ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DE LA RED DE DATOS DE LA MATRIZ DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL (MIES)

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

JOSÉ EDUARDO AGUILAR SÁNCHEZ
joseaguilarsanchez@hotmail.com

JUAN SEBASTIÁN RÍOS CARRIÓN
juan.rios.uio@outlook.com

DIRECTOR: ING. WILLAMS FERNANDO FLORES CIFUENTES
fernando.flores@epn.edu.ec

Quito, Junio 2016

DECLARACIÓN

Nosotros, José Eduardo Aguilar Sánchez y Juan Sebastián Ríos Carrión 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.

_____ _____

José Aguilar Juan Ríos

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por José Eduardo Aguilar Sánchez y Juan Sebastián Ríos Carrión, bajo mi supervisión.

_____

Ing. Fernando Flores

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

A nuestro tutor el Ing. Fernando Flores por su constante ayuda para culminar este proyecto.

Al personal del Departamento de Tecnología del Ministerio de Inclusión Económica y Social por la información brindada.

A la Escuela Politécnica Nacional que me formó como profesional.

A mi familia que siempre me motivó para seguir cumpliendo mis metas.

José Eduardo

AGRADECIMIENTOS

Agradezco principalmente a mi mamita Rosita, a mi papi Javier y a mi hermano Emilio, que con su gran esfuerzo, enseñanzas, valores, amor y paciencia me ayudaron a cumplir esta y muchas metas a lo largo de toda mi existencia incondicionalmente.

Agradezco a Mayra, el amor de mi vida, que ha estado junto a mí en esta etapa de mi vida con mucho esmero, amor y dedicación, enseñándome muchas cosas, siendo mi alegría y complementando mi vida.

Agradezco a José, mi compañero de tesis y amigo, por su valioso apoyo y paciencia para terminar este proyecto tan importante.

Agradezco al Ing. Fernando Flores por su gran apoyo y paciencia, cuyo esfuerzo nos ha guiado a culminar esta importante meta.

Agradezco al personal de TI del Ministerio de Inclusión Económica y Social. Con su ayuda y disponibilidad pudimos avanzar en este proyecto.

Agradezco a los docentes y a la Escuela Politécnica Nacional, que compartieron su sabiduría conmigo para formarme como profesional y como persona.

Agradezco a mis amigos, que estuvieron en todo momento de mi vida brindándome una sincera amistad y ayudándome a ser una mejor persona de muchísimas maneras.

Finalmente agradezco a todas las personas que de manera directa e indirecta han influenciado en mi vida para llegar a cumplir este gran objetivo personal con todo el apoyo que les ha sido posible otorgarme.

Juan Sebastián

DEDICATORIA

El presente trabajo lo dedico a mi familia que siempre estuvo a mi lado y me brindaron su apoyo incondicional.

A mi madre Gladys, a mi padre José Eduardo, a mis hermanas Karen y Verónica.

José Eduardo

DEDICATORIA

Este proyecto está dedicado a mis padres, a mi hermano, al amor de mi vida, a mi sobrino y a todos quienes han sido un apoyo, guía e inspiración para ayudarme a llegar hasta aquí.

A mi mamita Rosita por su amor incondicional y sacrificio constante que me ayudó a llegar a todas mis metas, a mi papi Javier por su esfuerzo, paciencia y valiosas enseñanzas, a mi hermano Emilio por estar conmigo en todo momento, a Mayra por su amor y cariño que complementa mi vida y a mi sobrino Emilio por ser una luz inspiradora.

Juan Sebastián

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El Ministerio de Inclusión Económico y Social “MIES”, es una institución pública encargada de ejecutar políticas, regulaciones, programas y servicios en favor de generar oportunidades para que las ciudadanas y ciudadanos superen su condición de pobreza y obtengan seguridad (de manera no contributiva) con prioridad a niñas, niños, adultos mayores, personas con discapacidad y la población en situación de pobreza y vulnerabilidad. El presente proyecto tiene como finalidad el rediseño de la red de datos actual de la matriz del Ministerio de Inclusión Económica y Social. Para llegar a este objetivo se ha tomado como base la sustentación teórica acorde a los temas a tratarse, una recopilación y análisis de la situación actual de la red de datos, el rediseño en función de los problemas encontrados durante el análisis, la elección de una solución tecnológica adecuada y las conclusiones y recomendaciones generadas durante la realización del proyecto.

En el primer capítulo se recogen varios fundamentos teóricos relacionados a los temas a tratarse más adelante. Se incluyen aspectos teóricos de redes de comunicación, topologías de redes, estándares de cableado estructurado, seguridad y gestión de la red y aspectos del software libre.

El segundo capítulo contiene información respectiva al estado de la actual red del Ministerio de Inclusión Económica y Social. Se detallan aspectos relacionados a la infraestructura de red, vista desde su parte física y su parte lógica. El análisis se realiza en cada uno de los pisos que conforman la planta de la matriz.

El tercer capítulo consta del rediseño de la red de datos, enfocándose tanto en la red pasiva como en la activa. En lo relacionado a la red pasiva, se propone la instalación de un sistema de cableado estructurado que permita satisfacer la necesidad de la red actual en función de la cantidad de usuarios y los problemas encontrados con el cableado actual. En lo referente a la red activa se propone el uso adecuado de los equipos que actualmente posee la institución, así como la propuesta de nuevos equipos que permitan complementar el servicio de manera adecuada. Se incluyen los costos que derivan de esta implementación.

El cuarto capítulo se enfoca en un prototipo que permite comprobar la factibilidad de la implementación del diseño, a una escala menor, junto con las respectivas pruebas de funcionamiento.

Finalmente, el quinto capítulo incluye las conclusiones y recomendaciones obtenidas durante la realización del presente proyecto.

PRESENTACIÓN

El Ministerio de Inclusión Económica y Social tiene una importante función dentro de las políticas sociales de la sociedad ecuatoriana. Sus esfuerzos se enfocan en la población más vulnerable y con mayores riesgos intrínsecos a la situación de pobreza. Sus servicios tienen mayor prioridad en los sectores donde la niñez, los adultos mayores y las personas con discapacidad se encuentran en situaciones desfavorables. Impulsan económicamente a familias en situación de pobreza, así como generan las situaciones favorables para superarla. Las poblaciones que se encuentran en riesgos o contingencias son otros sectores donde el Ministerio brinda su ayuda y de manera urgente.

La matriz del Ministerio de Inclusión Económica y Social es el lugar de concentración tecnológica de varias entidades afines y subrogadas que prestan sus servicios a varios lugares geográficos dentro del país. Este despliegue permite que las políticas impulsadas por el Ministerio se cumplan de una manera más eficiente y uniforme. Por ello, las tecnologías de la información tienen un papel fundamental y su óptima operación garantiza que los servicios prestados a la ciudadanía sean efectivos y oportunos.

Este proyecto tiene como propósito realizar el rediseño de la red de dato de la matriz del Ministerio de Inclusión Económica y Social. El análisis de su situación y las acciones correctivas que permitan corregir sus fallas, asegurar la continuidad de sus servicios y mejorar su eficiencia en pro de modernizar y permitir la convergencia de sus servicios y aplicaciones son los contenidos que se pretende abarcar en el presente proyecto de titulación.

Las instalaciones físicas de la matriz de MIES han alcanzado su límite, por lo que su proyección a futuro no se enfoca en el crecimiento de la institución, sino en la mejora del servicio para poder enlazarse a otras entidades y a modernizar su funcionamiento constantemente, por lo que es importante asegurar una adecuada infraestructura de red y un funcionamiento continuo que no degrade el servicio a la comunidad.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1. CONCEPTO DE REDES DE COMUNICACIÓN

Una red de comunicación es un conjunto o grupo de equipos conformados por hardware y software, conectados entre sí por dispositivos físicos que se comunican entre ellos por medios de transporte: guiados (alámbricos) o no guiados (inalámbricos), para compartir información, recursos o brindar servicios.

Una red de comunicación debe cumplir con las siguientes características:

- Integridad. La información se debe mantener a lo largo de los medios de información y solo puede ser modificada por la o las personas autorizadas y de una manera controlada.
- Confidencialidad. La información solo debe ser visualizada por personal autorizado y se la debe proteger de terceros.
- Disponibilidad. La información siempre debe estar disponible para la o las personas que lo necesiten.
- Confiabilidad. La información viaja por medio de nodos interconectados entre sí de tal manera que llegue hacia su destino. La probabilidad de que un nodo falle o no permita la entrega de la información oportuna mide la confiabilidad de una red de comunicaciones.
- Autenticación. Proceso mediante el cual una entidad demuestra su identidad frente a un sistema o frente a otra entidad por medio de sus credenciales.
- Calidad de Servicio. Capacidad de un elemento, dispositivo o software que permita controlar la utilización de los recursos de la red para priorizar el tráfico y brindar un servicio aceptable al usuario final.

Una de las principales características de una red de información es la velocidad a la que opera, tanto de la información que se transmite como de la información recibida.

1.1.1. ELEMENTOS DE UNA RED DE COMUNICACIÓN

Una red de comunicación consta tanto de hardware como de software para su funcionamiento. Entre los principales elementos que se necesitan para una red de comunicación se encuentran los siguientes:

1.1.1.1. Dispositivos que intervienen en una red

Un dispositivo de red es todo aquel equipo que se conecta a un segmento de red. Los dispositivos que interviene en una red se pueden clasificar en dos grupos: dispositivos intermedios y dispositivos finales.

Los *dispositivos finales* son utilizados directamente por los usuarios, entre los cuales se puede mencionar a los siguientes: computadoras, escáneres, impresoras, fax, cámaras de seguridad, dispositivos móviles de mano, etc.

Los *dispositivos intermedios* son los encargados de proporcionar conectividad entre las redes, transportar la información por diferentes medios hasta llegar hacia su destino final.

Entre los dispositivos intermedios de red más importantes tenemos los siguientes:

1.1.1.1.1. Switch

El switch nace de la necesidad de realizar la interconexión de equipos dentro de una misma red sin la necesidad de enviar la información hacia todos sus puertos, en otras palabras el switch o conmutador es un dispositivo electrónico responsable de direccionar y asegurar que la comunicación se realice y llegue al destino indicado dentro de su misma red.

Un switch tiene la capacidad de almacenar direcciones MAC[1] dentro de una red determinada (direcciones de Capa 2), permitiendo la comunicación entre dispositivos, ya que la conmutación se realiza entre los puertos cuyas direcciones MAC de origen y destino se encuentren en la cabecera de la trama.

El switch es un equipo que se lo utiliza para realizar múltiples conexiones de red, además tiene la función de filtro, mejora el rendimiento de la red y además

[1] Dirección MAC, (Control de Acceso al Medio) identifica físicamente a una tarjeta o interfaz de red, conformada por 48 bits, diseñada para ser un identificador global único

garantiza que la información tanto enviada como recibida esté correctamente dirigida a su destino.

Los switches tienen la capacidad de realizar lo que se conoce como encapsulamiento, este puede entenderse como el proceso mediante el cual los datos se empaquetan con información de protocolos que son necesarias antes de que comience el tránsito por la red.

De esta manera cada vez que los datos pasan a través de las capas del modelo OSI[2], reciben información adicional como por ejemplo encabezado y *trailer*.

Los encabezados y los trailers tienen información de control para dispositivos de red y dispositivos finales, para que se realice una apropiada entrega de los datos y el destinatario interprete correctamente la información.

1.1.1.1.2. Router

Es un dispositivo que permite la comunicación de datos entre computadoras desde una LAN hacia otras LANs que se encuentran en otro segmento de red[3]. El router permite dirigir o encaminar los paquetes de datos a su respectivo destino.

Entre las principales funciones de un router están: recibir paquetes, procesarlos en función de su encapsulamiento y encaminar los paquetes por sus diferentes interfaces.

Los componentes de memoria básicos de un enrutador son los siguientes:

ROM: contienen parte o todo el sistema operativo (IOS) del router. Como el IOS se encuentra en la ROM se puede recuperar en caso de borrado de la memoria flash.

NVRAM: contiene el archivo de configuración de la RAM. La NVRAM mantiene la información incluso si se interrumpe la corriente en el router.

---

[2] Modelo OSI, modelo de referencia conformado por 7 capas creado por la ISO (Organización Internacional de Normalización), que divide el proceso de transmisión de la información en casa una de las capas que lo conforman.

[3] Segmento de red, conjunto de direcciones IP que pueden comunicarse entre sí sin la necesidad de utilizar un equipo que haga las funciones de enrutamiento (capa 3).

Flash RAM: es un tipo especial de memoria ROM, se utiliza para almacenar el IOS que se ejecutan en el router y se puede almacenar versiones alternativas del IOS.
RAM: proporciona almacenamiento temporal de la configuración, tiene información como la tabla de encaminamiento que esté utilizando. La RAM almacena la configuración del router que se está ejecutando.
INTERFACES: para la conexión del router con el exterior:

- *Interfaces LAN:* puertos para conexiones con redes de área local.
- *Interfaces WAN:* puertos para conexiones con redes WAN.
- *Puertos de consola:* puertos que se utilizan para ingresar a la configuración del equipo vía CLI (Interfaz de Línea de Comandos).

1.1.1.1.3. Servidor

El servidor u ordenador es un equipo especializado con altas capacidades de procesamiento, que provee diferentes servicios tanto a clientes finales como a otros equipos especializados o servidores.

Los servidores pueden ser montados tanto sobre *appliances* especializados o sobre equipos o computadoras con mejoras en sus características tanto de procesamiento como de memoria RAM, dependiendo de la carga y servicios que estos pueden ofrecer.

Una de las principales características de los servidores especializados o appliances es que permiten resolver ciertos fallos de manera automática, además poseen sistemas de alarmas en caso de fallos de operación de datos críticos, ya que depende de estos equipos el correcto funcionamiento de los servicios de las empresas.

Entre los servidores más comunes que posee una red se pueden encontrar los siguientes:

- Servidor de DHCP (Dynamic Host Control Protocol): servicio que permite la administración de las direcciones IPs en una organización o empresa, facilitando la entrega del direccionamiento a los diferentes equipos dentro de su red de manera automática.

- Servidor WEB: servicio que permite almacenar información que se basa en diferentes lenguajes de programación como: PHP, HTML, etc.; para ser publicados en el Internet o la intranet y los usuarios los puede visualizar mediante la utilización de los diferentes exploradores de Internet.
- Servidor de Base de Datos: es utilizado para almacenar, recuperar, administrar y gestionar la información que es utilizada por una organización. El servidor permite gestionar el acceso simultáneo de servidores o usuarios garantizando la integridad y seguridad de los datos que posee.
- Servidor de correo: servicio que permite el envío y recepción de correo electrónico tanto interno como externo a una organización, mediante la utilización de los protocolos: SMTP (Protocolo simple de transferencia de correo) y POP (Protocolo de oficina de correos).
- Servidor de DNS (Servicio de Nombre de Dominio): servicio que permite que los usuarios utilicen nombres en lugar de direcciones IP para identificar a diferentes hosts tanto dentro como fuera de su red.

1.1.1.1.4. Firewall

Elemento de la red indispensable que permite la protección a una o varias redes de computadoras de intrusos o hackers que provienen de redes externas con la intención de capturar información interna de la red.

El firewall es un sistema o software perimetral que permite filtrar o bloquear los paquetes tanto de entrada como de salida de la red para evitar ataques tanto internos como externos a las principales aplicaciones o información de una organización, mediante el uso de reglas dentro de la política de seguridad de la organización.

1.1.2. CLASIFICACIÓN DE LAS REDES DE COMUNICACIÓN POR ALCANCE

1.1.2.1. Red de área personal (PAN)

Es una red que permite la comunicación entre dispositivos que se encuentran en un entorno personal de los usuarios, a cortas distancias (menores a 10 metros), entre los principales dispositivos podemos encontrar los siguientes: PDAs,

computadoras portátiles, impresoras, auriculares inalámbricos, cámaras digitales, teléfonos celulares, etc.

Las PAN pueden tener una capacidad en el rango de 1 Mbps hasta los 10 Mbps[4]. La principal tecnología PAN (Bluetooth) opera en la frecuencia de 2.4 GHz.

Entre las principales características de las PAN se puede mencionar las siguientes:

- Facilidad en la conexión y configuración de la red.
- Movilidad en un rango corto de conexión.
- En la mayoría de casos no se necesita una conexión cableada.

Figura 1.1. Red de Área Personal[5]

1.1.2.2. Red de área local (LAN)

Las redes de área local permiten la conexión de dispositivos en un área generalmente limitada a un piso o un edificio.

La distancia que cubre una LAN se encuentra estimada a un máximo de 1 KM.

Los medios de transmisión que generalmente utiliza pueden ser: cable UTP, cable coaxial o fibra óptica; lo cual permite una reducción considerable en la tasa de errores en la transmisión y permite también la transmisión a altas velocidades.

Las Redes de Área Local permiten compartir bases de datos, programas y periféricos, permiten la administración y gestión de los equipos centralizadamente.

---

[4] Información obtenida de: https://es.scribd.com/doc/53055243/REDES-PAN
[5] Figura obtenida de: http://grantipoderedes.blogspot.com/

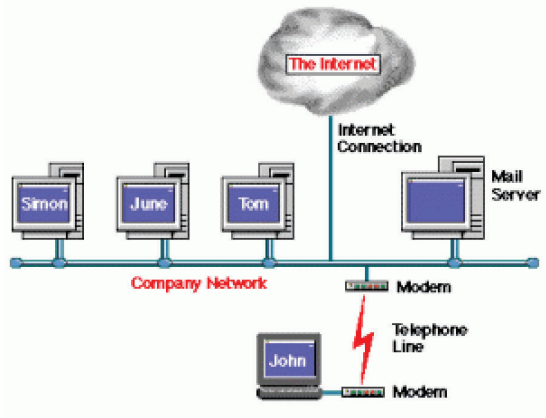

Figura 1.2. Red de Área Local[6]

1.1.2.3. Red de área metropolitana (MAN)

Representan la evolución del concepto de las LAN a un ámbito más amplio, comprende un área geográfica más extensa que una LAN y gracias a su alta capacidad de velocidad proporciona la posibilidad de integración de múltiples servicios sobre medios de transmisión tales como fibra óptica, par trenzado y medios inalámbricos.

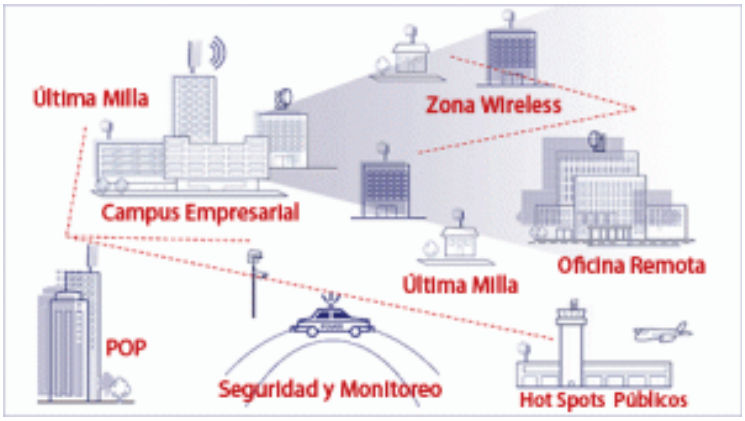

Figura 1.3. Red de Área Metropolitana[7]

Las redes de área metropolitana permiten realizar, por ejemplo, la interconexión de redes de área local, permitiendo alcanzar coberturas de redes que se encuentran en un diámetro de 50 km que va a depender del alcance que se tiene en los nodos de la red y el tipo de cableado que se utiliza para su interconexión.

[6] Figura tomada de: https://redesadsi.wordpress.com/clasificacion-de-las-redes/
[7] Figura tomada de: https://redesadsi.wordpress.com/clasificacion-de-las-redes/

Las redes de área metropolitana permiten superar los 500 nodos de acceso a la red, por lo que se hace muy eficaz para entornos públicos y privados con un gran número de puestos de trabajo.

Una de las principales ventajas de trabajar con redes de área metropolitana es que poseen mecanismos automáticos de recuperación frente a fallos, si se presenta un fallo en un nodo es rápidamente detectado y aislado, en el caso del cable de cobre se utiliza la tecnología bonding EFM, la cual "*permite la agregación de caudal en múltiples cables, el bonding EFM permite a la red recuperar la operación normal, ante la rotura de uno de los cables, cualquier fallo en un nodo de acceso o cable es detectado rápidamente y aislado*"[8].

