y los equipos de acceso a la WAN.

Access Point	
Estándares WLAN soportados	IEEE 802.11g, IEEE 802.11n
Protocolos de gestión	SNMP, HTTP
Algoritmos de Cifrado	MD5, SHA, AES
Método de autenticación	RADIUS, Personal
Interfaces	Ethernet RJ45 10/100Base-TX
Estándares Soportados	IEEE 802.3af, IEEE 802.3x, IEEE 802.3q, IEEE 802.3p, IEEE 802.3ab, IEEE 802.11i.
Características Adicionales	Filtrado de direcciones, DHCP
Certificación WI-FI	
Cobertura mínima en interiores 100 metros	
La fuente de alimentación permitirá una fuente de energía continua (Adaptador DC) o Power over Ethernet (*PoE).*	
Antena Omnidireccional	

Tabla 3.25 Especificaciones Access Point

- 1 rack de piso de 42 unidades (73.5 pulgadas) ubicado en el primer piso del edificio principal, junto al departamento de Obras Públicas y que mantendrá los equipos de conectividad correspondientes a este piso.
- 1 rack de 24 unidades (47.25 pulgadas) ubicado en la planta baja del edificio principal, junto a las ventanillas de recaudación y que mantendrá los equipos de conectividad correspondientes a este piso.
- 1 rack de 24 unidades (47.25 pulgadas) ubicado en el primer piso del edificio secundario y que mantendrá los equipos de conectividad para todo el edificio.
- 1 rack de 24 unidades (47.25 pulgadas) ubicado en el segundo piso del edificio principal para los servidores.

La distribución de los equipos de conectividad en los racks se muestra en el anexo F.

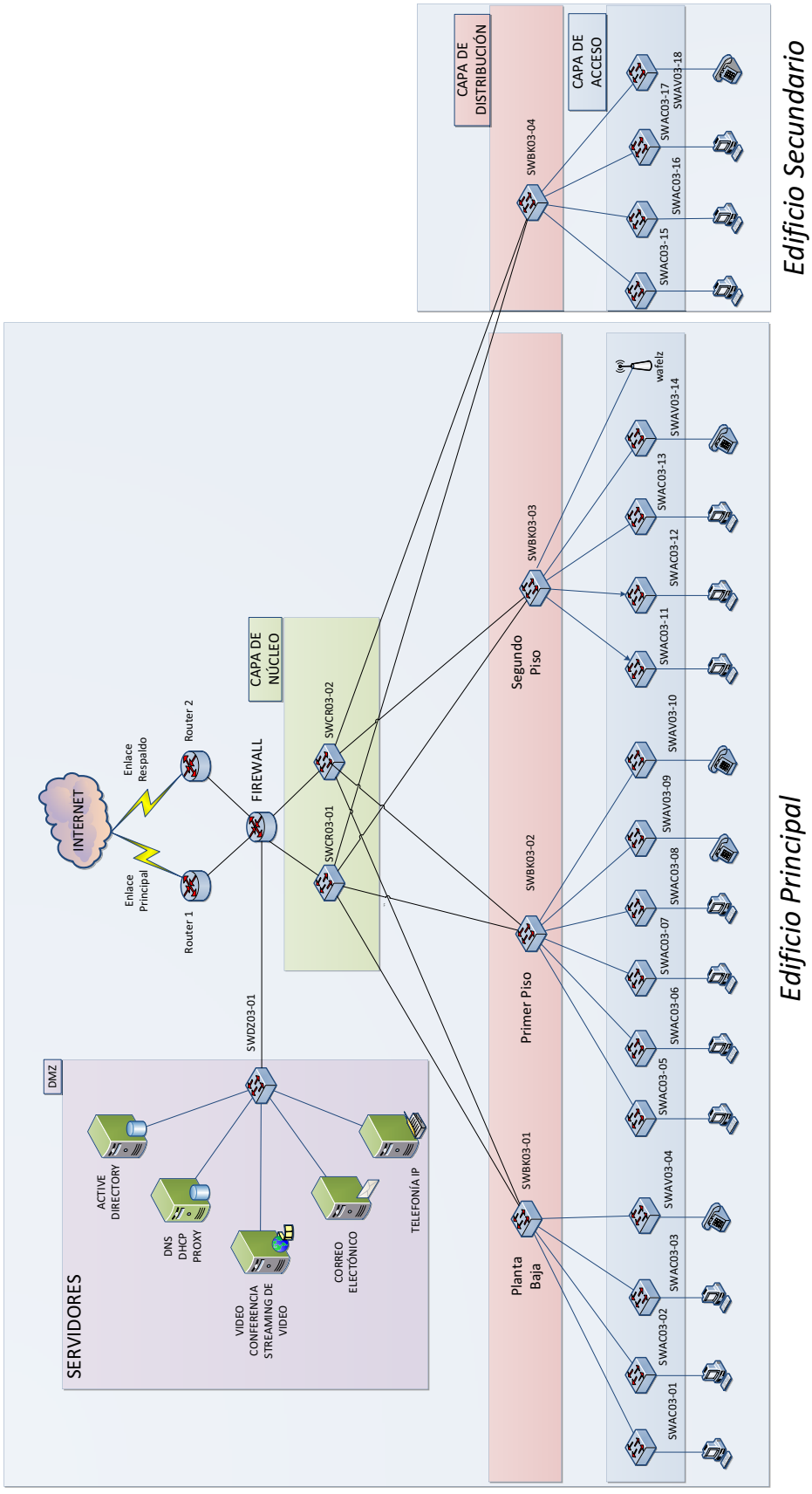


Figura 3.13 Diagrama de red del rediseño

3.3.8 TELEFONÍA IP

Los requerimientos de comunicación de voz serán suplidos mediante la unificación de la red de datos y voz, por ello es necesario el estudio correspondiente de las características a ser provistas para este servicio.

La AZEA contará con 97 extensiones que se distribuirán en ambos edificios. Su distribución responde a la necesidad de cada departamento y a la importancia del cargo de los funcionarios.

3.3.8.1 Plan de Numeración

El plan de numeración tomará en cuenta el piso en el que se encuentra ubicado el terminal telefónico, designando un dígito para este fin, seguido por dos dígitos que identificarán la extensión del teléfono dentro del piso.

La tabla 3.26 muestra el plan de numeración a utilizarse en la AZEA.

Edificio	Planta	Prefijo	Número Inicial	Número Final
Principal	Planta Baja	1	101	199
	Primer Piso	2	201	299
	Segundo Piso	3	301	399
Secundario	Planta Baja	4	401	499
	Primer Piso	5	501	599

Tabla 3.26 Plan de numeración

3.3.8.2 Categorización de Usuarios

Partiendo del organigrama mostrado en el capítulo anterior y de acuerdo a las necesidades de los usuarios, se puede clasificar a los mismos en usuarios de nivel Administrativo y usuario de nivel Operativo.

Usuarios de nivel Administrativo, en este nivel se ha considerado al Administrador y la Secretaría del mismo, los jefes de cada departamento de la AZEA, la zona de Información en el Balcón del Servicio y todos los usuarios del Departamento de Cultura.

Nivel	Usuario	Internacional	Nacional	Local	Regional	Celular	Interno	Números de emergencia
Administrativo	Administrador y Secretaría	✓	✓	✓	✓	✓	✓	✓
	Jefes de Departamentos de la AZEA.	✗	✓	✓	✓	✓	✓	✓
Operativo	Información	✗	✓	✓	✓	✓	✓	✓
	Departamento de Cultura.	✗	✓	✓	✓	✓	✓	✓
	Todo el personal	✗	✗	✗	✗	✗	✓	✓

Tabla 3.27 Perfil de usuarios telefónicos de la AZEA

Usuarios de nivel Operativo, en este nivel se ha considerado a todos los usuarios que no están contemplados en el nivel Administrativo.

Los usuarios podrán acceder a los servicios de llamadas internacionales, nacionales, regionales, locales, internas, emergencia y celulares respecto a la tabla 3.27 que relaciona el nivel del funcionario con los servicios disponibles.

3.3.8.3 Circuitos troncales hacia la red publica

Los circuitos troncales son aquellos que permiten acceder a la red de telefonía pública, y su número debe ser dimensionado de acuerdo a las necesidades en cuanto a la cantidad de llamadas y a su duración.

Para la obtención de la información pertinente a la duración de las llamadas telefónicas así como de su distribución en el tiempo se ha realizado una encuesta, cuyos resultados son mostrados en el anexo H.

Para complementar esta información se ha procedido a la recopilación de la información pertinente a las troncales telefónicas usadas en la AZEA, proporcionada por la Corporación Nacional de Telecomunicaciones. Acorde a los cálculos realizados se obtienen los resultados mostrados en la tabla 3.28.

Horario	8:00 - 11:00	11:00 - 14:00	14:00 - 16:00	Total
Horas	3	3	2	
Llamadas	93	74	106	273
Porcentaje	34,07	27,27	38,66	100
Intensidad Tráfico [Erlang]	1,6	1,3	2,7	
Intensidad Tráfico proyectado	2,25	1,82	3,8	

Tabla 3.28 Resumen del tráfico de voz

Con el objetivo de disponer de una probabilidad de pérdida de llamadas menor al 1%, es necesario el uso de al menos 10 troncales.

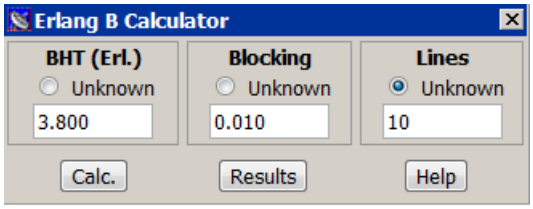


Figura 3.14 Calculadora Erlang B

3.3.8.4 Códec de Audio [PW64] [PW65] [PW66] [PW67]

La compresión y codificación de las señales de voz para que estas puedan atravesar por la red multi-servicios, son factores muy importantes ya que permiten optimizar los recursos de red sin perder la calidad de la señal.

Códec	Payload (bytes / paquete)	Paquetes / Segundo	Ancho de banda promedio WAN (kbps)		Porcentaje de reducción
			Sin compresión	Con compresión	
G.711 (64 kbps)	160	50	84	68,5	~ 18%
G.729 A (8 kbps)	20	50	27,5	13	~ 53 %
G.723.1 (5,3 kbps)	20	33	18	9	~ 50 %
G.723.1 (6,3 kbps)	24	33	19	10	~ 47 %

Tabla 3.29 Especificaciones de Codecs usados en telefonía IP [T2]

La tabla 3.29 muestra las especificaciones de Codecs, de acuerdo a esto se puede definir que el códec G.711 tiene una mejor señal porque su reducción es apenas del 18 % con respecto a los otros Codecs que están con una reducción

alrededor del 50%, esto se puede corroborar en la tabla 3.30 en la que se puede ver el parámetro MOS (*Mean Opinion Score*), que es una unidad de medida referente a la calidad de habla humana en sistemas de telefonía IP, siendo malo (1) su peor valor y excelente (5) su mejor valor.

Códec	Bit rate (kbps)	MOS
G.711	64	4.1
G.729 A	8	3.7
G.723.1	6.3	3.9
G.723.1	5.3	3.65

Tabla 3.30 MOS, *Mean Opinion Score* [PW68]

:: DATOS TELEFONICOS ::		
Número Telefónico	Razón Social / Nombre del Propietario	Dirección
23110801	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110802	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110803	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110804	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110805	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110806	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110807	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110808	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110809	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110812	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110814	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110815	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110816	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110817	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110818	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110819	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110821	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR
23110822	ADMINISTRACION ELOY ALFARO / ADM. MUNICIPAL ZONA ELOY ALFARO	CAPITAN CESAR CHIRIBOGA 0 Y ALONSO DE ANGULO EDF ADM ZONA SUR EDF-ADM ZONA SUR

Figura 3.15 Troncales telefónicas disponibles en la AZEA

Debido a que en la red multi-servicios, el ancho de banda no es un condicionante el códec recomendado para ser usado es el de G.711, que garantiza una alta calidad de la señal de voz.

3.3.8.5 Alternativas para la implementación

Para la implementación del servicio de telefonía IP se puede disponer de varias alternativas, cada una de las cuales dispone de características específicas que dictarán su elección en base a los requerimientos, para su posterior implementación.

3.3.8.5.1 Telefonía IP por hardware [T2]

En el mercado existen diferentes fabricantes de equipos de *Networking* que ofrecen sus productos especializados en telefonía IP o equipos con la capacidad de integrar distintos servicios mediante la adición de componentes o módulos específicos para este fin.

En el presente caso es necesaria la implementación de equipos que permitan el manejo del servicio de telefonía IP y dispongan de módulos para su futura expansión, los mismos deben soportar los protocolos y demás normas asociadas a telefonía IP como *SIP*, *h323* entre otros.

Las funciones de gestión propias de la *PBX* son realizadas por un *call center* que se encarga de las operaciones de admisión, establecimiento, desconexión entre otras. El servidor puede ser uno solo o estar constituido por varios equipos, mediante la técnica de *clustering*[10].

Para la comunicación hacia la central telefónica analógica es necesario usar un dispositivo que permita convertir las señales digitales a analógicas, este dispositivos es denominado *Gateway*.

[10]Conglomerados de computadoras construidos mediante la utilización de hardware común y que se comportan como si fuesen una única computadora.

Los dispositivos terminales de telefonía IP se conectan a la red mediante el uso de un puerto en un switch y todos deberían tener la capacidad para ser configurado en forma remota, permitiendo centralizar la administración de los mismos.

La implementación de este sistema en la AZEA demanda la adquisición de equipos nuevos destinados para este fin, así como de las licencias y demás requerimientos asociados a estos equipos.

3.3.8.5.2 Telefonía IP por central telefónica hibrida IP-PBX

La AZEA dispone de una central telefónica hibrida IP-PBX Panasonic KX-TDA-200 que puede soportar tanto los terminales de usuario análogos y digitales, siendo necesaria la instalación de módulos de expansión para soportar los nuevos servicios.

Algunos inconvenientes asociados al uso de la central telefónica son el manejo de protocolos propietarios que limitan su interoperabilidad con otros equipos, la necesidad de disponer de equipos terminales del mismo fabricante para garantizar un funcionamiento correcto, la administración y configuración de la central requiere de personal especializado dificultando la recuperación del sistema en caso de un fallo.

Acorde a los inconvenientes presentados se define que la solución de telefonía con el uso de una central hibrida no es la mejor opción para suplir los requerimientos de la AZEA.

3.3.8.5.3 Telefonía IP por servidores de software libre

Una solución de telefonía IP es la implementación de servidores con el uso de software libre especializado en este servicio y la adición de tarjetas *PCI* para el soporte de las nuevas funcionalidades.

Actualmente se disponen de varias soluciones en cuanto a software libre, entre las que se destacan Asterisk y Elastix permitiendo su implementación sin el pago

de licencias asociadas a su uso y permiten una administración a través de una interfaz Web.

Figura 3.16 Diagrama básico de conexión del servidor de voz IP [PW69]

Para la comunicación a la red pública analógica se utilizan tarjetas o equipos con puertos *FXO*, que en el caso de las tarjetas, estas son instaladas en los puertos *PCI* del servidor, lo que implica que el equipo destinado a convertirse en servidor de telefonía debe disponer de algunos puertos PCI libres. Los puertos *FXO* se conectan a las líneas telefónicas contratadas por el proveedor de servicios y las llamadas salientes son enrutadas hacia ellas mediante la gestión del servidor.

Los servidores de software libre pueden soportar diversos tipos de terminales, entre los que cuentan los teléfonos IP que se conectan a la red a través de los switches de acceso, los teléfonos IP por software o softphones que hacen uso de un equipo terminal (computadora, laptop), equipos de telefonía analógica que pueden conectarse a la red mediante los puertos *FXS* del servidor, etc.

Esta solución es la más recomendable a implementarse en la AZEA pues dispone de una excelente escalabilidad y soporte a las terminales.

3.3.8.6 Elastix [PW70]

Elastix es un software de código abierto para el establecimiento de comunicaciones unificadas. El objetivo de Elastix es incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial.

El proyecto Elastix se inició como una interfaz de reportación para llamadas de Asterisk y fue liberado en Marzo del 2006. Posteriormente el proyecto evolucionó hasta convertirse en una distribución basada en Asterisk.

Elastix incluye en su solución los medios de comunicación mostrados en la figura 3.17.

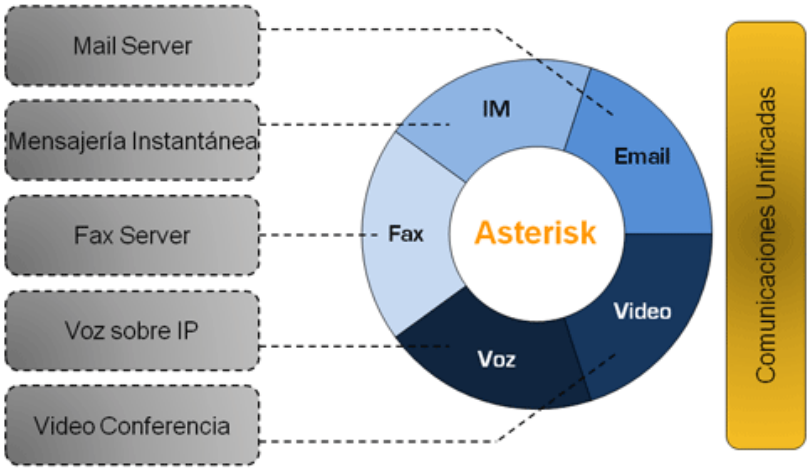


Figura 3.17 Medios de comunicación manejados por Elastix [PW71]

Elastix tiene múltiples características y funcionalidades relacionadas con los servicios que presta: Telefonía IP, Servidor de Correo, Servidor de Fax, Conferencias, Servidor de Mensajería Instantánea, entre otros. Nuevas características, funcionalidades y servicios son añadidos en el desarrollo de nuevas versiones.

- Grabación de Llamadas.
- Centro de Conferencias con Salas Virtuales.
- Correo de Voz.
- Soporte para protocolos SIP e IAX, entre otros.
- Correo de voz-a-Email.
- Codecs soportados: ADPCM, G.711 (A-Law &μ-Law), G.722, G.723.1 (pass through), G.726, G.728, G.729, GSM, iLBC (opcional) entre otros.
- Soporte para Interfaces Análogas como FXS/FXO (PSTN/POTS).
- Soporte para Sintetización de Voz.
- Soporte para interfaces digitales E1/T1/J1 a través de los protocolos PRI/BRI/R2.
- Identificación de llamadas (Caller ID).
- Troncalización.
- Provisionador de Teléfonos vía Web.

- Soporte para videófonos.
- Interfaz de detección de Hardware.
- Soporte para grupos de timbrado.
- Servidor DHCP para asignación dinámica de IP's.
- Panel de Operador basado en Web.
- Parqueo de llamadas.
- Soporte para PIN's de seguridad.
- Reporte de detalle de llamadas (CDR).
- Tarifación con reporte de consumo por destino.
- Soporte para Callback.
- Reportes de uso de canales.
- Soporte para colas de llamadas.

3.3.9 SERVICIOS DE VIDEO

3.3.9.1 Streaming de Video [PW34]

El servicio de streaming de video presentará una serie de videos institucionales que pueden ser accedidos desde cualquier computador de la AZEA mediante un navegador Web.

El servidor utilizará el software de código abierto RED5, mismo que está diseñado como un servidor multimedia, un poderoso servidor de streaming de video y como una alternativa al Adobe Flash Media Server.

El servidor RED5 permitirá la entrega del streaming de video mediante el protocolo *RTMP* (*Real Time Messaging Protocol*) hacia el reproductor que se colocará en la página web.

El dispositivo terminal que desee reproducir los videos debe disponer de un navegador web, tal como Internet Explorer, Mozilla Firefox, Google Chrome y debe contar con los plugins necesarios para reproducir contenido en Flash, Adobe Flash Player.

Para la reproducción de los videos en las páginas web es necesaria la implementación de un reproductor flash, para lo cual se establece el uso del reproductor JWPlayer.

JWPlayer es un reproductor de video, puede manejar videos en formato FLV, H.264, MP4, WebM[11], VP8, así como música en formato mp3, a ello se suma el soporte para varios formatos de streaming y listas de reproducción incluyendo *rtmp* y *http*.

La implementación de este servidor se la realizará sobre un sistema operativo de código abierto, pudiendo ser GNU/Linux en su distribución Ubuntu o CentOS.

3.3.9.2 Video Conferencia

La videoconferencia definida en el presente diseño tiene por objetivo brindar este servicio para la comunicación entre las distintas áreas de la AZEA sin necesidad de desplazarse a un punto de encuentro común.

Debido a que este servicio será usado en forma esporádica, no es conveniente la inversión en equipos especializados para este fin, por ello se recomienda el uso de software de código abierto para soportar este servicio. Existen algunas opciones para la implementación de este servicio, pero se dará preferencia a aquella que permita su acceso mediante un navegador web, logrando tener una implementación más rápida

Entre las opciones en software libre presentes en el mercado, se recomienda el uso de OpenMeetings, que se encuentra soportado por la fundación Apache.

3.3.9.2.1 OpenMeetings [PW72]

Openmeetings proporciona video conferencia, mensajería instantánea, una pizarra para compartir, edición colaborativa de documentos y otras

[11] Los archivos de video WebM son reproducidos directamente en el navegador web usando HTML5, sin la necesidad de plugins adicionales.

herramientas de trabajo en grupo utilizando las funciones de la interfaz del servidor de streaming Red5 para la interacción remota.

Características Principales

- Se dispone de cuatro opciones para usar las funciones de audio y video, mismas que pueden ser elegidas durante una sesión de conferencia.
  - Audio y Video
  - Solamente Audio
  - Solamente Video
  - Solamente una imagen
- Grabación de reuniones y compartición de pantalla
  - Las sesiones grabadas contienen todo, incluyendo el sonido proveniente de todos los flujos de audio en forma exacta como fueron presentadas en la conferencia.
  - Las sesiones grabadas pueden ser descargadas como archivos AVI/FLV.
  - Posibilidad de compartir un área de la pantalla para compartir.
  - Posibilidad de visualizar y organizar las grabaciones en un explorador integrado.
- Explorador de archivos
  - Se dispone de un explorador de archivos en cada sala de conferencia, con una interfaz para arrastrar y soltar los archivos subidos al servidor, incluyendo la posibilidad de crear árboles de documentos con carpetas.
- Sistema de moderación
  - Durante la conferencia, los moderadores pueden ajustar los permisos de los usuarios en forma individual.
- Pizarra multiusuario y chat
  - Se tiene pizarras que pueden añadirse, cada una de las cuales tiene una gran cantidad de herramientas para la edición y documentos.
  - Se pueden importar una gran cantidad de formatos de documentos (PDF, DOC, ODT, PPT, etc.).
- Administración de usuarios y salas

- Se puede administrar usuarios y varias organizaciones en una sola instancia de Openmeetings.
- Cada usuario tiene por defecto dos salas que son siempre accesibles, exclusivamente para ese usuario.
- Es posible asignar salas de conferencia para todos los usuarios, o solamente para usuarios específicos.

OpenMeetings puede ser implementado sobre la mayoría de distribuciones GNU/Linux, se recomienda la instalación de este servicio sobre una distribución CentOS, por tratarse de una distribución destinada a la implementación de servidores.

Para la instalación de este servidor es necesario tener ciertas dependencias previamente instaladas, entre las que se tiene: MySQL, SWFtools, OpenOffice, Sendmail, ImageMagick, Lame, LibMad, YASM, Ffmpeg, SOX.

3.3.10 DISPONIBILIDAD

La AZEA depende casi completamente de la conectividad hacia los servidores centrales, ubicados en la Administración General para brindar los servicios al público en general. En particular el servicio Web, pues los trámites realizados se encuentran en dependencia de los archivos generales.

3.3.10.1 Redundancia

Para brindar continuidad a la operación de la red ante el posible fallo de un enlace, se ha definido el uso de enlaces redundantes en la capa de distribución, esto responde principalmente a que la mayoría de los servicios ofrecidos a la comunidad por parte de la AZEA requieren del acceso WEB a los servidores centrales del IMQ.

3.3.10.2 Suministro de Energía Eléctrica y Aire Acondicionado

Una de las primeras medidas para proveer una alta disponibilidad es disponer de una fuente de energía eléctrica ininterrumpida. Problemas en el suministro de energía eléctrica conlleva posibles daños a los equipos de conectividad y la caída

del servicio de comunicación. Debido a ello se debe disponer de una fuente de energía ante posibles fallos en la red eléctrica, por tal motivo a eso se debe usar un UPS (*Uninterruptible Power Supply*), o una planta eléctrica a diesel.

3.3.10.2.1 UPS, Uninterruptible Power Supply

Los sistemas de UPS suministran energía eléctrica, a los equipos durante una falla de la red eléctrica pública, para mantenerlos activos y continuar su operación con normalidad durante un cierto periodo de tiempo. Los equipos críticos que no deben perder energía son los servidores, switches, routers, módems y firewalls. A más de estos deben considerarse los equipos que usen PoE, ya que su funcionamiento dependerá del switch al que se conecten y este consumo se reflejará en la cantidad de potencia requerida por el switch.

Acorde a las características del cuarto de equipos, se define la utilización de un UPS de una capacidad de alrededor de 8000 VA. Este cálculo es mostrado en el anexo G.

3.3.10.2.2 Planta de Energía Eléctrica Alterna

Debido a cortes en el suministro de energía eléctrica durante periodos de sequía, la AZEA usualmente contrata los servicios de una planta de energía eléctrica alterna, con ello se busca brindar continuidad a sus operaciones. Durante el proceso de cambio entre la energía eléctrica de la red pública y la planta alterna los dispositivos obtendrán energía del UPS.

3.3.10.2.3 Aire Acondicionado

El cuarto de equipos ubicado en el segundo piso del edificio principal debe brindar las condiciones adecuadas para el correcto funcionamiento de los elementos instalados y evitar problemas de sobrecalentamiento. El cuarto de equipos debe mantener una temperatura entre los 18 y 24 grados centígrados, y una humedad entre un 33% y 55% medida a 1.5 metros desde el piso.