1.1.2.4. Red de área extensa (WAN)

Son redes que cubren áreas geográficas extensas y la función principal es la interconexión de redes que se encuentran ubicadas en diferentes lugares geográficos distantes, los enlaces que utilizan las WAN para comunicarse con las diferentes redes atraviesan redes públicas y privadas, pudiendo ser redes propias o alquiladas.

Las WAN pueden transportar tanto tráfico de voz, datos y video. La WAN por lo general trabajan en las tres primeras capas del modelo OSI: Capa Física, Capa Enlace de Datos, Capa Red. La velocidad a la que trabajan es mucho menor a la velocidad de una LAN, ya que deben transportar gran cantidad de información.

Por lo general una WAN puede utilizar enlaces satelitales para la transmisión de la información por lo que se convierte en una red con alto porcentaje de pérdidas de datos, además se puede encontrar elementos que encaminen los datos (enrutadores), ya que deben pasar por una gran cantidad de subredes hasta alcanzar su destino final.

La movilidad que permite este tipo de redes es una de las principales características que tiene ya que los usuarios pueden acceder a la información de la organización desde cualquier lugar.

---

[8] Información obtenida de: http://repositorio.utc.edu.ec/bitstream/27000/1311/1/T-UTC-0904.pdf

1.1.3. TECNOLOGÍAS WAN [F2]

Para realizar la conmutación entre los diferentes nodos por donde circula la información hasta que llegue a su destino se pueden utilizar técnicas de conmutación entre las cuales tenemos: conmutación de paquetes, conmutación de circuitos y conmutación de mensajes.

1.1.3.1. Conmutación de circuitos

Tipo de conmutación en la cual se utiliza un canal dedicado, una vez terminada la comunicación se libera el canal, además de que se necesitan los siguientes pasos:

1. Establecimiento del circuito: el emisor solicita un nodo para establecer la conexión al receptor por medio de un canal dedicado, además dicho nodo encaminará la información hacia el destino.
2. Transferencia de información: una vez que se encuentra establecido el circuito por el canal dedicado, el emisor empieza la transmisión de datos hacia el receptor.
3. Desconexión del circuito: al momento de terminar la transmisión y recepción de datos se indica a los nodos que ha finalizado la conexión para liberar el canal dedicado.

1.1.3.2. Conmutación de paquetes

La conmutación se basa principalmente en ensamblar paquetes antes de transmitir la información, dichos paquetes son divididos y enviados individualmente por medio de diferentes rutas hacia su destino. Una vez que llegan a su destino los paquetes son re-ensamblados.

1.1.3.3. Conmutación de mensajes

Conmutación pensada en mejorar la conmutación de circuitos, la conmutación de mensajes pasa de un nodo hacia otro liberando la ruta antes utilizada para alcanzar el nodo, el camino es utilizado por diferentes mensajes simultáneamente,

pero los nodos necesitan de capacidades elevadas de memoria para almacenar los mensajes por lo que este tipo de conmutación no es muy utilizado.

1.2. TOPOLOGÍAS LAN [F1] [PW5]

La topología de red es la representación o la forma en la que los elementos de la red se encuentran conectados tanto de forma lógica como física.

Las topologías más usadas son las siguientes:

1.2.1. TOPOLOGÍAS FÍSICAS

Forma física que forman los nodos que se encuentran conectados a la red, entre las topologías físicas tenemos:

- Topología tipo bus: Todos los hosts se conectan directamente a un backbone.
- Topología tipo anillo: cada host se conecta de forma consecutiva con el siguiente y el último host con el primero.
- Topología tipo estrella: se conectan todos los host con un punto central de la red.
- Topología tipo malla: topología implementada para proveer una mayor protección y evitar una interrupción del servicio.

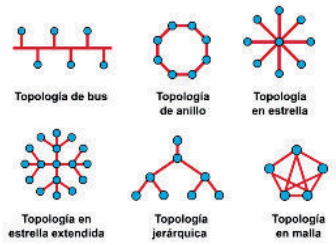

Figura 1.4. Topologías Físicas[9]

1.2.2. TOPOLOGÍAS LÓGICAS

La topología lógica es la forma o la manera en que la información es transmitida de un nodo al siguiente, la capa de enlace de datos es la encargada de controlar el acceso de los datos al medio.

[9] Figura tomada de: http://iraniiaavendano.blogspot.com/2015/05/tipologia-de-redes.html

1.3. MODELO OSI[10]

Es un modelo de red que ayuda tanto a los diseñadores de red como a los ingenieros a implementar redes que puedan comunicarse y trabajar en conjunto.

El concepto de capas permite comprender el proceso de comunicación desde que sale la información desde un host hasta que llega a su destino.

1.3.1. CAPA 7: LA CAPA APLICACIÓN

La capa aplicación suministra la interfaz y los servicios que utiliza el usuario final, entre los servicios que provee la capa aplicación al usuario se encuentran los siguientes: la Web, servicios de correo electrónico, aplicaciones de bases de datos (cliente servidor).

1.3.2. CAPA 6: LA CAPA PRESENTACIÓN

La capa presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. La capa de presentación traduce entre varios formatos a un formato común.

1.3.3. CAPA 5: LA CAPA DE SESIÓN

La capa de sesión establece mantiene y finaliza las sesiones entre dos hosts que se están comunicando.

La capa de sesión proporciona sus servicios a la capa de presentación y sincroniza la comunicación entre las capas de presentación de los hosts y administra su intercambio de datos. Permite una eficiente transferencia de datos de la capa de sesión, presentación y aplicación.

1.3.4. CAPA 4: LA CAPA DE TRANSPORTE

La capa de transporte segmenta los datos originados en el emisor y los reensambla dentro del sistema del host receptor. La capa de transporte establece, y libera adecuadamente las conexiones en. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

---

[10] Información obtenida de: http://www.info ab.uclm.es/labelec/Solar/Comunicacion/Redes/index_files/Modelos.htm

1.3.5. CAPA 3: LA CAPA DE RED

La capa de red proporciona conectividad y selección de la ruta entre dos sistemas que están ubicados en redes geográficamente distintas.

1.3.6. CAPA 2: LA CAPA DE ENLACE DE DATOS

La capa de enlace de datos proporciona el tránsito de datos confiable a través de un enlace físico. La capa de enlace de datos se ocupa del direccionamiento físico, la topología física de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

1.3.7. CAPA 1: LA CAPA FÍSICA

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales. Define características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos, etc.

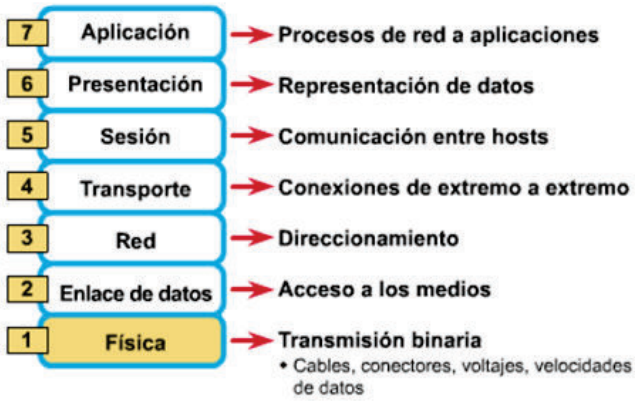

Figura 1.5. Modelo OSI[11]

1.4. CABLEADO ESTRUCTURADO [L1]

El diseño e implementación del cableado estructurado se realiza en base a normas establecidas con el fin de instalar una infraestructura de telecomunicaciones dentro de una edificación, permitiendo la interconexión de dispositivos de comunicación con flexibilidad, independencia de fabricantes y

[11] Figura tomada de: http://www.infoab.uclm.es/labelec/Solar/Comunicacion/Redes/index_files/Modelos.htm

compatibilidad de tecnologías, capacidad de crecimiento y facilidad de administración. Dichas normas consisten en una recopilación ordenada de guías técnicas para la instalación de cableado en los distintos tipos de edificación en la cual se desea implementarse así como publicaciones para la manufactura de los componentes de sistemas de cableado debidamente reconocidos y estandarizados.

Las normas son complementarias en cuanto se refieren a características, componentes, diseño, implementación, administración y varios aspectos relacionados. Para el cableado orientado a edificios comerciales y ambientes de oficina se consideran las siguientes normas:

El estándar que abarca los aspectos relacionados a la instalación del sistema de cableado estructurado, elementos que lo conforman y características relacionadas a los requisitos mínimos se encuentran especificados en las normas TIA/EIA 568-C.

Los aspectos relacionados al diseño y la construcción de espacios y rutas de telecomunicaciones dentro de edificios comerciales se contemplan en las normas TIA/EIA 569-A.

Los aspectos relacionados a la administración para la infraestructura de telecomunicaciones se contemplan en las normas TIA/EIA 606-A.

Los aspectos relacionados al aterrizamiento (conexión a tierra) de telecomunicaciones se contemplan en la norma TIA/EIA 607.

1.4.1. ESTÁNDAR TIA/EIA 568 C

Constituye un grupo de estándares para cableado de telecomunicaciones en edificios comerciales, en el cual se consideran las normas TIA/EIA 568-B.1, TIA/EIA 568-B.2, TIA/EIA 568-B.3 y otros adendas relacionados a la norma previa, conocida como TIA/EIA 568-B.

El alcance de las normas permite garantizar un correcto funcionamiento de la infraestructura de telecomunicaciones por un lapso de al menos 15 años para los edificios comerciales. Esto se debe a que las tecnologías de la red tienden a exigir

un mejor desempeño del cableado a un ritmo relativamente corto por los continuos cambios y mejoras en sus servicios.

Bajo esta perspectiva, las normativas permiten garantizar que el diseño del cableado estructurado se mantenga al margen de las aplicaciones y servicios que utilizan la red. Además, se especifican otros aspectos como parámetros de rendimiento y desempeño, distancias recomendadas, guías para la instalación y descripción de los elementos de los subsistemas de cableado estructurado.

Las especificaciones que comprende el estándar se divide en los siguientes grupos:

1.4.1.1. TIA/EIA 568-C.0

Comprende los parámetros de planificación para la implementación de sistemas de cableado estructurado relacionados a todo tipo de edificios. Con esto se consigue que las especificaciones se ajusten a entornos de varios protocolos o plataformas.

1.4.1.2. TIA/EIA 568-C.1

Comprende la información relacionada a la planificación, implementación y verificación del sistema de cableado estructurado para edificios comerciales, además incluye parámetros adicionales como nomenclatura relacionada a los subsistemas de cableado. Estas recomendaciones son aplicables tanto a edificios comerciales y residenciales.

1.4.1.3. TIA/EIA 568-C.2

Comprende información acerca de requerimientos técnicos de los cables de pares trenzados balanceados, respecto a sus partes y parámetros específicos.

1.4.1.4. TIA/EIA 568-C.3

Comprende especificaciones de componentes de fibra óptica, relativo a parámetros físicos, eléctricos y de compatibilidad.

1.4.2. COMPONENTES DEL CABLEADO ESTRUCTURADO [F3]

En la figura 1.6 se puede verificar un esquema que contiene los componentes principales dentro del sistema de cableado estructurado. La nomenclatura usarse es la siguiente:

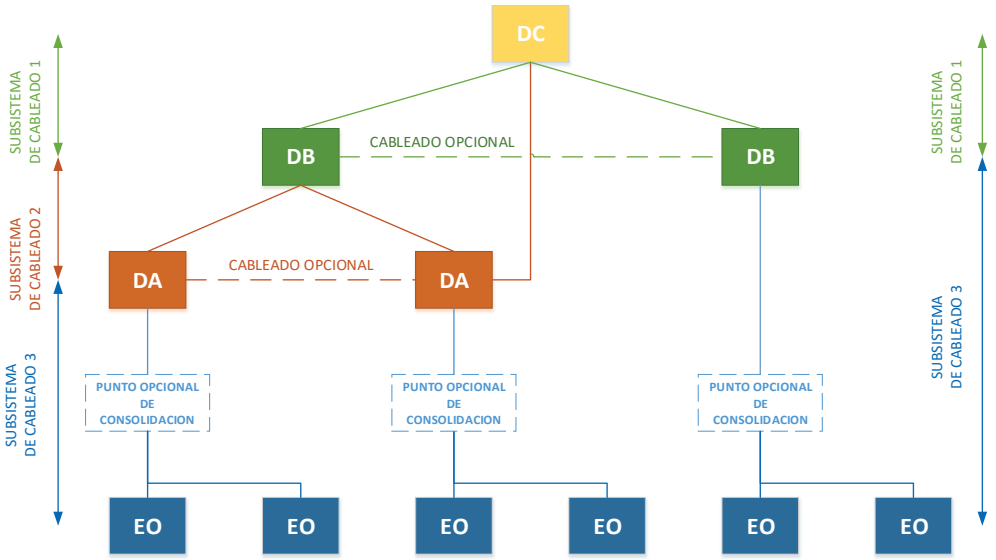

Figura 1.6. Principales componentes de Cableado[12]

- EO: equipment outlet (salida hacia los equipos o áreas de trabajo)
- DA: distribuidor A
- DB: distribuidor B
- DC: distribuidor C

1.4.2.1. Subsistema de cableado 1

Comprende el tramo que une los puntos que van desde el distribuidor A hasta las áreas de trabajo. Esto equivaldría al segmento de cableado que une el cuarto de telecomunicaciones hasta las áreas de trabajo en el mismo piso.

1.4.2.2. Subsistema de cableado 2

Comprende el segmento de cableado que une al distribuidor A con el distribuidor B (segundo nivel de distribución).

[12] Figura tomada de:
http://www.fing.edu.uy/iie/ense/asign/ccu/material/docs/Cableado%20Estructurado%202009.pdf/

1.4.2.3. Subsistema de cableado 3

Comprende el segmento de cableado que va desde el distribuidor B de hasta el distribuidor C (distribuidor principal del edificio).

El distribuidor A es el primer nivel de distribución que se conecta directamente a las áreas de trabajo, mientras que distribuidor B es un conector que actúa como intermediario entre distribuidor A y distribuidor C. Cuando no existe distribuidor A, las áreas de trabajo se conectan directamente al distribuidor B. El distribuidor C es siempre el distribuidor principal en el edificio. Finalmente la salida hacia los equipos (o áreas de trabajo) son el punto final de cableado, los equipos activos no se incluyen en este componente.

1.4.3. TIA/EIA 658-C.1

En este estándar se tienen los mismos criterios contenidos en TIA-568B.1[13] en lo que refiere a la estructura y cobertura. Se han añadido recomendaciones respecto a la fibra multimodo para láser de 50 µm y 850 nm, además se incluyen recomendaciones para armarios de telecomunicaciones. La distancia máxima que se especifica en estas normas es de 100 m, al margen del medio de transmisión usado.

Adicional a todo esto, se pueden resaltar las siguientes consideraciones:

- Se reconoce la categoría 6a como medio de transmisión.
- En el caso de utilizar fibra óptica multimodo el backbone del cableado estructurado, se recomienda el uso de láser optimizado de 850 nm.
- Se ha eliminado de la lista de medios de transmisión reconocidos los cables UTP categoría 5, el cable STP de 150 ohmios y el cable coaxial de 50 y 75 ohmios.

Los componentes funcionales definidos por el estándar son los siguientes:

- Instalaciones de entradas (o acometida)
- Distribuidor principal y secundarios (Cross-Connect principal y secundarios)

[13] TIA-568B.1, Norma especificada para edificios comerciales, recomendación para diseñar el cableado estructurado en estrella y se define una nueva nomenclatura en los diferentes subsistemas de cableado estructurado.

- Distribución central de cableado (Backbone)
- Distribuidores o repartidores horizontales (Cross-Connect horizontal)
- Distribución horizontal de cableado
- Áreas de trabajo

La relación entre los componentes genéricos de la norma 568-C.0 y 568-C.1 se describe en la tabla 1.1:

Nomenclatura 568-C.0	Nomenclatura 568-C.1
Distribuidor C	Distribuidor principal *Main Crossconnect (MC)*
Distribuidor B	Distribuidor secundario *Intermediate Crossconnect (IC)*
Distribuidor A	Distribuidor horizontal Horizontal Crossconnect (HC)
Salida hacia los equipos(Equipment outlet)	Área de trabajo *Telecommunication Outlet*
Subsistema de cableado 3	Backbone externo I*nterbuilding Backbone Cabling*
Subsistema de cableado2	Backbone interno Intrabuilding Backbone Cabling
Subsistema de cableado 1	Cableado horizontal *Horizontal Cabling*

Tabla 1.1. Relación de nomenclatura entre normas 568-C.0 y 568-C.1

1.4.3.1. Acometida

En esta categoría se define la instalación de entrada, siendo el punto en el que ingresan los servicios de telecomunicaciones al edificio. Los servicios de telecomunicaciones ingresan a este lugar donde se puede encontrar equipos activos.

Este lugar se conoce como punto de demarcación, y en el caso de no existir los prestadores del servicio pueden usar el cuarto de equipos para colocar sus equipos.

1.4.3.2. Distribuidor o repartidor principal y secundarios (*Cross-Connect* principal y secundarios)

El distribuidor principal y secundario, constituye una estructura jerárquica en estrella de no más de dos niveles en la que se interconecta el cuarto de equipos con los cuartos de telecomunicaciones. Esta jerarquía permite brindar suficiente flexibilidad al backbone.

El distribuidor principal, se encuentra comúnmente en el cuarto de equipos, y es el encargado de conectar los servidores con el backbone. De esta manera se brinda el servicio a las áreas de trabajo, atravesando los cuartos de telecomunicaciones y en algunos casos los distribuidores secundarios.

En la siguiente figura (Fig. 1.7) se puede verificar de mejor manera la estructura de la jerarquía de los distribuidores mencionados.

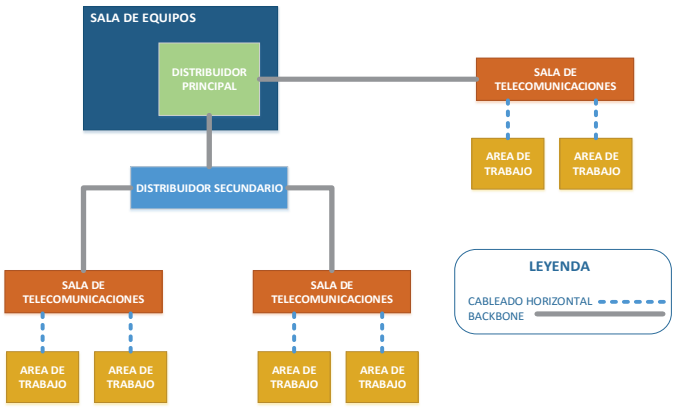

Figura 1.7. Conexiones de Cableado Estructurado[14]

1.4.3.3. Distribución central de cableado (*Backbone*)

El backbone, tiene como objeto proveer la interconexión entre el cuarto de equipos y los armarios de telecomunicaciones, así como las instalaciones de entrada y el cuarto de equipos. A través de este atraviesa la gran parte del tráfico de la red. Los componentes del cableado del backbone con son: medio de transmisión, repartidores principales y secundarios, terminaciones mecánicas y cables de enlace (*jumpers*).

[14] Figura tomada de:
http://www.fing.edu.uy/iie/ense/asign/ccu/material/docs/Cableado%20Estructurado%202009.pdf

Durante el diseño del cableado de backbone, se deben satisfacer las necesidades inmediatas, así como se debe prever necesidades futuras reservando los elementos necesarios para cubrir un posible incremento en la demanda. Además se debe seguir el sistema de estrella jerárquica limitando a 2 puntos de interconexión desde el cuarto de equipos al armario de telecomunicaciones.

Para este estándar se definen los siguientes medios de transmisión para backbone.

- Cable UTP de 100 ohm (sin malla)
- Fibra óptica multimodo de 50/125 µm
- Fibra óptica multimodo de 62.5/125 µm
- Fibra óptica monomodo
- Cable STP-A de 150 ohm (con malla)

1.4.3.4. Distribuidores o repartidores horizontales (*Cross-Connect* horizontal)

La función de los repartidores horizontales es la de interconectar el cableado que se extiende hacia las áreas de trabajo horizontal con el cableado que proviene del cuarto de equipos (backbone). Normalmente los repartidores horizontales constan de paneles de interconexión donde terminan los cableados horizontales y los cableados verticales (backbone). A través de cables de interconexión se conectan los puntos de terminación de cualquier cableado horizontal con cualquiera del cableado de backbone y/o equipo activo intermedio que permita la interconexión de estos. Cualquier equipo activo que se acople a los repartidores horizontales no conforma parte del cableado.

Los componentes que conforman los repartidores horizontales tanto en los paneles (*patch panels*) como los cables de interconexión (*patch cords*) deben cumplir con las características mecánicas y eléctricas de la categoría del resto del sistema de cableado estructurado.

Al disponer de equipos activos como hubs o switches en el cuarto de telecomunicaciones se permite que los paneles del cableado horizontal que van hacia las estaciones de trabajo se conecten directamente a los equipos activos por medio de cables de interconexión (patch cords) adecuados.

1.4.3.5. Distribución horizontal de cableado

Corresponde al segmento de cableado que interconecta las áreas de trabajo con el armario o cuarto de telecomunicaciones. Los elementos que se incluyen son los cables de distribución horizontal, conectores de telecomunicaciones en área de trabajo, cordones de interconexión (*patch cords*), terminaciones mecánicas y puntos de consolidación (opcionalmente).

La distribución del cableado horizontal sigue una topología de tipo estrella concentro en el armario de telecomunicaciones o cuarto de equipos y con sus extremos en cada una de las áreas de trabajo.

No se admiten empalmes en toda esta trayectoria, excepto en caso de existir un punto de consolidación.

La distancia máxima del cable de distribución horizontal es de 90 m, mientras que los cordones de interconexión tanto en el área de trabajo como en armario de telecomunicaciones no deben superar 10 m. Es decir que el conjunto entero de punta a punta debe tener una distancia máxima de 100 m. Los cables reconocidos en este tipo de distribución son:

- UTP o ScTP de 100 y cuatro pares
- Fibra óptica multimodo de 50/125 µm
- Fibra óptica multimodo de 62.5/125 µm

1.4.3.6. Área de trabajo

Comprende la sección donde se encuentran los conectores de telecomunicaciones y los cables de interconexión (*patch cord*) que van a los equipos del usuario. Los equipos del usuario pueden ser computadores, impresoras, etc. pero no son parte de esta sección. La recomendación del estándar es de que el cable de interconexión no supere los 5 metros.

El estándar establece equipar con 2 salidas de telecomunicaciones en cada área de trabajo. Esta previsión permite asociar comúnmente un punto para servicios de voz y un punto para servicios de datos, lo cual puede variar basándose en las necesidades del diseño. Aunque se puede elegir entre cables UTP de 100 ohms y

fibra óptica multimodo para estos puntos, es muy común el uso de cables UTP de 100 ohms con la misma categoría del resto del sistema de cableado.

La distancia máxima del cableado horizontal es de 90 metros por lo que la suma de los cables de conexión podría tener como máximo una distancia de 10 metros para sumar la distancia máxima de 100 metros.

Las recomendaciones del estándar establecen que los patch cords ubicados en el área de trabajo tengan 3 metros de longitud para cumplir con las distancias mencionadas, sin embargo pueden tener una distancia máxima de 20 metros siempre y cuando la suma de las distancias de los cables de conexión y del cableado horizontal no sobrepase los 100 metros.

Se establece que por cada área de trabajo se dispongan dos cables (puntos de red), sin embargo se deben evaluar las necesidades futuras para optar por instalar uno o más puntos adicionales.

1.4.4. CANALIZACIÓN [PW3]

La canalización será la encargada de encaminar el cableado y su área transversal dependerá del número de cables que se van a colocar. Como parte del diseño se debe dejar un espacio adecuado para nuevos cables según sea la proyección del crecimiento de la red. En la siguiente tabla se muestran el número de cables permitidos en la canalización en función de su diámetro:

Diámetro interno de la canalización		Diámetro externo del cable (mm)				
(mm)	Pulgadas	3,3	4,6	5,6	6,1 (CAT6)	7,4 (CAT 6A)
15,8	1/2	1	1	0	0	0
20,9	3/4	6	5	4	3	2
26,6	1	8	8	7	6	3
35,1	1 1/4	16	14	12	10	6
40,9	1 1/2	20	18	16	15	7
52,5	2	30	26	22	20	14
62,7	2 1/2	45	40	36	30	17
77,9	3	70	60	50	40	20

Tabla 1.2. Cables permitidos en función de su diámetro[15]

[15] Tabla tomada de:
http://www.fing.edu.uy/iie/ense/asign/ccu/material/docs/Cableado%20Estructurado%202009.pdf

La canalización interna del backbone permite unir las instalaciones de entrada con el cuarto de equipos, y a éstos con el cuarto o armario de telecomunicaciones.

Los elementos que integran la canalización pueden ser: ductos, bandejas o escalerillas portacables.

Los elementos de la ductería pueden distribuirse de manera vertical u horizontal dependiendo de las necesidades.

1.4.5. TIA/EIA 568 C.2 (COMPONENTES DE CABLEADOS UTP)

En este estándar se hacen especificaciones acerca de las características de los componentes físicos del cableado estructurado.

Se recogen los aspectos mecánicos, eléctricos y de transmisión. Dentro del estándar se reconocen las siguientes categorías de cables:

CATEGORÍA	IMPEDANCIA	ANCHO DE BANDA	OBSERVACIONES
Categoría 5e	100 ohmios	100 MHz	Mejora de parámetros de la Categoría 5
Categoría 6	100 ohmios	250 Mhz	Se especifica parámetros de transmisión hasta 250 MHz
Categoría 6a	100 ohmios	500 MHz	Diseñado para 10 Gigabit Ethernet

Tabla 1.3. Cables UTP reconocidos por el estándar[16]

1.4.6. TIA/EIA 568 C.3

Análogamente al estándar TIA/EIA 568-C.2, este estándar especifica las características de los elementos y parámetros de transmisión para el cableado de fibra óptica, para fibras multimodo de 50/125µm y 62.5/125µm y fibras monomodo.

Según las recomendaciones del estándar TIA/EIA 568-B.3 los cables de fibra óptica deben cumplir con algunos requerimientos tal como se describe en la Tabla 1.4, donde se puede observar la longitud de onda, máxima atenuación por distancia y mínima capacidad de transmisión de información por distancia, en este caso las distancias se miden en kilómetros:

[16] Tabla tomada de:
http://www.fing.edu.uy/iie/ense/asign/ccu/material/docs/Cableado%20Estructurado%202009.pdf

TIPO DE CABLE	Longitud de onda	Máxima atenuación [dB/km]	Mínima capacidad de transmisión de información [MHz·km]
Multimodo de 50/125 µm	850	3,5	500
	1300	1,5	500
Multimodo de 62.5/125 µm	850	3,5	160
	1300	1,5	500
Monomodo de interior	1310	1	N/A
	1550	1	N/A
Monomodo de exterior	1310	0,5	N/A
	1550	0,5	N/A

Tabla 1.4. Requerimientos de fibra óptica aceptados por el estándar[17]

El estándar TIA/EIA 568-C.3 admite el uso de empalmes de fibra óptica, sea por fusión o físicamente, siempre y cuando la pérdida o atenuación en el mismo no supere los 0.3 dB.

1.4.7. SALA DE EQUIPOS

Es el espacio que se destina a los equipos de telecomunicaciones y servidores de la red.

La extensión de la misma se establece en función de algunos parámetros entre los que se incluyen: número de usuarios, métodos de seguridad de los equipos, formas de interconexión, etc.

Durante el diseño del mismo se deben tomar algunas consideraciones como la posibilidad de expansión, la prevención de ubicar los equipos cerca de instalaciones de agua, facilidad de movilización de equipos de tamaño considerable, ubicar el espacio preferentemente cerca de las canalizaciones de backbone, alejado de fuentes de interferencia electromagnética y vibración, buena iluminación, buen suministro eléctrico y una conexión a tierra correctamente realizada.

El control de la temperatura es otro factor importante. Se debe mantener el cuarto entre los 18 y 27 grados centígrados y una humedad relativa entre el 30% y el

[17] Tabla tomada de: http://docplayer.es/3092884-Onss-spa-ons-2-linked-in-with-the-future.html

55%. Debe adecuarse además un sistema de detección y extinción de incendios con productos especializados para equipamiento de red[18].

1.4.8. CUARTO DE TELECOMUNICACIONES

Son los espacios donde se alojan equipos de interconexión, que se encuentran en un punto intermedio entre la sala de equipos y los usuarios finales (transformando las conexiones verticales de backbone en conexiones horizontales), y que por lo general se destinan a un área definida de cobertura. Normalmente se pueden encontrar equipos de red, equipamiento de control, conexiones y terminaciones de cableado.

Las recomendaciones en el diseño de estos espacios indican que debe tratarse de un lugar seguro físicamente, destinado exclusivamente a usarse con este propósito (no compartir con otras áreas ni usarse con otros propósitos). Adicionalmente se establecen otros criterios durante la ubicación del cuarto de telecomunicaciones:

- Se recomienda instalar un cuarto de telecomunicaciones por cada 1000m² de área utilizable.
- La distancia de las canalizaciones desde la sala de telecomunicaciones hacia las áreas de trabajo no debe superar los 90 metros. En caso de que este criterio no se pueda satisfacer será necesario poner otro cuarto de telecomunicaciones en el trayecto.
- Es recomendable ubicar el cuarto de telecomunicaciones en el centro del área a la que se va a dar cobertura con la canalización horizontal con el fin de mantener una adecuada simetría y distribución del cableado.
- El tamaño recomendado para cada uno de los cuartos de telecomunicaciones se establece en la Tabla 1.4 (asumir que cada área de trabajo tiene alrededor de 10m²):

Área utilizable	Tamaño recomendado del cuarto de telecomunicaciones
500 m²	3 m x 2.2 m

[18] Información obtenida de: http://es.slideshare.net/guesta4d883/cuarto-de-telecomunicaciones-1166154

800 m²	3 m x 2.8 m
1.000 m²	3 m x 3.4 m

Tabla 1.5. Tamaño de cuarto de telecomunicaciones en función del área[19]

1.5. SOFTWARE LIBRE [PW17]

Se considera a un software bajo la definición de "Software Libre" cuando éste ofrece al usuario la libertad de: ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Debido al anglicismo "Free Software" de donde proviene la definición, la traducción literal puede malinterpretarse como software gratuito, siendo esto algo no necesariamente cierto porque existe software libre gratuito así como también existe software libre pagado.

Dentro del sentido estricto de la definición, el software libre goza de cuatro libertades fundamentales:

- Libertad 0: El software puede ser ejecutado con cualquier propósito.
- Libertad 1: El software puede ser estudiado en todos sus detalles, y puede ser cambiado para darle un nuevo propósito. Esta libertad implica que el software debe ser distribuido con su respectivo código fuente.
- Libertad 2: Las copias del software pueden ser redistribuidas a terceros.
- Libertad 3: Las versiones modificadas del software pueden ser distribuidas a terceros. Nuevamente, (debido a la libertad 1) el software modificado debe ser redistribuido junto con su respectivo código fuente.

La comunidad de software libre considera que las cuatro libertades fundamentales deben cumplirse para que el software pueda ser considerado libre.

Un método para que las copias de un programa o software en general no tengan restricciones infundadas a futuro consiste en incluir Copyleft.

De esta manera se asegurará que las versiones modificadas (en caso de que existan) sean libres.

La información referente a las definiciones y aproximaciones referentes al software libre se encuentran auspiciados por la Free Software Fundation (FSF), los mismos que comunitariamente apoyan al proyecto GNU (Sistema Operativo

[19] Tabla tomada de: http://es.slideshare.net/vafalungo/cuarto-de-telecomunicaciones-3294524

GNU), en el portal web www.gnu.org. Actualmente el proyecto utiliza como núcleo del sistema operativo GNU a Linux, por lo que se denomina GNU/Linux.

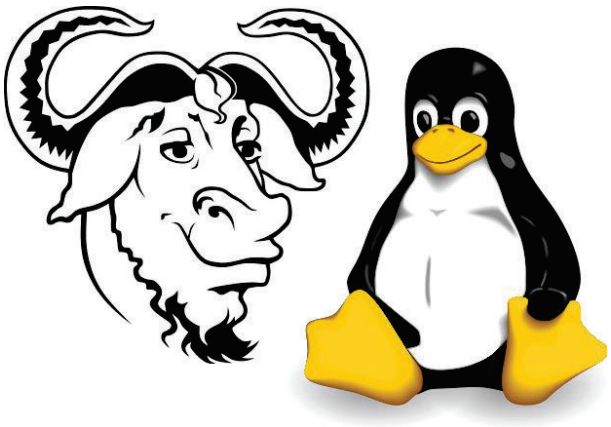

Figura 1.8. Logo de GNU/Linux

1.5.1. TIPOS DE LICENCIAS

La formalización que se le otorga a un software para autorizar su uso o explotación por parte de un autor a un usuario final se define como una licencia (tanto para software privativo o libre), y tiene una calidad de contrato.

Dentro del software libre existen algunas variaciones y versiones, entre las cuales destacan:

1.5.1.1. Licencias GPL.

De las siglas de "Licencia Pública General", consiste en un tipo de licenciamiento en el que el autor conserva sus derechos de autor, y la redistribución como la modificación de su trabajo tendrá que cumplir a cabalidad con la misma licencia, asegurando que las futuras versiones estarán licenciadas.

La licencia GPL aplicada a cualquier código terminará licenciando de la misma manera a cualquier modificación del código original, inclusive si se utiliza un tercer código que contenga otro tipo de licencia. Desde esta perspectiva la GPL es bastante restrictiva y absorbente, por lo que esta práctica no siempre puede llevarse a cabo. Existen códigos que por su naturaleza y origen propietario no pueden añadirse a códigos licenciados bajo GPL, para lo cual se usa otro tipo de licenciamiento. El portal de GNU GPL detalla una lista de licencias en las que

describe si son consideradas compatibles con GPL, y en el caso de que no lo sean, los motivos que la comunidad han encontrado para excluirla del grupo.

1.5.1.2. Licencias BSD (Berkeley Software Distribution)

Son distribuidas junto al software que conforma el sistema operativo BSD (por esta razón el nombre).

El funcionamiento es muy similar al de la licencia GPL, con la diferencia de que el autor se libera de garantías y se atribuye su autoría en trabajos derivados del código original.

Es mucho más permisiva que la GPL, por lo cual ambas son compatibles. El usuario final incluso puede redistribuir el software como software no libre debido a la libertad ilimitada que tiene con esta licencia.

1.5.1.3. Licencias MPL y sus versiones

De las siglas Mozilla Public License, tiene la suficiente flexibilidad de incluir en una sola obra partes de código que tienen GPL con otros que no necesariamente lo tienen, pero en conjunto tendrán en su totalidad o individualmente la licencia MPL y dualmente la licencia GLP.

1.5.2. SOFTWARE LIBRE EN ECUADOR [PW1]

El día 10 de abril de 2008, el Presidente de la República del Ecuador firmó el decreto 1014, en el que se adopta el Software Libre como una política de Estado con el objetivo de ser usado en todas las entidades públicas.

El decreto como tal busca hacer uso en la medida de lo posible software libre, salvo con las siguientes excepciones:

- Que no exista una alternativa al software propietario que pueda ser suplida por software libre.
- Cuando un proyecto informático se encuentre en un punto de no retorno, es decir, el análisis de costo-beneficio de la implementación de software libre o del remplazo de software privativo por software libre demuestre que no es razonable ni conveniente hacerlo.

- Que la implementación de software libre ponga en riesgo la seguridad nacional, entendiéndose ésta como la supervivencia de la colectividad y la defensa del patrimonio nacional.

Se estipula que se haga seguimiento constante a todas las aplicaciones de software privativo con la finalidad de migrar a software libre en la medida de lo posible mediante evaluación.

El artículo 5 del decreto 1014 además establece un orden de preferencia para la adquisición de alguna solución de software libre o privativo:

"Artículo 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica.
b) Locales que permita soberanía tecnológica
c) Regionales donde se tengan acuerdos o convenios
d) Regionales con componente nacional.
e) Regionales bajo supervisiones internacionales.
f) Regionales con acuerdos internacionales.
g) Regionales con proveedores nacionales.
h) Internacionales con componente nacional.
i) Internacionales con proveedores nacionales.

A partir de la publicación del decreto No. 1014, el ente encargado de la elaboración, ejecución de planes, políticas y reglamentos para el uso de software libre en el Gobierno Central está a cargo de la Subsecretaría de Gobierno Electrónico.

Los sistemas de mayor relevancia del Estado ecuatorianos basados en software libre que han sido desarrollados son: el Sistema Nacional de Compras Públicas, el Sistema Nacional de Recursos Humanos y el Sistema de Gestión Documental (este último conocido como "Quipux")[20].

[20] Información obtenida de: http://www.estebanmendieta.com/blog/wp _ content/uploads/Decreto_1014_software_libre_Ecuador.pdf

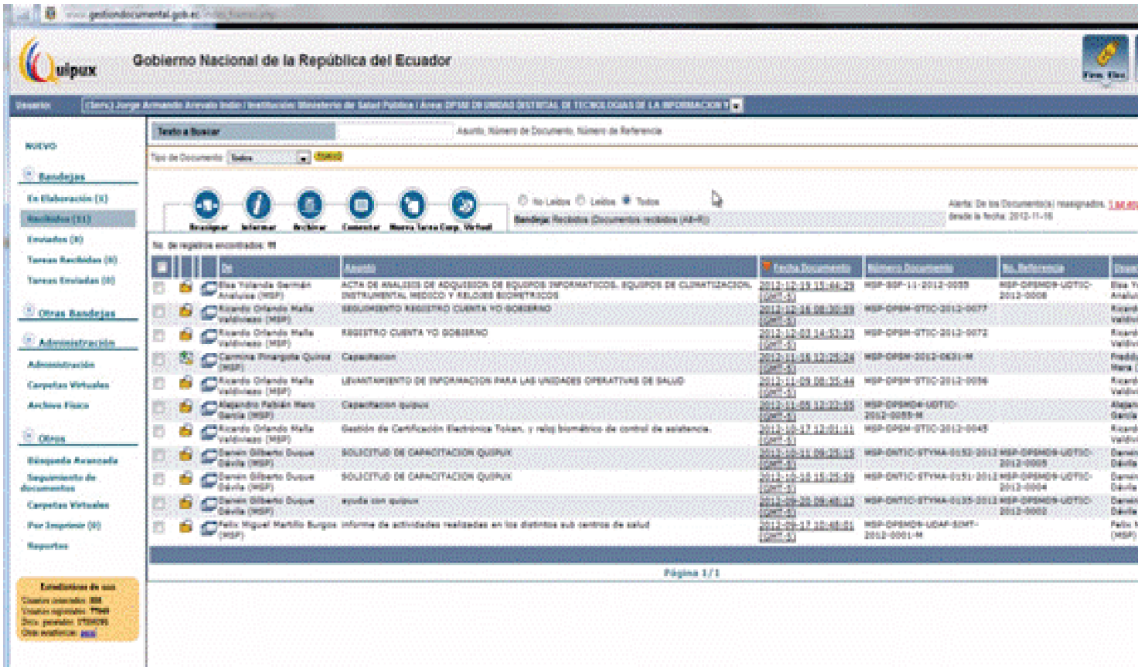

Figura 1.9. Captura de la pantalla principal de un usuario en Quipux[21]

1.6. SEGURIDADES EN LA RED [L3] [PW15]

La seguridad de la red es un conjunto de consideraciones, procedimientos y técnicas que permiten mantener protegidos los recursos y la información perteneciente a la red, de tal manera que se permite mantener el control de lo actuado en la misma.

En este sentido, por la naturaleza de la información y los medios que la soportan, se destacan dos objetivos principales dentro de la institución que implementa seguridad dentro de su red; la seguridad física y la seguridad lógica.

Los esfuerzos destinados a la seguridad de la información en la red se sustentan en las personas que administran la red y de las personas que usan la misma. De los primeros nacen los criterios y las normas que regirán a los segundos.