Relación entre calor y potencia [T1] [P9]

La potencia que consumen los equipos de telecomunicaciones es convertida en calor. La potencia es comúnmente expresada en vatios (W) y en calor en *British thermal units* por hora (BTUs/h). La conversión entre vatios a BTU/h se la consigue usando la siguiente relación:

$$1W = 3.412BTU/h$$

Para encontrar la capacidad de disipación de los equipos de aire acondicionado se debe tomar en cuenta la potencia total de los equipos y las características del cuarto de equipos, para eso se usa la siguiente expresión:

$$DT = PT_{eq} * 3.412 + (1.25 * A * \Delta T)$$

Dónde: DT: Capacidad total de disipación del aire acondicionado [BTU/h]

PT_{eq}: Potencia total de los equipos [w]

A: Área total de las superficies del cuarto de equipos [pie^2]

ΔT: Diferencia entre la temperatura externa al cuarto y la temperatura interna deseada en el cuarto [ºF].

En el anexo G se definen las características físicas y térmicas del cuarto de equipos junto con la capacidad del aire acondicionado.

3.3.11 SEGURIDAD DE LA RED [T4]

Con el objeto de garantizar el correcto funcionamiento de la red, mitigar los riesgos a los que se exponen los componentes de hardware, software y proteger la información que se transporta sobre la misma, es necesario definir políticas de seguridad acordes a los procesos que se llevan a cabo en la AZEA.

Una política de seguridad la constituyen todas las normas que definen la forma en que los equipos deben ser utilizados, entre sus prioridades se encuentran la

prevención al acceso no autorizado, autenticación y servicio a usuarios legítimos, respecto a todos los niveles de administración, entre otras.

Con el objeto de establecer la política de seguridad, es indispensable la identificación de los activos así como de los riesgos a los que se encuentran sujetos dentro del aspecto de redes de datos.

Las políticas de seguridad deben ser adecuadamente comunicadas al personal de la AZEA, definiendo en forma clara los procedimientos y el objetivo de los mismos.

3.3.11.1 Identificación de Activos

Un activo es todo aquello que tiene valor para la empresa y por ende debe protegerse. Por tal motivo, es necesario diferenciar los activos, pues existe una gran cantidad de ellos, por lo que se usa la siguiente clasificación.

Los activos de la red de la AZEA se encuentran detallados en el capítulo 2, en el que se muestran los servicios y los equipos de la red actual.

3.3.11.2 Seguridad Lógica

Los activos de información lógica son aquellos que generan, transmiten y destruyen información. Dentro de ellos se pueden incluir los archivos, bases de datos, documentos del sistema, servicios, utilidades generales, equipos de comunicaciones, etc.

3.3.11.2.1 Control de Acceso

- El acceso a cualquier sistema de red debe ser precedido por un proceso de identificación del usuario, pudiendo ser mediante el uso de claves con un nivel adecuado de complejidad o mediante otros sistemas de autenticación.
- Para un adecuado control de acceso es necesario disponer de un registro completo de todos los usuarios de los sistemas de la AZEA, así como la definición de un nivel de acceso adecuado a los recursos de red o perfil asignado para el desarrollo de sus actividades.

- La creación de cuentas para el acceso a los servicios deberá ser documentada adecuadamente, para ello es recomendable la creación de un documento formal que sea referido a la autoridad pertinente, pudiendo ser el Jefe del departamento de Informática, mismo que detallará datos del funcionario solicitante.
- Seguido a la correcta verificación de los datos proporcionados por el funcionario solicitante, se dispondrá la creación de las cuentas y configuración de equipos asociados.
- Las cuentas de los usuarios pueden ser creadas solamente por personal autorizado y si el proceso lo amerita, se realizarán peticiones a la administración general para su creación, todos estos procesos deberán ser adecuadamente documentados.
- Las cuentas de los usuarios deberán contar con procedimientos de seguridad tales como el cambio de la clave seguridad en forma periódica, mensajes de notificación, confirmación de datos que permitirán minimizar los riesgos, entre otros.
- En caso de darse un cambio administrativo, este deberá comunicarse en la brevedad posible al departamento de informática para la readecuación de los permisos del usuario a su nuevo perfil, de ser el caso.

3.3.11.2.2 Estaciones de trabajo y acceso a la red

- Una vez creadas las credenciales para el inicio de sesión, la primera acción a realizarse por parte del usuario es el cambio de clave, exigiendo un nivel de complejidad adecuado para la misma, es decir, debe comprender el uso de caracteres, números y letras mayúsculas.
- El perfil asignado al usuario dependerá de las características del trabajo desempeñado y el software necesario para el mismo, limitando los permisos del usuario de acuerdo a sus necesidades.
- A todo usuario que se le asigne un equipo terminal, recibirá su equipo debidamente configurado y listo para entrar en funcionamiento, debiendo previamente explicarle las responsabilidades que implica disponer del equipo y aclarar que debe ser usado en forma personal.

- La entrega de un equipo terminal se registrará mediante un documento, detallando el estado de los equipos entregados y la aceptación por parte del usuario.
- En caso de suscitarse una falla en un equipo terminal, se debe reportar el evento a la Jefatura Zonal de Informática, para su solución y posterior estudio de las causas. Nunca se debe permitir que personal no autorizado manipule los equipos terminales.

3.3.11.2.3 Usuarios del Sistema Telefónico

- Los equipos de telefonía IP son responsabilidad de sus usuarios, teniendo cada uno un número de extensión y un buzón de voz personal. El uso del servicio puede ser compartido con otros usuarios, previo el consentimiento del usuario titular.
- Los mantenimientos realizados a estos equipos deberán ser documentados adecuadamente.
- Los teléfonos mantendrán una configuración IP estática.

3.3.11.2.4 Aplicaciones y Módulos

- El Jefe del Departamento de Informática definirá el nivel de acceso, perfiles, permisos y demás características necesarias para el acceso a los servicios de la red. También se encargará de la gestión de credenciales y de la gestión de usuarios.
- Se mantendrá documentadas adecuadamente las aplicaciones utilizadas en la AZEA, identificando su uso, permisos, versiones, etc.

3.3.11.2.5 Correo Electrónico

- Las cuentas de correo electrónico serán creadas mediante el procedimiento definido por el Centro de Atención Tecnología de IMQ y serán solicitadas por el Jefe Zonal del Departamento de Informática de la AZEA.
- Las cuentas de correo electrónico son personales y sus credenciales no podrán ser compartidas a otras personas.
- Se definirá tamaños máximos de archivos adjuntos a ser enviados.
- Se encuentra totalmente prohibido el uso del correo institucional para recibir correos personales o reenviar cadenas de correos.

3.3.11.2.6 Antivirus

- El funcionamiento del antivirus deberá ser comprobado en forma periódica en búsqueda de problemas relacionados con falla de software o desactualización, Se recomienda la adquisición de un software de administración centralizada para la gestión del mismo y la capacitación a los usuarios para la verificación del estado del antivirus en cada equipo terminal que lo disponga.
- La actualización de los antivirus se realizará en forma diaria, descargando las actualizaciones a un servidor interno que posteriormente las distribuirá en la intranet, evitando que cada equipo se conecte a internet para obtenerla.
- Todo equipo debe contar con un antivirus adecuadamente configurado antes de ser entregado al usuario.
- Cualquier malfuncionamiento de antivirus detectado por el usuario debe ser reportado inmediatamente a la Jefatura Zonal de Informática para su pronta reparación.

3.3.11.2.7 Gestión de Usuarios

- La creación de las cuentas de usuarios demandará la información de los datos personales y los datos institucionales.
- Para dar de baja a un usuario se deben eliminar las cuentas de todos los servicios en los que se tenía acceso, y la información de la persona se respaldará por un tiempo limitado, usando para ello herramientas de compresión de información.
- Un nuevo usuario podrá recibir los equipos terminales usados, previo un proceso de cambio de usuario que constará de los siguientes pasos.
  - Respaldo de la información del usuario anterior.
  - Formateo del equipo en bajo nivel e instalación del sistema operativo, evitando la posterior recuperación de información.
  - Instalación del software necesario para el desarrollo de las actividades del usuario.
  - Configuración necesaria (dominio, proxy, antivirus, etc.)

- Entrega del equipo, documentando el estado de entrega de los equipos y la aceptación por parte del usuario.

3.3.11.2.8 Contraseñas

Con el objeto de proveer un nivel adecuado de seguridad en las contraseñas utilizadas, es necesario definir lineamientos que guíen la creación de las mismas, entre los cuales se pueden mencionar:

- Longitud de al menos 8 caracteres.
- No debe ser una palabra del diccionario.
- No debe ser una palabra explícitamente relacionada con la persona (nombre, fecha de nacimiento, números secuenciales).
- Debe usar al menos una letra capital y al menos un número.
- Debe establecer un máximo de intentos fallidos previo el bloqueo de la cuenta.
- Una vez bloqueada una cuenta, debe ser restaurada mediante la presentación por escrito de una solicitud a la Jefatura de Zonal de Informática.
- Las contraseñas deberán ser cambiadas en forma periódica.

Las contraseñas nunca deben ser reveladas a otros usuarios, y para protegerlas en la red ante los posibles ataques, se debe procurar encriptarlas mediante algún método que evite la transmisión en texto plano.

3.3.11.3 Seguridad lógica en la Red

Para mantener un buen nivel de seguridad en la red es necesario tomar en cuenta ciertos puntos importantes, mismos que permitirán implementar medidas de seguridad más complejas. Entre los puntos bases se tiene:

- En lo posible se debe realizar la transmisión de la información sensible en forma encriptada, debiendo las diferentes aplicaciones usadas en la AZEA soportar este modo de comunicación.

- Mantener un registro actual de toda la red, tanto a nivel físico como a nivel lógico. En casos de cambios en la red se debe documentar y modificar los registros para mantener la información al día.
- Mantener almacenada en un medio seguro el registro de la red, así como las credenciales para el acceso a los diferentes equipos administrables de la misma.

En general, es imperativo disponer de un adecuado registro de la red para brindar soluciones inmediatas ante cualquier situación fortuita que se presente.

3.3.11.3.1 Seguridad del cableado estructurado

- El cableado estructurado de la AZEA deberá cumplir con las normas enunciadas por la TIA/EIA, por lo que todos los elementos de la red serán correctamente identificados.
- El cuarto de equipos y los cuartos de telecomunicaciones deberán garantizar el acceso solo al personal autorizado, en base a ello se deberá contar con seguros en las puertas que impidan el libre acceso a los equipos.
- EL jefe Zonal de Informática mantendrá las llaves en un sitio seguro si fuere el caso, y mantendrá un registro de acceso a los cuartos de telecomunicaciones junto con el motivo de los mismos.

3.3.11.3.2 Conexión a Internet

Dado que la mayoría de servicios que la AZEA brinda a la comunidad son dependientes de la correcta comunicación con los servidores en la Administración General, es importante definir políticas que reduzcan los riesgos de perder esta comunicación. Por ello se debe tener en cuenta los siguientes puntos:

- El enlace WAN brindado por el proveedor debe responder a un Acuerdo de Nivel de Servicio, en el que se detallen claramente los niveles de confiabilidad, tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio entre otros.
- El administrador de la red filtrará el contenido web al que los usuarios pueden acceder. Para ello se podrá usar las direcciones IP asignadas a

cada equipo. Deben crearse distintas reglas para el acceso, ya que la naturaleza del trabajo de los funcionarios de la AZEA es distinta.

- Se bloqueará todo contenido web cuyo acceso pueda poner en riesgo la integridad de la red o disminuya la productividad. Entre las páginas bloqueadas se tendrá aquellas que contengan: juegos en línea, Messenger como Ebuddy, redes sociales como Facebook, música, video streaming como YouTube, servidores de descarga de archivos como Mediafire, entre otras.
- Se limitará el sentido del tráfico interno de los datos de red, en base a las subredes existentes.
- Se establecerá un documento que tenga la lista de las páginas web permitidas y bloqueadas, definiendo el motivo de su clasificación.

3.3.11.3.3 Seguridad en la red inalámbrica

- La red inalámbrica deberá disponer de una sistema de protección adecuado para evitar que el tráfico de la misma sea vulnerado, por ello se recomienda el uso de WPA2 para protegerla.
- La clave de acceso será entregada solamente a personal autorizado, y en caso de visitantes, se proveerá una clave de acceso de invitado que limite el acceso a los servicios de la AZEA.
- Los equipos de la red inalámbrica deberán ser ubicados sobre el cielo falso del auditorio, evitando que pueda ser visto y accedido fácilmente.
- Se monitoreará el número de usuarios de la red inalámbrica en forma constante, con el objeto de identificar posibles usuarios no autorizados o problemas en la red.

3.3.11.3.4 Firewall

El firewall de la red deberá proteger el intercambio de información entre la red interna e internet, para ello implementará políticas de permisión y prohibición.

- Los puertos permitidos serán abiertos solamente en función de la necesidad, se manejará una política restrictiva, es decir, se mantendrán cerrados todos aquellos que no sean necesarios.

- Los protocolos de red responderán a las necesidades de la AZEA, los que no se usen serán bloqueados.
- El firewall deberá ser implementado mediante hardware.
- Controlará el acceso a internet por parte de los equipos internos mediante un filtro de direcciones IP.

3.3.11.3.5 Protección de los Sistemas Operativos

- Mantener los sistemas operativos actualizados en lo posible.
- Usar sistemas operativos adecuadamente licenciados.
- Utilizar sistemas operativos especializados en el servicio a prestar.
- Definir una clave de administrador local en los equipos que cuente con el nivel de seguridad adecuado y que será usado solo por el personal designado.
- Mantener un registro adecuado de las aplicaciones utilizadas, así como de sus versiones y sus requerimientos para la instalación.
- La compartición de carpetas en la red será configurada solo por personal autorizado, debiendo el usuario justificar el motivo, para así definir los permisos de acceso que dispondrán otros usuarios.
- Se mantendrá adecuadamente organizada la información de los sistemas operativos así como los medios físicos de instalación.

3.3.11.4 Seguridad Física de la red

La seguridad física de la red garantizará el acceso a los equipos solamente por parte de personal autorizado, así como también tendrá las características adecuadas para el cuarto de equipos y los cuartos de telecomunicaciones, para proteger a los equipos.

- Ubicación adecuada de los equipos: los equipos deben ser instalados en los lugares destinados para ello, donde cuenten con las seguridades adecuadas que garanticen un correcto funcionamiento de los mismos.
- Adecuado control de temperatura y humedad dentro del cuarto de equipos, para lo cual se recomienda el uso de un sistema de aire acondicionado, con las características presentadas en el literal 3.3.10.2.3 del presente capítulo.

- Un sistema de suministro de energía, contemplando un adecuado sistema de puesta a tierra y el uso del UPS.
- Verificación constante de los equipos de ventilación.
- La manipulación de equipos será realizada solamente por personal calificado, mismo que contará con los materiales adecuados acorde al proceso a realizarse.
- Mantener los equipos adecuadamente identificados mediante el uso de etiquetas.

3.3.11.4.1 Control de acceso

- No se permite el acceso por parte de personal no autorizado a los cuartos de telecomunicaciones ni al cuarto de equipos.
- Implementación de un sistema de acceso que permita la identificación del usuario que accede a los distintos cuartos protegidos.
- El acceso por parte de personal no autorizado responderá solamente a situaciones emergentes, previo el consentimiento del Jefe de Informática.

3.3.11.4.2 Cableado Estructurado

- El cableado estructurado deberá ser adecuadamente guiado por las canaletas, escalerillas o tuberías según sea el caso, evitando que se exponga.
- Las rutas deben ser adecuadamente documentadas en los planos de la AZEA, identificando el número de cables que pasa por cada canaleta.
- Cumplimiento de las normas establecidas por la EIA/TIA para el cableado estructurado.

3.3.11.4.3 Sistema de Respaldo

- La información de los servidores debe ser respaldada mediante el uso de arreglos de discos.
- Debe monitorearse continuamente el enlace de respaldo.
- Se debe disponer de un sitio seguro y de fácil acceso para los equipos de respaldo.

3.3.12 ADMINISTRACIÓN DE LOS EQUIPOS DE RED

Los equipos de red serán manipulados solamente por personal autorizado, pudiendo estos llevar a cabo las tareas de mantenimiento preventivo, correctivo y predictivo. Todos los mantenimientos deberán ser programados en forma tal, que minimicen el impacto a la continuidad de las operaciones de la AZEA y deberán ser documentadas adecuadamente.

Se deberá disponer de un software que permita una administración adecuada de los equipos, así como de los servicios.

3.4 EQUIPOS DE CONECTIVIDAD

Los equipos de conectividad a ser contemplados para su adquisición comprenden a los switches, access point y el firewall a ser adquiridos. Cabe resaltar que se reutilizarán los siguientes equipos que forman parte de la red actual de la AZEA.

Equipos de conectividad que pueden ser reusados			
Tipo	Marca	Modelo	Uso en la nueva red
Switch	3Com	Super Stack 4 5500 G	Switch de Núcleo
Switch	3Com	Super Stack 4 5500 G	Switch de Núcleo
Switch	3Com	Super Stack 3 4226 T	Switch de acceso

Tabla 3.31 Equipos de conectividad que pueden ser reusados

3.4.1 SWITCHES

A continuación se presentaran dos alternativas para la implementación en dos marcas de gran renombre en el mercado, Cisco y HP que adquirió a 3Com.

3.4.1.1 Cisco

3.4.1.1.1 Cisco Catalyst 3560X 24T-S [PW73]

El switch Cisco 3560X 24T-S es un switch de 24 puertos 10/100/1000 base-T administrable que cuenta con las características mostradas en la tabla 3.32 y que puede ser implementado en la capa de núcleo.

Figura 3.18 Switch Cisco Catalyst 3750X 24T-L

Características del switch CiscoCatalyst3560X 24T-S	
Interfaces	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 USB : 1 x 4 PIN USB tipo A 1 x consola - mini USB tipo B - gestión 1 x RS-232 - RJ-45 - gestión 1 x 10Base-T/100Base-TX - RJ-45 - gestión
Rendimiento	Banda ancha de fibra de interconexión : 160 Gbps
Capacidad	Interfaces virtuales (VLAN) : 1005
Protocolo de direccionamiento	RIP-1, RIP-2, HSRP, direccionamiento IP estático, RIPng
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI
Algoritmo de cifrado	SSL
Método de autentificación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1ae
Memoria RAM	256 MB
Memoria Flash	128 MB Flash
Indicadores de estado	Estado puerto, actividad de enlace, velocidad de transmisión del puerto, modo puerto dúplex, alimentación, sistema
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.32 Características del switch Cisco Catalyst 3560X 24T-S

3.4.1.1.2 Cisco Catalyst WS-C2960S-24TS-L [PW74]

El switch Cisco 2960 24TS-L es un switch de 24 puertos 10/100 base-T administrable que cuenta con las características mostradas en la tabla 3.33 y que puede ser implementado en la capa de distribución.

Figura 3.19 Switch Cisco Catalyst WS-C2960S-24TS-L

Características del switch Cisco Catalyst2960 24TS-L	
Interfaces	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 USB : 1 x 4 PIN USB tipo A 1 x consola - mini USB tipo B - gestión 1 x consola - RJ-45 - gestión 1 x 10Base-T/100Base-TX - RJ-45 - gestión 4 x SFP (mini-GBIC)
Rendimiento	Capacidad de conmutación : 176 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 41.7 Mpps
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH
Algoritmo de cifrado	SSL
Método de autentificación	Secure Shell (SSH), RADIUS, TACACS+
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Memoria RAM	128 MB
Memoria Flash	64 MB Flash
Indicadores de estado	Estado puerto, actividad de enlace, velocidad de transmisión del puerto, modo puerto dúplex, alimentación, sistema
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.33 Características del switch Cisco Catalyst WS-C2960S-24TS-L

3.4.1.1.3 Cisco Catalyst WS-2960-24PC-L [PW75]

Figura 3.20 Switch Cisco Catalyst WS-2960-24PC-L

El switch Cisco Catalyst 2960-24PC-L es un switch de 24 puertos administrable que cuenta con las características mostradas en la tabla 3.34 y que puede ser implementado en la capa de acceso para los teléfonos IP.

Características del switch Catalyst 2960-24PC-L	
Interfaces	24 x 10Base-T/100Base-TX - RJ-45 - PoE 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x SFP (mini-GBIC)
Rendimiento	Capacidad de conmutación : 32 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 6.5 Mpps
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH
Algoritmo de cifrado	SSL
Método de autentificación	Secure Shell (SSH), RADIUS, TACACS+
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Memoria RAM	64 MB
Memoria Flash	32 MB
Indicadores de estado	Actividad de enlace, velocidad de transmisión del puerto, modo puerto dúplex, alimentación, sistema
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.34 Características del switch Cisco Catalyst WS-2960-24PC-L.

3.4.1.1.4 Cisco Catalyst WS-2960-24TC-L [PW76]

El switch Cisco Catalyst 2960-24PC-L es un switch de 24 puertos administrable que cuenta con las características mostradas en la tabla 3.35 y que puede ser implementado en la capa de acceso para los equipos terminales que no requieran de PoE.

Figura 3.21 Switch Cisco Catalyst WS-2960-24TC-L

Características del switch Catalyst 2960-24TC-L	
Interfaces	24 x 10Base-T/100Base-TX - RJ-45 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x SFP (mini-GBIC)
Rendimiento	Capacidad de conmutación : 32 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 6.5 Mpps
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH
Algoritmo de cifrado	SSL
Método de autentificación	Secure Shell (SSH), RADIUS, TACACS+
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Memoria RAM	64 MB
Memoria Flash	32 MB Flash
Indicadores de estado	Actividad de enlace, velocidad de transmisión del puerto, modo puerto dúplex, alimentación, sistema
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.35 Características del switch Cisco Catalyst WS-2960-24TC-L

3.4.1.2 Hewlett Packard (HP)

3.4.1.2.1 HP A5500-24G JD377A [PW77] [PW78]

Figura 3.22 Switch HP A5500-24G JD377A

El switch HP A5500-24G JD377A es un switch de 24 puertos 10/100/1000 Base-T administrable que cuenta con las características mostradas en la tabla 3.36 y que puede ser implementado en la capa de núcleo.

Características switch HPA5500-24GJD377A	
Interfaces	1 x consola - RJ-45 - gestión 24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 4 x SFP (mini-GBIC)
Rendimiento	Capacidad de conmutación: 128 Gbps Rendimiento de reenvío: hasta 95,2 millones de pps
Tamaño de tabla de dirección MAC	12000 de entradas
Protocolo de direccionamiento	OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMPv2, IGMP, VRRP, OSPFv2, PIM-SM, PIM-DM, IGMPv3, GRE, OSPFv3, PIM-SSM, MSDP, enrutamiento IPv4 estático, enrutamiento IPv6 estático, ECMP, RIPng
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, CLI
Algoritmo de cifrado	SSL
Método de autentificación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3i, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1ad, IEEE 802.1ab (LLDP)
Memoria RAM	256 MB – SDRAM
Memoria Flash	32 MB Flash
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.36 Características del switch HP A5500-24GJD377A

3.4.1.2.2 HP A5120-24G JE068A [PW79] [PW80]

El switch HP A5120-24G es un switch de 24 puertos 10/100/1000 Base-T administrable que cuenta con las características mostradas en la tabla 3.37 y que puede ser implementado en la capa de distribución.

Figura 3.23 Switch HP A5120-24G JE068A

Características del switch HP A5120-24G JE068A	
Interfaces	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x consola - RJ-45 - gestión 4 x SFP (mini-GBIC)
Rendimiento	Capacidad de conmutación: 144 Gbps Rendimiento de reenvío: hasta 107.2 millones de pps
Tamaño de tabla de dirección MAC	16K de entradas
Protocolo de direccionamiento	Enrutamiento IPv4 estático, enrutamiento IPv6 estático
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, CLI
Algoritmo de cifrado	SSL
Método de autentificación	Secure Shell (SSH), RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 ¦ 1 x consola - RJ-45 - gestión ¦ 4 x SFP (mini-GBIC)
Memoria RAM	128 MB - SDRAM
Memoria Flash	16 MB Flash
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.37 Características del switch HP A5500-24GJE068A

3.4.1.2.3 HP 2620-24 J9623A [PW81] [PW82]

El switch HP 2620-24 es un switch de 24 puertos administrable que cuenta con las características mostradas en la tabla 3.38 y que puede ser implementado en la capa de acceso para los equipos terminales que no requieran de PoE.

Figura 3.24 Switch HP 2620-24

3.4.1.2.4 HP E2610-24 J9087A [PW83] [PW84]

El switch HP 2510-24es un switch de 24 puertos administrable que cuenta con las características mostradas en la tabla 3.39 y que puede ser implementado en la capa de acceso para los equipos terminales que requieran de PoE.