En definitiva se busca que todo el grupo de personas de la organización cumpla con un buen uso tanto de recursos como de contenidos. Al tratarse de un asunto humano, es posible encontrarse con fallas durante la marcha. Se estima que los problemas de seguridad se deben en un 80% a factores humanos dentro de la

[21] Figura tomada de: http://www.gestiondocumental.gob.ec/

organización (errores, deshonestidad y descuidos) mientras que el 20% restante se debe a ataques o a la integridad física de las instalaciones.

Las medidas que se tomen dentro de la institución en cada caso dependerán de la forma en cómo se maneja el recurso humano y de las buenas prácticas que pueda infundir en conjunto con el personal de TI (Tecnologías de la Información).

1.6.1. SEGURIDAD FÍSICA

La organización debe mantener todos sus sistemas de telecomunicación y servidores en una o varias áreas específicas, con la infraestructura adecuada para el efecto y con la limitación adecuada para que los usuarios no tengan acceso directo a los mismos.

Algunas de las políticas más comunes incluyen:

- El acceso de personal a los datacenters o cuartos de equipos y/o telecomunicaciones debe ser identificado, controlado y vigilado.
- En caso de ingreso de personal interno o externo, debe ser necesaria la presencia de al menos una persona a cargo del área de TI (Tecnologías de la Información), dentro de un horario determinado para el efecto.
- Los ingresos, extracciones o movimientos de equipos de cómputo estarán a cargo del área de TI de la institución o superiores al área, con la respectiva documentación.
- El data center debe tener las instalaciones adecuadas, de tal manera que se pueda favorecer el control de acceso del personal.
- Los sistemas eléctricos deben estar correctamente instalados, junto con un buen sistema de tierra física. Se debe asegurar de igual modo que haya un respaldo eléctrico.
- El Data Center debe mantener una temperatura adecuada, un control de aseo periódico, control de humedad, y el sistema completo de prevención y detección de incendios.

- Será necesario establecer un programa periódico de respaldos, ya sea de forma manual o automática, que se debe cumplir para mantener asegurada la información en caso de algún daño dentro del sistema.
- Los mecanismos para generar respaldos pueden incluir servidores externos como por ejemplo el uso de alguna nube (cloud), sin embargo no se deberán almacenar los datos en cuentas individuales.
- En caso de utilizar discos duros para los respaldos, se recomienda mantener la información encriptada. También se recomienda disponer de un grupo de discos duros y hacerlos rotar en función de la obtención de respaldos. También se aplican a las cintas de respaldo.

1.6.2. SEGURIDAD LÓGICA [L5]

El uso de las redes dentro de la institución facilitan el intercambio y la transformación de la información entre cada uno de los usuarios. En este sentido el usuario final es responsable de cumplir las políticas establecidas por el departamento de TI, lo que comúnmente requiere de un entrenamiento y una capacitación con el objetivo de minimizar los problemas que se puedan dar a futuro.

Algunas recomendaciones comunes dentro de las instituciones son las siguientes:

- El uso de correo electrónico será normado en función de las necesidades de la institución, comúnmente no se permite el uso del mismo para envío masivo, de mensajes personales, o de actividades ajenas.
- Dependiendo de las políticas institucionales, el uso del correo puede estar restringido tanto en horario, como en el uso exclusivo interno de la institución.
- El usuario es responsable de su equipo, por lo tanto, nadie puede hacer uso de la información que se encuentra en el mismo, sin su consentimiento.
- El área de TI no puede hacerse responsable por el contenido ni por el tráfico que circula. Es responsabilidad del usuario final y de la gestión de

los recursos humanos disponer qué tipo de información es generada por cada usuario. Sin embargo, es responsabilidad del área de TI la gestión de equipos que permitan prevenir ataques externos, así como filtrar la información que entra y sale de la red si la política de seguridad se lo permite; en este caso se utiliza el firewall y/o proxy para cumplir con el objetivo.

- Solo el personal de TI tiene la potestad de utilizar programas para el análisis de tráfico dentro de la institución. No se permite que usuarios comunes utilicen herramientas de auditoría de la red o del sistema.
- Será necesario que el personal de TI elabore un plan de contraseñas seguras para cada una de las cuentas que maneje cada usuario dentro de la institución. La forma de transferir esta información al usuario final debe hacerse de manera personal. El usuario debe manejar su contraseña de una manera personal y responsable. Las contraseñas deben generarse con los criterios adecuados para garantizar que sean lo suficientemente robustas.
- Los equipos finales de usuario deben disponer de antivirus.
- Ningún usuario debe instalar programas sin autorización del área de TI, mucho más si se tratan de programas o contenidos que pueden poner en riesgo los equipos.

1.6.3. FIREWALL [PW18]

El firewall es un dispositivo o un software capaz de permitir o negar el tráfico entre varias redes (al menos dos redes). El proceso de permitir o denegar el paso de tráfico también se conoce como filtrado de tráfico. Un firewall puede ser un equipo especializado para trabajar como tal (appliance) o puede trabajar sobre un equipo con varias interfaces y un software especializado que le permita trabajar como firewall.

Para realizar el filtrado de paquetes el firewall debe decidir qué hacer con el mismo. El tráfico se constituye de paquetes provenientes de una arquitectura de red, por ejemplo TCP/IP, en cuyo caso el dispositivo puede discriminar el tipo de

paquete, hacia dónde se dirige y qué tipo de información lleva cuando la información no está encriptada. La decisión de permitir, denegar o alterar el paquete que entra o sale de una red se realiza en base a un conjunto de reglas, las cuales son programadas en base a las políticas de seguridad perimetral de la institución.

Normalmente, una red institucional tiene uno o algunos servidores que deben ser utilizados dentro de su red, pero también deben ser expuestos hacia Internet para que usuarios o clientes puedan también acceder a sus servicios (por ejemplo un portal web o un correo electrónico institucional). Este modelo describe al menos tres segmentos de red que deben ser manejados por el firewall para prevenir y actuar frente a algún ataque; el segmento de red que permite comunicarse hacia Internet (segmento del proveedor), el segmento que contiene a los servidores que estarán expuestos hacia Internet y finalmente el segmento de red que contiene la red de área local. A continuación se detalla en la Figura 1.11 los segmentos de red antes mencionados.

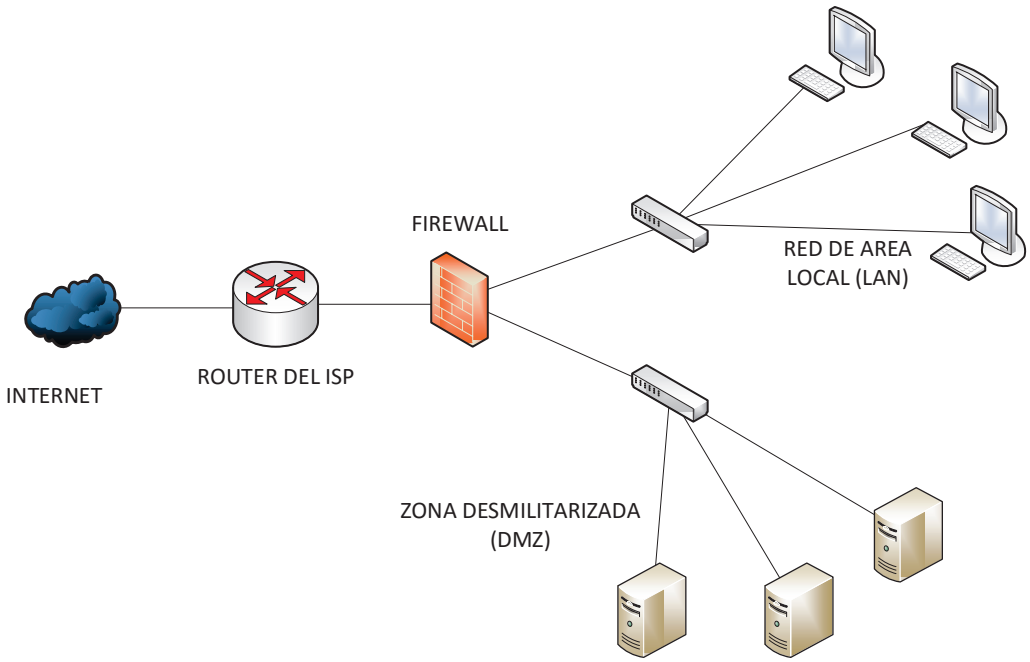

Figura 1.10. Esquema de red con firewall

La red que contiene los servidores expuestos hacia el tráfico de Internet se conoce como zona desmilitarizada o DMZ. Normalmente se ingresa a la DMZ

tanto desde la red interna de la institución así como desde fuera a través de Internet, por lo que el firewall debe tener la capacidad de permitir el paso de peticiones desde cualquiera de las dos redes, con la condición de que el tráfico es permitido exclusivamente para los servicios que ofrecen los servidores y que además sea capaz de denegar o bloquear peticiones anómalas que pueden deberse a ataques y que pueden detener la continuidad del servicio.

Por otro lado la red interna de la institución (LAN) debe estar bloqueada hacia el tráfico proveniente de Internet, mientras que debe permitir la salida de tráfico hacia Internet originado en la LAN, y permitir el paso de la respuesta a dicha petición únicamente. En este segmento se pueden establecer reglas respecto a los contenidos que los usuarios de la red pueden tener acceso y a los que no.

Además el firewall se comporta como un proxy para este segmento; normalmente se utiliza uno o varios puntos de salida a Internet pero siempre en un número muchísimo menor a la cantidad de equipos que se encuentran dentro de la red, entonces el firewall se comporta como un mediador que concentra las peticiones de los equipos de la LAN y los envía hacia Internet, luego las respuestas a dichas peticiones se entregan a cada uno de los equipos en el orden correcto. Para poder hacer esta relación entre paquetes salientes y paquetes entrantes en respuesta a los paquetes salientes el firewall modifica los campos de dirección y puerto a lo que se les llama NAT y PAT respectivamente. De esta manera se economiza la cantidad de puntos y la capacidad del servicio de Internet para la institución y se controla los contenidos a los que debe acceder el usuario en base a las reglas programadas. Además del acceso a Internet también se administra el acceso al segmento de la DMZ desde la red de área local.

1.7. GESTIÓN DE LA RED [L2] [L4] [P1]

El uso de las tecnologías de la información y de las redes de telecomunicaciones ha permitido que exista un constante y notorio crecimiento tanto en cantidad como en complejidad, además de la gran cantidad de fabricantes que fabrican sus propias tecnologías. Por este motivo se requiere de una adecuada gestión de todos los elementos de la red para permitir un funcionamiento adecuado y una planificación acorde al crecimiento que ésta pueda experimentar.

“La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable”[22].

1.7.1. COMPONENTES DE LA GESTIÓN [PW4]

La gestión de la red subyace en tres componentes principales: componente organizacional, componente técnico y componente funcional.

1.7.1.1. Componente Organizacional

El componente organizacional se enfoca en la estructuración propia del proceso de gestión y la generación de estrategias en base al giro del negocio. Se ataca el proceso con la conformación de grupos de trabajo en cuatro aspectos principales:

- El control operacional se enfoca en mantener en forma dinámica el nivel de servicio de la red.
- La administración, que se enfoca en hacer un seguimiento al control operacional y generar reportes en base a ello.
- El análisis, se enfoca en garantizar la calidad del servicio.
- La planificación, que en base al giro del negocio se ocupa de buscar las necesidades que requiere la red.

1.7.1.2. Componente Técnico

El componente técnico se encarga de buscar las soluciones que permiten gestionar la red, y realizar su implementación en la infraestructura de red.

En este componente se define un paradigma común para cada una de las herramientas de gestión; el modelo de Gestor - Agente.

Pese a la heterogeneidad de los elementos que conforman una red, respecto a sus tecnologías y debido a sus fabricantes, el objetivo de una Gestión Integrada

[22] Información obtenida de: T. Saydam y Magedanz T., “Redes, gestión de redes y servicio de administración", Diario de Redes y Sistemas de Gestión, Vol. 4, No. 4 (Dic 1996).

es poder administrar cualquier tecnología de manera transparente, junto con los servicios de voz, datos y video.

El sistema de Gestión de Red es conformado por todo el conjunto de elementos de hardware y software que permiten administrar la red, también conocido este concepto como Red de Gestión.

Para establecer un conjunto de especificaciones y convenciones que determinan la comunicación de los elementos y procesos que conforman el sistema de gestión es necesario un protocolo. La mayoría de fabricantes usan el protocolo SNMP (Protocolo de Gestión de Red Simple) como protocolo de gestión de red. SNMP es parte del stack de protocolos de TCP/IP.

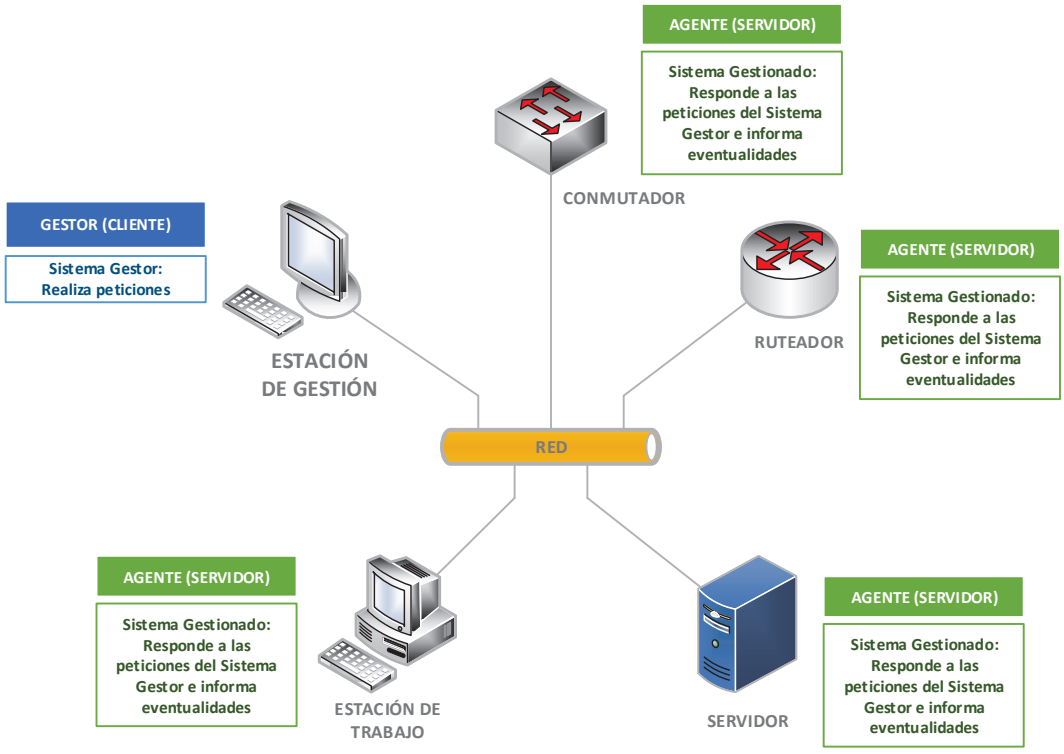

Figura 1.11. Esquema general de una red gestionada[23]

1.7.2. MODELO GESTOR - AGENTE

El modelo de gestor - agente establece dos entidades fundamentales dentro de una red de gestión: la NME (Network Management Entity) conocida generalmente

[23] Figura tomada de: Diapositivas Materia Administración y Gestión de Redes, Ing. Xavier Calderón, 2013

como Agente y la NMA (Network Management Application) conocido también como Sistema Gestor o NMS.

El agente es un software que se localiza en el dispositivo gestionado. Esta entidad recolecta información sobre el funcionamiento del o los dispositivos de la red. Cuando se presenta alguna eventualidad en el funcionamiento de la red la NME genera una notificación a la NMA, esta notificación es conocida como trap. También el agente interactúa con la NMA para atender peticiones cuando recibe comandos por parte de ésta.

El agente tiene la capacidad de representar los recursos reales de hardware (del dispositivo gestionado) mediante un repositorio de información de gestión, conocido como MIB (Management Information Base), en el cual se almacenan objetos de gestión (conocidos como MO). Los objetos de gestión representan a su vez una parte de la información de gestión, y son una característica específica del hardware. La manera en cómo se instancian los MO que conforman la MIB depende del modelo de gestión.

Por otra parte, el Sistema Gestor es un software o plataforma que permite la realización de dos procedimientos básicos con el fin de realizar la gestión: monitorización y control. Es responsable de iniciar y terminar las tareas de gestión y provee una interfaz humana del funcionamiento del sistema de gestión.

Dentro del modelo gestor - agente, está en capacidad de realizar peticiones hacia los dispositivos gestionados (a sus NMEs), para luego recibir las respectivas respuestas a las peticiones generadas. También puede recibir las traps generadas por las NMEs o alarmas de otras NMAs.

1.7.3. MONITORIZACIÓN [PW18]

Las tareas de monitorización dentro de los sistemas de gestión se ocupan de la adquisición de datos relacionados al estado de los recursos gestionados, siendo esta tarea especialmente pasiva. En la monitorización se da seguimiento principalmente a cuatro aspectos:

- Sistemas y servicios: se verifica que exista disponibilidad y que sea alcanzable.

- Recursos: verificación de planes de crecimiento y disponibilidad de los mismos.
- Rendimiento: verificación de tiempos de ida y vuelta, latencia, velocidad de transmisión.
- Cambios y configuraciones: verificación de registros del sistema (logs), control de versiones, documentación.

La monitorización se apega a las políticas establecidas previamente que garantizan determinada calidad del servicio para el usuario de la red. La medida de ésta no es subjetiva, responde al aseguramiento de niveles de servicio. Se utilizan Acuerdos de Nivel de Servicio (también conocidos como SLA o Service Level Agreement) que consisten en políticas que permiten determinar el porcentaje de tiempo que el servicio estará activo.

1.7.4. CONTROL [PW19]

Por otra parte, las tareas de control se sustentan en la información tomada durante la monitorización para actuar sobre los elementos de la red de gestión para cambiar su funcionalidad según las circunstancias. Esta parte de la gestión se utiliza para tomar medidas, por lo que el carácter de las tareas es fundamentalmente activo.

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL (MIES)

2.1. INTRODUCCIÓN

El presente capítulo comprende el levantamiento de información del edificio principal del Ministerio de Inclusión Económica y Social (MIES), en el cual define el estado actual de la infraestructura física de la red, equipos de networking, además del estado de la red de datos, voz y video vigilancia. Posteriormente se utilizará la información presente en este capítulo para realizar la reestructuración y mejoramiento de la red tanto pasiva como activa, dependiendo de los requerimientos y el alcance del presente proyecto.

2.2. OBJETIVO DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

"Recuperar su rol rector en la formulación de políticas públicas, excelencia de servicios y nueva institucionalidad mediante la depuración y especialización de las competencias propias en los ámbitos de su competencia[24]."

"Unificar en una sola estructura con dos grandes campos de acción: la inclusión social y el aseguramiento, instancias que se conforman de las atribuciones anteriores del MIES, más las atribuciones del Instituto Nacional del Niño y la Familia (INFA) y el Programa de Protección Social (PPS)[25]."

"Re-distribuir el poder y democratización de la sociedad que se fundamenta en un nuevo modelo de Estado cimentado en la recuperación de su capacidad de rectoría, regulación, control, coordinación y se reafirma el rol de la re-distribución,

[24] Tomado de: http://www.inclusion.gob.ec/objetivo-estrategico/
[25] Tomado de: http://www.inclusion.gob.ec/objetivo-estrategico/

dentro de un proceso de racionalización de la administración pública con clara división de competencias[26]."

2.3. ANTECEDENTES

Mediante el decreto supremo N. 3815 publicado en el Registro Oficial N. 3815 del 12 de junio de 1980 se crea el Ministerio de Bienestar Social, con las atribuciones para formular, dirigir y ejecutar la política estatal en materia de seguridad social, protección de menores, cooperativismo y la promoción popular y bienestar social.

Figura 2.1. Antiguo Ministerio de Bienestar Social

Posteriormente el Decreto Ejecutivo N. 828 publicado en el Registro Oficial N. 175 de 23 de septiembre de 2003 se cambia la denominación de Ministerio de Bienestar Social por la de Ministerio de Desarrollo Humano. Por último mediante el decreto presidencial número 580 firmado el 23 de agosto de 2007, el cual se

[26] Tomado de: http://www.inclusion.gob.ec/objetivo-estrategico/

cambia el nombre de Ministerio de Desarrollo Humano al de Ministerio de Inclusión Económica y Social.

“El cambio tiene como meta pasar a un modelo de inclusión y aseguramiento, que genere oportunidades para que los ciudadanos (as) superen su condición de pobreza. Este nuevo enfoque institucional se centra en dos áreas: Inclusión al Ciclo de Vida y la Familia y Aseguramiento para la Movilidad Social. Dentro de la Inclusión al ciclo de vida se incluirán los siguientes programas: Desarrollo Integral, que centrará su atención a las necesidades específicas de la población de atención prioritaria, dirigidas a su desarrollo integral, y Protección Especial, enfocado en la prevención de la violación de derechos, y atención a la población en vulneración de derechos.[27]”

Figura 2.2. El Ministerio de Inclusión Económica y Social

[27] Tomado de: http://www.inclusion.gob.ec/nuevo-mies/

2.4. VISIÓN DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

"Ser la entidad pública que ejerce la rectoría y ejecuta políticas, regulaciones, programas y servicios para la inclusión social y atención durante el ciclo de vida con prioridad en la población de niños, niñas, adolescentes, jóvenes, adultos mayores, personas con discapacidad y aquellos y aquellas que se encuentran en situación de pobreza, a fin de aportar a su movilidad social y salida de la pobreza.[28]"

2.5. MISIÓN DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

"Establecer y ejecutar políticas, regulaciones, estrategias, programas y servicios para la atención durante el ciclo de vida, protección especial, aseguramiento universal no contributivo, movilidad social e inclusión económica de grupos de atención prioritaria (niños, niñas, adolescentes, jóvenes, adultos mayores, personas con discapacidad) y aquellos que se encuentran en situación de pobreza y vulnerabilidad."

2.6. VALORES

"La gestión del MIES se sustentará en los siguientes valores:

- Ética
- Transparencia
- Responsabilidad
- Honestidad
- Respeto
- Calidad
- Calidez
- Lealtad
- Eficiencia

[28] Tomado de: http://app.mies.gob.ec/lotaip/images/Autoridades/plan_estrategico.pdf

- Eficacia
- Compromiso
- Consideración
- Trabajo en equipo.[29]”

2.7. ORGANIGRAMA INSTITUCIONAL

La estructura organizacional del Ministerio de Inclusión Económica y Social se basa principalmente en cinco ejes para su funcionamiento:

- Coordinaciones Generales
- Subsecretarías
- Direcciones por área
- Coordinaciones zonales
- Direcciones Distritales

De tal manera que la estructura organizacional a partir del decreto presidencial del año 2007 es la siguiente:

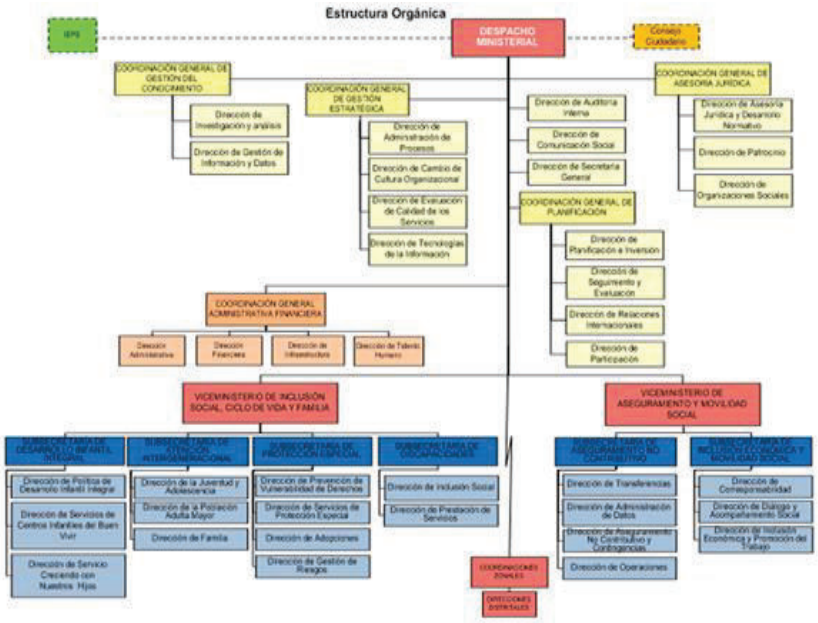

Figura 2.3. Estructura Organizacional del Ministerio de Inclusión Económica y Social

[29] Tomado de: http://www.inclusion.gob.ec/valores-mision-vision/

2.8. UBICACIÓN ACTUAL

El Ministerio de Inclusión Económica y Social se encuentra funcionando en el mismo edificio donde funcionaba hasta el año 2003 el Ministerio de Bienestar Social o Desarrollo Humano, Se ubica en el centro norte de la ciudad de Quito, barrio de La Mariscal, calles Robles entre 9 de Octubre y Páez, como se describe en la figura 2.4.

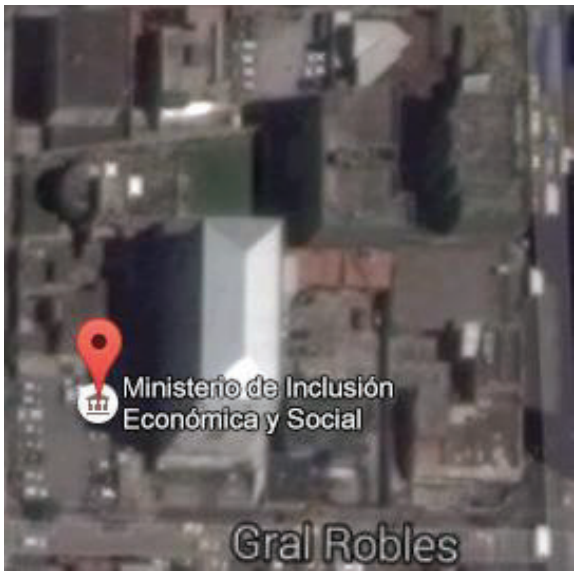

Figura 2.4. Vista Satelital del Ministerio de Inclusión Económica y Social

2.9. INFRAESTRUCTURA FÍSICA DEL EDIFICIO MATRIZ DEL MIES

El Ministerio de Inclusión Económica y Social cuenta con un edificio de once pisos dedicados a las diferentes áreas de especialización y ayuda social, además de contar con tres subsuelos dedicados a parqueaderos.

El edificio matriz del Ministerio se encuentra construido por hormigón armado y después de remodelaciones a causa de los saqueos ocurridos el 20 de abril de 2005 fueron reestructurados los dos primeros pisos del edificio.

Las áreas por piso son por lo general simétricas con pequeñas excepciones tanto en la planta baja como en el subsuelo 1, subsuelo 2, y subsuelo3, que son áreas más amplias dedicadas a parqueaderos de automóviles propiedad del Ministerio.

El área total del edificio sin tomar en cuenta las áreas de los subsuelos es de 5.257,64 m^2 distribuida de la manera, que se explica en la tabla 2.1:

Edificio Matriz MIES	
PISO	*Area [m^2]*
Planta Baja	776.44
Primer Piso	448.12
Segundo Piso	448.12
Tercer Piso	448.12
Cuarto Piso	448.12
Quinto Piso	448.12
Sexto Piso	448.12
Séptimo Piso	448.12
Octavo Piso	448.12
Noveno Piso	448.12
Décimo Piso	448.12
TOTAL	5.257,64

Tabla 2.1. Área por piso del edificio matriz del MIES

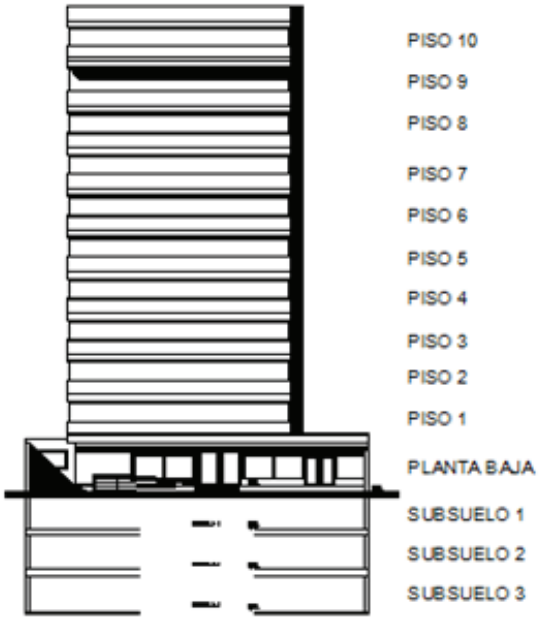

Figura 2.5. Distribución de Pisos Edificio Matriz MIES

2.10. DESCRIPCIÓN DEL SISTEMA DE VOZ, DATOS, VIDEOVIGILANCIA Y VIDEOCONFERENCIA

El MIES cuenta con una infraestructura de datos separada tanto para el sistema de datos como para el sistema de voz, el cableado estructurado se encuentra en malas condiciones, además no se tomó en cuenta el crecimiento que el Ministerio iba a tener, así que se puede encontrar instalaciones sin tomar en cuenta las normas o procedimientos necesarios para que opere de una manera óptima.

Por tal motivo se presenta un bajo rendimiento y desempeño en la red, por lo que para el personal de soporte técnico se ha vuelto un dolor de cabeza la administración tanto de la red de datos y equipos de conectividad como del cableado estructurado.

El cableado estructurado en algunos casos es guiado por escalerillas metálicas acompañadas de tubería metálica o plástica, pero en las áreas que no se ha tomado en cuenta el crecimiento de la red se puede observar instalaciones y extensiones del cableado sin ningún tipo de protección ni normas básicas de cableado estructurado, llegando a realizar perforaciones en las paredes y techos para llegar con puntos de datos a usuarios finales. La categoría de cable UTP que predomina en las instalaciones es Cat 5e pero también se puede encontrar cable UTP Cat 5.

Además se puede observar que debido al gran número de usuarios que necesitan conexión tanto cableada como inalámbrica, el personal de la Dirección de Tecnologías de la Información se han visto en la necesidad de colocar equipos de red tipo HOME como switches en cascada a partir de un punto de datos para usuarios finales generando inconvenientes y molestias tanto a los usuarios como a los administradores de la red, además se han colocado access points en las áreas donde más se ha requerido este servicio sin realizar ningún tipo de estudio del nivel de señal inalámbrico.

La central telefónica que utiliza el MIES actualmente es una central AVAYA Ip office 500 que cuenta actualmente con 554 extensiones de las cuales se ocupan 276, la cual tiene funcionalidades de: buzón de voz, troncales IP H323, SIP,

soporta extensiones analógicas, digitales e IP, admite usar extensiones SIP con licencias.

El equipo de seguridad perimetral que utiliza el MIES es un firewall marca SOPHOS UTM 525 que se encuentra configurado en clúster con otro equipo SOPHOS de las mismas características, además de ser un firewall de seguridad perimetral también realiza la función de controlador de equipos inalámbricos (access point) de la misma marca SOPHOS, además se encuentran nueve access point de marca CISCO home edition y SOPHOS, ubicados en diferentes pisos del edificio solo como una solución temporal de red inalámbrica.

La Videovigilancia cuenta con 28 cámaras de video distribuidas de la siguiente manera: dos por cada piso, incluyendo los tres subsuelos utilizados como estacionamientos que dan un total de 28 cámaras activas en el MIES.

Las características de la PC donde se encuentra el software y la base de datos de las cámaras de seguridad son las siguientes:

- DELL PC clon con servidor VIVOTEK ST 7501 Live Client versión 1.6.1.11
- Procesador Core i7.
- RAM: 16 Gbps
- Sistema operativo Windows 7 Professional.
- Cuenta con 5 discos duros externos de 1 Tera Byte cada uno.

Presentan una salida hacia Internet de 200 Mbps con 150 Mbps de Internet y 50 Mbps para datos; además de tener un enlace por el Anillo Interministerial el cual cuenta con 10 Mbps para Internet y 10 Mbps para datos.

La videoconferencia en el MIES se maneja por medio de SABA, una plataforma que se administra en la nube y se requiere instalar un agente en los equipos que requieran ingresar a la videoconferencia, las principales características de SABA son:

- Incorpora usuarios de manera rápida y fácil.
- Se puede incluir la compartición de documentos o presentaciones para que los usuarios puedan interactuar.

- El usuario se puede conectar desde cualquier dispositivo con salida hacia internet.
- Se debe asegurar un mínimo de 1 Mbps para el correcto funcionamiento de la herramienta[30].
- Posibilidad de programar una videoconferencia que permita audio video y compartición de archivos.
- Permite chat entre los usuarios de la videoconferencia.

Actualmente el MIES ha adquirido 4 salas virtuales de videoconferencia con 50 usuarios simultáneos por sala sin límite de tiempo en la conexión.

La videoconferencia se encuentra en la VLAN 26, la cual presenta una reserva de ancho de banda de 2 Mbps por usuario, la cual administra el equipo de seguridad perimetral SOPHOS.

La topología que predomina en los diferentes pisos es en estrella aunque en lugares donde se han colocado equipos de red sin previo estudio para cubrir las necesidades de conectividad de los clientes se puede observar que se maneja también la topología estrella extendida.

Entre los equipos de conectividad se puede encontrar switches en los diferentes pisos que en la mayoría de casos son administrables y otros no, los equipos no administrables permanecen con su configuración de fábrica y permiten cubrir la necesidad ante la ausencia de equipos para conectar a usuarios a la red.

Entre los equipos de conectividad que se puede encontrar tanto en los cuartos de telecomunicaciones como en los racks y en los gabinetes de comunicaciones instalados en los diferentes pisos se tiene lo siguiente:

EQUIPO	CANTIDAD
Switch de núcleo	1
Switch de acceso	25
Router	3
Access Point	14
Firewall	3

[30] Información tomada de: https://www.saba.com/mx/solutions/by-industry/public-sector/education/

TOTAL	35

Tabla 2.2. Equipos de conectividad existentes en la red del MIES

2.11. DESCRIPCIÓN DEL SISTEMA DE ENERGÍA DE RESPALDO (UPS)[31]

Actualmente el MIES posee 2 UPSs (Sistemas de alimentación ininterrumpidos) en el Data Center ubicados en el quinto piso del edificio matriz del Ministerio de Inclusión Económica y Social.

Se encuentran actualmente funcionando e instalados 8 bancos de batería los cuales entregan un total de 60 KVA.

Los bancos de batería son marca APC Smart-ups RT 2200VA 120V como se indica en la siguiente figura:

Figura 2.6. UPS utilizado en el MIES

Mediante información solicitada a los administradores de red, los UPSs fueron instalados en el año 2014, los cuales tienen un promedio de consumo del 28% en pruebas realizadas por la empresa que se adjudicó el contrato.

[31] UPS: (Uninterrupted Power Supply), presenta dos características importantes: proteger equipos electrónicos delicados y convertir la tensión de las baterías (continua) a la tensión con 110 V (voltios)

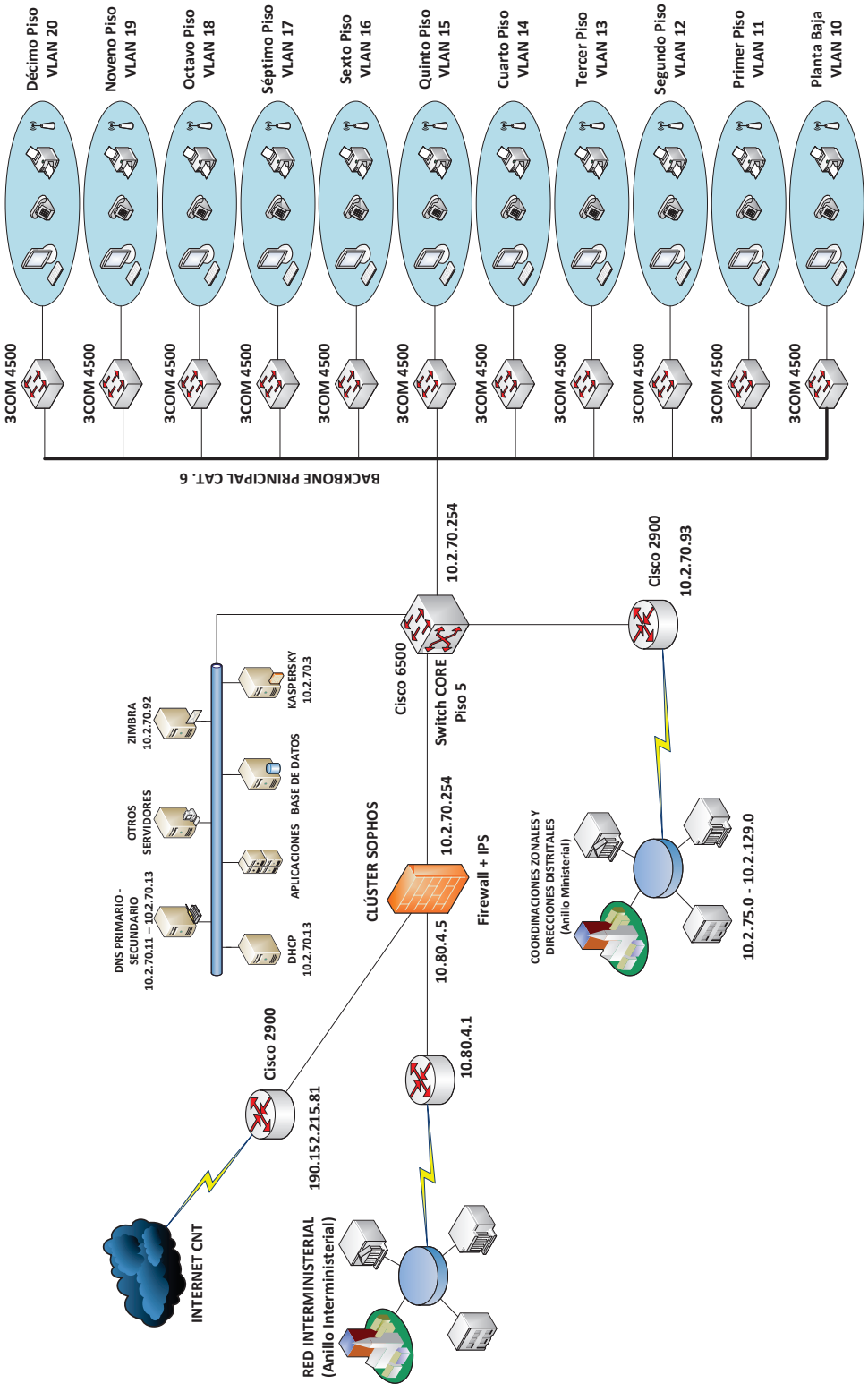

Figura 2.7. Diagrama actual de la red de datos del MIES

La administración y gestión de los equipos de comunicación, servidores, cableado estructurado, servicios y soporte a usuarios finales dentro del edificio Matriz del MIES está a cargo de la Dirección de Tecnologías de la Información conformada por las siguientes áreas de trabajo:

- Desarrollo
- Help Desk
- Redes y conectividad
- Infraestructura

2.12. DESCRIPCIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO

Tomando en cuenta que se heredaron las instalaciones del antiguo Ministerio de Bienestar Social y posteriormente se realizaron cambios en la organización interna del MIES, se puede verificar que no se realizó la proyección del crecimiento que tuvo el MIES a lo largo de estos años, ya que se evidencian varios problemas a causa de un inadecuado estudio y crecimiento del ministerio.

Como resultado de esto se presentan problemas de atenuaciones de señal principalmente en la red inalámbrica, intermitencias en la red tanto cableada como inalámbrica, caída parcial de la red en diferentes áreas del edificio, etc.

2.13. DESCRIPCIÓN DE LA LAN

La LAN del MIES trabaja principalmente con las siguientes capas del modelo jerárquico de Cisco:

- Capa de acceso
- Capa de núcleo

Actualmente se tiene un switch de núcleo marca Cisco, modelo 6500-E y se cuenta con veinte y cinco switches de acceso entre los cuales se pueden encontrar las siguientes marcas y modelos:

- 3COM 4500 3CR17561-91

- DLINK DES-1016D
- TPLINK TL-SF1008D
- Cisco 2960-S

Los switches de acceso se encuentran distribuidos en los once pisos del edificio, dependiendo del número de usuarios por piso. Además se tienen switches de diferentes marcas, no administrables colocados en cascada a partir de los switches de acceso.