Figura 3.25 Switch HP E2610-24 J9087A

Características del switch HP 2620-24 J9623A	
Interfaces	24 x 10Base-T/100Base-TX - RJ-45 2 x SFP (mini-GBIC) Serial:1 x consola - RJ-45 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45
Rendimiento	Capacidad 9.5 Mpps Capacidad de conmutación:12.8 Gbps
Tamaño de tabla de dirección MAC	16000 de entradas
Protocolo de direccionamiento	RIP-1, RIP-2, IGMPv3, MLDv2, MLD
Protocolo de gestión remota	SNMP 1, RMON 2, RMON, Telnet, SNMP 3, SNMP 2c, HTTPS, TFTP, SMON
Algoritmo de cifrado	SSL
Método de autentificación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1v, IEEE 802.1ab (LLDP)
Memoria RAM	512 MB – SDRAM
Memoria Flash	4 MB Flash
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.38 Características del switch HP 2620-24 J9623A

Características del switch HP E2610-24 J9087A	
Interfaces	24 x 10Base-T/100Base-TX - RJ-45 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x RJ-45 - gestión 2 x SFP (mini-GBIC)
Rendimiento	12,8 Gbps Rendimiento de reenvío: hasta 9,5 millones de pps
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de direccionamiento	IGMPv3
Protocolo de gestión remota	RMON 2, Telnet, HTTP, SSH, SSH-2
Algoritmo de cifrado	SSL

Método de autentificación	Secure Shell (SSH), RADIUS, TACACS+
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1af
Memoria RAM	128 MB – SDRAM
Memoria Flash	16 MB Flash
Garantía del fabricante	Garantía limitada de por vida

Tabla 3.39 Características del switch HP E2610-24 J9087A

3.4.2 FIREWALLS

3.4.2.1 Cisco ASA 5510-K8 [PW85]

Figura 3.26 Firewall CISCO ASA 5510-K8

Características del firewall CISCO ASA 5510-K8	
Interfaces	5 x red - Ethernet 10Base-T/100Base-TX - RJ-45 1 x serial - auxiliar - RJ-45 2 x Hi-Speed USB - 4 PIN USB tipo A
Rendimiento	Capacidad del cortafuegos : 300 Mbps Tasa de conexiones : 9.000 conexiones por segundo Capacidad de la VPN : 170 Mbps
Sesiones concurrentes	50.000
Algoritmo de cifrado	DES
Cantidad de túneles VPN	50
Características adicionales	Protección firewall, asistencia técnica VPN, equilibrio de carga, soporte VLAN
Memoria RAM	1 GB
Memoria Flash	256 MB

Tabla 3.40 Características del firewall Cisco ASA 5510-K8

3.4.2.2 HP S200-S UTM APPLIANCE [PW86]

Figura 3.27 Firewall HP S200-S UTM APPLIANCE

Características del firewall HP S200-S UTM APPLIANCE	
Interfaces	5 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x serial - RJ-45
Rendimiento	Capacidad del cortafuegos : 200 Mbps Capacidad IPS : 30 Mbps Rendimiento del antivirus : 30 Mbps Capacidad VPN (DES IPSec) : 100 Mbps
Capacidad	Conexiones concurrentes : 60000 Zonas de seguridad : 32 Cortafuegos virtuales : 4 Túneles IPSec VPN simultáneos : 500 Asociaciones seguras : 24000 Interfaces de router IP : 4000 Rutas RIP/OSPF : 10000
Algoritmo de cifrado	DES, Triple DES, IKE, AES de 128 bits, AES de 192 bits, AES de 256 bits
Protocolos de gestión remota	SNMP 1, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, FTP, SSH
Método de Autenticación	RADIUS, certificados X.509, TACACS+
Cantidad de túneles VPN	512
Características adicionales	Protección firewall, Encaminamiento IP, soporte de NAT, asistencia técnica VPN, soporte ARP, soporte VLAN, limitación de tráfico, prevención contra ataque de DoS (denegación de servicio), soporte IPv6, análisis de antivirus, Sistema de prevención de intrusiones (IPS), filtrado de URL, prevención de ataque DDos, protección anti-spam, Quality of Service (QoS), Servidor DHCP, DNS proxy
Protocolo de direccionamiento	RIP-1, RIP-2, BGP, IGMPv2, IGMP, VRRP, OSPFv2, PIM-SM, direccionamiento IP estático, PIM-DM, IGMPv3, GRE, OSPFv3, RIPng

Tabla 3.41 Características del firewall HP S200-S UTM APPLIANCE

En base a la selección de equipos realizada anteriormente, es recomendable el uso del firewall HP S200-S UTM APPLIANCE, para mantener una heterogeneidad en la red así como por sus características que suplen las necesidades presentes en la AZEA.

Es importante resaltar que los servicios adicionales para mitigar riesgos necesitan de la adquisición de licencias adicionales, tales costos se ven reflejados en la tabla 3.42.

Características del firewall CISCO ASA 5510-K8	
Descripción	Costo
HP S200-S UTM APPLIANCE	1.616,25
HP Sec Path U200-S 1 Year AV Updates	558,73
HP Sec Path U200-S 1 Year Anti-Spam Serv	757,83
Total	2.432,81

Tabla 3.42 Costos del firewall [PW87]

Dichos servicios adicionales pueden ser suplidos a través de otros métodos, quedando a criterio de los administradores de red la adquisición de dichas licencias.

3.4.3 ACCESS POINTS

3.4.3.1 Cisco AIR-LAP1262N-A-K9 [PW88]

Figura 3.28 Access Point CISCO AIR-LAP1262N-A-K9

Características del Access Point Cisco AIR-LAP1262N-A-K9	
Interfaces	1 x red / energía - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x gestión - consola - RJ-45 6 x antena
Velocidad de transferencia de datos	300 Mbps
Método de espectro expandido	OFDM
Protocolo de gestión remota	SNMP
Algoritmo de cifrado	AES, TLS, PEAP, TTLS, TKIP, WPA, WPA2
Características adicionales	Auto-sensor por dispositivo, alimentación mediante Ethernet (PoE), tecnología MIMO, soporte Wi-Fi Multimedia (WMM), tecnología M-Drive de Cisco
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n
Cumplimiento de	IEEE 802.11b, IEEE 802.11a, IEEE 802.11d, IEEE

normas	802.11g, IEEE 802.1x, IEEE 802.11i, IEEE 802.11h, IEEE 802.11n
Memoria RAM (max)	128 MB
Memoria Flash (max)	32 MB
Garantía	Garantía limitada de por vida

Tabla 3.43 Características del Access Point Cisco AIR-LAP1262N-A-K9

3.4.3.2 HP E-MSM430 Dual Radio 802.11n AP J9651A [PW89]

Figura 3.29 Access Point HP E-MSM430 Dual Radio 802.11n AP

Características del Access Point Cisco AIR-LAP1262N-A-K9	
Interfaces	1 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x serial - consola - RJ-45
Velocidad de transferencia de datos	450 Mbps
Antena	Integrada, Omnidireccional, 6 antenas
Protocolo de gestión remota	SNMP 3, SNMP 2c
Algoritmo de cifrado	AES, TLS, PEAP, TTLS, TKIP, WPA, WPA2, MD2
Características adicionales	Señal ascendente automática (MDI/MDI-X automático), Intrusion Detection System (IDS), Sistema de prevención de intrusiones (IPS), filtrado de direcciones IP, soporte Wi-Fi Multimedia (WMM), Quality of Service (QoS), admite varios SSID
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 801.1p, IEEE 802.11i, Wi-Fi CERTIFIED, IEEE 802.11e, IEEE 802.11n
Admite Power over Ethernet	Sí
Garantía	Garantía limitada de por vida

Tabla 3.44 Access Point HP E-MSM430 Dual Radio 802.11n AP

3.4.4 SELECCIÓN DE LA SOLUCIÓN

Esta decisión también se ve influenciada por el costo de la implementación de la misma, pues la solución de HP presenta características similares a las de Cisco pero con un menor costo.

Los equipos de las dos soluciones presentadas anteriormente cumplen con las características mínimas especificadas para obtener un correcto funcionamiento de la red multi-servicios a ser implementada.

Se recomienda el uso de la solución presentada por HP debido a:

- La reutilización de equipos que se podría dar con los switches de núcleo y que son de marca 3Com, brindaría homogeneidad en el fabricante de dispositivos, facilitando su interoperabilidad.
- La solución propuesta por Cisco, a pesar de cumplir con los requisitos mínimos, hace uso de una gran cantidad de protocolos propietarios que limitan el uso de ciertas características en la red.
- La decisión también se vio influenciada por el costo de la implementación de la misma, pues la solución de HP presenta características similares a la de Cisco pero con un menor costo.

3.4.5 SERVIDORES

De acuerdo a las características descritas en la tabla 3.17 acerca de las características de los servidores acorde al sistema operativo y servicio a prestar, se procede a la selección de los servidores que cumplan con las mismas. Los servidores recomendados pertenecen a la marca *DELL* y son: *Power Edge T110 II* y *Power Edge R310.* Su selección obedeció a que cumplen con las características mínimas especificadas a más de fiabilidad, escalabilidad, buen rendimiento y flexibilidad.

La tabla 3.45 muestra el precio referente a los servidores junto a las características de los mismos, el precio enunciado corresponde a los servidores con el hardware adecuado.

Figura 3.30 Servidores Dell: Power Edge T110 II y Power Edge R310 [PW90]

Cabe resaltar que con la finalidad de reducir los costos en la implementación de los servidores es posible el uso de la virtualización, sin embargo la presente configuración de la red no hace uso de tal técnica pero los servidores mencionados dan soporte para este tipo de implementación.

Características de los servidores		
Características	Power Edge T110 II	Power Edge R310
Procesador	Intel Xeon E3-1220v2 3.10 GHz, 8M Cache, Turbo, Quad Core/4T (69W)	Intel® Xeon® X3440, 2.53 GHz, 8M Cache, Turbo, HT
Memoria RAM	4GB Memory (2x2GB), 1333MHz, Single Ranked UDIMM	4GB Memory (2x2GB), 1333MHz Single Ranked UDIMM
Interfaces de red	Adaptador Gigabit Ethernet Integrado de un solo puerto, Broadcom 5709 Dual Port 1GbE NIC w/TOE iSCSI, PCIe-4.	Adaptador Gigabit Ethernet Integrado de doble puerto
Disco duro	2 Discos Duros 500GB 7.2K RPM Near-Line SAS 3.5" 6Gps	2 Discos Duros 500GB 7.2K RPM SATA 3.5in Cabled Hard Drive

Tabla 3.45 Características de los servidores Dell [PW91]

Los servidores no incluyen un sistema operativo de fábrica, lo que implica que se debe realizar el proceso de instalación y configuración de los servicios previamente a su uso, es importante destacar que los servidores alojarán sistemas de software libre que no implica ningún gasto por licencias de uso a excepción del servidor de respaldo que es gestionado por la Administración General del IMQ.

3.4.6 TELEFONÍA IP

3.4.6.1 Teléfonos IP

3.4.6.1.1 Yealink SIP – T20P [PW92]

El teléfono IP Yealink SIP – T20P es un teléfono IP con 2 líneas y 2 cuentas SIP, voz HD y que además tiene 2 puertos RJ-45 con POE que cuenta con las características mostradas en la tabla 3.46.

Figura 3.31 Teléfono IP Yealink SIP – T20P

Características del Teléfono IP Yealink SIP – T20P	
Teléfono	2 cuentas VoIP, línea directa, llamada de emergencia, llamada en espera, transferencia de llamadas, desvío de llamadas, identificador de llamadas, lista de llamadas, conferencia de 3 vías, multilenguaje (20 idiomas), descolgado de marcación automática, respuesta automática, plan de marcación flexible.
Red	SIP v1 (RFC2543), v2 (RFC3261), IPV6, DNS SRV (RFC3263), DTMF: In-Band, RFC2833, SIP Info, modo proxy and modo de enlace SIP peer-to-peer, direccionamiento IP: Estático/DHCP/PPPoE, cliente TFTP/DHCP/PPPoE, servidor Telnet/HTTP/HTTPS, cliente DNS, servidor NAT/DHCP
Codecs y voz	Códec de banda ancha: G.722, Códec de banda estrecha: G.711µ/A, G.723.1, G.726, G.729AB VAD, CNG, AEC, PLC, AJB, AGC, Full-dúplex altavoz con AEC
Calidad de servicio	VLAN QoS (802.1pq)
Seguridad	802.1x, VLAN QoS (802.1pq), LLDP, Transport Layer Security (TLS), HTTPS (servidor/cliente), SRTP (RFC3711) Autenticación implícita utilizando MD5/MD5-sess Archivo de configuración a través de encripción segura AES Bloqueo de teléfono para la protección de la privacidad personal Modo de configuración Admin/VAR/Usuario nivel 3
Administración	FTP / TFTP / HTTP / PnP de aprovisionamiento automático, Configuración: Navegador / teléfono / auto-prestación Llamada directa IP sin proxy SIP

	Marcación del número a través del servidor SIP Marcación de la URL a través de un servidor SIP
Sistema de integración IP PBX	Plan de marcado, marcado ahora, correo de voz, MWI, Intercom, captura de llamadas, tono de timbre distintivo
Física	TITAN chipset TI LCD de 3 líneas con una línea de iconos y 2x15 líneas de caracteres 31 teclas incluyendo 9 teclas de función 4 LEDs: 1xpower, 2xline, 1xmessage 1xRJ9 del puerto del auricular 2xRJ45 10/100M Ethernet Montaje en pared Fuente de alimentación: AC 100 ~ 240V de entrada y de salida de CC 5V/1.2A Power over Ethernet (IEEE 802.3af) Consumo de energía: 1.4-2.6W Peso neto: 0.77kg Dimensiones: 185 x 200 x 90mm Humedad: 10 ~ 95% Temperatura de almacenamiento: hasta 60 ° C
Admite Power over Ethernet	Sí
Garantía	1 año contra fallas de fábrica

Tabla 3.46 Características del teléfono IP Yealink SIP – T20P

3.4.6.1.2 Grandstream GXP1450 [PW93]

El teléfono IP Grandstream GXP1450 es un teléfono IP con 2 líneas y 2 cuentas SIP, voz HD y que además tiene 2 puertos de red con POE integrado que cuenta con las características mostradas en la tabla 3.47.

Figura 3.32 Teléfono IP Grandstream GXP1450

Características del Teléfono IP Grandstream GXP1450	
Teléfono	2 líneas y 2 cuentas SIP, transferencia de llamadas, hacia delante, conferencia de 3 vías, llamada en espera , registro de llamadas, XML de personalización de la pantalla, descolgado de marcación automática, respuesta automática, plan de marcación flexible, escritorios compartidos, tonos de llamada personalizados de música y música en espera, Multilenguaje.
Red	SIP RFC2361, TCP / IP / UDP, RTP, HTTP / HTTPS, ARP / RARP, ICMP, DNS (un registro, SRV, NAPTR), DHCP, PPPoE, Telnet, TFTP, NTP, STUN, SIMPLE, TR-069, 802,1x.
Codecs y voz	Soporte para G.723.1, G.729A / B, G.711u / a, G.726-32, G.722 (banda ancha), iLBC, en banda y fuera de banda DTMF (en audio, RFC2833 , SIP INFO) Avanzado Procesamiento Digital de Señales (DSP), Supresión de Silencio, VAD, CNG, AGC
Calidad de servicio	Capa 2 (802.1Q, 802.1p) y Capa 3 (ToS, DiffServ, MPLS) QoS
Seguridad	Contraseñas a nivel de usuario y de administrador, autenticación basada en MD5 y MD5-sess, archivo de configuración de seguridad basado en AES, SRTP, TLS, 802.1x.
Administración	TFTP / HTTP
Física	Pantalla iluminada LCD gráfica 180x60 con hasta 4 niveles de grises 2 teclas de línea con LED de dos colores y 2 cuentas SIP independientes, , 5 teclas de navegación/menú/volumen, 10 teclas de función 1xRJ9 del puerto del auricular Dos puertos conmutados 10/100Mbps con PoE integrado. Montaje en pared Adaptador de corriente incluido: Entrada: 100-240VAC 50-60Hz, salida: 5 V DC, 800 mA Power over Ethernet (IEEE 802.3af) Consumo de energía: 2.5W Peso neto: 0.8kg Dimensiones: 186 x 210 x 81mm Humedad: 10 ~ 90% Temperatura de almacenamiento: hasta 40 ° C
Admite Power over Ethernet	Sí
Garantía	1 año contra fallas de fábrica

Tabla 3.47 Características del teléfono IP Grandstream GXP1450

3.4.6.2 Tarjetas PCI

3.4.6.2.1 Digium TDM808E – 8 FXO Ports [PW94]

Figura 3.33 Tarjeta Digium TDM808E

La tarjeta Digium TDM808E – 8 FXO Ports – Includes Echo Cancellation es un tarjeta analógica con puertos FXO y cancelación de echo que cuenta con las características mostradas en la tabla 3.48.

Características de la tarjeta Digium TDM808E	
Puertos FXO	8
Cancelación de eco	Sí
Interface	PCI estándar
Compatibilidad con Elastix	Sí
Garantía	1 año contra fallas de fábrica

Tabla 3.48 Características de la tarjeta Digium TDM808E

3.4.6.2.2 Sangoma A20004D 8 FXO analog card w/Ecan PCI [PW95]

Figura 3.34 Tarjeta Sangoma A20004D.

La tarjeta Sangoma A20004D 8 FXO analog card w/Ecan PCI es un tarjeta analógica con puertos FXO y cancelación de echo que cuenta con las características mostradas en la tabla 3.49.

Características de la tarjeta Sangoma A20004D	
Puertos FXO	8
Cancelación de eco	Sí
Interface	PCI estándar
Compatibilidad con Elastix	Sí
Garantía	1 año contra fallas de fábrica

Tabla 3.49 Características de la tarjeta Sangoma A20004D

3.5 PLAN DE MIGRACIÓN [PW96] [PW97] [PW98]

Ante las necesidades de la AZEA, un plan de migración, permitirá de forma ágil y en el menor tiempo posible el traspaso del entorno de la red de datos actual hacia un entorno basado en el nuevo diseño de red para ofrecer múltiples servicios, que ayudará a los empleados de la Administración a brindar una atención eficiente y de calidad al público, contemplando además que la Administración debe continuar prestando sus servicios a la población de manera ininterrumpida.

3.5.1 OBJETIVO

Al finalizar la migración se pretende que todos los equipos de red, estén trabajando en ambiente multi-servicios. Así también todos los empleados de la AZEA que tengan acceso a una estación de trabajo, se encuentren debidamente capacitados ante el nuevo entorno de trabajo.

3.5.2 FASES PARA LA MIGRACIÓN

Para llevar a cabo un efectivo plan de migración, se debe considerar varias fases con el propósito de simplificar el proceso que implica el cambio de una red de datos, a la que se han acostumbrado por varios años, a una red de datos convergente capaz de proporcionar varios servicios, que para el usuario final puedan ser totalmente nuevos y desconocidos.

En gran parte, el éxito de la migración dependerá de la asimilación de los usuarios finales hacia los nuevos servicios y sus funcionalidades. Para ello se propone realizar el proceso en 3 fases que facilitarán la migración progresiva hacia la nueva red de datos permitiendo el desarrollo de las actividades en la AZEA.

3.5.2.1 Primera fase: levantamiento de información

En esta fase se debe obtener los datos y toda la información concerniente a la AZEA que sea relevante para el plan de migración. Los principales recursos que influyen directamente en el plan son: el personal, hardware, software, requerimientos de red y áreas críticas.

- Personal: El personal de la AZEA se puede clasificar en personal técnico y usuario final.
    - El personal técnico, son aquellas personas de la Jefatura Zonal de Informática, quienes se encargarán de atender a los usuarios finales, así también serán los encargados de la instalación, configuración, mantenimiento y soporte de los nuevos servicios, una vez que se ha implementado la red multi-servicios.
    - Los usuarios finales, corresponden al personal de la AZEA que disponen de una estación de trabajo.

  El personal de la AZEA durante el tiempo que ha estado trabajando no ha usado herramientas para videoconferencia (Openmeetings) y streaming de video (red5), por tal motivo se establece que el personal desconoce totalmente este tipo de aplicaciones, las cuales necesitan un navegador web y flash para funcionar correctamente.
- Hardware: Es importante tener detallado este tipo de recurso ya que permite conocer si el hardware actual puede o no soportar los nuevos servicios. Los recursos de hardware que posee la Administración se encuentran referidos en el capítulo 2.
- Software: La información del software instalado en las máquinas, permite establecer si ya existen aplicaciones cliente que usarán los nuevos servicios. Los recursos de software que posee la Administración se encuentran referidos en el capítulo 2.
- Requerimientos de red: Los requerimientos de red para los servicios en la AZEA se encuentran referidos en el capítulo 2.
- Áreas críticas: De acuerdo a la función que cumple la AZEA, los departamentos más sensibles que se han establecido, son aquellos que atienden directamente al usuario. A continuación se detallan los

departamentos de acuerdo al grado de sensibilidad. En la tabla 3.50 se puede observar los departamentos según su grado de sensibilidad.

Sensibilidad	Edificio	Piso	Departamento
Alta	Principal	Planta Baja	Recaudación Rentas Gestión Urbana Jefatura Zonal de Avalúos y Catastros Secretaría General Información
Media Alta			Comunicación Social
		Primer Piso	Subprocuraduría Zonal
		Segundo Piso	Administrador y Secretaría Jefatura Zonal de Financiero
Media		Planta Baja	Archivo Coordinación Zonal de Territorio Escuela de Formación Ciudadana Jefatura Zonal de Coordinación Parroquial
		Primer Piso	Jefatura Zonal de Control de la Ciudad Coordinación de Gestión y Control Coordinación de Desarrollo Zonal Jefatura Zonal de Educación, Cultura, Deportes y Recreación Jefatura Zonal de Fiscalización Gerencia de Espacio Público (EMMOP) Gestión Urbana Jefatura Zonal de Medio Ambiente Jefatura Zonal de Territorio y Vivienda Jefatura Zonal de Obras Públicas, Parques y Jardines Jefatura Zonal de Salud Jefatura Zonal de Seguridad Ciudadana
		Segundo Piso	Jefatura Zonal Administrativo Auditorio Coordinación Zonal de Administración y Servicios Jefatura Zonal de Informática Jefatura de Proyectos Jefatura Zonal de Talento Humano
	Secundario	Planta Baja	Centro de Equidad y Justicia, Comisarías de Laderas
		Primer Piso	Comisaría de Salud y Ambiente Comisaría Sur este Comisaría Sur Oeste Dispensario Médico

Tabla 3.50 Departamentos según su grado de sensibilidad

3.5.2.2 Segunda Fase: Capacitación

En el proceso de migración, se debe dar una alta prioridad a la instrucción del personal que usará los servicios del nuevo diseño, ya que de la aceptación y/o resistencia de ellos a la red multi-servicios depende el éxito del rediseño.

La capacitación se dará al personal referido en la primera fase:

- Capacitación al personal técnico: La capacitación al personal técnico tiene como objetivo agilizar el proceso de migración, así también tener personal que pueda cumplir con el mantenimiento de la nueva red y sus servicios, luego de haber sido instalada.
- El personal técnico deberá seguir cursos encaminados a comprender las nuevas herramientas que proporciona la red multi-servicios. Estos cursos deberán estar orientados al manejo de servidores y aplicaciones que soporten videoconferencia, streaming de video y telefonía IP; servidores DNS, DHCP, Proxy, correo electrónico, firewall, etc.
- Capacitación al usuario final: la capacitación al usuario final tiene como objetivo minimizar el impacto que pueden implicar los nuevos servicios y la forma de usarlos. De igual manera se pretende que el usuario final se adapte a ellos y pueda utilizarlos como una herramienta a favor de sus actividades diarias en la AZEA.
- Para llevar a cabo la capacitación, se recomienda que el personal reciba cursos orientados al manejo de las aplicaciones, que ofrecerán los nuevos servicios, explicándoles además, para qué son útiles, así como los beneficios que existen al usarlos. En la tabla 3.51 se muestran algunos cursos recomendados.

3.5.2.3 Tercera Fase: Migración

En esta fase se especifica la manera en que se llevará a cabo el cambio de la red actual a la red multi-servicios. Para ello se realizará la migración en dos etapas. La primera etapa considera que, todos los trabajos que se realicen serán llevados a cabo en horario laboral (lunes a viernes de 8:00 a 16:00), y la segunda etapa se

realizará en horario especial (lunes a viernes de 17:00 a 22:00, además sábados y domingos, dependiendo de la tarea).

Cursos Recomendados				
Nombre	Modalidad	Duración [horas]	Costo [$]	Personal
Linux Administrador I	Virtual	45	135	Técnico
TCP/IP sobe Linux	Presencial	32	199	Técnico
Servidores Web sobre Linux	Presencial	32	199	Técnico
Diseño e Implementación de telefonía IP con Elastix	Presencial	32	199	Técnico
Uso de Aplicaciones en tiempo real	Presencial	5	35	Técnico Usuario Final

Tabla 3.51 Cursos recomendados para el personal de la AZEA

3.5.2.3.1 Primera Etapa

La primera etapa contempla:

- Configuración de los equipos de red, tales como el access point, switches y routers, para soportar el rediseño de la red y los nuevos servicios que se proporcionarán. Tabla 3.52

Cantidad	Equipos	Tiempo estimado [minutos]	Tiempo estimado [horas]
1	Router Cisco 1	50	0,83
1	Router Cisco 2	50	0,83
1	Firewall	50	0,83
1	Switch Núcleo	50	0,83
1	Switch Núcleo Respaldo	50	0,83
1	Switch DMZ	50	0,83
4	Switch Distribución	200	3,33
18	Switch Acceso	780	13,00
1	Access Point	120	2,00
29	TOTAL	1220	23,33
	Días laborables	2,92	
	Tiempo destinado [días]	3	
	Personas	1	

Tabla 3.52 Tiempo estimado para configuración de equipos

- Se establece que el tiempo estimado para la instalación de los sistemas operativos y sus respectivas actualizaciones para cada servidor, en el hardware recomendado será de 5 horas, al ser cuatro servidores, se tiene un total de 20 horas.
- El tiempo estimado para la configuración de servicios se muestra en la tabla 3.53.

SERVICIOS	Tiempo estimado [minutos]	Tiempo estimado [horas]
Turnos	120	2
Gdoc	120	2
Active Directory	360	6
DNS	180	3
DHCP	120	2
Proxy	180	3
Videoconferencia	960	16
Streaming de video	960	16
Correo electrónico	360	6
Telefonía IP	2400	40
Total	5760	96
Tiempo destinado [horas]	72	
Tiempo destinado [días]	9	
Personas	2	

Tabla 3.53 Tiempo estimado para configuración de servicios

- Preparación y adecuación de los cuartos de telecomunicaciones y cuarto de equipos, con el fin de que estén listos para la colocación del nuevo cableado y los equipos.

Cantidad	Concepto	Tiempo estimado [días]	Precio [$]
3	Cuartos de telecomunicaciones	35	200
1	Cuarto de Equipos		

Tabla 3.54 Tiempo estimado para adecuar los cuartos [12]

- Perforación de paredes. El tiempo que tomará en realizar las perforaciones se muestran en la tabla 3.55.

[12] Herrera. G., Obra Civil, Telf.: 097338321, Quito, Ecuador.

- La perforación del piso para la interconexión entre edificios se estima que se realizará en dos semanas, esto implica la perforación del canal para poner el tubo que interconecta al edificio principal con el edificio secundario, ubicación del tubo por el canal, paso de los cables por el tubo y el relleno del canal.

Cantidad	Concepto	Tiempo estimado [horas]	Precio [$]
44	Perforación de Pared	44	880
	Días laborables	5,50	
	Tiempo destinado [días]	3	
	Personas	2	

Tabla 3.55 Tiempo estimado para perforaciones de pared [G1]

Cantidad	Concepto	Tiempo estimado [minutos]	Tiempo total [minutos]
2	Colocación de tubo	120	240
8	Pasar cable	10	80
16	Poncheo	2	32
8	Testeo	2	16
16	Etiqueta	2	32
		Total	400
	Tiempo destinado [días]	2	
	Personas	2	

Tabla 3.56 Tiempo estimado para la instalación del backbone [PW99]

- Implementación del backbone de la nueva red, esto implica ubicación del tubo, el paso de cables por el mismo, ubicación de los racks, instalación de los switches y patch panels, parcheo y etiquetado correspondiente.

  El detalle completo de la estimación de tiempo del backbone se encuentra en el anexo J-1.

  La ubicación de racks, patch panels y equipos de red se estima que tomará 3 horas.

- Implementación del cableado estructurado en el Departamento de Informática, para llevar a cabo las pruebas necesarias. El tiempo estimado

para tener listo el cableado en este departamento es de aproximadamente 7 horas y será llevado a cabo por 2 personas. El cálculo detallado del tiempo de estimación se encuentra en el anexo J-4.

- Ubicación de canaletas, según las necesidades del nuevo cableado, en lugares donde no se altere la continuidad del trabajo del personal de la AZEA, ya que son lugares amplios en los cuales se puede instalar el cableado sin generar tantas molestias (en horario laborable).

A continuación se presenta un ejemplo para la estimación del tiempo que tomará instalar el cableado estructurado en el Auditorio.

Auditorio				
Cantidad	Concepto	Tiempo estimado [minutos]	Puntos de red [minutos]	Tiempo estimado [horas]
30	Colocación de canaleta	12	360	6,00
7	Pasar cable	10	70	1,17
14	Poncheo	2	28	0,47
7	Colocación de face-plate	3	21	0,35
7	Testeo	2	14	0,23
14	Etiqueta	2	28	0,47
		Total	521	8,68
	Tiempo destinado [horas]	5		
	Personas	2		

Tabla 3.57 Tiempo estimado para el Auditorio [PW99]

En la tabla 3.58 se muestra el tiempo estimado que tomaría realizar el cableado estructurado en los lugares donde las molestias son mínimas.

En las zonas amplias el tiempo total estimado es aproximadamente de 32 horas. El cálculo completo de cada uno de los departamentos que se ha establecido como zonas amplias se encuentra en el anexo J-2.

- La ubicación del Access Point, se estima que tomará 2 horas.
- La configuración de las estaciones de trabajo para soportar las nuevas aplicaciones, se basa en la instalación de Adobe Flash Player, ya que

funcionan mediante un navegador web y la herramienta antes mencionada. El tiempo estimado para realizar esta tarea se encuentra en la tabla 3.59.

Edificio	Piso	Departamento	Puntos de red	Tiempo estimado [horas]
Principal	Segundo Piso	Auditorio	7	8,68
		La parte de Secretaría del Administrador	5	6,92
Secundario	Primer Piso	Dispensario Médico	9	5,45
	Planta Baja	Centro de Equidad y Justicia	18	9,90
		Total	39	30,95
		Tiempo destinado [horas]	18	
		Personas	2	

Tabla 3.58 Zonas amplias en la AZEA y tiempo de instalación del cableado

Cantidad	Concepto	Tiempo estimado x1 [minutos]	Tiempo estimado [horas]
24	Estaciones de trabajo	15	6
	Tiempo destinado [horas]	4	
	Personas	2	

Tabla 3.59 Tiempo estimado para la configuración de las estaciones de trabajo de la primera etapa

- Los teléfonos IP deberán ser configurados de forma manual, ingresando la IP, máscara de red, gateway, extensión y nombre. En la tabla 3.60 se ve el tiempo estimado que tomaría configurar estos equipos.

Cantidad	Concepto	Tiempo estimado x1 [minutos]	Tiempo estimado [horas]
14	Teléfonos IP	20	4,67
	Tiempo destinado [horas]	3	
	Personas	2	

Tabla 3.60 Tiempo estimado para la configuración de teléfonos IP

- Realización de pruebas, para determinar si el cableado junto con los servicios que se han instalado, incluido el backbone, funcionan correctamente o no. Si las pruebas son positivas, se continuará normalmente con el calendario establecido. Si las pruebas no concuerdan con lo requerido, se establecerá el tiempo necesario (de 1 hora a 15 días laborables) para cumplir con los requerimientos o corregir fallas en la instalación del cableado estructurado.

  Las pruebas se realizarán como ya se mencionó desde el Departamento de Informática y contemplarán los posibles entornos en que una aplicación podría ser usada por el personal de la AZEA, para lo cual se verificará:

  - Conectividad en cada punto que se ha instalado, haciendo el test correspondiente.
  - Comprobar la accesibilidad hacia los servicios.
  - Compatibilidad y funcionamiento de las aplicaciones con los servicios.
  - Comprobar la estabilidad de los servicios, así como de las aplicaciones.
  - Comprobar que el software y hardware usado cumplan las expectativas de la AZEA.

3.5.2.3.2 Segunda Etapa

La segunda etapa contempla:

- Implementación del cableado estructurado en las áreas de alta sensibilidad que se mencionan en la primera fase. Esto se lo debe hacer en un fin de semana por turnos rotativos, comenzando a las 17:00 horas del viernes, a partir de ese momento se dispone de 60 horas para terminar, es decir que el cableado y los servicios en aquellas aéreas se encontrarán listos el lunes desde 5:00 en adelante, para no alterar la continuidad de las labores de los funcionarios de la AZEA.

En total en ésta área se instalarán 52 puntos, incluidos voz y datos. Se estima que se tomará un tiempo de 40 horas, para tener listo el cableado en esta zona.

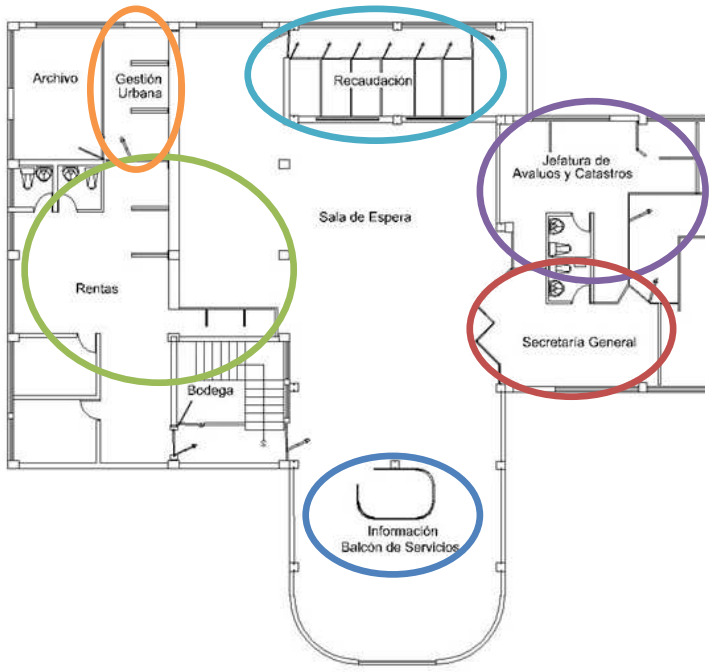


Figura 3.35 Áreas de Alta Sensibilidad. Panta Baja, Edificio Principal

En el anexo J-3 se muestra el detalle del cálculo de las áreas de alta sensibilidad.

Departamento	Puntos de red	Tiempo estimado [horas]
Gestión Urbana	5	5
Información	10	7
Recaudación	8	6
Rentas	10	8
Secretaría General	5	5
Jefatura Zonal de Avalúos y Catastros	13	10
Total	51	41
Tiempo destinado [horas]	60	
Personas	4	

Tabla 3.61 Áreas de alta sensibilidad y tiempo de instalación del cableado

- Implementación del cableado estructurado en el Segundo Piso del Edificio Principal, en este piso existen 59 puntos, que en la primera etapa no fueron tomados en consideración para el cableado, estos se irán implementando en horarios nocturnos a partir de las 17:00 en adelante.

Departamento	Puntos de red	Tiempo estimado [horas]
Administrador	5	3,92
Jefatura de Proyectos	3	3,15
Jefatura Zonal de Financiero	17	11,52
Jefatura Zonal Administrativo	15	10,75
Bodega	3	4,15
Jefatura Zonal de Talento Humano	8	6,07
Coordinación Zonal de Administración y Servicios	8	8,07
Total	59	47,62
Tiempo destinado [horas]	30	
Personas	2	

Tabla 3.62 Departamentos del segundo piso, edificio principal considerados para la segunda etapa

En el tiempo que se destina, ya se encuentran consideradas las pruebas por punto y las pruebas de servicios. En el anexoJ-4 se encuentra el detalle del cálculo de esta zona.

- Implementación del cableado estructurado en el Primer Piso del Edificio Secundario. En este piso se consideran para esta etapa el cableado de 43 puntos de red.

  Como se mencionó en el punto anterior, en estos cálculos ya se consideran los test por puntos y las pruebas de servicios. En el anexo J-5 se encuentra el detalle del cálculo de esta zona.
- Implementación del cableado estructurado en la Planta Baja del Edificio Principal. En tabla 3.64 se muestra el resumen de puntos y el tiempo estimado de instalación del cableado estructurado en esta zona.

  En el anexoJ-6 se encuentra el detalle del cálculo de esta zona.

Departamento	Puntos de red	Tiempo estimado [horas]
Comisaria Sur Oeste	10	6,83
Despacho 1	3	4,15
Despacho 2	3	3,55
Comisaria Sur Este	10	7,23
Bodega	3	1,95
Comisaria Salud y Ambiente	14	8,37
Total	43	32,08
Tiempo destinado [horas]	20	
Personas	2	

Tabla 3.63 Departamentos del primer piso, edificio secundario considerados para la segunda etapa

- Implementación del cableado estructurado en el Primer Piso del Edificio Principal, primera parte. En la figura 3.36 se muestra la primera parte y los departamentos implicados en ella.

Departamento	Puntos de red	Tiempo estimado [horas]
Comunicación Social	6	5,30
Jefatura Zonal de Coordinación Parroquial	10	7,83
Archivo	3	3,15
Seguridad	3	2,15
Escuela de Formación Ciudadana	8	6,07
Coordinación Zonal de Territorio	6	4,30
Total	36	28,80
Tiempo destinado [horas]	18	
Personas	2	

Tabla 3.64 Departamentos de la planta baja del edificio principal considerados para la segunda etapa

Los departamentos implicados, el número de puntos y el tiempo estimado se muestran a continuación en la tabla 3.65.

En el anexo J-7 se encuentra el detalle del cálculo de esta zona.

- Implementación del cableado estructurado en el Primer Piso del Edificio Principal, segunda parte.

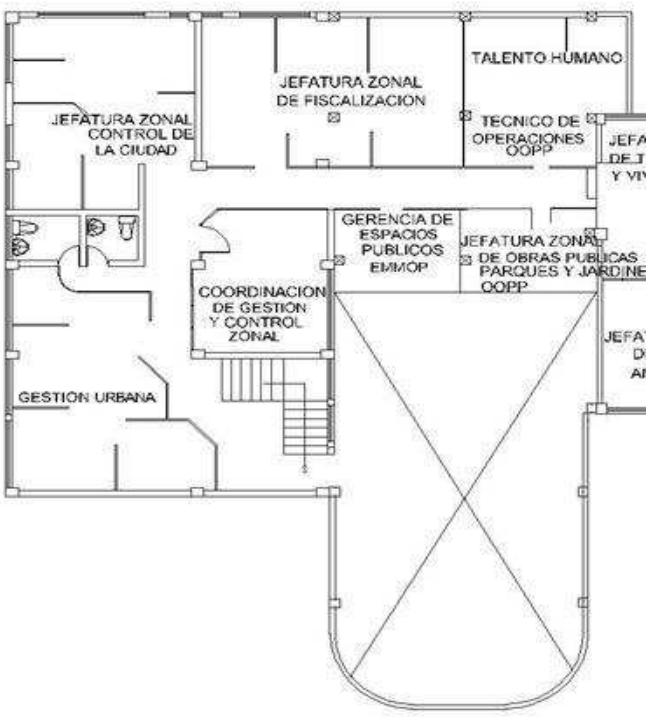


Figura 3.36 Primera parte del primer piso del edificio principal

Departamento	Puntos de red	Tiempo estimado [horas]
Jefatura Zonal de Control de la Ciudad	12	10,60
Jefatura Zonal de Fiscalización	15	10,75
Gerencia de Espacio Público (EMMOP)	4	4,93
Gestión Urbana	11	9,22
Coordinación de Gestión y Control	3	5,15
Jefatura Zonal de Obras Públicas, Parques y Jardines	14	8,77
Total	59	49,42
Tiempo destinado [horas]	31	
Personas	2	

Tabla 3.65 Departamentos de la primera parte del Primer Piso del Edificio Principal

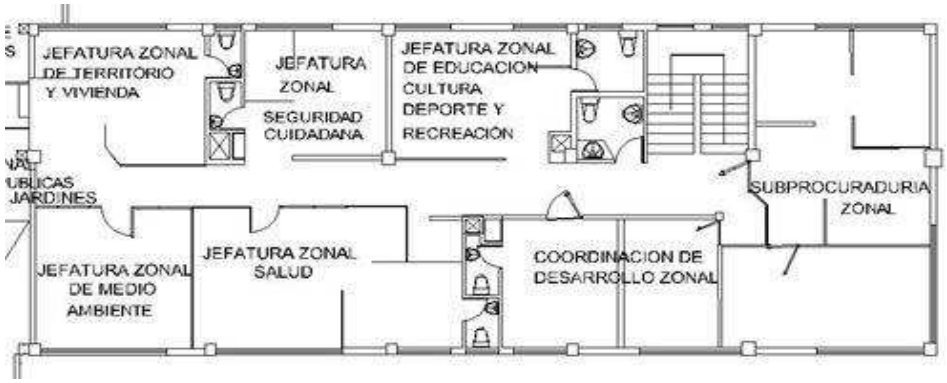


Figura 3.37 Segunda parte del primer piso del edificio principal

Los departamentos implicados en la segunda parte, el número de puntos y el tiempo estimado se muestran en la tabla 3.66.

En el anexo J-7 se encuentra el detalle del cálculo de esta zona.

- Implementación del cableado estructurado en la Planta Baja del Edificio Secundario, tabla 3.67.

  En el anexo J-8 se encuentra el detalle del cálculo de esta zona. Con esto queda terminada la implementación del cableado estructurado en sí, de la AZEA y sus dos edificios.

Departamento	Puntos de red	Tiempo estimado [horas]
Jefatura Zonal de Educación, Cultura, Deportes y Recreación	11	9,22
Jefatura Zonal de Medio Ambiente	8	5,07
Jefatura Zonal de Territorio y Vivienda	7	5,68
Jefatura Zonal de Salud	10	6,83
Coordinación de Desarrollo Zonal	6	9,30
Jefatura Zonal de Seguridad Ciudadana	9	6,85
Subprocuraduría Zonal	12	9,60
Total	63	52,55
Tiempo destinado [horas]	33	
Personas	2	

Tabla 3.66 Departamentos de la segunda parte del primer piso del edificio principal

Departamento	Puntos de red	Tiempo estimado [horas]
Comisaria de Laderas	8	6,07
Policía Metropolitana	3	4,15
Total	11	10,22
Tiempo destinado [horas]	8	
Personas	2	

Tabla 3.67 Departamentos de la planta baja del edificio secundario

- Para terminar esta fase, como en la primera etapa, se estima el tiempo de configuración de las estaciones de trabajo, de los teléfonos IP y la realización de las respectivas pruebas. El tiempo estimado para realizar la configuración de las estaciones de trabajo se encuentra en la tabla 3.68

Cantidad	Concepto	Tiempo estimado x1 [minutos]	Tiempo estimado [horas]
176	Estaciones de trabajo	15	44
	Tiempo destinado [horas]	25	
	Personas	2	

Tabla 3.68 Tiempo estimado para la configuración de estaciones de trabajo de la segunda etapa

- Los teléfonos IP, así como en la primera etapa deberán ser configurados de forma manual, ingresando la IP, máscara de red, gateway, extensión y nombre. En la tabla 3.69 se ve el tiempo estimado que tomaría configurar estos equipos.

Cantidad	Concepto	Tiempo estimado x1 [minutos]	Tiempo estimado [horas]
83	Teléfonos IP	20	27,67
	Tiempo destinado [horas]	15	
	Personas	2	

Tabla 3.69 Tiempo estimado para la configuración de teléfonos IP de la segunda etapa

- La realización de pruebas, contemplará el cableado que se implementa en la segunda etapa junto con los servicios que se han instalado, incluido el backbone. Como en la primera etapa, si las pruebas no concuerdan con lo

requerido, se establecerá el tiempo necesario (en este caso serán 30 días) para cumplir con los requerimientos o corregir fallas en la instalación del cableado estructurado. si las pruebas son positivas, se dará por terminada la tercera fase.

Las pruebas se realizarán desde todos los departamentos de la AZEA con el fin de determinar exactamente, la existencia de algún problema en el nuevo cableado, así como en los servicios del rediseño.

3.5.3 SOPORTE POSTERIOR A LA MIGRACIÓN

El soporte posterior a la migración será proporcionado por el personal de la Jefatura Zonal de Informática de la AZEA, quienes con la capacitación recibida podrán solucionar cualquier inconveniente que pueda presentarse en los servidores, en los equipos de red, y con las nuevas aplicaciones en las estaciones de trabajo.

3.5.4 DOCUMENTACIÓN

Todo el proceso deberá ser documentado. La documentación de las pruebas que se realicen en la primera etapa de la tercera fase, así como la documentación de todo el proceso realizado, permitirá tener material de apoyo o de referencia para el proceso que se desarrollará en la segunda etapa. En el anexo J-9 se encuentra el formato para llevar la documentación, donde se detallarán los objetivos, las actividades realizadas y los resultados obtenidos.

3.5.5 INCONVENIENTES EN LA MIGRACIÓN

Los principales inconvenientes que se pueden presentar en el proceso de migración son:

- La resistencia a la aceptación de los nuevos servicios por parte del usuario final.
- El costo que implica la capacitación.
- El costo que significa todo el rediseño de la red y su implementación, ya que es una institución pública.

3.5.6 INFORMAR AL PERSONAL

Se debe elaborar la promoción correspondiente para la comunicación y divulgación del rediseño de la nueva red y su correspondiente implementación, especificada en el plan de migración.

El objetivo de informar al personal todos los aspectos del rediseño y la migración, es mitigar la resistencia que pueda existir por parte de los empleados de la AZEA hacia los nuevos servicios y sus funciones.

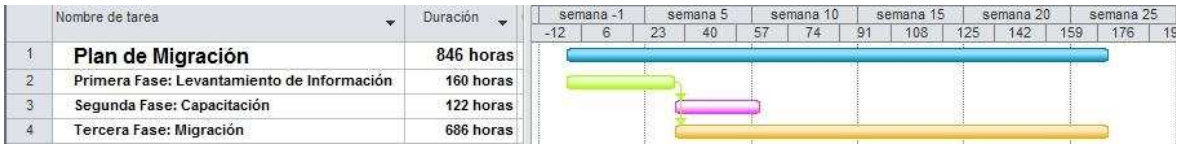
Para llevar a cabo la difusión se recomienda crear eventos informativos, folletos, envío de la información a través del correo electrónico, videos, entre otros, permitiendo conocer los objetivos, alcances, beneficios, fases y resultados.

Se aconseja realizar el siguiente plan de información:

- Comunicar a todo el personal que en los próximos meses se realizará una migración de la red de datos y las implicaciones que esto conlleva.
- Terminada la primera fase, se debe notificar todos los cambios al personal, y cuando serán realizados dichos cambios, así el personal sabrá cuando va a ocurrir la migración y en donde se producirá.
- Realizar una reunión general inmediata al cambio, para informar posibles modificaciones al plan inicial de migración.
- Realizar reuniones de control, en las que se pueda comprobar la adaptación de los usuarios al cambio, con el propósito de solucionar problemas o inquietudes que se presenten.

3.5.7 TIEMPOS DE MIGRACIÓN

El tiempo de migración será de aproximadamente 25 semanas, la primera fase tardará alrededor de 4 semanas, luego de la primera fase se empezará con la segunda y tercera fase simultáneamente, la segunda fase comprenderá aproximadamente 5 semanas y la tercera fase tomará alrededor de 21 semanas, como se puede notar en la figura 3.38. Los detalles de las tareas con sus tiempos asignados se pueden encontrar el en anexo J-10.



	Nombre de tarea	Duración
1	Plan de Migración	846 horas
2	Primera Fase: Levantamiento de Información	160 horas
3	Segunda Fase: Capacitación	122 horas
4	Tercera Fase: Migración	686 horas

Figura 3.38 Tiempo total estimado del plan de migración

3.6 DESARROLLO DEL PLAN DE CONTINGENCIA

3.6.1 DESCRIPCIÓN GENERAL

3.6.1.1 Propósito

Este plan de contingencia establece los procedimientos para la recuperación de la red de datos de la AZEA ante una posible interrupción debida a agentes externos y fallo en los equipos de conectividad. Los siguientes objetivos han sido establecidos para el presente plan:

- Maximizar la efectividad de la operaciones de contingencia a través de un plan establecido que consiste de las siguiente fases:
  - *Notificación/fase de activación*.- para detectar, evaluar el daño y activar el plan.
  - *Fase de Recuperación.*-para restaurar temporalmente las operaciones en la red y recuperar los daños causados al sistema original.
  - *Fase de Reconstitución.*- pararestaurarla capacidad de procesamiento del sistema a capacidades normales.
- Identificar las actividades, recursos y procedimientos a ejecutarse durante interrupciones.
- Asignar responsabilidades y proporcionar orientación para la recuperación de la red de la AZEA durante largos periodos de interrupción de las operaciones normales.

3.6.1.2 Aplicabilidad

Este plan de contingencia se aplica a las funciones, operaciones y recursos necesarios para recuperar y reanudar la red de datos de la AZEA en las instalaciones ubicadas en el sur de Quito.

3.6.1.3 Alcance

3.6.1.3.1 Principios de Planeación

Varios escenarios han sido contemplados para formar una base del plan, y varias hipótesis fueron hechas.

3.6.1.3.2 Suposiciones

Las siguientes suposiciones fueron hechas al desarrollar el plan de contingencia.

- El personal de la AZEA ha sido identificado y capacitado en su respuesta de emergencia y funciones de recuperación; ellos también son capaces de activar el Plan de Contingencia de la AZEA.
- Se dispone de la comunicación con el CAT (Centro de Atención Tecnológica) de la Administración General, que proveerá guía en los problemas suscitados en los servicios que maneja la AZEA, así como problemas en el servidor de réplica SRV03DC12y que se encuentra soportado por ellos.
- Los controles preventivos (por ejemplo, *UPS*, extintores de incendios, y la asistencia del departamento de bomberos) están en pleno funcionamiento en el momento del incidente y han contado con un mantenimiento adecuado.
- El equipo de cómputo central, incluyen dos componentes de apoyo, se conectan a una fuente de alimentación ininterrumpida, que ofrece al menos 15 minutos de electricidad durante un corte de energía eléctrica.
- Se dispone de copias de seguridad actualizadas del software de aplicación de los servidores y de la configuración de los equipos de conectividad, los datos están intactos y disponibles en las instalaciones de almacenamiento fuera del sitio.

El presente plan de contingencia de la AZEA no se aplica a las siguientes situaciones:

- De recuperación total y para la continuidad de las operaciones.

- De evacuación de emergencia del personal.

3.6.1.4 Línea de Sucesión

La AZEA cuenta con un orden de sucesión enunciado en su organigrama y en coordinación con ese orden se ha establecido la autoridad para la ejecución del plan de contingencia. El jefe zonal de Informática es el responsable de garantizar la seguridad del personal y la ejecución de los procesos documentados dentro de este plan. Si el jefe del área de informática no puede cumplir con sus funciones o decide delegar esta responsabilidad, el delegado debe actuar como tal autoridad.

A continuación del jefe zonal se encuentra un ingeniero que brinda apoyo en este departamento.

3.6.1.5 Responsabilidades

Debido a que la Jefatura Zonal de Informática cuenta con dos personas trabajando en forma continua, no es factible la formación de grupos para manejar algún evento anormal que afecte a la red de datos, por ello los dos funcionarios deben participar activamente en las distintas etapas para la recuperación y restauración de la red.

Los dos funcionarios han sido capacitados para responder a un evento de contingencia que afecte a los equipos de red. El jefe zonal es quien tendrá el liderazgo ante un fallo y será apoyado por su compañero.

3.6.1.6 Notificación y Fase de Activación

Esta fase aborda las medidas iníciales adoptadas para detectar y evaluar los daños causados por una interrupción a la red de datos de la AZEA. Basándose en la evaluación del evento, el plan puede ser activado por el coordinador de planes de contingencia.

En caso de emergencia, la prioridad de la AZEA es la de preservarla salud y la seguridad de su personal antes de proceder a la notificación y los procedimientos de activación.

La secuencia de notificación es la siguiente:

- La primera respuesta es para notificar al Jefe Zonal de Informática o coordinador de Planes de Contingencia. Toda la información debe ser transmitida al Coordinador de Planes de Contingencia.
- El Jefe Zonal de Informática debe notificar a los miembros del departamento y dirigirá completarlos procedimientos de evaluación descritos a continuación para determinar la extensión del daño y el tiempo estimado de recuperación.

El plan de contingencia debe ser activado según uno o más de los siguientes criterios:

- Si la red de datos de la AZEA se ve afectada por un fallo en los equipos de conectividad o servidores.
- Si las instalaciones se encuentran dañadas y repercuten a la red de datos.