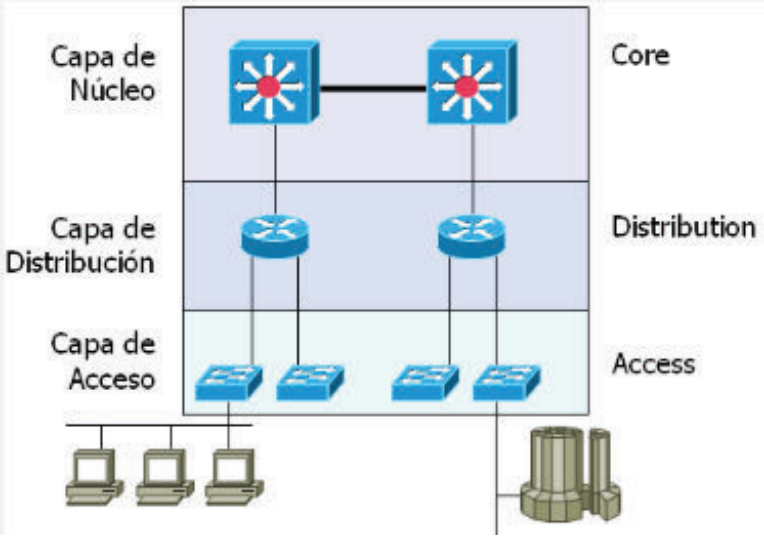

Figura 2.8. Modelo Jerárquico de 3 capas de Cisco[32]

El tendido de backbone de la red se encuentra implementado sobre cableado UTP Cat. 6ª. En el Data Center ubicado en el quinto piso donde se encuentra el switch de núcleo se distribuyen las conexiones troncales hacia los diferentes switches de acceso de los pisos del edificio, no se tiene redundancia entre dichos switches de acceso, por lo general el último puerto de cobre (puerto 48) se encuentra dedicado a la conexión troncal hacia el switch de núcleo.

Se realizó un estudio de la cobertura wireless en el edificio del MIES en el cual se puede revisar en el Anexo 21. Para dicho estudio se utilizó una tarjeta 802.11 b/g Tarjeta Mini de media altura WLAN Wireless-N DW1501 integrada en una laptop DELL INSPIRON N4110, el software utilizado es inSSIDer-Installer-2.1.5.1393 se instaló sobre la laptop antes mencionada

[32] Información obtenida de: https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

2.13.1. DIRECCIONAMIENTO IP ACTUAL

Se utilizan diferentes segmentos de red para las VLAN configuradas en el switch de núcleo donde se encuentran configuradas la puertas de enlace para cada VLAN, se tiene configurada una VLAN por cada piso, además de tener VLAN de: servidores, impresoras, cámaras de video vigilancia, biométricos y telefonía. A continuación se detalla la distribución de las VLAN con su correspondiente direccionamiento IP:

ID de VLAN	NOMBRE DE LA VLAN	DIRECCIÓN DE RED	PUERTA DE ENLACE
3	Wireless	192.168.3.0/24	192.168.3.1
10	Planta Baja	192.168.10.0/24	192.168.10.1
11	Piso 1	192.168.11.0/24	192.168.11.1
12	Piso 2	192.168.12.0/24	192.168.12.1
13	Piso 3	192.168.13.0/24	192.168.13.1
14	Piso 4	192.168.14.0/24	192.168.14.1
15	Piso 5	192.168.15.0/24	192.168.15.1
16	Piso 6	192.168.16.0/24	192.168.16.1
17	Piso 7	192.168.17.0/24	192.168.17.1
18	Piso 8	192.168.18.0/24	192.168.18.1
19	Piso 9	192.168.19.0/24	192.168.19.1
20	Piso 10	192.168.20.0/24	192.168.20.1
21	Servidores	192.168.21.0/29	192.168.21.1
22	Impresoras	192.168.22.0/26	192.168.22.1
23	Cámaras de video	192.168.23.0/27	192.168.23.1
24	Biométricos	192.168.24.0/28	192.168.24.1
25	Telefonía IP	192.168.25.0/24	192.168.25.1
26	Videoconferencia	192.168.26.0/26	192.168.26.1

Tabla 2.3. VLAN y direcciones de red

2.14. SITUACIÓN ACTUAL PLANTA BAJA

En este piso se puede encontrar un gabinete de comunicaciones ubicado en la parte de la bodega, donde dicho gabinete no se encuentra con ninguna seguridad por lo que se puede ingresar a los equipos de comunicaciones sin ningún tipo de inconveniente, además el gabinete no posee ningún mecanismo de ventilación ni extracción de calor para los equipos instalados.

En la planta baja se tienen dos access point instalados, uno instalado en la Secretaría General (SOPHOS AP 30) y otro en el Auditorio (SOPHOS AP 30).

La ubicación del access point no permite cobertura para todos los usuarios inalámbricos de la Planta Baja y se recomienda la reubicación del access point que se encuentra en la Secretaría General hacia el pasillo de Recepción.

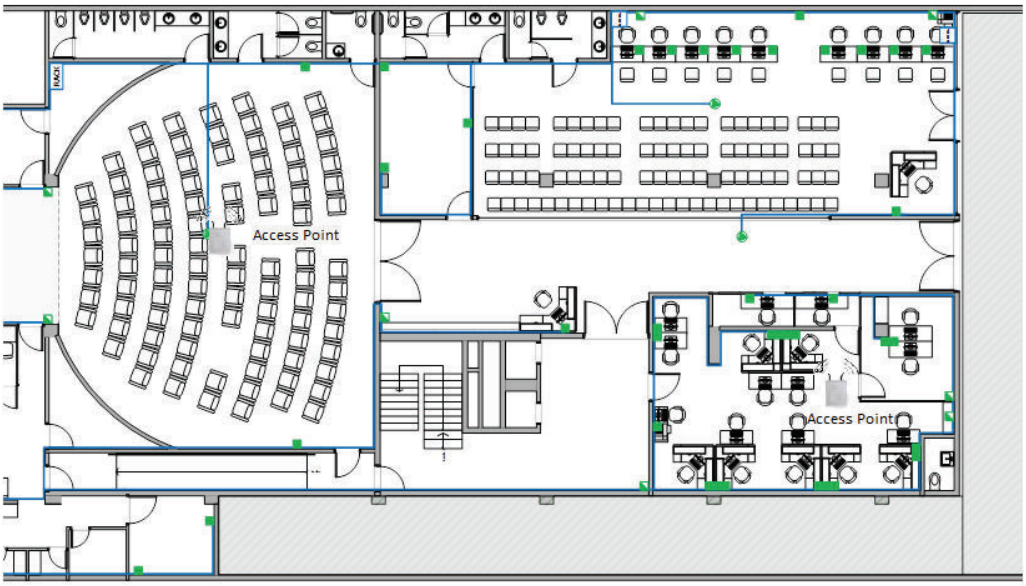

Figura 2.9. Ubicación actual access point Planta Baja

El área donde se encuentra el gabinete de comunicaciones no es la ideal, ya que como es utilizado como bodega existe gran cantidad de documentación archivada lo cual genera polvo y es un lugar donde existe gran probabilidad de generarse un incendio, como se puede observar en la siguiente figura:

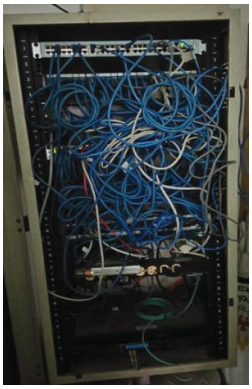

Figura 2.10. Gabinete de comunicaciones Planta Baja

2.14.1. ÁREAS DE TRABAJO PLANTA BAJA

- Servicio de atención al ciudadano
- Recepción
- Secretaría General
- Auditorio
- Balcón de servicios

2.14.2. CABLEADO ESTRUCTURADO PLANTA BAJA

El cableado se presenta en ciertas áreas ordenado protegido por canaletas plásticas pero se puede observar en áreas como en balcón de servicios que se ha realizado un cableado sin seguir normas o estándares.

Se puede observar que el cableado además de no estar identificado correctamente se encuentra sin ningún tipo de organización:

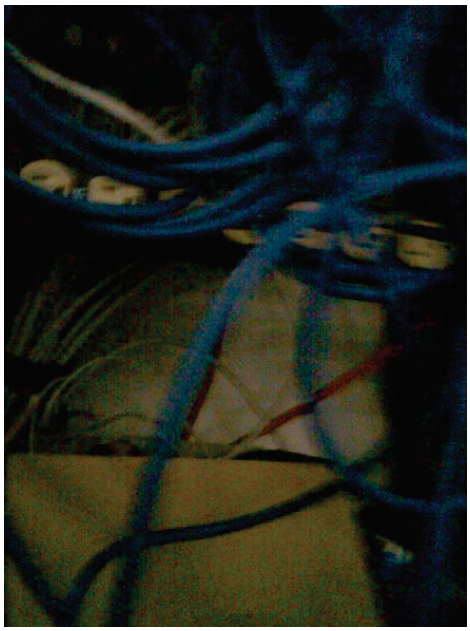

Figura 2.11. Estado del cableado estructurado Planta Baja

2.14.3. EQUIPOS DE RED PLANTA BAJA

En el gabinete de comunicaciones podemos encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO

Switch	1	3COM	4500 3CR17562-91 50 Puertos
Switch	1	Cisco	2960-S 48 Puertos
Switch	1	DLINK	Des-1008d 8 Puertos
Access point	2	Sophos	AP 30

Tabla 2.4. Equipos de red Planta Baja

2.15. SITUACIÓN ACTUAL PRIMER PISO

En este piso se puede encontrar un gabinete de comunicaciones ubicado en la parte de la Sala de Test, la puerta del gabinete se encontraba con seguro y una vez abierto el gabinete se pudo observar que se encontraba desorganizado el cableado estructurado, además de que se necesita un mantenimiento físico de los equipos por la cantidad de polvo dentro del gabinete de comunicaciones.

En el área de la sala de reuniones se encuentra instalado un access point que cubre solo dicha área, pero el equipo inalámbrico no tiene la capacidad de cubrir todo el piso, por lo que en todo el piso excepto en la sala de reuniones no existe señal inalámbrica. Como se puede observar en la siguiente figura el gabinete de comunicaciones se encuentra en un área que se ha convertido en una bodega donde se puede verificar que el acceso es complicado y se encuentra gran cantidad de papel, cajas y archivos del Ministerio:

Figura 2.12. Gabinete de comunicaciones Primer Piso

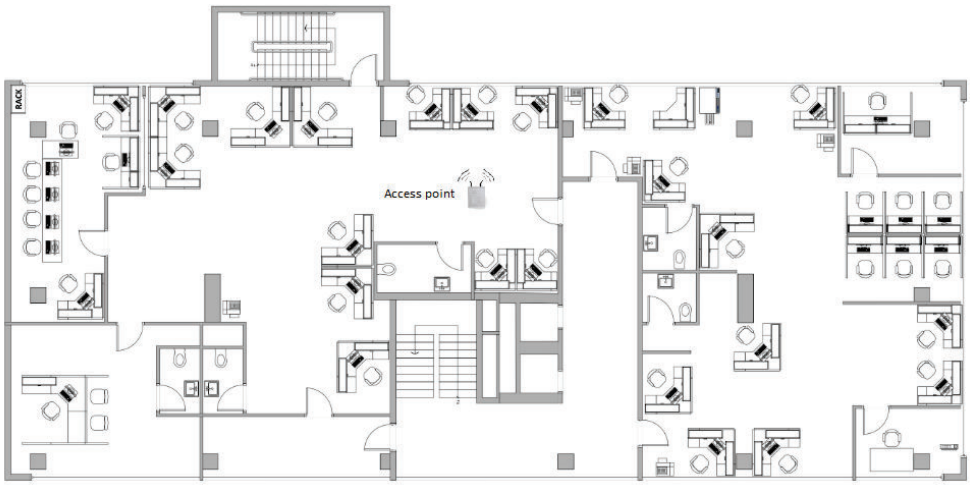

Figura 2.13. Ubicación actual access point Primer Piso

2.15.1. ÁREAS DE TRABAJO PRIMER PISO

- Dirección de Talento Humano
- Sala de reuniones
- Archivo
- Sala de test

2.15.2. CABLEADO ESTRUCTURADO PRIMER PISO

A diferencia de la planta baja el cableado estructurado se encuentra totalmente desorganizado en el gabinete de comunicaciones, los patch panels se encuentran etiquetados pero no coincide la nomenclatura utilizada en los puertos del patch panel con la asignada en los faceplates de cada usuario final.

Ninguno de los cables UTP que se encuentran en los puertos del switch están etiquetados, por lo que dificulta la identificación para los administradores de la red.

2.15.3. EQUIPOS DE RED

En el gabinete de comunicaciones se puede encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 Puertos

Switch	1	HP	1910-48G - 48 Puertos
Access Point	1	SOPHOS	AP30

Tabla 2.5. Equipos de red Primer Piso

2.16. SITUACIÓN ACTUAL SEGUNDO PISO

El gabinete de comunicaciones se encuentra ubicado en la Dirección Administrativa donde existe seguridad en la puerta del gabinete de comunicaciones, una vez abierto el gabinete se puede observar que solo el switch Cisco está conectado con el switch de núcleo y los dos switches Linksys se encuentran conectados en cascada con el switch de acceso Cisco 2960.

Se encuentra funcionando un access point Sophos AP 30 ubicado en la Dirección Administrativa, el cual no cubre la totalidad del área del segundo piso.

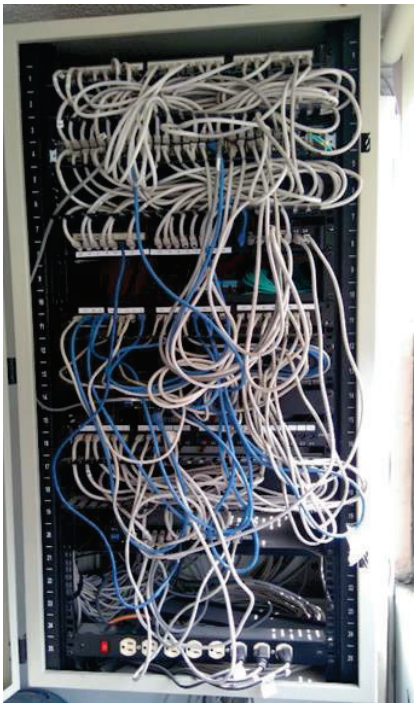

Figura 2.14. Gabinete de comunicaciones Segundo Piso

2.16.1. ÁREAS DE TRABAJO SEGUNDO PISO

- Dirección Administrativa
- Auditoría Interna
- Sala de reuniones

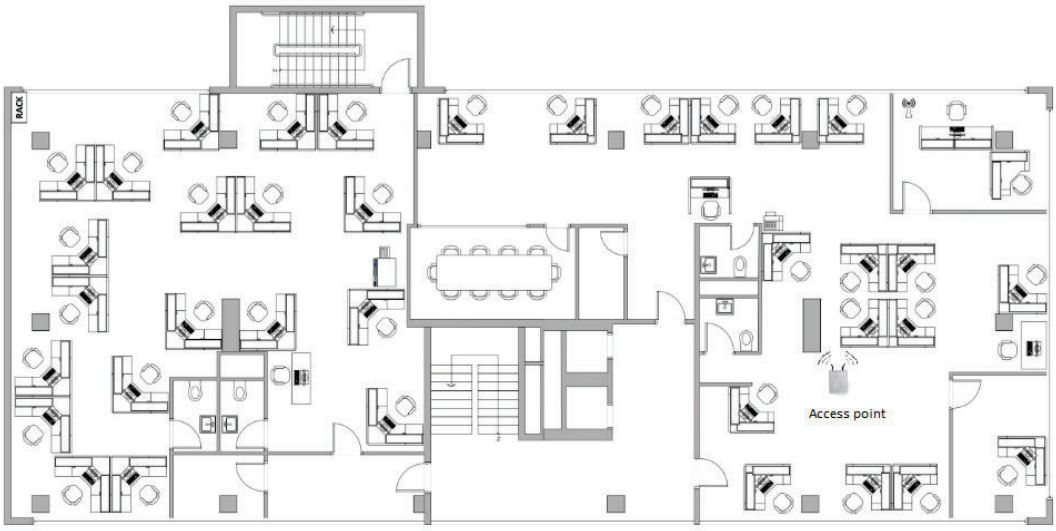

Figura 2.15. Ubicación actual access point Segundo Piso

2.16.2. CABLEADO ESTRUCTURADO SEGUNDO PISO

El cableado dentro del gabinete de comunicaciones se encuentra desorganizado. Los cables UTP se encuentran desordenados en las canaletas que se dirigen a los respectivos cajetines para que los usuarios finales se conecten. Además se observa que una canaleta interrumpe la salida de emergencia como se puede observar en la siguiente figura:

Figura 2.16. Estado actual cableado estructurado Segundo Piso

2.16.3. EQUIPOS DE RED

En el gabinete de comunicaciones podemos encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 Puertos
Switch	2	LINKSYS	SR224 DE 24 Puertos
Access Point	1	SOPHOS	AP30

Tabla 2.6 Equipos de red Segundo Piso

2.17. SITUACIÓN ACTUAL TERCER PISO

El gabinete de comunicaciones se encuentra desorganizado, donde los cables UTP no permiten cerrar la puerta del gabinete ya que no son de la extensión adecuada para una distancia pequeña entre los switches de acceso y los patch panels, además ningún cable UTP se encuentra etiquetado, únicamente los patch panels se encuentran etiquetados y no coincide la nomenclatura del etiquetado de los patch panels con los faceplates de las estaciones de trabajo.

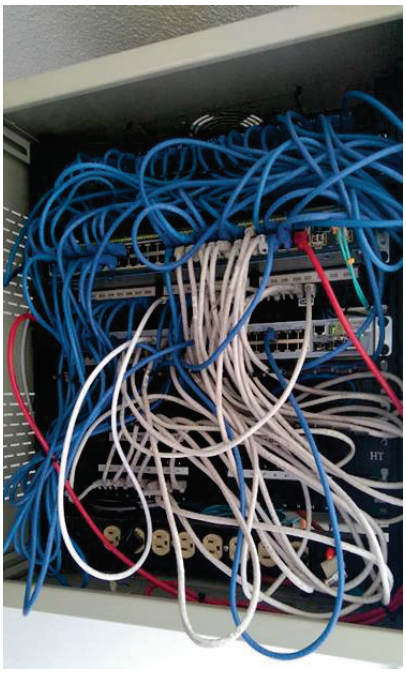

Figura 2.17. Gabinete de comunicaciones Tercer Piso

El gabinete se encuentra ubicado en el área de la Dirección Financiera donde se pueden encontrar cajas y archivos de dicho departamento.

El access point SOPHOS AP 30 se encuentra en la parte central del piso, cerca de las escaleras, el access point no cubre con las necesidades de cobertura ni de número de usuarios conectados.