3.6.1.7 Análisis de Impacto

Basado en la información obtenida en consultas a los funcionarios de la AZEA, se han definido los siguientes eventos como críticos, identificando su soporte como vital para la continuidad de la operación de la red de datos.

Evento	Probabilidad de Ocurrencia
Corte de Energía Eléctrica	Alta
Falla de Hardware: Servidores Equipos de conectividad	Alta
Falla de Software: Sistema Operativo Sistema de Aplicación Bases de Datos	Alta
Terremoto	Medio
Incendio	Baja
Sabotaje	Baja
Acceso no autorizado	Baja

Tabla 3.70 Eventos contemplados en el plan de contingencia

3.6.2 FASE DE RECUPERACIÓN

La fase de recuperación empieza una vez que el plan de contingencia ha sido activado y la evaluación de daños ha sido completada (si fuese posible) y el personal ha sido notificado. La fase de recuperación se enfoca en las medidas de contingencia destinadas a recuperar la capacidad de procesamiento de la red, a reparar el daño y restaurar la capacidad operativa de la instalación original.

3.6.3 PROCEDIMIENTOS DE RECUPERACIÓN

Para facilitar las operaciones en la fase de recuperación, el plan de contingencia debe proveer procedimientos detallados para restaurar los componentes de la red.

3.6.3.1 Corte de energía eléctrica

Un corte intempestivo del suministro de energía eléctrica puede ser ocasionado por algún factor externo, como son (corte de la línea de transmisión, accidentes, falla en los sistemas de protección, etc.) o por fallas en la red eléctrica local.

En el origen del evento como al final, se pueden causar daños a los equipos por lo que se debe tomar en cuenta las siguientes consideraciones.

Consideraciones previas

- Los usuarios deben respaldar adecuadamente la información en un tiempo razonable y apagar el computador. Cada estación de trabajo se encuentra conectada a la red eléctrica respaldada por una UPS, la que permite ejecutar, en un tiempo aproximado de 5 minutos, el procedimiento.
- Cada usuario deberá mantener su PC apagado y sólo lo encenderá una vez recibida la autorización de parte del Jefe del Departamento de Informática durante la emergencia.
- El Jefe del Departamento de Informática, será el responsable de apagar los servidores y reiniciarlos una vez reintegrada la energía eléctrica.

- Las acciones realizadas durante la contingencia deberán registrarse debidamente en la Bitácora, indicando fecha y hora, acciones realizadas, observaciones, además de la identificación del ejecutante y responsable, con su respectiva firma.

Plan de acción

1. Revisar la carga del UPS que alimentan los equipos, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.
2. Por seguridad utilizar la energía que se tiene en los UPS para apagar los equipos en forma correcta.
3. Llamar a Empresa Eléctrica Quito S.A., para identificar si la falla es del sistema general, o es un problema aislado, en las instalaciones de la AZEA.
4. Si la falla es originada en el sistema general, se debe esperar a que se normalice, (siempre en coordinación), para proceder a encender los equipos y conectar a los usuarios.
5. Si la falla es originada por algún factor local, deberá, proceder a revisar, los elementos de la instalación eléctrica local, como fusibles, cables flojos, o revisar si existe algún equipo que esté ocasionando la falla, si no se detecta localmente se debe proceder a revisar las conexiones, en la subestación de donde se está independizando la energía, revisar los bornes flojos u otros, Si aún no se detecta la falla, ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc., y que hayan conectado a la red ocasionando un corto circuito, que no permita, restituir la energía en forma normal.
6. Si la falla es en el sistema Interconectado (general) se deberá esperar que se restituya la energía, más un tiempo de 15 minutos, aproximadamente para que se estabilicé y se puedan levantar los sistemas.
7. Si la falla es local proceder a la reparación, o reemplazo, de los elementos que causaron la falla, para esto se debe solicitar el apoyo de los técnicos de emergencia, (se recomienda tener fusibles, y una llave térmica de respaldo de acuerdo a la capacidad de su tablero). Una vez reparada la falla se debe conectar la energía para ver el comportamiento de esta y no

encender los equipos de cómputo hasta después de 15 minutos aproximadamente luego de la restitución de la energía.

8. Reiniciar las operaciones

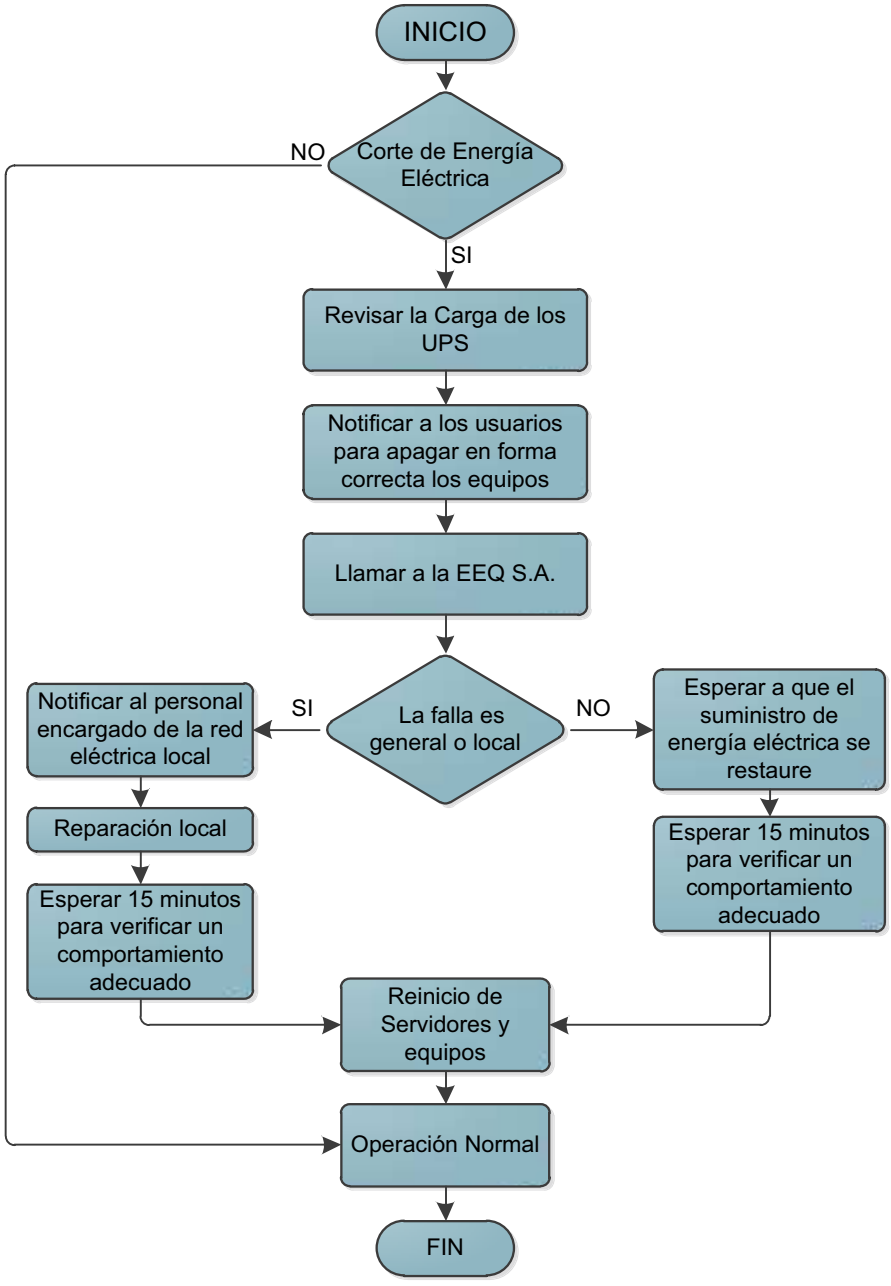


Figura 3.39 Flujograma ante un corte de energía eléctrica

3.6.3.2 Falla de Hardware o Software

Las alteraciones que sufran los servidores y los equipos de conectividad en hardware o software pueden ser corregidas en la mayoría de los casos, sin embargo en algunas ocasiones, las alteraciones llegan a ser tan grandes que el

tiempo requerido para el reinicio de las operaciones normales puede extenderse hasta por días sin tener la absoluta certeza de que las correcciones que se hicieron fueron las necesarias, por tal motivo es mejor acudir a los respaldos de información y restaurar los datos.

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos o a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si éstas se derivan del mal funcionamiento del hardware o de la pérdida de su configuración (software). En el caso de presentarse una falla en un equipo de conectividad se procederá de la siguiente manera:

1. Evaluación de las fallas.
2. Si las fallas se derivan del mal funcionamiento del hardware de un equipo se procede a su reemplazo inmediato.
3. Si resulta ser un problema de configuración, se procede a su reconfiguración inmediata.
4. Revisar y probar la integridad de las comunicaciones.
5. Reiniciar las operaciones.

3.6.3.3 Falla de Hardware

3.6.3.3.1 Servidores

En la AZEA se tiene 4 servidores ubicados bajo una mesa, existiendo una gran cantidad de cables de energía y de red que dificultan su administración, por lo que como medida preventiva se recomienda el organizar adecuadamente el espacio y el cableado.

Como consideración previa, la manipulación y configuración del servidor SRV03DC12 está a cargo de la administración general, y en caso de un desperfecto se deberá comunicar a la Administración General y seguir el procedimiento que esta determine.

Ante un posible fallo en un servidor marca HP ProLiant de la serie 300 o del servidor PC03GESTIO-05 se aplicarán las medidas correctivas necesarias.

Plan de acción

1. En base a los servicios perdidos identificar el servidor que falla, para ello se puede referirse a la tabla 3.71.
2. Desplazarse hacia el espacio donde está el servidor y verificar si se encuentra encendido.
3. Si el servidor no se encuentra encendido, se debe verificar que se encuentre conectado adecuadamente al suministro de energía eléctrica.
4. Si tiene una correcta alimentación de energía eléctrica y el servidor no enciende, verificar la fuente de poder, para ello se puede utilizar una fuente de poder de respaldo.

Puerto en el Switch de núcleo	Servidor Marca	Servicios	Dirección IP
7	SRV03DC12 IBM SYSTEM X 3200 M2	DNS, DHCP, Autenticación, Active Directory	172.20.6.8/24
8	SRV03APL01 HP Proliant ML370GS	GDOC, FTP	172.20.6.3/24
9	0173BDD1 HP Proliant ML350	FTP	172.20.6.2/24
10	PC03GESTIO-05 Clon	Turnos en el balcón de servicios	172.20.6.192/24

Tabla 3.71 Servidores y servicios actuales

5. Si el servidor se encuentra encendido, verificar que el servidor no se encuentre inhibido, en caso de estarlo, reiniciar el servidor mediante el botón de reset o pulsar el botón de Power por más de 10 segundos.
6. Si al reiniciar se presentan nuevamente los problemas en el arranque, se debe referir al manual de solución de problemas provisto por el fabricante del equipo, mismo que debe mantenerse en la Jefatura Zonal de Informática.
7. Reiniciar las operaciones.

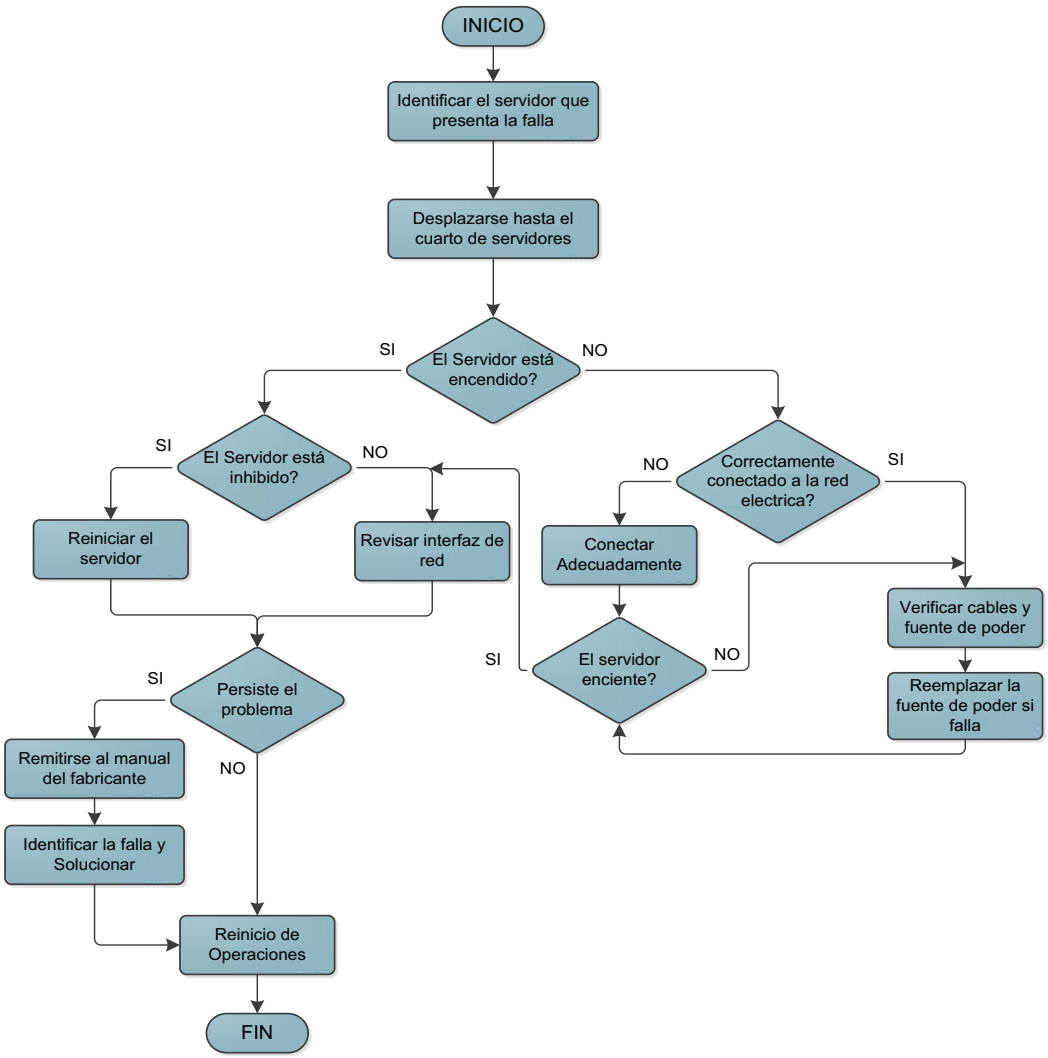


Figura 3.40 Flujograma ante una falla de hardware en los servidores

3.6.3.3.2 Switches

La AZEA cuenta con 32 switches en total, de los cuales se tienen 27 equipos en uso y 5 equipos disponibles.

Para la identificación de la avería de un switch se debe realizar el siguiente procedimiento.

1. Identificar el departamento y piso afectado por el fallo en la red.
2. Identificar los switches que dan servicio al departamento o área afectada y desplazarse hasta su ubicación, los departamentos y switches asociados son mostrados en el Anexo I.

3. Desplazarse hacia el espacio donde está el switch y verificar si está encendido.
4. Si el switch no se encuentra encendido, se debe verificar que se encuentre conectado adecuadamente al suministro de energía eléctrica.
5. Verificar la adecuada conexión de los *patch cords* en los puertos del switch.
6. Si tiene una correcta alimentación de energía eléctrica y el switch no enciende, reemplazarlo con uno de similares características, acorde a la tabla 3.72.

Equipo a ser reemplazado		Posible Reemplazo	
Equipo	Etiqueta	Equipo	Etiqueta
3Com 5500G-EI	SW3-01	3Com 5500G-EI	SW3-29
3Com 4226T	SW3-03	3Com 4226T 3Com Baseline 2024	SW3-28 SW3-30
3Com Baseline 2024	SW3-02, SW3-04, SW3-08, SW3-12, SW3-25	3Com 4226T 3Com Baseline 2024	SW3-28 SW3-30
3Com Baseline 10/100	SW3-10, SW3-11, SW3-17, SW3-18, SW3-19, SW3-24	3Com 4226T 3Com Baseline 2024	SW3-28 SW3-30
3Com Office Connect Fast Ethernet	SW3-14, SW3-23	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32
3Com Office Connect Dual Switch	SW3-22, SW3-26	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32
D-Link Des-1008d	SW3-05, SW3-09, SW3-13, SW3-15, SW3-21	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32
D-Link 100link/act	SW3-06	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32

3Com 3cgsu08-Aa	SW3-16, SW3-20	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32
TRENDnet TEG-S8	SW3-27	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32
Nexxt	SW3-07	3Com 4226T 3Com Baseline 2024 Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-28 SW3-30 SW3-31 SW3-32

Tabla 3.72 Reemplazos de los switches

7. Si el switch se encuentra encendido, verificar la adecuada conexión de los *patch cords* en los puertos del switch.
8. Si el switch se encuentra correctamente conectado a la energía eléctrica, y *patch cords* y puertos adecuadamente conectados, y no funciona correctamente, se procederá al reinicio del equipo, mediante la desconexión del enchufe.
9. Si posteriormente al reinicio, la falla continua, se debe reemplazar al equipo con uno de similares características.
10. Reiniciar las Operaciones.

3.6.3.3.3 Hubs

Como primera medida a tomarse es el reemplazo de los hubs por switches, en especial el HB3-01 que se encuentra en el backbone de la red.

En caso de una falla en los Hubs, se procederá a realizar el mismo procedimiento definido ante la falla de un switch, con la consideración de que los posibles equipos a reemplazar a los hubs son mostrados en la tabla 3.73.

Equipo a ser reemplazado		Posible reemplazo	
Equipo	Etiqueta	Equipo	Etiqueta
3Com Dual speed Hub 24 puertos	HB-01	3Com 4226T 3Com Baseline 2024	SW3-28 SW3-30
3Com Dual speed Hub 8 puertos	HB-02	Office Connect Fast Ethernet Office Connect Fast Ethernet	SW3-31 SW3-32

Tabla 3.73 Reemplazo de los Hubs

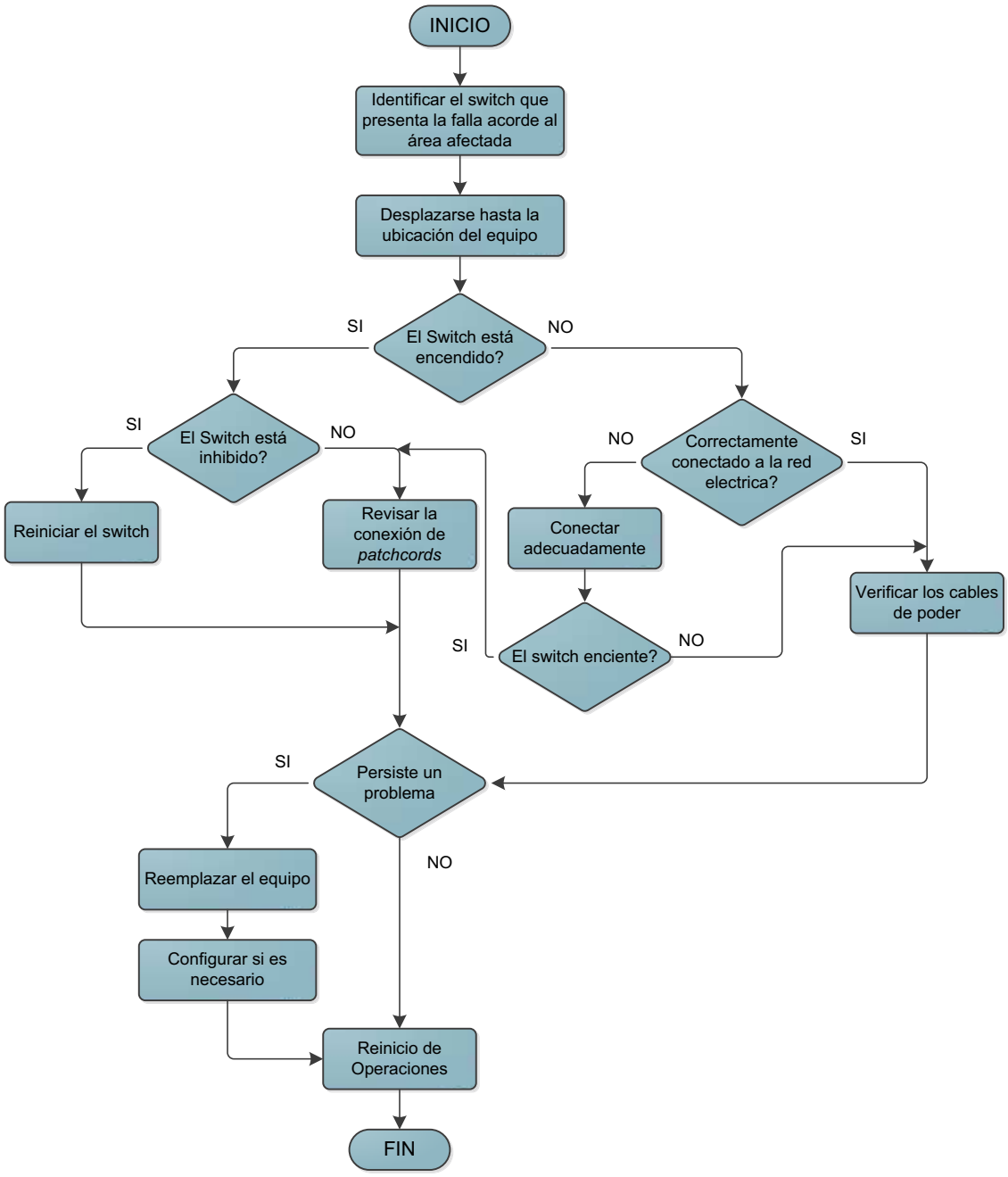


Figura 3.41 Flujograma ante problemas en switches

3.6.3.3.4 Routers

La AZEA no tiene acceso a la configuración propia del router, su administración se gestiona a través de la Corporación Nacional de Telecomunicaciones, y ante un posible fallo de este dispositivo se debe llamar a esta entidad.

El procedimiento para la identificación de un problema en el router es el siguiente:

1. Una vez reportado el problema de conectividad externo, realizar una prueba de conectividad hasta el router, para ello se procede a ejecutar el comando ping hacia la dirección 172.20.6.10, que corresponde a la dirección IP de la interfaz del router.
2. Si el resultado del ping es negativo, desplazarse hacia el lugar donde se encuentra instalado el Router y verificar que se encuentre encendido.

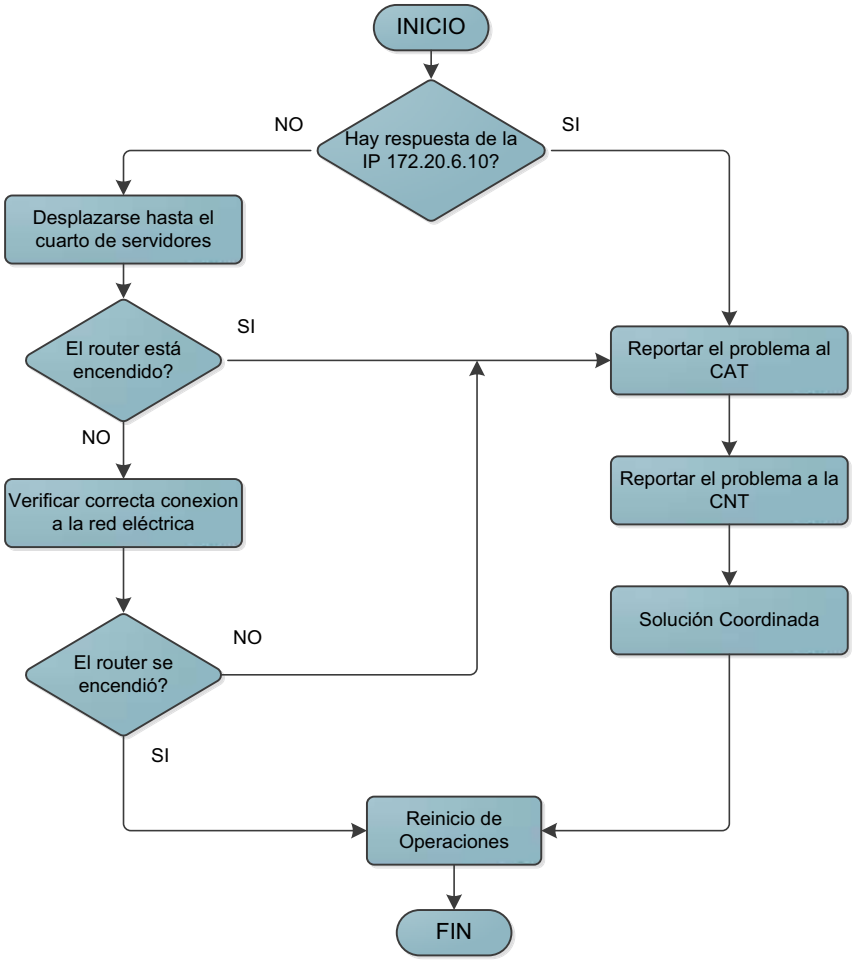


Figura 3.42 Flujograma ante problemas en el router WAN

3. Si el equipo no se encuentra encendido, verificar que se encuentre correctamente conectado a la red eléctrica, en caso de estarlo, llamar a la CNT para reportar el problema y pedir la solución del mismo en el menor tiempo posible.
4. Si el equipo está correctamente conectado a la red eléctrica, y se encuentra encendido, reportar el problema a la administración general y a la CNT para su inmediata solución.

3.6.3.4 Falla de Software

3.6.3.4.1 Servidores

Consideraciones previas

- La administración del servidor de réplica es manejada por la Administración General, en caso de una falla de software en este servidor, se debe reportar el evento al CAT (Centro de Atención Tecnológica) y proceder de acuerdo a las instrucciones proporcionadas por esta instancia.
- En la Jefatura Zonal de informática se cuenta con la documentación pertinente a los servicios que se prestan a través de sus servidores, identificando la forma de configurarlos y reiniciarlos adecuadamente.

Plan de acción

En el caso que la alteración del software en los servidores de la AZEA haga imposible el inicio inmediato o tardío de las operaciones se procede como sigue:

1. Identificar el servidor afectado por la falla de software. En caso de una falla en el servidor de réplica, reportar su malfuncionamiento a la Administración General.
2. Identificar y reiniciar el servicio acorde a las características propias del mismo, para esto se cuenta con los manuales de los servicios.
3. Si al reiniciar el servicio se presentan errores o problemas, recurrir a los archivos de log de los servicios o al manual para identificar el problema y su solución.

4. Revisar y probar el correcto funcionamiento del servicio y la integridad de los datos.
5. Reiniciar las operaciones.

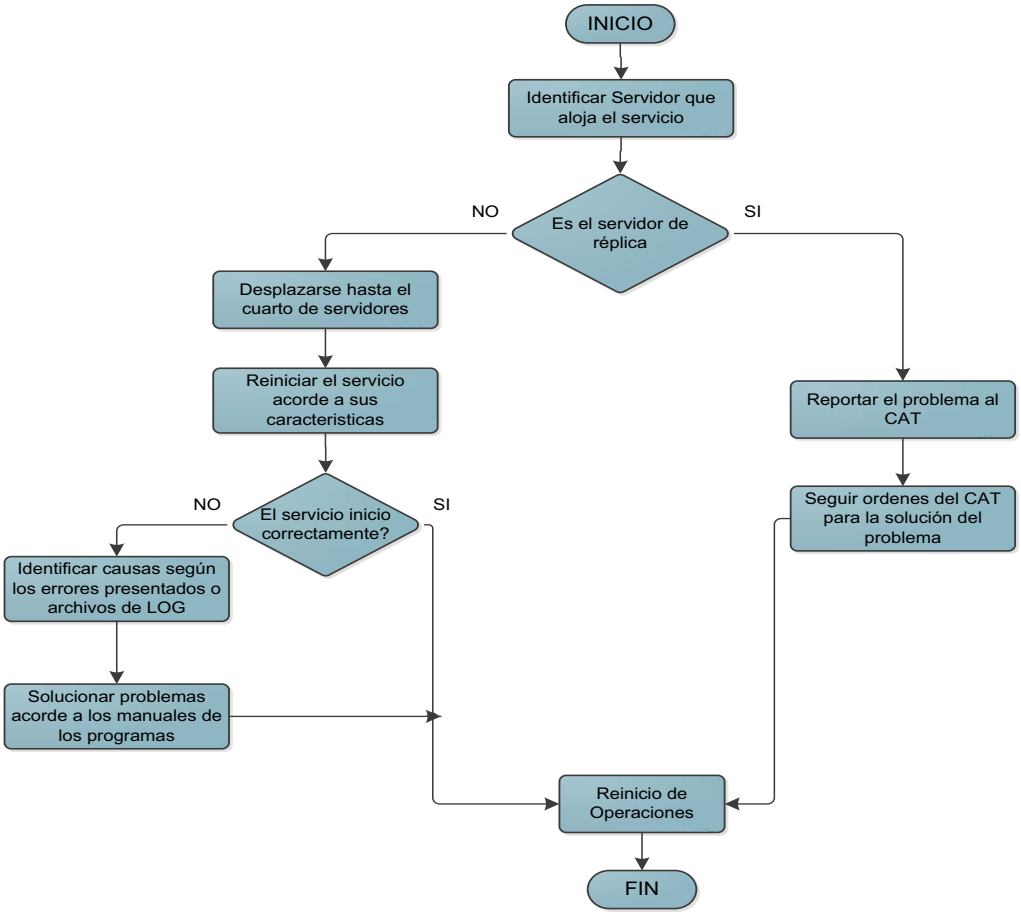


Figura 3.43 Flujograma ante problemas de software en los servidores

3.6.3.4.2 Equipos de Conectividad

Consideraciones previas

- Los equipos administrables de respaldo cuentan con una dirección IP que no entra en conflicto con los dispositivos de la red.
- Se tiene documentada adecuadamente la configuración de los equipos así como las claves de acceso.
- Se tienen adecuadamente respaldadas las configuraciones de los equipos, así como el resultado de la aplicación MD5 a cada una de ellas.

- Se tienen plenamente identificados los equipos de respaldo, con sus etiquetas correspondientes.

Plan de Acción

En el caso que la alteración del software en los equipos de conectividad de la AZEA imposibilite la comunicación interna entre los dispositivos terminales, se procederá a realizar el siguiente procedimiento:

1. Determinar el equipo afectado, para lo cual se define que los únicos equipos que pueden sufrir daños en su configuración son el switch de núcleo etiquetado SW3-01 y el switch Super Stack 3 4226T etiquetado como SW3-03.
2. Ingresar a una interfaz de administración del dispositivo a través de las claves que se deben tener previamente documentadas.
3. Verificar la integridad de la configuración, para ello se compara el resultado del algoritmo de reducción criptográfica MD5 de la configuración actual con uno previamente generado.
4. En caso de el resultado de la comparación sea negativo, se debe restaurar la configuración en base a los backups.
5. En caso de no funcionar, reemplazar el equipo por un equipo de características similares y configurarlo adecuadamente.
6. Reiniciar las operaciones.

3.6.3.5 Terremoto

Consideraciones previas

En caso de un daño mayor, el cual haga imposible la continuación de las operaciones en la AZEA, los procesos de atención al público en general deben ser llevados a cabo por las Administraciones Zonales que puedan continuar sus operaciones.

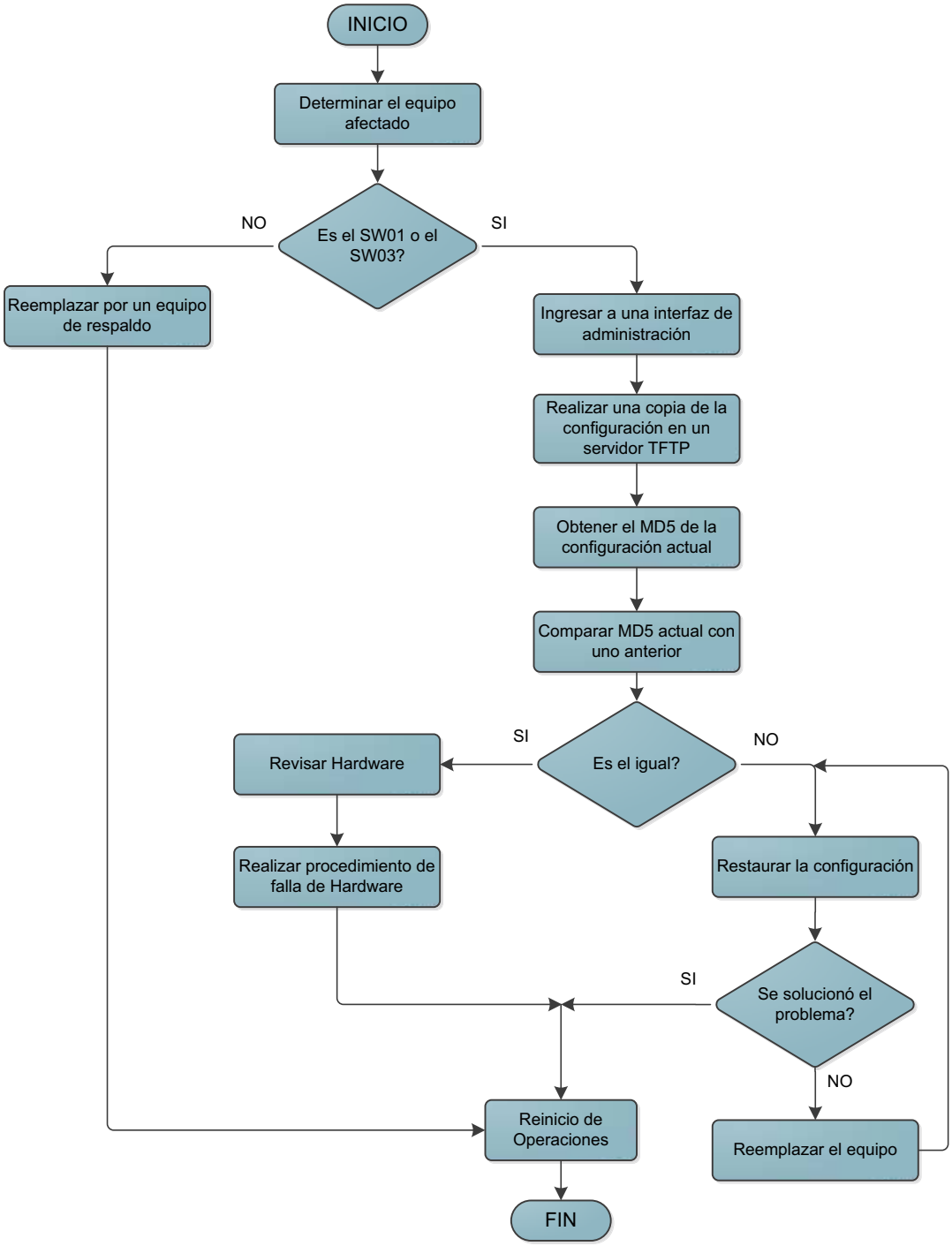


Figura 3.44 Flujograma ante problemas de software en los equipos de conectividad

Mientras las operaciones continúan en las instalaciones de las Administraciones Zonales operacionales, se evaluará la posibilidad de regresar a las instalaciones actualmente afectadas, o establecer operaciones en un nuevo sitio.

En caso de daño menor, y donde la infraestructura de los edificios no comprometan la seguridad de las personas, se procederá acorde al siguiente plan de acción.

Plan de acción

1. Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
2. Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.
3. Instalar los equipos.
4. Restaurar la información de configuración en los equipos afectados.

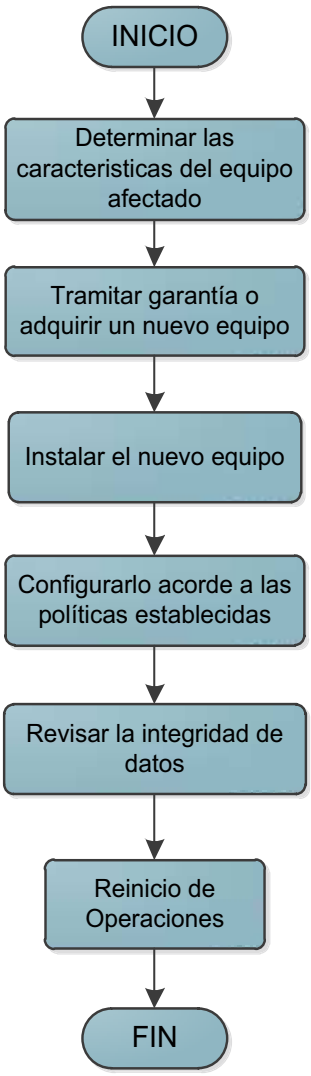


Figura 3.45 Flujograma posterior al terremoto

5. Revisar y probar la integridad de los datos.
6. Reiniciar las operaciones.

La continuidad de las operaciones en este tipo de siniestros dependerá del grado de afección de la estructura del edificio, ya que las afecciones pueden ir desde el no daño de la estructura, daño parcial, hasta la inhabilitación completa del edificio.

Se considera daño mayor a toda aquella afección que imposibilite la utilización de los equipos y que ésta afección no tenga reparación o bien por su naturaleza dicha reparación tarde un periodo prolongado.

3.6.3.6 Incendio

La AZEA, a pesar de que cuenta con sistemas de protección contra incendios, como son, extintores manuales y vías de acceso y de evacuación amplias, no se encuentra exenta de algún incidente involuntario que puede ocasionar el inicio de un incendio, para lo cual se deberá proceder de la siguiente manera.

Consideraciones previas

- Verificar periódicamente el estado de las instalaciones eléctricas.
- Evitar concentrar grandes cantidades de material inflamable.
- Evitar fumar cerca de químicos o sustancias volátiles.
- Almacenar productos de fácil combustión en forma adecuada.
- Evitar sobrecargar los circuitos eléctricos.
- Mantener el área de trabajo siempre limpia y en orden.
- Mantener un control adecuado sobre los equipos de seguridad como extintores.

Plan de Acción

1. Si el inicio del incendio se produce en horas laborables, se deberá dar la alarma a todo el personal de la oficina y colindantes, y a los bomberos.
2. Desconectar las fuentes de alimentación eléctricas (sin riesgo de exponer la vida).

3. Si el tiempo lo permite y si la fuente del siniestro está lejos, pero se puede propagar hacia los equipos principales de computo (servidores), se deberá retirar los equipos hacia un lugar seguro, discos o últimas copias que se tenga a la mano (sin que esto signifique riesgo de exponer la vida).
4. Se deberá proceder a sofocar el fuego utilizando el extintor correcto para el tipo de fuego.
5. Si el fuego está fuera de control, se llevará a cabo la evacuación del personal.
6. Si hay humo en la zona y no se tiene una salida, mantenerse a ras de piso y usar un pañuelo mojado para respirar.
7. Las personas que se encuentren en los pisos superiores deberán mantener abiertas las ventanas para que salga el humo, hasta que se despeje una vía de salida.

Posterior al evento

- Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
- Recuperar los respaldos de datos, programas, manuales u claves del lugar destinado a su almacenamiento.
- Instalar el sistema operativo según sea necesario.
- Restaurar la información y configuración de los servidores y equipos de conectividad.
- Revisar la integridad de datos.
- Poner en marcha las operaciones.

Se debe realizar una correcta evaluación del daño de los equipos, ya que su grado de afectación puede variar desde un simple daño superficial hasta un daño severo que inutilice al equipo y no tenga reparación.

3.6.3.7 Sabotaje, Acceso no autorizado

Consideraciones previas

- Mantener un respaldo de los datos, configuraciones, programas y claves en un sitio seguro.
- Definir medidas de prevención ante el acceso a la información o configuración de los equipos de red.

En el caso que el sabotaje imposibilite el inicio inmediato de las operaciones se realizará el siguiente procedimiento

1. Recuperar los respaldos de datos, configuraciones, programas y claves del lugar donde se encuentren respaldadas.
2. Restaurar la información al equipo afectado.
3. Revisar la integridad de datos.
4. Iniciar las operaciones.

3.6.4 FASE DE RECONSTITUCIÓN

3.6.4.1 Retorno a las operaciones Normales

Para regresar a las operaciones normales, los equipos de telecomunicaciones deben ser probados por parte de la Jefatura Zonal de Informática. Teniendo en cuenta esta premisa, se debe verificar lo siguiente:

- Los switches no administrables deben mostrar el estado de las interfaces mediante el encendido o parpadeo de los indicadores led, acorde a los puertos en uso.
- Los switches administrables deben permitir el ingreso a su interfaz de administración ya sea mediante un cable de consola o Web, acorde a su configuración.
- Los servidores deben tener todos los servicios que manejan iniciados, permitiendo que los distintos procesos de la AZEA puedan llevarse a cabo con normalidad.
- El enlace WAN debe trabajar correctamente, para ello se debe realizar pruebas de conectividad hacia los servidores remotos de la Administración General.

Una vez que se ha restaurado la red de datos a su capacidad normal de procesamiento, se debe tramitar la garantía de los equipos afectados (si es el caso), o la adquisición de nuevos equipos que reemplazarán a los equipos dañados, para ello el Jefe del Departamento de Informática hará el pedido y definirá las características de los equipos a adquirirse.

El procedimiento de reemplazo de los equipos se muestra en la figura 3.46. Es importante recalcar que los equipos dañados deben ser reemplazados por equipos nuevos, y solo durante el periodo comprendido entre la falla del equipo antiguo y la adquisición del nuevo equipo, debe mantenerse el equipo de respaldo en funcionamiento.

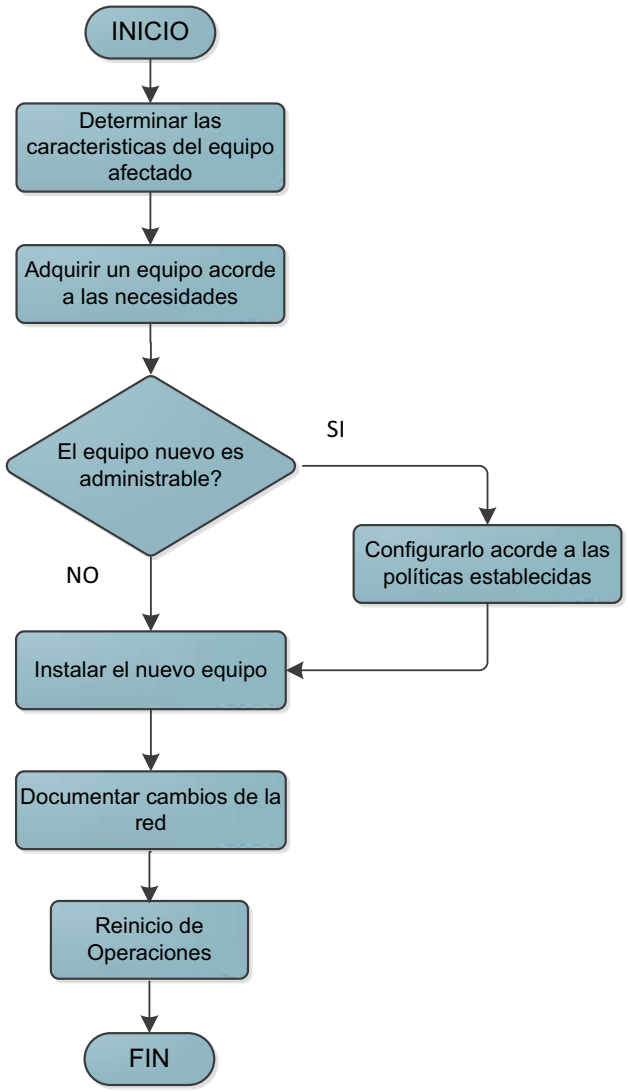


Figura 3.46 Procedimiento de recambio de equipos de red

Una vez superada la fase de reconstitución, se debe documentar adecuadamente los eventos que produjeron la falla, las medidas tomadas y el resultado de cada acción, para así tomar medidas preventivas que mitiguen los efectos de un problema similar en un caso futuro.

CAPÍTULO 4

PRESUPUESTO DE EQUIPAMIENTO PARA LA RED Y PRUEBAS CON EL PROTOTIPO

Después de haber establecido la situación actual de la AZEA habiendo obtenido las características necesarias de los elementos que se usarán en el rediseño, el presente capítulo contempla la especificación del presupuesto de equipamiento de la solución que se presentó en el capítulo 3.

En este capítulo también se presentará la descripción de las pruebas de funcionamiento del prototipo y los resultados obtenidos de las mismas.

4.1 COSTOS DE LA RED PASIVA

Dentro de los costos de la red pasiva se incluyen todos los elementos referentes a la implementación del sistema de cableado estructurado propuesto, contando además con la certificación de los puntos de red a ser instalados.

La tabla 4.1 muestra el desglose de los costos implicados en la red pasiva, teniendo en el anexo K-1 el detalle de la cotización de los elementos a utilizarse.

ITEM	Costo [$]
Materiales	23.681,76
Instalación de 372 puntos de red	11.532,00
Certificación de 372 puntos de red	1.860,00
Instalación de racks y accesorios	1.500,00
Identificación de red	40,00
Obra Civil	1.080,00
TOTAL	39.693,76

Tabla 4.1 Costos del sistema de cableado estructurado de la AZEA

4.2 COSTOS DE LA RED ACTIVA

La red activa consta de los equipos de conectividad que comprende a los switches de las distintas capas, el firewall, y los servidores a ser adquiridos para proveer los servicios descritos en el capítulo anterior.

Acorde a las características mínimas de los equipos presentadas en el capítulo anterior destinadas a garantizar el correcto funcionamiento de la red multi-servicios, se muestran los costos asociados a cada uno de los elementos necesarios.

4.2.1 COSTO TOTAL DE LA SOLUCIÓN CISCO

El costo de los equipos Cisco fue provista por la empresa Andean Trade, misma que ofrece el servicio de instalación de los mismos por $ 5.000,00 adicionales. En el anexo K-2 se detalla la cotización de estos equipos.

Costos en solución Cisco				
Ítem	Modelo	Cantidad	Precio Unitario [$]	Total Cisco [$]
Switch de acceso sin PoE	2960-24TC-L	13	1.179,44	15.332,72
Switch de acceso con PoE	2960-24PL-C	5	2.228,09	11.140,45
Switch de Distribución	2960S-24TS-L	4	2.945,46	11.781,84
Switch de Núcleo	C3560X-24T-S	3	4.970,86	14.912,58
Access Point	AIR-LAP 1262N-A-K9	1	1.301,64	1.301,64
Firewall	ASA 5510-K8	1	3.490,91	3.490,91
Total				57.960,14

Tabla 4.2 Comparación de precios de las soluciones presentadas

4.2.2 COSTO TOTAL DE LA SOLUCIÓN HP

El costo del equipamiento de los equipos HP fue provisto por la empresa MR Consulting & Solutions y SAZ Computers a través de su página web. La cotización provista por MR Consulting & Solutions se detalla en el anexo K-3.

Costos en solución HP				
Ítem	Modelo	Cantidad	Precio Unitario [$]	Total Cisco [$]
Switch de acceso sin PoE	HP 2620-24 J9623A	13	609,16	7.919,08
Switch de acceso con PoE	2610-24-Poe J9087A	5	1.327,70	6.638,50
Switch de Distribución	A5120-24G EI JE068A	4	1.533,16	6.132,63
Switch de Núcleo	5500-24G EI JD377A	3	2.631,65	7.894,95
Access Point	E-MSM430 Dual Radio 802.11n AP J9651A	1	695,61	695,61
Firewall	HP S200-S UTM APPLIANCE	1	1.616,25	1.616,25
Total				30.897,02

Tabla 4.3 Costo de la solución HP

4.2.3 COSTO DE LOS SERVIDORES

En base al cumplimiento de las características mínimas sugeridas en el capítulo anterior se ha optado por seleccionar los servidores provistos por el fabricante DELL, modelos Power Edge T110 II y modelo Power Edge R310. Se ha seleccionado el uso de un servidor en torre correspondiente al Power Edge T110 II acorde a la necesidad de instalar las tarjetas de expansión PCI en el servidor de telefonía IP.

Costos de los servidores Dell			
Modelo	Cantidad	Precio Unitario [$]	Precio Total [$]
Power Edge T110 II	1	1.778,00	1.778,00
Power Edge R310	3	1.939,00	5.817,00
Total			7.595,00

Tabla 4.4 Costo de servidores Dell [PW91]

Los servidores mencionados disponen de un año de garantía contra defectos de fábrica y es posible contratar el servicio de administración preventiva de sistemas de Dell, que se trata de una plataforma de aplicaciones de software basadas en la nube, que habilita el soporte remoto para los dispositivos de almacenamiento y servidores Dell™ y que está diseñada para brindar vistas consolidadas del entorno de TI y así poder tomar las medidas necesarias para ayudar a reducir el

tiempo de inactividad, este servicio consta de mantenimiento proactivo, 1 evento por año y asistencia remota durante 3 años por un precio de $675,00 dólares adicionales. [PW91]

La información específica referente a la cotización de los servidores Dell se encuentran en el anexo K-4.

4.2.4 COSTO DE TELEFONÍA

El costo de la implementación del servicio de telefonía demanda a más de la adquisición del servidor destinado a alojar este servicio, la adquisición de tarjetas para la conexión a la PSTN y los teléfonos IP a ser utilizados por los funcionarios de la AZEA.

Las tarjetas PCI mostradas en el capítulo anterior cumplen con las necesidades del rediseño, sin embargo se recomienda el uso de la tarjeta Digium TDM808E ya que posee un diseño más práctico en cuanto a hardware para la adaptación al servidor, así como mayor compatibilidad con Asterisk y Elastix.

Del mismo modo, en cuanto a los teléfonos IP se recomienda el uso de los teléfonos Grandstream GXP1450 puesto a que los Yealink SIP-T20P presentan ciertos inconvenientes de seguridad que aún no han sido completamente subsanados por el fabricante [PW94] [PW95] [PW96].

El costo a ser añadido por concepto de telefonía es mostrado en la tabla 4.5.

Costos Telefonía IP				
Ítem	Modelo	Cantidad	Precio Unitario	Total [$]
Teléfono IP	Grandstream GXP1450	97	92,00	8.924,00
Tarjeta PCI	Digium TDM808E	2	1.120,00	2.240,00
Total				11.164,00

Tabla 4.5 Costos de telefonía IP

En el anexo K-5 se puede ver la cotización de los teléfonos IP y de las tarjetas PCI.

4.3 COSTO DE OPERACIÓN Y MANTENIMIENTO

Para que el rediseño pueda funcionar con normalidad se ha incluido los costos de operación y mantenimiento que se muestran en la tabla 4.6

Ítem	Descripción	Costo [$]
Administrador de red	Sueldo para la persona encargada de administrar la red, incluido beneficios de ley, desde las 8:00 am hasta las 16:00 pm.	850,00
Antivirus	Costo de licencias para 250 equipos.	442,66
Internet	Enlace de 8 Mbps simétrico mediante F.O.	135,00
	Enlace de 2 Mbps simétrico	59,50
Total mensual		1.487,16

Tabla 4.6 Costo de operación y mantenimiento

4.4 COSTO TOTAL

El costo total de la implementación de la solución contemplando tanto la red pasiva como activa se detalla en la tabla 4.7.

Ítem	Costo [$]
Red pasiva	39.693,76
Equipos de conectividad	30.897,02
Servidores	7.595,00
Telefonía	11.164,00
Subtotal	89.349,78
IVA	10.721,97
TOTAL	100.071,75

Tabla 4.7 Costo total de la red multi-servicios.

4.5 PROTOTIPO

Con el objeto de corroborar el adecuado funcionamiento de la red multi-servicios diseñada se implementará un prototipo que mantenga una topología similar a la planteada y que brinde los servicios descritos en el capítulo anterior.

El prototipo presentará la topología física mostrada en la figura 4.1.