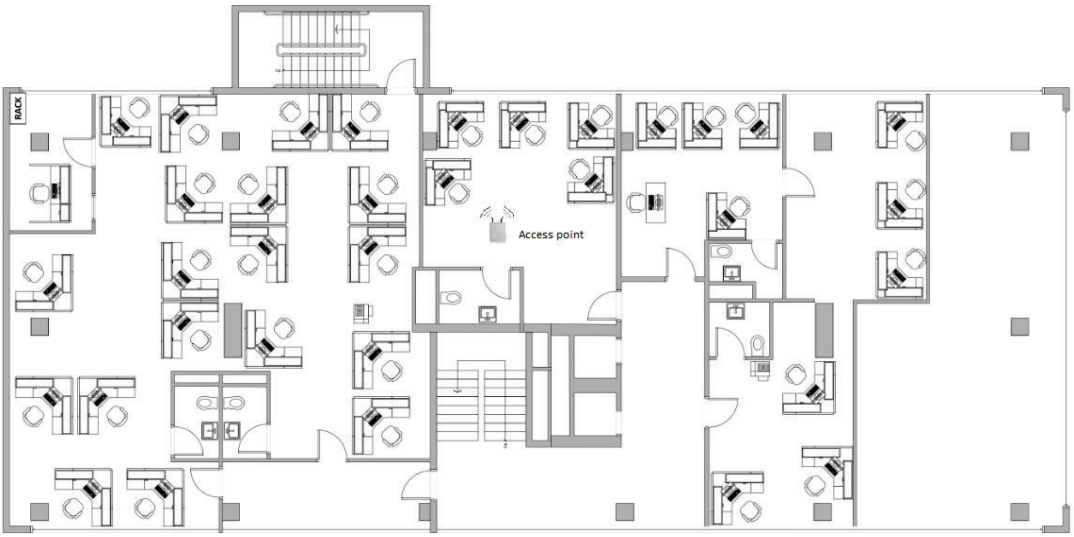

Figura 2.18. Ubicación actual access point Tercer Piso

2.17.1. ÁREAS DE TRABAJO TERCER PISO

- Coordinación General Administrativa Financiera
- Dirección Financiera
- Archivo Financiero

2.17.2. CABLEADO ESTRUCTURADO TERCER PISO

El cableado dentro del gabinete de comunicaciones se encuentra totalmente desordenado y permanece el gabinete con la puerta abierta, además los cables UTP no se encuentran etiquetados.

No existe seguridad ni una adecuada ventilación para los equipos, en la parte superior del gabinete se puede observar que colocan cajas y cables sobrantes.

2.17.3. EQUIPOS DE RED

En el gabinete de comunicaciones se pueden encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 Puertos
Switch	1	3COM	4500 48 Puertos
Access Point	1	SOPHOS	AP30

Tabla 2.7. Equipos de red Tercer Piso

2.18. SITUACIÓN ACTUAL CUARTO PISO

El gabinete que se encuentra en el cuarto piso presenta desorden tanto en la distribución de los cables UTP como en la colocación de los switches de acceso, ya que por falta de espacio físico en el gabinete de comunicaciones los switches D-LINK y TPLINK están colocados en la parte superior del gabinete (fuera del gabinete de comunicaciones), además dichos switches se encuentran conectados en cascada con el switch de acceso Cisco 2960.

La cobertura wireless en este piso es crítica ya que no se encuentra instalado ningún access point, además existe una señal inalámbrica muy tenue tanto del piso superior como en el inferior.

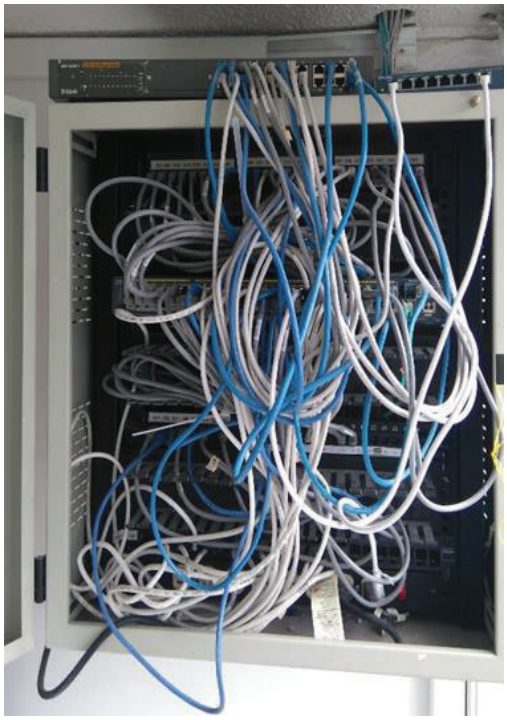

Figura 2.19. Gabinete de comunicaciones Cuarto Piso

2.18.1. ÁREAS DE TRABAJO CUARTO PISO

- Dirección de cambio de cultura organizacional
- Dirección de Administración de procesos
- Servicio Médico
- Servicio de Bienes

2.18.2. CABLEADO ESTRUCTURADO CUARTO PISO

El cableado dentro del gabinete de comunicaciones se encuentra totalmente desordenado, además no existe el respectivo etiquetado tanto en los switches de acceso como en los patch panels.

En el área de los usuarios finales se pueden observar canaletas totalmente saturadas y perforaciones en las paredes realizadas para el paso del cableado estructurado sin ningún tipo de estudio previo, como se muestra a continuación:

Figura 2.20. Estado actual del cableado estructurado del Cuarto Piso

2.18.3. EQUIPOS DE RED

En el gabinete de comunicaciones podemos encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 Puertos
Switch	1	D-LINK	DES 1024R de 24 puertos
Switch	1	TPLINK	TL sg1008d

Tabla 2.8. Equipos de red Cuarto Piso

2.19. SITUACIÓN ACTUAL QUINTO PISO

El rack de comunicaciones del quinto piso se encuentra ubicado en el Data Center del edificio, como se puede observar en la siguiente figura existe un orden entre los cables UTP dentro del gabinete de comunicaciones, además se puede observar que en algunos casos existen cables etiquetados que van desde el switch hasta el patch panel.

Figura 2.21. Rack de comunicaciones Quinto Piso

Existen dos access point en el quinto piso, uno de ellos se encuentra en el área de la Dirección de Tecnologías de la Información y uno adicional en la Dirección de Cultura Organizacional, los cuales solo dan servicio a estas áreas ya que se trata de equipos que no cuentan con las características necesarias para cubrir en

el área del quinto piso, además no se encuentran instalados en el techo de cada área sino que están colocados uno encima de un escritorio y el segundo sobre una caja de cartón.

Figura 2.22. Access point Quinto Piso

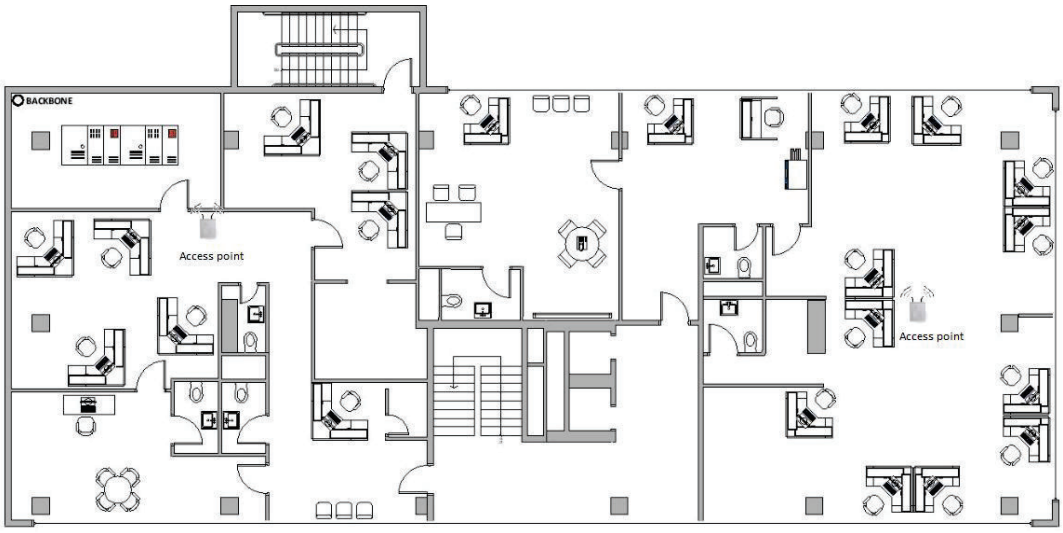

Figura 2.23. Ubicación actual access points Quinto Piso

2.19.1. ÁREAS DE TRABAJO QUINTO PISO

- Coordinación General de Gestión Estratégica
- Dirección de Calidad
- Dirección de Tecnologías de la Información
- Dirección de Cultura Organizacional

2.19.2. CABLEADO ESTRUCTURADO QUINTO PISO

El cableado dentro del gabinete de comunicaciones se encuentra totalmente ordenado y organizado, se puede observar que existen algunos puntos que van conectados al switch de acceso que se pueden identificar a donde van conectados por medio del etiquetado. Se han realizado conexiones hacia equipos DLINK en cascada para poder cubrir los requerimientos de usuarios que se conectan de forma cableada.

Los access points que se encuentran en este piso han sido colocados en lugares donde se ha realizado un previo estudio de cobertura y no existe una cobertura total en el piso quedando sin cobertura wireless el área de Dirección de Calidad.

2.19.3. EQUIPOS DE RED

En el gabinete de comunicaciones se puede encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch de acceso	1	Cisco	2960-S 48 Puertos
Switch de acceso	1	Cisco	2960-S 48 Puertos
Access Point	1	Cisco	Cisco WAP4410N
Access Point	1	Sophos	AP30
Switch de núcleo	1	Cisco	6500-E
Firewall	3	Sophos	UTM 525
Router	3	Cisco	2900
Servidor de telefonía	1	AVAYA	IP OFFICE 500

Tabla 2.9. Equipos de red Quinto Piso

2.20. SITUACIÓN ACTUAL SEXTO PISO

El gabinete de comunicaciones del sexto piso se encuentra ubicado en el área de la Dirección de Análisis de la Información, donde se encuentran dos switches de acceso, uno de los cuales de marca Cisco se encuentra con sus 48 puertos

utilizados, mientras que el switch de marca HP se encuentra ocupado en un 37,5% (9 puertos).

Se pudo observar que los cajetines donde se conectan los usuarios finales a un punto de red no se encuentran etiquetados, ni tampoco se encuentran etiquetados los cables UTP que se encuentran conectados a los switches de acceso del piso.

Figura 2.24. Estado del cableado en el gabinete de comunicaciones Sexto Piso

En el sexto piso se encuentra un access point en el área de Dirección de Patrocinio, por lo que la señal inalámbrica existe pero en ciertas áreas del piso (Dirección de Patrocinio), mientras que en el resto del piso se recibe una señal muy tenue tanto del piso superior como del inferior.

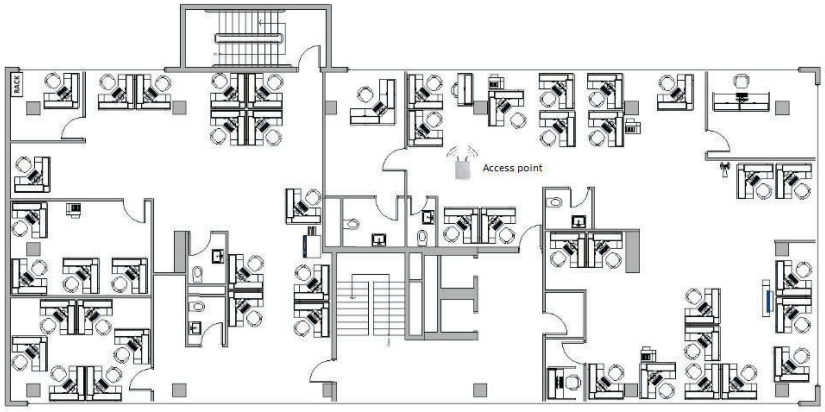

Figura 2.25. Ubicación actual access points Sexto Piso

2.20.1. ÁREAS DE TRABAJO SEXTO PISO

- Dirección de Patrocinio
- Coordinación General de Gestión de Conocimiento
- Dirección de Análisis de Información
- Dirección de Investigación

2.20.2. CABLEADO ESTRUCTURADO SEXTO PISO

Dentro del gabinete de comunicaciones se puede observar que se encuentra desordenado, sin ningún tipo de etiquetado en los cables UTP, existen dos organizadores horizontales para el cableado, lo cual es suficiente para los puertos utilizados en los switches de acceso pero falta colocar el cableado en los organizadores horizontales.

El cableado estructurado que se dirige a los usuarios finales se presenta en desorden, además se puede observar cables UTP sin ninguna protección ni colocadas sobre canaletas, como se puede observar en la siguiente figura existen cables de red fuera de sus respectivas canaletas:

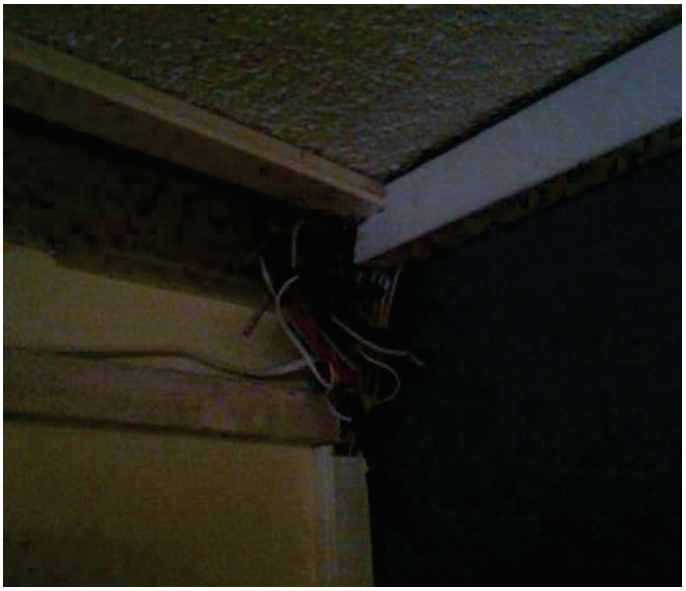

Figura 2.26. Estado del cableado Sexto Piso

2.20.3. EQUIPOS DE RED

En el gabinete de comunicaciones se puede encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 puertos
Switch	1	HP	1910-48 puertos
Access Point	1	Sophos	AP 30

Tabla 2.10. Equipos de red Sexto Piso

2.21. SITUACIÓN ACTUAL SÉPTIMO PISO

El estado del gabinete de comunicaciones del séptimo piso presenta organización del cableado estructurado el cual tiene dos organizadores horizontales para el cableado, se observa que el patch panel se encuentra etiquetado con las estaciones finales de trabajo.

Los cajetines donde se encuentran los jacks para que los usuarios finales se conecten se encuentran en mal estado, en algunos casos los cajetines se encuentran abiertos y los jacks se encuentran desprotegidos, por lo que pueden ser desconectados de los pares del cable UTP en el momento de realizar la limpieza diaria de las instalaciones

Figura 2.27. Estado del cableado en el gabinete de comunicaciones Séptimo Piso

En el séptimo piso se encuentra un access point marca SOPHOS instalado en la sala de reuniones, ya que es un área donde no se encuentran puntos de datos y se ve la necesidad de tener acceso inalámbrico. Ya que solo existe una access

point instalado en el área de la sala de reuniones no tiene la capacidad de cubrir todo el piso ya que cubre el área de la sala de reuniones y parte de la dirección de Organizaciones Sociales.

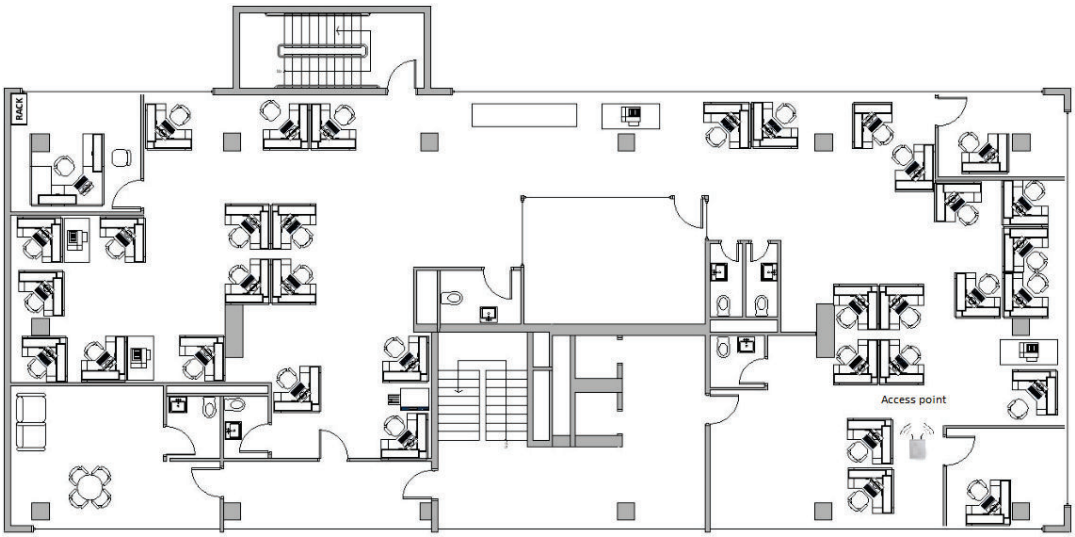

Figura 2.28. Ubicación actual access points Séptimo Piso

2.21.1. ÁREAS DE TRABAJO SÉPTIMO PISO

- Dirección de Organizaciones Sociales
- Dirección de Asesoría Jurídica y Desarrollo Normativo
- Coordinación General de Asesoría Jurídica
- Sala de reuniones

2.21.2. CABLEADO ESTRUCTURADO SÉPTIMO PISO

El cableado dentro del gabinete de comunicaciones se encuentra organizado, pero en la parte inferior del gabinete existe exceso de cable UTP y se encuentra cercano a conexiones eléctricas de los equipos de red instalados.

Figura 2.29. Estado actual del cableado estructurado en el gabinete de comunicaciones Séptimo Piso

2.21.3. EQUIPOS DE RED

En el gabinete de comunicaciones se puede encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	3COM	4500 3CR17561-91 50 Puertos
Switch	1	Cisco	2960-S 48 puertos
Access point	1	SOPHOS	AP30

Tabla 2.11. Equipos de red Séptimo Piso

2.22. SITUACIÓN ACTUAL OCTAVO PISO

El gabinete de comunicaciones se encuentra desordenado ya que el switch de acceso tiene ocupado el 100% de sus puertos y se colocó un switch TPLINK de 8 puertos para cubrir las necesidades de acceso a la red por parte de usuarios finales.

Se encuentra un access point SOPHOS AP 30 en el área de Dirección de Planificación e Inversión, pero existen áreas como: la Dirección de Participación y Relaciones Internacionales donde se tiene una mínima señal inalámbrica de equipos tanto del piso superior como del inferior donde los usuarios se conectan con dificultad y se presenta intermitencia.

Figura 2.30. Estado actual gabinete de comunicaciones Octavo Piso

2.22.1. ÁREAS DE TRABAJO OCTAVO PISO

- Dirección de Planificación e Inversión
- Dirección de Participación
- Dirección de Relaciones Internacionales

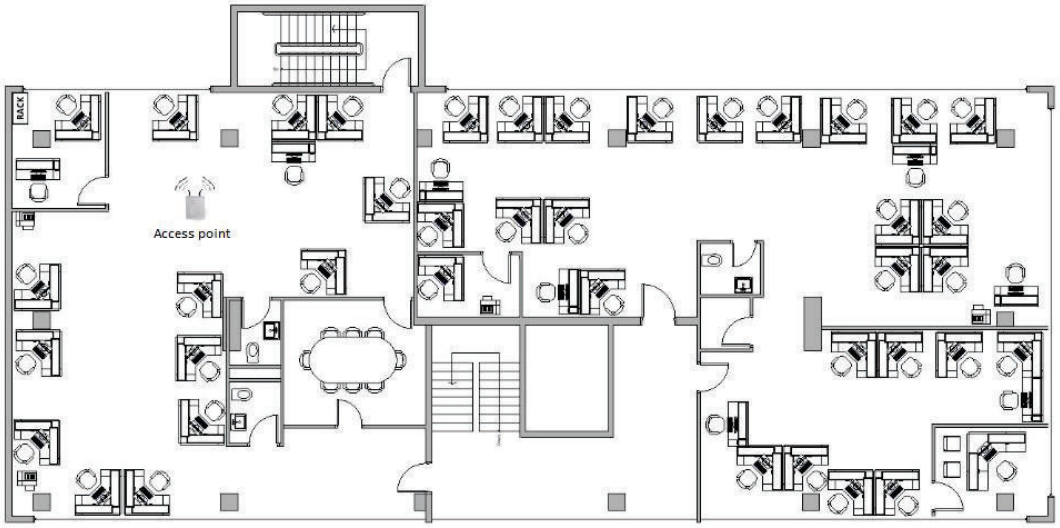

Figura 2.31. Ubicación actual access points Octavo Piso

2.22.2. CABLEADO ESTRUCTURADO OCTAVO PISO

El cableado estructurado en el piso presenta falta de etiquetado en el gabinete de comunicaciones, además los cajetines donde se encuentran los jacks para la conexión de los puntos de red se encuentran en mal estado, se puede observar cables y jacks fuera del cajetín, además ningún cajetín tiene un adecuado etiquetado, existen cables de red que no pasan ordenadamente por las canaletas del piso sino que se encuentran tendidos por encima del techo falso para llegar a los usuarios finales.