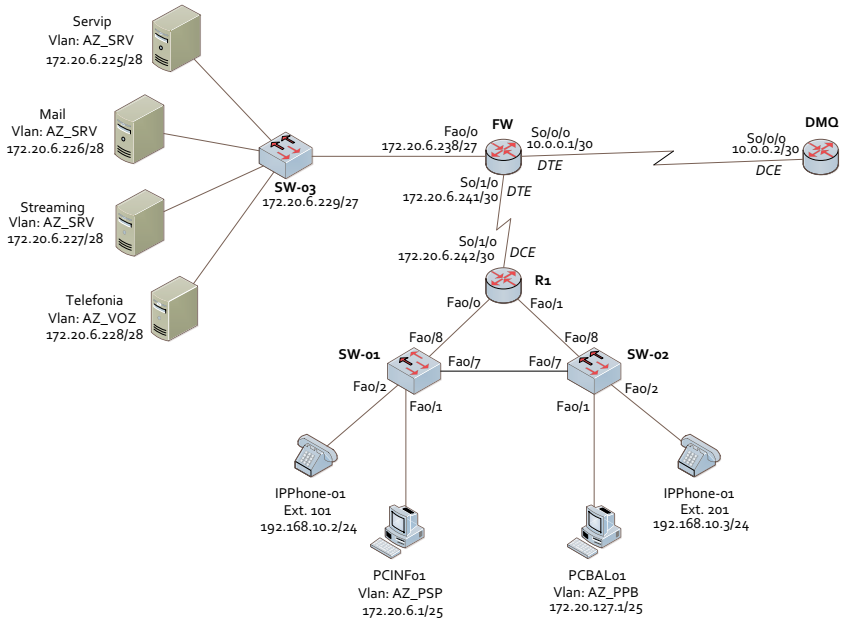


Figura 4.1 Topología física del prototipo

El prototipo implementará las *VLAN's* definidas en la tabla 4.8, definiendo en cada equipo los parámetros necesarios para su implementación.

Nombre VLAN	Número Dot1q	Subred/Mascara	Direcciones IP		Gateway
			Inicial	Final	
AZ_PPB	10	172.20.127.0/25	172.20.127.1	172.20.127.125	172.20.127.126
AZ_PPP	20	172.20.127.128/25	172.20.127.129	172.20.127.253	172.20.127.254
AZ_PSP	30	172.20.6.0/25	172.20.6.1	172.20.6.125	172.20.6.126
AZ_SE	40	172.20.6.128/26	172.20.6.129	17.20.6.189	172.20.6.190
AZ_SRV	50	172.20.6.224/28	172.20.6.225	172.20.6.237	172.20.6.238
AZ_VOZ	60	192.168.10.0/24	192.168.10.1	192.168.10.253	192.168.10.254

Tabla 4.8 VLAN's implementadas en el prototipo

Los equipos de conectividad, equipos terminales y los servidores mantendrán la configuración mostrada en la tabla 4.9.

Nombre del Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
Switches y Routers				
SW-01	AZ_ADM	172.20.6.202	255.255.255.224	172.20.6.220
SW-02	AZ_ADM	172.20.6.203	255.255.255.224	172.20.6.221
SW-03	AZ_ADM	172.20.6.204	255.255.255.224	172.20.6.222
R1	Fa0/0	172.20.6.242	255.255.255.252	--
R1	Fa0/1	Ver tabla de configuración		--
R1	Fa0/2	172.20.6.242	255.255.255.252	--
FW	Fa0/0	Ver tabla de configuración		--
FW	Fa0/1	172.20.6.241	255.255.255.252	--

FW	S0/0/1	10.0.0.1	255.255.255.252	--
DMQ	S0/0/1	10.0.0.2	255.255.255.252	--
Servidores				
servip	NIC	172.20.6.225	255.255.255.240	172.20.6.238
mail	NIC	172.20.6.226	255.255.255.240	172.20.6.238
stream	NIC	172.20.6.227	255.255.255.240	172.20.6.238
telfip	NIC	172.20.6.228	255.255.255.240	172.20.6.238
Equipos Terminales				
PCINF01	NIC	172.20.6.1	255.255.255.128	172.20.6.126
PCBAL01	NIC	172.20.127.1	255.255.255.128	172.20.6.126
IPPhone01	NIC	192.168.10.2	255.255.255.0	192.168.10.254
IPPhone02	NIC	192.168.10.3	255.255.255.0	192.168.10.254
Interfaces en R1				
Fa0/0.10	AZ_PPB	172.20.127.126	255.255.255.128	--
Fa0/0.30	AZ_PSP	172.20.6.127.126	255.255.255.128	--
Fa0/0.60	AZ_VOZ	192.168.10.254	255.255.255.0	--
Fa0/0.99	AZ_ADM	172.20.6.201.27	255.255.255.224	--
Interfaces en FW				
Fa0/0.50	AZ_ADM	172.20.6.238	255.255.255.240	--

Tabla 4.9 Tabla de direccionamiento del prototipo

4.5.1 CONSIDERACIONES

4.5.1.1 Equipos Terminales

Las computadoras PC-01 y PC-02 utilizarán el sistema operativo Windows, su configuración IP será otorgada automáticamente por parte del servidor DHCP habiendo previamente asociado las direcciones MAC de las interfaces de red al servicio DHCP.

La dirección del proxy será configurada en forma manual en cada uno de los navegadores web a ser probados con el objeto de verificar el correcto funcionamiento del servicio de proxy.

Los teléfonos IP serán implementados con la ayuda de software. Durante el desarrollo del prototipo se usarán los softphones provistos por CounterPath Corporation, X-lite 4.0.

4.5.1.2 Switches

Los distintos switches de la red serán implementados en base a switches Cisco, su configuración básica será:

- Hostname,
- Encriptación de claves,
- Claves de acceso para configuración,
- Creación de VLAN's,
- Asociación de puertos a VLAN's,
- Desactivación de puertos no usados,
- Definición de puertos troncales.

La configuración utilizada para este fin es mostrada en el anexo L.

4.5.1.3 Servidores

Los servidores serán implementados con el uso de software libre, ya sea en distribuciones CentOS, Ubuntu o Elastix, estos se encuentran especificados en la tabla 4.10.

Servidor	Servicios provistos	Sistema Operativo
Streaming	Streaming de Video, Videoconferencia	GNU/Linux Ubuntu 11.04
Mail	Correo electrónico	GNU/Linux CentOS 5.4
Telefonía	Telefonía IP	GNU/Linux Elastix 2.3.0
Servip	DNS, DHCP, Proxy	GNU/Linux CentOS 6.2

Tabla 4.10 Servicios provistos por los servidores del prototipo

4.5.1.4 Firewall

El firewall implementará reglas que eviten el tráfico no deseado, con este objetivo mantendrá una configuración de ACL's.

Su implementación en el prototipo será realizada en base a un ruteador Cisco que será configurado con ciertas reglas que limiten el tráfico no deseado.

4.5.1.5 DMQ-Centro

El objeto del router DMQ-Centro es comprobar la conectividad existente hacia los servidores de esta institución.

4.5.2 CONFIGURACIÓN DEL SERVIDOR DE TELEFONÍA IP

El servidor de telefonía IP será implementado con el uso del software de comunicaciones unificadas Elastix en su versión 2.3.0. Este servidor mantendrá dos clientes que podrán acceder a los servicios a ser configurados y establecer una llamada.

4.5.2.1 Instalación y Configuración

El servidor de telefonía Elastix 2.3.0 ha sido elegido para la implementación por su facilidad de instalación, posee el núcleo de VoIP Asterisk, que permite la configuración de la telefonía IP.

Este software cuenta con una interfaz amigable para el administrador, a más de ello cuenta con una gran cantidad de documentación y soporte en internet.

El proceso de instalación se realizó en base al artículo de instalación de un servidor Elastix. [PW100].

4.5.2.2 Configuración de servicios

El servidor Elastix puede ser configurado mediante la edición de los archivos ubicados en /etc/asterisk o mediante la interfaz web presentada por el servidor.

La modificación de estos archivos puede ser realizada con diferentes editores de texto tales como vi, vim, nano, entre otros.

Entre los principales archivos de configuración se pueden encontrar:

- extensions.conf. - contiene la información correspondiente al plan de numeración.
- sip.conf. - contiene la información pertinente al acceso SIP de los clientes.

El proceso de configuración del servicio es mostrado en el anexo M.

4.5.3 SERVIDOR DE STREAMING

El servidor de streaming brindará los servicios de streaming de audio y video y el servicio de videoconferencia.

Este servidor utilizará *Red5*, que permite la transmisión de datos de audio y video en tiempo real mediante la implementación de aplicaciones propias o en base a la utilización de los demos disponibles, mismos que pueden ser configurados a través de la interfaz web o mediante los archivos de configuración propios de la aplicación.

4.5.3.1 Instalación y configuración

La instalación del servidor *Red5* es realizada acorde a la información presentada en la guía del sitio oficial de *Red5.* [PW101]

La aplicación *JWPlayer* es usada para reproducir los videos almacenados en el servidor y que serán visualizados en la página web, para ello es necesaria la adición de las líneas de código necesarias en la página web, a más de la creación de una lista de origen de los videos a ser reproducidos, definiendo su ubicación dentro del servidor.

El servicio de videoconferencia será brindado a través de la aplicación *OpenMeetings*, misma que necesita de la existencia previa de *Red5*. La instalación de OpenMeetings fue realizada en base a la guía del grupo EcuaLUG. [PW102]

Una vez instalado el servicio de videoconferencia, es necesario definir los usuarios que formarán parte del mismo, este proceso es mostrado en el anexo N.

4.5.3.2 Configuración de servicios

En el servidor de streaming se definirá una configuración adecuada para los siguientes puntos:

- *Red5*.- Servidor de streaming de video en flash,

- *OflaDemo*.- Demo para el streaming de video,
- *Openmeetings*.- Servidor de Videoconferencia,
- Servidor web.- Páginas web para acceder a los servicios,
- *JWPlayer*.- reproductor de videos en flash.

El proceso de configuración del servicio de streaming así como el de videoconferencia se encuentra detallado en el anexo N.

4.5.4 SERVIDOR DE DNS, DHCP Y PROXY

El servidor que prestará los servicios de DNS, DHCP y Proxy deberá ser configurado de la siguiente forma:

- DNS
  - Definición de Zonas.- para resolver las direcciones IP a nombres y viceversa.
- DHCP
  - Definición de pozos de dirección a ser distribuidas.
  - Asociación de direcciones IP a direcciones MAC.
- Proxy
  - Listas de páginas web permitidas.
  - Página web de bloqueo.

La instalación de los servicios fueron realizados en base a la guía de prácticas del módulo número dos de la academia de certificación internacionales en tecnologías de información. [F4]

La configuración de los servicios y sus respectivos archivos es detallada en el anexo O.

4.5.5 SERVIDOR DE CORREO ELECTRÓNICO

El servidor de correo electrónico prestará los servicios de mensajería, dentro de la intranet.

El servidor utilizará el software *Zimbra Collaboration Suite – Open Source Edition* en la versión 7.2.0, proporcionado por *VMware*, ya que ofrece una interfaz web amigable para el usuario y el administrador, a más de las funcionalidades propias de un servidor de correo electrónico, como es enviar mensajes entre usuarios de la intranet.

La instalación se realizó con la ayuda del video: Servidor de Email con Zimbra 7 en CentOS 6 [PW103].

Las consideraciones que se deben tener presentes son:

- La IP, el nombre del servidor y el alias, deben ser ingresados en el archivo */etc/hosts*.
- El servidor DNS debe estar configurado adecuadamente, para comprobar aquello se puede utilizar los comandos dig o nslookup.
- Los servicios de Sendmail y postfix deben estar parados.
- La versión de Zimbra que se usará depende de la versión del sistema operativo, para este caso se usó la versión de 32 bit x86, para la plataforma Red Hat Enterprise Linux 5, y se la instaló sobre CentOS 5.4.
- Los paquetes que usará Zimbra deben estar instalados, esto dependerá de la versión del Sistema Operativo del Servidor.
- La partición */opt* debe tener por lo menos 5 GB de espacio libre, caso contrario el servidor de correo no se instalará.

Cabe recalcar que al usar una versión abierta como lo es, *Zimbra Collaboration Suite – Open Source Edition,* no es ético cambiar los logotipos, ni las interfaces que provee el software, ya que esa es la condición para poder usarlo. Por tal motivo en el prototipo no ha sido alterado ninguna de estas condiciones.

El proceso de configuración se encuentra detallado en el anexo P.

4.5.6 PRUEBAS CON EL PROTOTIPO

La presente sección define las pruebas realizadas sobre el prototipo y los resultados del mismo.

4.5.6.1 Puntos de prueba

La siguiente lista muestra los servicios que fueron probados en el prototipo:

- Servicio de DHCP
- Servicio de DNS
- Servicio de correo electrónico
- Servicio de streaming de video
- Servicio de videoconferencia
- Servicio de telefonía IP
- Servicio de Proxy

4.5.6.1.1 Servicio DHCP

La prueba consiste en configurar la adquisición automática de la dirección IP del dispositivo mediante el protocolo DHCP. Esta prueba tiene por objetivo asignar la dirección IP dentro de un rango de direcciones específico a un computador.

La dirección provista será la misma en cada petición a cada computador, existiendo una asociación previa entre la dirección MAC y la dirección IP.

Para su verificación se usara la información presentada por los mensajes del sistema, que se registran en el archivo /var/log/messages. Los resultados del funcionamiento del servicio son mostrados en la figura 4.2.

```
May 15 16:08:52 servip dhcpd: DHCPDISCOVER from 68:b5:99:5c:d1:0f via Auto_eth0
May 15 16:08:52 servip dhcpd: DHCPOFFER on 172.20.6.227 to 68:b5:99:5c:d1:0f via Auto_eth0
May 15 16:08:52 servip dhcpd: DHCPREQUEST for 172.20.6.227 (172.20.6.225) from 68:b5:99:5c:d1:0f via Auto_eth0
May 15 16:08:52 servip dhcpd: DHCPACK on 172.20.6.227 to 68:b5:99:5c:d1:0f via Auto_eth0
```

Figura 4.2 Ofrecimiento de una dirección IP por el servicio DHCP

4.5.6.1.2 Servicio DNS

La prueba de este servicio consiste en la resolución de nombres de dominio a direcciones IP y viceversa. Esta prueba tiene por objeto mostrar el adecuado funcionamiento de la resolución de nombres para el acceso a los diferentes equipos y servidores que mantienen un registro en el servidor.

Con el objeto de demostrar el correcto funcionamiento se usa del comando Dig (*Domain Information Grouper*) que permite comprobar tanto el mapeo de nombres a direcciones IP como el mapeo inverso hacia el nombre de dominio servip.azea.ec.

```
[root@servip ~]# dig servip.azea.ec

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2 <<>> servip.azea.ec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56467
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

;; QUESTION SECTION:
;servip.azea.ec.                        IN      A

;; ANSWER SECTION:
servip.azea.ec.         86400   IN      A       172.20.6.225

;; AUTHORITY SECTION:
azea.ec.                86400   IN      NS      servip.azea.ec.
azea.ec.                86400   IN      NS      mail.azea.ec.
azea.ec.                86400   IN      NS      stream.azea.ec.
azea.ec.                86400   IN      NS      telfip.azea.ec.

;; ADDITIONAL SECTION:
mail.azea.ec.           86400   IN      A       172.20.6.226
stream.azea.ec.         86400   IN      A       172.20.6.227
telfip.azea.ec.         86400   IN      A       172.20.6.228

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed May 16 09:47:43 2012
;; MSG SIZE  rcvd: 171
```

Figura 4.3 Resultado del comando *dig* a servip.azea.ec.

4.5.6.1.3 Servicio de correo electrónico

La prueba de este servicio consiste acceder a una cuenta de correo, escribir un mensaje de correo y enviarlo a otro usuario de la intranet, pudiendo adjuntar un archivo en dicho proceso. Esta prueba tiene por objeto demostrar el adecuado funcionamiento del servicio *DNS* y de correo electrónico.

4.5.6.1.4 Servicio de proxy

La prueba de este servicio consiste en intentar acceder a páginas no permitidas por este servicio a través del navegador web, esperando obtener la página una que indique la restricción que pesa sobre dicho recurso.

Figura 4.4 Interfaz de entrada de Zimbra

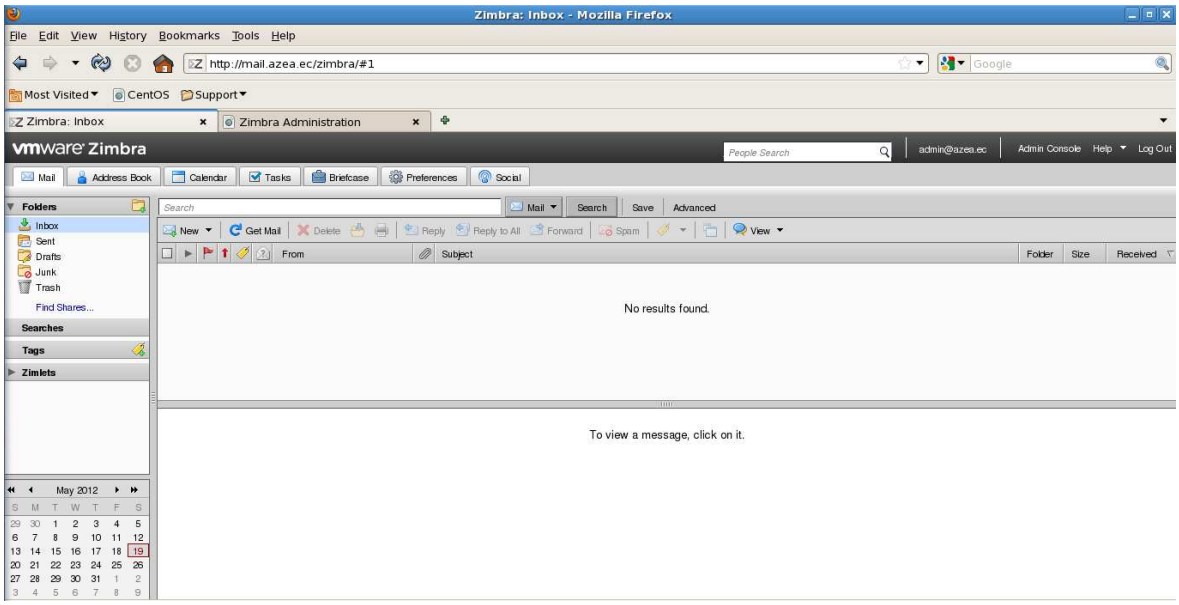


Figura 4.5 Interfaz de usuario de Zimbra

Esta prueba consiste en el intento de acceder a la página web www.youtube.com, teniendo por resultado una pantalla que indica limitación existente al acceso a ciertas páginas cuyo contenido se considera adverso para el buen desarrollo de las actividades en la AZEA.

4.5.6.1.5 Servicio de streaming de video

La prueba de este servicio consiste en la correcta visualización de los videos definidos en el servidor a través de un navegador web. Esta prueba tiene por objeto demostrar el correcto funcionamiento del servicio de *DNS*, Web y Red5 en el servidor de streaming.

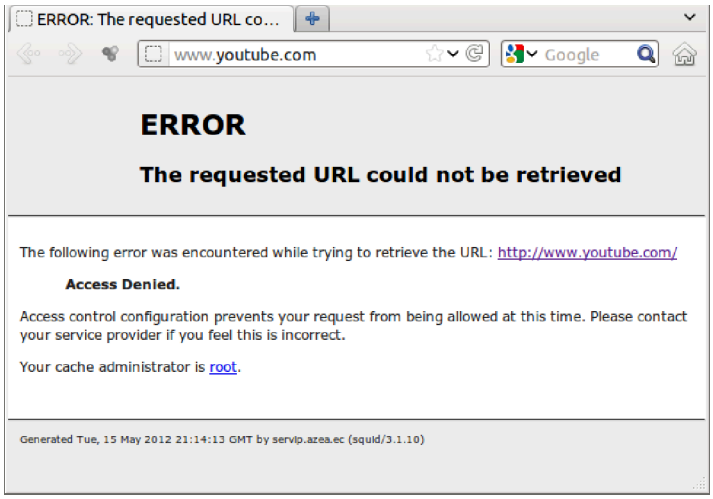


Figura 4.6 Resultado del bloqueo de una página por el servicio proxy

Para corroborar este servicio, se accede mediante un navegador web a la dirección http://stream.azea.ec, donde se selecciona un video para su reproducción, obteniendo los resultados mostrados en la figura 4.7.

Figura 4.7 Página web del servidor de streaming[13]

4.5.6.1.6 Servicio de videoconferencia

La prueba de este servicio consiste en el acceso al servicio e inicio de una videoconferencia con otro participante. Esta prueba tiene por objeto demostrar el correcto funcionamiento de los servicios de *DNS*, *Web*, *Red5,* y *OpenMeetings* en el servidor de streaming.

[13]Interfaz web de http://www.quito.gob.ec

Figura 4.8 Interfaz de OpenMeetings

4.5.6.1.7 Servicio de telefonía IP

La prueba del servicio de telefonía corresponde a la realización de llamadas, mismas que deben ser establecidas adecuadamente.

Los teléfonos a ser utilizados en la pruebo corresponden a los softphones X-Lite 4, mismos que se asocian al servidor de telefonía utilizando el protocolo SIP y utilizando las extensiones 102 y 201, el marcado y establecimiento de la llamada puede ser apreciado en las figuras 4.9 y 4.10.

Figura 4.9 Llamada usando softphones

Figura 4.10 Establecimiento de llamada en Elastix

4.5.6.1.8 Ruteador R1

El ruteador R1 cumple la función de encaminar adecuadamente los paquetes IP entre las distintas subredes que se encuentran configuradas en sus sub-interfaces e interfaces, a más de permitir alcanzar la red de los servidores, acorde a estas consideraciones, la prueba de este equipo consiste en acceder adecuadamente a los servidores.

4.5.6.1.9 Firewall

El firewall será el encargado de implementar políticas de seguridad mediante la definición de listas de acceso, por ello el prototipo implementará ciertas políticas como deshabilitar las peticiones y respuestas de eco a los servidores.

Las pruebas de este elemento cosiste en realizar peticiones de eco y verificar su restricción ante las mismas, obteniendo como resultado la respuesta de destino inaccesible, como se muestra en la figura 4.11.

Figura 4.11 Respuesta del Firewall a una petición de eco

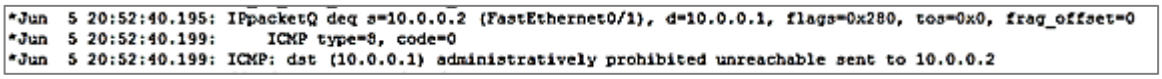


Figura 4.12 Resultados de la restricción en el ruteador

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La recopilación de información acerca de la situación actual de la red de datos de la AZEA permitió identificar los puntos de riesgo de la misma, siendo necesario primeramente definir la topología física y lógica que esta mantiene. Esta recopilación de información constituye el punto base para mejorar la administración, identificar los posibles puntos de falla, incrementar el rendimiento al reemplazar elementes obsoletos, entre otros.

- El rediseño de la red multi-servicios basa su esquema en un modelo jerárquico de capas que permite asociar funciones específicas a cada una, este esquema define tres niveles que son acceso, distribución y núcleo. Esta elección se basa en la facilidad en cuanto al diseño, implementación, administración, escalabilidad y confiabilidad que brinda este esquema.

- Con el objeto de brindar redundancia a la red, el diseño define el uso de dos switches en la capa de núcleo así como la disponibilidad de un enlace de respaldo hacia la red WAN, este mecanismo busca mantener la continuidad de las operaciones de la AZEA ante un posible fallo de uno de los switches en el núcleo o el fallo del enlace WAN.

- La implementación de una solución de telefonía IP permite obtener beneficios tales como la flexibilidad para la creación de las nuevas extensiones vía web, la convergencia de los servicios en una sola red, la instalación de equipos en forma sencilla mediante la utilización de la tecnología *Power over Ethernet*, mismos beneficios que no se pueden obtener con el uso de la central telefonía anteriormente instalada, cuya

administración se veía limitada al contacto y disponibilidad de personal especializado.

- La movilidad que se obtiene a través de la implementación de una red inalámbrica busca resolver los problemas de acceso a la red en sitios donde la implementación de la red cableada resulta complicado y donde la demanda de conectividad por parte de equipos que disponen de interfaces inalámbricas pueden ser suplidas.

- El dimensionamiento adecuado de los equipos así como la capacidad de los enlaces es de suma importancia para garantizar un buen desempeño de la red multi-servicios, los equipos deben manejar los estándares de la industria para garantizar su interoperabilidad con equipos similares de distintos fabricantes.

- En el plan de migración se ha previsto un tiempo aproximado de 25 semanas, sin embargo este tiempo variará de acuerdo a los recursos que en la práctica la AZEA como entidad pública pueda proporcionar, y a las facilidades necesarias que la Administración preste, como accesos al personal en todo el proceso hacia los lugares donde se deba trabajar.

- El análisis de la documentación que se irá recopilando durante el proceso de migración permitirá agilizar el trabajo, de la misma manera se podrá establecer las razones de los retrasos que puedan darse en el plan y con ello tomar las debidas precauciones para poder evitar situaciones similares hasta completar la transición.

- La definición de un plan de contingencia busca el mejorar los procedimientos a seguir ante un evento adverso, mismo procedimiento debe ser previamente instruido al personal que mantendrá un rol activo durante las acciones, cabe resaltar que la documentación actualizada de la red es un punto de vital importancia al momento de recuperarla.

- La capacitación del personal, tanto técnico como el de los usuarios finales, permitirá una mayor comprensión hacia la red multi-servicios y sus nuevas funcionalidades. Así también permitirá tener personal que de soporte posterior a la migración y que pueda solventar cualquier inconveniente que se presente.

- El uso de herramientas de código abierto permite tener mayor control en la seguridad de cada uno de los servicios que se ofrecen, así también permite disminuir costos en cuanto a implementación, licenciamientos de operación, adquisición de software o hardware que suelen tener protocolos propietarios que impiden tener compatibilidad con equipos que no sean de la misma marca.

- Es de suma importancia el uso de cables UTP y patch cords que mantengan los terminales RJ-45 en buen estado, pudiendo en caso contrario conllevar la caída de toda la red o el mal funcionamiento de los equipos sujetos a dicho terminal.

- Con el objeto de maximizar el rendimiento de la red es necesario eliminar el tráfico innecesario como es el caso del tráfico producido por los protocolos de enrutamiento como OSPF, para ello es importante identificar las interfaces que no deben propagar dichas notificaciones y desactivar aquella característica.

- El desempeño correcto de la red multi-servicios no depende solamente de los equipos de conectividad y el cableado estructurado subyacente, es necesario el brindar soporte a los dispositivos terminales como laptops y computadores de escritorio, para garantizar el acceso a servicios que requieren de elementos como cámaras web y micrófonos para su correcto funcionamiento.

- Es imperativo el realizar procedimientos destinados a mejorar la red actual en forma inmediata, tal como el reemplazo de los Hubs que forman parte

de la red actual, teniendo un impacto grave puesto que uno de ellos forma parte de la capa de distribución.

5.2 RECOMENDACIONES

- Se sugiere a la Administración Zonal Eloy Alfaro tomar en cuenta el cambio de red lo antes posible ya que la infraestructura actual de red no satisface las necesidades de los usuarios directos y por lo tanto tampoco de los usuarios indirectos como son los ciudadanos que hacen uso de los servicios debido a que la red actual ha presentado varios problemas como fallas en puntos de red, equipos, entre otros.

- Se recomienda el mantener la documentación correspondiente a topologías y usuarios totalmente actualizada, definiendo controles periódicos en los equipos de red para prever posibles fallas o identificar modificaciones en las conexiones de los equipos de red realizadas sin el consentimiento de la Jefatura de Informática.

- Se recomienda la desactivación de los puertos en desuso en los equipos que tengan capacidad administrativa, mitigando de esta forma el riesgo de adición de elementos ajenos a la red que puedan afectar su rendimiento.

- Se recomienda informar a los usuarios mediante varios medios como vía e-mail, afiches, etc., de los cambios que se van a realizar en la red y el tiempo contemplado para los mismos, con el fin de prever sus acciones durante la transición. Los tiempos de afectación deben durar el menor tiempo posible y una vez concluidos los trabajos se debe comunicarse a los usuarios para el reinicio inmediato de operaciones, así como proceder con la documentación de los resultados.
- Se recomienda al personal de la AZEA dar la importancia necesaria a la infraestructura de red tanto pasiva como activa ya que es uno de los recursos más importantes de la Administración pues la mayoría de los servicios que ofrece el Municipio de Quito lo hace a través de este medio. La red debe

cumplir con estándares y normas para un correcto funcionamiento de los servicios proporcionados y una rápida detección y solución de fallas.

- Se recomienda la adición de personal especializado a la Jefatura de Informática en vista de la importancia y magnitud de la red, del mismo modo es de suma importancia capacitar a los miembros de dicho departamento en cuanto al manejo de los servicios a ser provistos, una correcta administración de la red, un manejo correcto de las políticas de seguridad y los procedimientos a seguirse ante un posible fallo en la red.

- Se recomienda el establecimiento de políticas de seguridad destinadas a mitigar los riesgos a los que se expone actualmente la red de datos en forma inmediata, haciendo un especial énfasis en el manejo apropiado del acceso a los espacios donde son alojados los equipos de red.

- Se recomienda el programar a los servidores basados en Linux el inicio solo en modo texto, permitiendo que puedan utilizar la mayor cantidad de recursos disponibles en los servicios a ser soportados por los mismos.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

[L1] Stallings, R., “Cryptography and Network Security”, 3th edition, Prentice Hall, USA, 2002.

[L2] Sellés, F., “Introducción a la telefonía IP utilizando Estándares”, 1ra edición, Free Software Foundation, España, 2009.

[L3] Tanenbaum, A., “Redes de Computadoras”, 4ta edición, Prentice Hall, USA, 2003.

[L4] Stallings, W., “Comunicaciones y Redes de Computadores”, 6ta edición, Prentice Hall, USA, 2000.

[L5] Hesselbach, X., Altés, J., “Análisis de Redes y Sistemas de Comunicaciones”, 1ra edición, Editions UPC, España, 2002.

PUBLICACIONES (PAPERS, REVISTAS, ETC)

[P1] Programa de la Academia de Networking de Cisco CCNA1 v3.1, “Suplemento sobre cableado estructurado”, 2003.

[P2] Cisco Networking Academy CCNA Exploration 4.0, “Conceptos Básicos Sobre Networking”, 2008.

[P3] Cisco Networking Academy CCNA Exploration 4.0, “Conmutación y conexión inalámbrica de LAN”, 2008.

[P4] Cisco Networking Academy CCNA Exploration 4.0, “Acceso a la WAN”, 2008.

[P5] Forné, J., Melús, J., Soriano, M., “Criptografía y Seguridad en Comunicaciones”. Universidad Politécnica de Catalunya, 2005.

[P6] Postigo, M., García, J., Aguilar, M., “Transmisión Eficiente de Bloques en Tiempo Real sobre Redes IP”, Universidad Politécnica de Cataluña, 2010.

[P7] Telecommunication standardization sector of ITU, “H.320 System Implementors’ Guide”, 2004.

[P8] Cabrera, J., “Visión General Administración Zonal Eloy Alfaro”, 2011.

[P9] Cisco Systems, “Data Center Power and Cooling”, 2011.

TESIS

[T1] Morales, F., Saravia, D., "Reingeniería de la red de datos corporativa de la Empresa Alianza Compañía de Seguros y Reaseguros S.A. para la integración de servicios de telefonía IP", Ing. tesis, EPN, Quito, Ecuador, Noviembre 2011.

[T2] Bazurto, J., Mena, D., "Rediseño de la red del Instituto Tecnológico Superior Central Técnico", Ing. tesis, EPN, Quito, Ecuador, Octubre 2011.

[T3] Castillo, R., Tasintuña, F., "Implementación de soluciones de red en la infraestructura de comunicaciones de acería del Ecuador C.A.", Ing. tesis, EPN, Quito, Ecuador, Octubre 2011.

[T4] Perugachi, F., "Reingeniería de la red LAN del Ilustre Municipio del cantón Rumiñahui", Ing. tesis, EPN, Quito, Ecuador, Junio 2010.

[T5] Martínez, V., Suárez, V., "Estudio de Factibilidad para la implementación de recursos sincrónicos en la plataforma de educación virtual del servicio de rentas internas". Ing. tesis, EPN, Quito, Ecuador, Diciembre 2010.

FOLLETOS

[F1] Hidalgo, P., "Redes de Área Local (LAN)", 2009.

[F2] Sinche, S., "Redes de Área Extendida", 2009.

[F3] Hidalgo, P., "MultiProtocol Label Switching (MPLS)", 2009.

[F4] ACIERTE, "Programa de certificación Linux – LPI Módulo II: Administración de red y Seguridades", 2011.

INTERNET

[PW1] Wikitel, "Redes de Datos", [Recuperado el 2 de febrero de 2012] http://es.wikitel.info/wiki/Redes_de_datos

[PW2] Wikipedia, "Modelo OSI, capa aplicación", [Recuperado el 2 de febrero de 2012] http://es.wikipedia.org/wiki/Modelo_OSI#Capa_de_aplicaci.C3.B3n

[PW3] IEEE Standards Association, "IEEE 802.3: Ethernet", [Recuperado el 2 de febrero de 2012] http://standards.ieee.org/about/get/802/802.3.html

[PW4] Valarezo, D., “Enrutamiento entre VLAN”, [Recuperado el 5 de febrero de 2012] http://www.slideshare.net/darwinnano/enrutamiento-entre-vlan

[PW5] Kioskea, “VLAN-Redes virtuales”, [Recuperado el 5 de febrero de 2012] http://es.kioskea.net/contents/internet/vlan.php3

[PW6] Multingles, “Redes WiFi Inalámbricas”, [Recuperado el 5 de febrero de 2012] http://multingles.net/docs/Manual%20%20Redes%20WiFi%20inalambricas.pdf

[PW7] Masternetsc, “Normas para el cableado estructurado”, [Recuperado el 13 de febrero de 2012] http://www.masternetsc.com.ar/sitio/archivos/pdf/normas_cableado.pdf

[PW8] TIA, “Evolution of structured cabling”, [Recuperado el 20 de febrero de 2012] http://www.tiaonline.org/news_events/press_room/documents/evolution_of_structured_cabling.cfm

[PW9] Güimi, “Cableado Estructurado”, [Recuperado el 21 de febrero de 2012] http://guimi.net/monograficos/G-Cableado_estructurado/G-Cableado_estructurado.pdf

[PW10] Wikilearning, “Manual práctico de IPTABLES - Qué es un firewall”, [Recuperado el 15 de marzo de 2012] http://www.wikilearning.com/tutorial/manual_practico_de_iptables-que_es_un_firewall/9755-1

[PW11] Wikipedia, “Domain Name System”, [Recuperado el 16 de marzo de 2012] http://es.wikipedia.org/wiki/Domain_Name_System

[PW12] Microsoft TechNet, “Cómo funcionan las consultas DNS”, [Recuperado el 16 de marzo de 2012] http://technet.microsoft.com/es-es/library/cc775637%28WS.10%29.aspx

[PW13] Wikipedia, “BIND”, [Recuperado el 16 de marzo de 2012] http://es.wikipedia.org/wiki/BIND

[PW14] Internet Systems Consortium, “What is BIND and what does it do?”, [Recuperado el 16 de marzo de 2012] https://www.isc.org/software/bind/whatis

[PW15] Wikipedia, “Proxy”, [Recuperado el 16 de marzo de 2012] http://es.wikipedia.org/wiki/Proxy

[PW16] Squid-cache, “Squid: Optimizing Web Delivery”, [Recuperado el 16 de marzo de 2012] http://www.squid-cache.org/

[PW17] Universidad Manuela Beltrán, “Correo Electrónico”, [Recuperado el 21 de marzo de 2012] http://campovirtual.umb.edu.co/courses/212-ER12100/modulo3_serv/pdfs/Modulo3.pdf

[PW18] Internet Engineering Task Force, “Simple Mail Transfer Protocol”, [Recuperado el 30 de marzo de 2012] http://tools.ietf.org/html/rfc2821

[PW19] Wikipedia, “Simple Mail Transfer Protocol”, [Recuperado el 31 de marzo de 2012] http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[PW20] Wikipedia, “Post Office Protocol”, [Recuperado el 6 de abril de 2012] http://es.wikipedia.org/wiki/Pop3

[PW21] Universidad de Buenos Aires, “Correo Electrónico (RFC 822, MIME, SMTP, POP3 e IMAP)”, [Recuperado el 6 de abril de 2012] http://www-2.dc.uba.ar/materias/tc/downloads/apuntes/smtp_pop_imap.pdf

[PW22] Wikipedia, “Internet Message Access Protocol”, [Recuperado el 7 de abril de 2012] http://es.wikipedia.org/wiki/IMAP

[PW23] VMware, “Zimbra Messaging and Collaboration Suite 6.0” [Recuperado el 7 de abril de 2012] http://www.zimbra.com/buzz/index.es.html

[PW24] Telefónica, “Telefonía IP”, [Recuperado el 7 de abril de 2012] http://www.telefonica.com.pe/empresas/esolutions/IR_telefonia.shtml

[PW25] Wikitel, “H.323”, [Recuperado el 10 de abril de 2012] http://wikitel.info/wiki/H.323

[PW26] Microsoft MSDN, “The H.323 Standard”, [Recuperado el 10 de abril de 2012] http://msdn.microsoft.com/en-us/library/ms709083(v=vs.85).aspx

[PW27] Red Iris, “Videoconferencia H.323”, [Recuperado el 10 de abril de 2012] http://www.rediris.es/mmedia/Arquitectura.es.html

[PW28] Wikipedia, “Session Initiation Protocol”, [Recuperado el 13 de abril de 2012] http://es.wikipedia.org/wiki/Session_Initiation_Protocol

[PW29] Wikipedia, “Videoconferencia”, [Recuperado el 15 de abril de 2012] http://es.wikipedia.org/wiki/Videoconferencia

[PW30] Universidad de Alicante, “Tipos de Videoconferencia”, [Recuperado el 15 de abril de 2012] http://si.ua.es/es/videoconferencia/tipos-de-videoconferencias.html

[PW31] Universidad Autónoma del Estado de Hidalgo, “Acerca de Videoconferencia”, [Recuperado el 15 de abril de 2012] http://virtual.uaeh.edu.mx/riv/videoconferencia.php

[PW32] Wikipedia, “Streaming”, [Recuperado el 15 de abril de 2012] http://es.wikipedia.org/wiki/Streaming

[PW33] Grupo de Redes de Computadores, “Codificación y difusión de información multimedia”, [Recuperado el 15 de abril de 2012] http://www.grc.upv.es/docencia/tra/PPT/codificacion.ppt

[PW34] Comunidad Streaming, “Qué es RTMP?”, [Recuperado el 15 de abril de 2012] http://comunidadstreaming.com/foro-general-video-streaming/9-que-es-rtmp.html

[PW35] Adobe, “Real-Time Messaging Protocol (RTMP) specification”, [Recuperado el 15 de abril de 2012] http://www.adobe.com/devnet/rtmp.html

[PW36] Videolan, “VLC media player”, [Recuperado el 16 de abril de 2012] http://www.videolan.org/

[PW37] Red5, “Red 5 The Open Source Media Server”, [Recuperado el 17 de abril de 2012] http://www.red5.org/

[PW38] Slideshare, “RED5 Open Source Flash Server”, [Recuperado el 17 de abril de 2012] http://www.slideshare.net/gmoggia/red5-1685304

[PW39] Cisco, “Lo que usted necesita saber sobre seguridad de la red”, [Recuperado el 19 de abril de 2012] http://www.cisco.com/web/solutions/smb/espanol/productos/seguridad/security_primer.html

[PW40] Cisco, “Integrated Perimeter Defense”, [Recuperado el 20 de abril de 2012] http://www.cisco.com/en/US/products/sw/secursw/ps1018/index.html

[PW41] National Institute of Standards and Technology, “Contingency Plan Template”, [Recuperado el 24 de abril de 2012] http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc

[PW42] Quito Distrito Metropolitano, “Estructura”, [Recuperado el 28 de abril de 2012] http://www.quito.gob.ec/lotaip/cat_view/34-lotaip-2010/78-a-organizacion-interna/79-a1-estructura-organica-funcional.html

[PW43] Wikipedia, “10Base2”, [Recuperado el 2 de mayo de 2012] http://es.wikipedia.org/wiki/10Base2

[PW44] Avira, “Manual Usuarios Puntomatico”, [Recuperado el 4 de mayo de 2012] http://avira.webgate/3871329168/complete/intranet.oscus.coop/intranet/ManualUsusarioPuntomatico.pdf?file=ManualUsusarioPuntomatico.pdf

[PW45] Microsoft, “Office Communication Server: una plataforma de colaboración”, [Recuperado el 6 de mayo de 2012] http://www.microsoft.com/latam/technet/articulos/tn/2007/jun-01.mspx

[PW46] Microsoft TechNet, “Mediation Server”, [Recuperado el 7 de mayo de 2012] http://technet.microsoft.com/en-us/library/bb894504(office.12).aspx

[PW47] Microsoft TechNet, “Exchange Server 2007”, [Recuperado el 7 de mayo de 2012] http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

[PW48] Isatel Telefonía, “Centralita privada PBX-IP híbrida”, [Recuperado el 9 de mayo de 2012] http://www.isatel.cl/manuales/Primeros_pasosTDA.pdf?file=Primeros_pasosTDA.pdf

[PW49] Wikispaces, “Construcción de un latiguillo de red”, [Recuperado el 10 de mayo de 2012] http://kortxero.wikispaces.com/PRACTICA+N%C2%BA3

[PW50] Hrprofessionals, “Notas sobre el nuevo estándar para aterramiento de telecomunicaciones TIA 607-B”, [Recuperado el 25 de agosto de 2012] http://hrprofessionals.webcindario.com/wordpress/?p=131

[PW51] IHI Connectors, “Cross Reference Table: Awg, "Aught" (# / 0), MCM / kcmil”, [Recuperado el 25 de agosto de 2012] http://www.ihiconnectors.com/AWG%20wire%20sizes.htm

[PW52] Commscope, “GigaSPEED® X10D F/UTP and S/FTP Cabling System Earthing (Grounding) and Bonding Guidelines”, [Recuperado el 25 de agosto de 2012] http://docs.commscope.com/Public/GigaSPEED_X10D_FTP_EGB_Guidelines.pdf

[PW53] Panduit, “Network Bonding and Grounding: TIA-607-B – Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises”, [Recuperado el 26 de agosto de 2012] http://www.usmp.edu.pe/vision2012_lima/SEMINARIOS/seminarios/Sistemas_de_aterramiento.pdf

[PW54] Paul Kish, “Bonding & grounding de-mystified”, [Recuperado el 26 de agosto de 2012] http://www.belden.com/docs/upload/cnsstandardsmarapr2012.pdf

[PW55] YouTube, “Encoding settings for live streaming”, [Recuperado el 15 de mayo de 2012] http://support.google.com/youtube/bin/answer.py?hl=en&answer=1723080

[PW56] Wikipedia, “CentOS”, [Recuperado el 20 de mayo de 2012] http://es.wikipedia.org/wiki/CentOS

[PW57] Ubuntu, “Preparing to Install”, [Recuperado el 20 de mayo de 2012] https://help.ubuntu.com/11.04/serverguide/C/preparing-to-install.html

[PW58] Wikipedia, “Windows Server 2008”, [Recuperado el 20 de mayo de 2012] http://es.wikipedia.org/wiki/Windows_Server_2008#Windows_Server_2008_R2

[PW59] Linuxsilo, “Zimbra 5, suite de mensajería y colaboración”, [Recuperado el 21 de mayo de 2012] http://linuxsilo.net/articles/zimbra.html#requerimientos

[PW60] Elastix, “What is the Elastic *PBX* system requirements urgent”, [Recuperado el 22 de mayo de 2012] http://www.elastix.org/es/component/kunena/20-elastix-community-/29958-what-is-the-elastic-pbx-system-requirementsurgent.html

[PW61] Squid Users Guide, “Installing Squid”, [Recuperado el 25 de mayo de 2012] http://www.deckle.co.za/squid-users-guide/Installing_Squid

[PW62] RED5, “System Requirements For Red5”, [Recuperado el 28 de mayo de 2012] http://red5.electroteque.org/dev/doc/html/SystemRequirementsForRed5.html

[PW63] Kioskea, “Introducción a Wi-Fi (802.11 o Wi Fi)”, [Recuperado el 28 de mayo de 2012] http://es.kioskea.net/contents/wifi/wifiintro.php3

[PW64] Universidad Alas Peruanas, “Propuesta de diseño de infraestructura de voz sobre IP para el hostal Ilo”, [Recuperado el 30 de mayo de 2012] http://www.slideshare.net/lexruso/voz-sobre-ip-para-hotel

[PW65] Irontec, “Voz sobre IP y Asterisk”, [Recuperado el 1 de junio de 2012] http://documentacion.irontec.com/cursoAsteriskVozIP-1-introduccion-SIP.pdf

[PW66] Cisco, “Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation”, [Recuperado el 4 de junio de 2012] http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml

[PW67] ITWorld, “What's toll-quality voice?”, [Recuperado el 5 de junio de 2012] http://www.itworld.com/ITW849

[PW68] Telefoniavozip, “MOS, Mean Opinion Score”, [Recuperado el 7 de junio de 2012] http://www.telefoniavozip.com/glosario-voip/m/mos.htm

[PW69] 3CX, “Explicación sobre FXS y FXO”, [Recuperado el 8 de junio de 2012] http://www.3cx.es/voip-sip/fxs-fxo.php

[PW70] Elastix, “Información del Producto”, [Recuperado el 9 de junio de 2012] http://www.elastix.org/index.php/es/informacion-del-producto/informacion.html

[PW71] Elastix, “Comunicaciones Unificadas”, [Recuperado el 10 de junio de 2012] http://www.elastix.org/images/elastix.org/images/all_images/comunicaciones-unificadas.gif

[PW72] Apache incubator, “OpenMeetings”, [Recuperado el 11 de junio de 2012] http://incubator.apache.org/openmeetings/

[PW73] Hardware, “Switch Cisco WS-C3560X-24T-S”, [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/cisco/WS-C3560X-24T-S

[PW74] Hardware, “Switch Cisco WS-C2960S-24TS-L”, [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/cisco/WS-C2960S-24TS-L

[PW75] Hardware, “Switch Cisco WS-C2960-24PC-L”, [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/cisco/WS-C2960-24PC-L

[PW76] Hardware, “Switch Cisco WS-C2960-24TC-L”, [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/cisco/WS-C2960-24TC-L

[PW77] Hardware, “HP A5500-24G EI Switch”, [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/hp/JD377A

[PW78] Hewlett Packard, “Switch HP 5500-24G-SFP EI Switch”, [Recuperado el 12 de junio de 2012] http://hp.controlp.com/HP-A5500-24G-SFP-EI-SWITCH---CONMUTADOR----L4---GE_103710_P.asp

[PW79] Hardware, “HP A5120-24G EI Switch” [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/hp/JE068A

[PW80] Hewlett Packard, “HP A5120-24G-PoE+ EI Switch”, [Recuperado el 12 de junio de 2012] http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00778577&lang=es&cc=mx&taskId=110&prodSeriesId=4174705&prodTypeId=12883

[PW81] Senetic, “HP 3600-24 v2 EI Switch”, [Recuperado el 12 de junio de 2012] http://www.senetic.mx/product/JG299A

[PW82] Manchanet, “HP 3600-24 V2 EI Switch”, [Recuperado el 12 de junio de 2012] http://tienda.manchanet.es/networking/lan/switches-y-hubs/hp/hp-jg299a-3600-switch-en-paratupc-ficha-tecnica-747545.html

[PW83] Hardware, “HP E2610-24-PoE Switch”, [Recuperado el 12 de junio de 2012] http://es.hardware.com/tienda/hp/J9087A

[PW84] Hewlett Packard, “Switch HP 2610-24-PoESwitch”, [Recuperado el 12 de junio de 2012] http://h10010.www1.hp.com/wwpc/es/es/sm/WF06b/12883-12883-4172267-4172277-4172277-3751584-3658869.html?dnr=1

[PW85] Cisco, **“**ASA 5510-K8**”,** [Recuperado el 12 de junio de 2012] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

[PW86] Hewlett Packard, “HP S200-S UTM Appliance”, [Recuperado el 12 de junio de 2012] http://www.almacen-informatico.com/HP_hp-s200-s-utm-appliance-JD273A_150374_p.htm

[PW87] Senetic, “HP SecPath U200-S 1 Year Anti-Spam Serv”, [Recuperado el 12 de junio de 2012] http://www.senetic.mx/product/JG075B

[PW88] Cisco, “Cisco Aironet 1260 Series Access Point Data Sheet”, [Recuperado el 12 de junio de 2012] http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10980/data_sheet_c78-593663.html

[PW89] Hewlett Packard, “Punto de acceso 802.11n de radio doble HP MSM430”, [Recuperado el 12 de junio de 2012] http://h10010.www1.hp.com/wwpc/ec/es/sm/WF06b/12883-12883-1137927-4172284-4172284-5037566-5049423.html?dnr=1

[PW90] Dell, “Servidor en torre compacto Power Edge T110 II de Dell”, [Recuperado el 13 de junio de 2012] http://www.dell.com/ec/empresas/p/poweredge-t110-2/pd

[PW91] Dell, “Personalice su sistema Dell”, [Recuperado el 13 de junio de 2012] http://configure.la.dell.com/dellstore/config.aspx?c=ec&cs=ecbsdt1&fb=1%20&l=es&model_id=poweredge-t110-2&oc=lpt112fix&s=bsd&vw=classic

[PW92] Yealink, “SIP-T20P”, [Recuperado el 13 de junio de 2012] http://www.yealink.com/index.php/Products/detail/id/4

[PW93] Grandstream, “GXP1450 HD Enterprise IP Phone”, [Recuperado el 13 de junio de 2012] http://www.grandstream.com/index.php/products/ip-voice-telephony/enterprise-ip-phones/gxp1450

[PW94] Voiplink, “Digium TDM808E - 8 FXO Ports - Includes Echo Cancellation”, [Recuperado el 13 de junio de 2012] http://www.voiplink.com/Digium_TDM808E_p/digium-tdm808e.htm

[PW95] Voiplink, “Sangoma A20004D 8 FXO analog card w/Ecan PCI”, [Recuperado el 13 de junio de 2012] http://www.voiplink.com/Sangoma_A20004d_p/sangoma-a20004d.htm

[PW96] Scribd, “Guía para el plan de migración a software libre en la administración pública nacional (APN) de la república bolivariana de

Venezuela", [Recuperado el 14 de junio de 2012] http://es.scribd.com/doc/6442474/Guia-para-el-plan-de-migracion-a-Software-Libre-en-la-Administracion-Publica-Nacional

[PW97] Software público, "Migración a Software Libre. Guía de Buenas Prácticas", [Recuperado el 18 de junio de 2012] http://www.softwarepublico.gob.pe/files/secciones/migracional softwarelibre.pdf

[PW98] Software libré, "Migración a Software Libre a Nivel Corporativo y Gubernamental", [Recuperado el 20 de junio de 2012] http://softwarelibre.eventos.usb.ve/files/presentaciones/Presentacion_ USB.pdf

[PW99] Universidad Nacional del Nordeste, "Cableado Estructurado", [Recuperado el 22 de junio de 2012] http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/Cableado_Estructurado-TP08.pdf

[PW100] Asterisk Colombia, "Tutorial de Elastix: Instalación", [Recuperado el 24 de junio de 2012] http://www.asteriskcolombia.org/documentacion/elastix/tutorial-de-elastix-instalacion/

[PW101] Red5, "Install", [Recuperado el 26 de junio de 2012] http://trac.red5.org/wiki/Install

[PW102] Ecualug, "Instalar Openmeetings en Debian Lenny", [Recuperado el 27 de junio de 2012] http://www.ecualug.org/2009/07/15/blog/razametal/instalar_openmeetings_en_debian_lenny

[PW103] YouTube, "Servidor de Email com Zimbra 7 e CentOS 6", [Recuperado el 28 de junio de 2012] http://youtu.be/0Yxc0O4GAKM