2.22.3. EQUIPOS DE RED

En el gabinete de comunicaciones podemos encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	3COM	4500 3CR17561-91 50 Puertos

Switch	1	TPLINK	TL-SF1008D
Access Point	1	Sophos	AP 30

Tabla 2.12. Equipos de red Octavo Piso

2.23. SITUACIÓN ACTUAL NOVENO PISO

En el noveno piso se encuentra un cuarto de comunicaciones donde se encuentran dos switch de acceso Cisco uno de 48 puertos y el otro de 24 puertos. El cuarto de comunicaciones es utilizado también como bodega como se puede observar en la siguiente figura:

Figura 2.32. Estado del cuarto de comunicaciones Noveno Piso

Se encuentra instalado un access point marca SOPHOS en el área de Coordinación General pero la cobertura no cubre todo el noveno piso y existe más del 65% del piso que no tiene cobertura wireless.

2.23.1. ÁREAS DE TRABAJO NOVENO PISO

- Dirección de Comunicación Social
- Coordinación General de Planificación
- Dirección de Seguimiento y Evaluación

2.23.2. CABLEADO ESTRUCTURADO NOVENO PISO

Los cables UTP se encuentran desordenados en el cuarto de comunicaciones, así como tampoco se encuentran etiquetados los cables conectados al switch de acceso de 48 puertos, se tiene un switch Cisco de acceso el cual tiene ocupado más del 90% (45 puertos) y el segundo switch de 24 puertos tiene ocupado la mitad de sus puertos.

El cableado estructurado que va desde el gabinete de comunicaciones hasta los usuarios finales se encuentra en buen estado, además los cajetines donde se encuentran los jacks se encuentran etiquetados para conocer la ubicación de cada punto de datos al switch de acceso del piso.

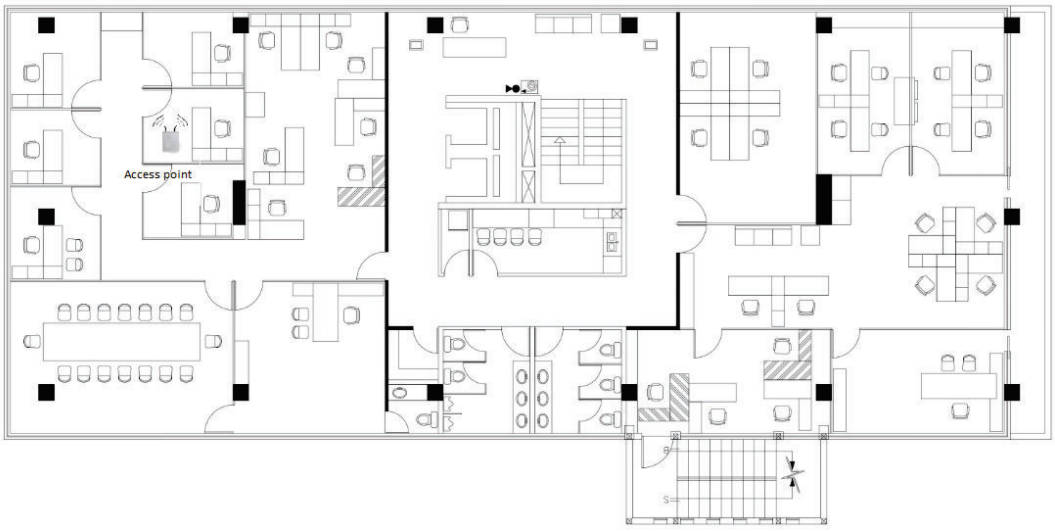

Figura 2.33. Ubicación actual access points Noveno Piso

2.23.3. EQUIPOS DE RED

En el gabinete de comunicaciones podemos encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 puertos
Switch	1	Cisco	2960-S 24 puertos
Access Point	1	SOPHOS	AP30

Tabla 2.13. Equipos de red Noveno Piso

2.24. SITUACIÓN ACTUAL DÉCIMO PISO

El décimo piso es dedicado a la Ministra y a sus colaboradores, se puede observar una mejor organización en las canaletas que se dirigen a los faceplates de los usuarios finales.

Se encuentran instalados dos switches de acceso marca Cisco, además de tres access point marca SOPHOS que cubren el área tanto del despacho como de los asesores. Cabe resaltar que el site survey realizado muestra una buena cobertura wireless en todo el piso.

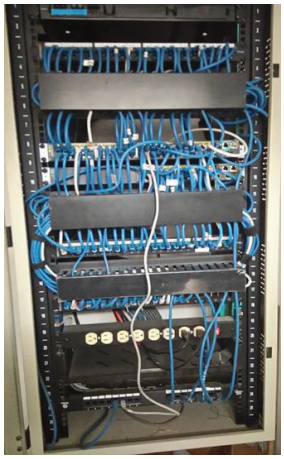

Figura 2.34. Estado del gabinete de comunicaciones Décimo Piso

El cableado en ciertas áreas del piso se encuentra mal organizado y fuera de la canaleta como se muestra en la siguiente figura:

Figura 2.35. Estado del cableado estructurado Décimo Piso

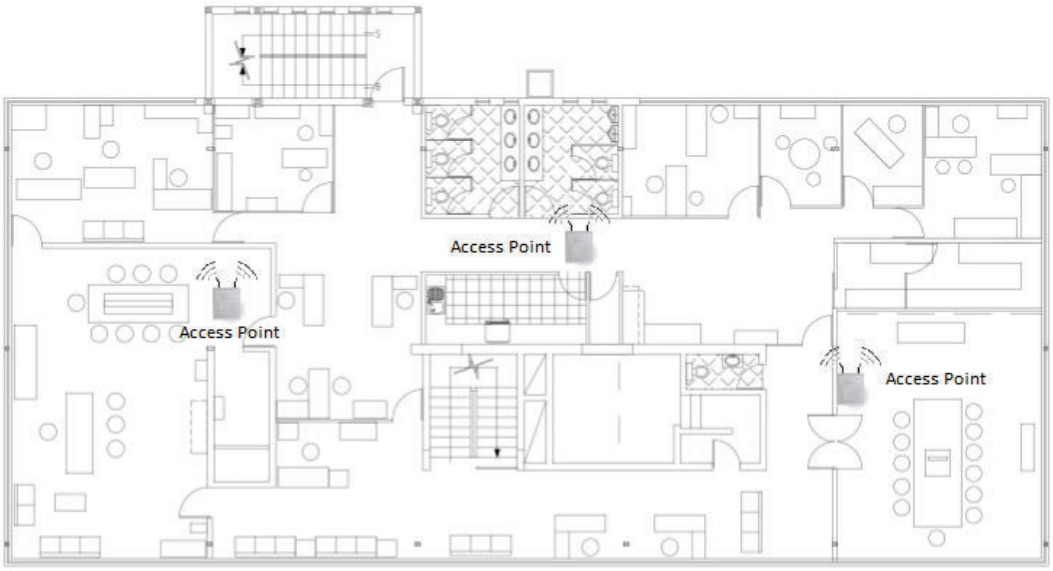

Figura 2.36. Ubicación actual access points Décimo Piso

2.24.1. ÁREAS DE TRABAJO DÉCIMO PISO

- Despacho Ministerial
- Salas de Asesores

2.24.2. CABLEADO ESTRUCTURADO DÉCIMO PISO

Falta organizar de mejor manera ciertos cables UTP que se encuentran fuera de los organizadores horizontales, pero persiste el problema de la falta de etiquetado en los cajetines donde se conectan los usuarios finales a los puntos de red, se puede observar que se improvisa el tendido de cableado estructurado a los usuarios finales sin seguir ninguna norma, no se coloca el cable UTP sobre las respectivas canaletas.

2.24.3. EQUIPOS DE RED

En el gabinete de comunicaciones se puede encontrar los siguientes equipos de red:

EQUIPO	CANTIDAD	MARCA	MODELO
Switch	1	Cisco	2960-S 48 puertos
Switch	1	Cisco	2960-S 24 puertos
Access Point	3	SOPHOS	AP30

Tabla 2.14. Equipos de red Décimo Piso

2.25. ANÁLISIS DE EQUIPOS DE INTERCONEXIÓN

El MIES presenta una variedad de equipos de interconexión que debido al crecimiento de la Institución han sido colocados para satisfacer las necesidades de conectividad de los usuarios, pero es necesario complementar dichos equipos con otros que cumplan los requerimientos para satisfacer las necesidades de los usuarios y brindar un buen servicio.

2.25.1. CARACTERÍSTICAS DE LOS EQUIPOS ACTUALES DE INTERCONEXIÓN

2.25.1.1. Switch de núcleo, Cisco 6509E

El switch de núcleo presenta las siguientes características:

- Contienen diversos tipos de interfaces para redes LAN, WAN y MAN.
- Número variable de puertos (desde 48 a 336 puertos Ethernet de 10/100/1000 Mbps)
- Velocidad de proceso de cientos de millones de paquetes por segundo que admiten múltiples enlaces gigabit y de 10 gigabit por segundo.
- Módulos Fast Ethernet (IEEE con 802.3af Power over Ethernet [PoE])
- Módulos de 10 Gigabit Ethernet
- Módulo de Servicios Firewall: Cada módulo a 4 Gbps y 100.000 conexiones por segundo, con inspección integrada hasta de capa 7.
- Multi-Gigabit servicios de los módulos (servicios de contenido, firewall, detección de intrusos, seguridad IP (IPSec), VPN, análisis de redes, y Secure Sockets Layer (SSL) aceleración.
- Doble fuente redundante de 3000 W.
- Supervisor Engine 720-3B, puerto de consola, puerto RJ-45 10/100/1000 Ethernet (con LED indicativo del link).
- Ejecuta protocolos: Spanning-Tree, Per VLAN Spanning-Tree, CDP y VTP.
- Maneja Protocolos y servicios: HTTP, Telnet, SNMP.

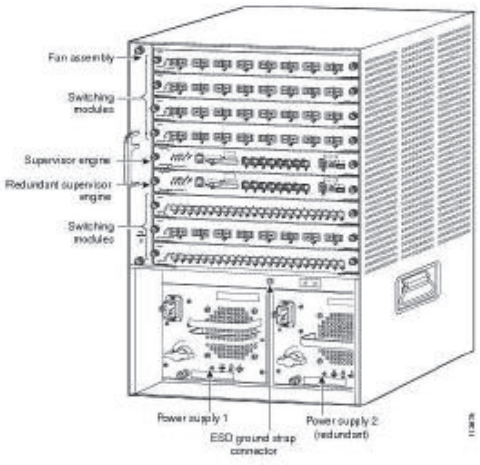

Figura 2.37. Esquema de hardware del switch Cisco Catalyst 6509[33]

2.25.1.2. Switch de acceso 3COM 4500 3CR17562-91 50 puertos

El switch de acceso presenta las siguientes características:

- Switch 3COM con puertos 10/100 Ethernet apilable y dos puertos Gigabit Ethernet.
- Capacidad de stack de hasta ocho switches.
- Los puertos Gigabit ofrecen selección de cobre o fibra: 1000Base-T (mediante RJ45), o 1000Base-X.
- Administrable mediante interfaz de línea de comando (CLI), o por medio del protocolo SNMP.
- Ofrece funcionalidades de Capa 2 y routing dinámico de Capa 3.
- Auto-negociación configurados como auto MDI/MDIX.
- Autenticación de usuario 802.1X.
- Fuente de alimentación integrada: Frecuencia de línea AC: 50/60 Hz, Tensión de entrada: 90-240 VAC, Corriente nominal: 1,0A máx.
- Estándares de IEEE: 802.1D (STP), 802.1p (CoS), 802.1Q (VLAN), 802.1w (RSTP), 802.1X (Seguridad), 802.3 (Ethernet), 802.3ad (Agregación de enlaces), 802.3ab (1000BASE-T), 802.3i (10BASE-T), 802.3u (Fast Ethernet), 802.3x (Control de flujo), 802.3z (Gigabit Ethernet).

[33] Figura tomada de: https://openaccess.uoc.edu/webapps/o2/bitstream/10609/28625/6/aobisTFC0114memoria.pdf

Figura 2.38. Switch 3COM 4500 3CR17562-91 50 Puertos[34]

2.25.1.3. Switch de acceso Cisco Catalyst 2960-S 48 puertos

- Trabaja con puertos Gigabit Ethernet (10/100/1000)
- Ofrece la tecnología Power over Ethernet Plus (PoE+)
- Permite realizar operaciones de switching de capa 2.
- Poseen de una fuente de alimentación fija con una fuente de alimentación externa redundante.
- Switches escalables y flexibles por medio del apilamiento que permite hasta 8 switches, brinda 80 Gbps de ancho de banda de apilamiento.
- Presenta una fuente de alimentación de 740 W, que puede alimentar la totalidad de los 48 puertos para PoE o los 24 puertos para PoE+. PoE.
- Switches son compatibles con NetFlow-Lite

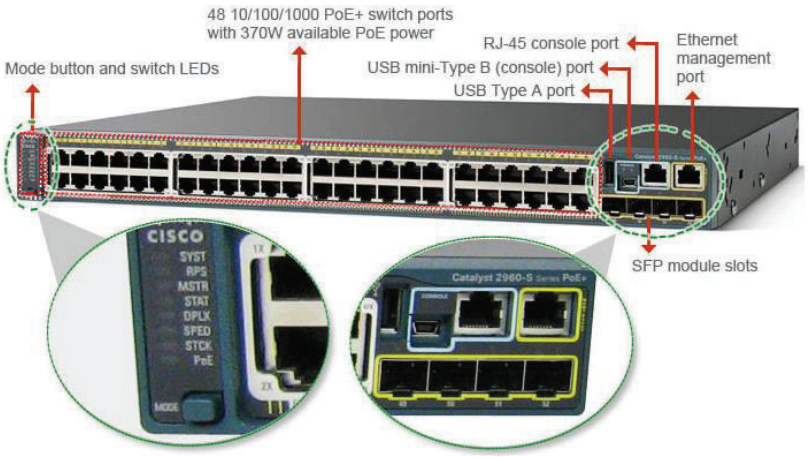

Figura 2.39. Switch Cisco Catalyst 2960-S 48 puertos[35]

[34] Información obtenida de: https://pcel.com/3Com-3CR17562-91-57888 https://pcel.com/3Com-3CR17562-91-57888

2.25.1.4. Switch de acceso DLINK Des-1008d 8 Puertos

- Conmutación Capa 2, no administrable.
- Presenta 8 puertos 10/100Mbps.
- Soporte full-dúplex y half-dúplex para cada puerto.
- Presenta control de flujo IEEE 802.3x.
- Porcentajes filtro/envío de los paquetes Ethernet: 14,880 pps por puerto.
- Soporta auto MDI/MDIX.

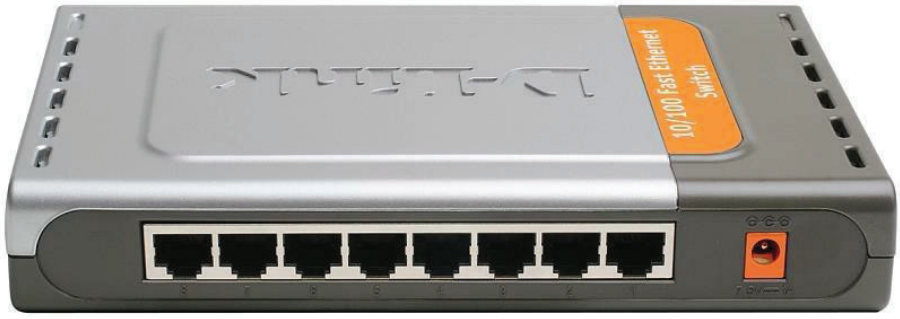

Figura 2.40. Switch Cisco Catalyst 2960-S 48 puertos[36]

2.25.1.5. Switch de acceso HP v1910-48G - 48 Puertos

- Switch administrable via: Web, CLI y SNMP.
- Presenta 48 puertos RJ-45 10/100/1000 de negociación automática (IEEE 802.3 tipo 10Base-T, IEEE 802.3u tipo 100Base-TX y cuatro puertos Gigabit SFP adicionales.
- Memoria Flash de 128 MB, tamaño de búfer de paquetes: 512 KB, RAM de 128 MB
- Capacidad de encaminamiento/conmutación
- Interfaz de línea de comandos limitada; Navegador de Web; Administrador de SNMP
- Voltaje de entrada: De 100 a 240 V CA

---

[35] Información obtenida de: http://www.router-switch.com/ws-c2960s-48lps-l-p-1513.html
[36] Información obtenida de: http://articulo.mercadolibre.com.ve/MLV-460223099-switch-de-8-puertos-dlink-des-1008d-10100-mbps-zonawifimcy-_JM

- enrutamiento estático de nivel 3, listas de control de acceso para una seguridad mejorada, VLAN de voz automática, asignación de prioridades de tráfico QoS, LLDP, protocolos Spanning Tree y Power over Ethernet.

Figura 2.41. Switch HP v1910-48G - 48 Puertos[37]

2.25.1.6. Switch de acceso LINKSYS SR224 DE 24 Puertos

- Posee 24 puertos Ethernet 10Base-T, Ethernet 100Base-TX.
- Modo comunicación: Half dúplex, Full duplex.
- Trabaja con normas: IEEE 802.3, IEEE 802.3u.
- Alimentación externa de 12.5 W.

Figura 2.42. Switch LINKSYS SR224 24 puertos[38]

2.25.1.7. Switch de acceso TPLINK TL SG1008d

- Posee 8 puertos Gigabit Ethernet.
- Soporta control de flujo IEEE 802.3x en modo Full Duplex.
- Presenta un conector RJ-45 y detección automática de velocidad.

---

[37] Imagen obtenida de: http://www.solucionesxiomel.com/prestashop/home/232-switch-administrable-hp-1920-48g-poe-370w-gigabit-48-puertos-poe-capa-2-4-puertos-sfp-jg928a.html

[38] Imagen obtenida de: http://computacion.mercadolibre.com.ve/switches-y-hubs/switch-cisco-sr224-24-puertos-10%2F100

- Soporta MDI/MDIX de forma automática.
- Presenta un buffer de 2 MB, con una capacidad de conmutación de 16 Mbps.
- El consumo máximo es de 4,63W.

Figura 2.43. Switch TP-LINK TL-SG1008D[39]

2.25.1.8. Access Point AP 30

- Una Interfaz LAN de 10/100 Base-TX.
- Soporta los estándares: 802.11 b/g/n.
- 3 antenas internas direccional de 2.4 GHz
- Fuente de poder de 100-240 VAC, 50/60 Hz, max. 0.5 A
- Número máximo de usuarios: 30, a una velocidad de 300 Mbps.

Figura 2.44. Access point SOPHOS AP 30[40]

[39] Imagen obtenida de: http://www.tp-link.es/products/details/cat-4763_TL-SG1008D.html
[40] Imagen obtenida de: https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophosutm220dsna.aspx

2.25.1.9. Firewall SOPHOS UTM 525

Equipo de gestión de seguridad que, que cuenta con las siguientes características: cortafuegos, antivirus, VPN SSL, VPN IPsec, IPS, Filtrado WEB, Control de aplicaciones, protección email y controlador inalámbrico. También cuenta con una administración centralizada.

Actualmente posee la licencia de protección básica que presenta las siguientes características:

	BasicGuard
Moduly – vyberte si ty potřebné	
Essential Firewall - Free Network Firewall, NAT, Native Windows Remote Access	Completo
Network Protection IPSec/SSL, ATP, VPN, IPS, DoS Protection	Básica
Web Protection URL Filtering, Application Control, Dual Engine Antivirus	Básica
Email Protection Anti-spam, Email Encryption and DLP, Dual Engine Antivirus	Básica
Wireless Protection Wireless Controller, Multi-SSID Support, Captive Portal	Básica
Webserver Protection Web Application Firewall, Reverse Proxy, Antivirus	-
Endpoint Protection Antivirus, HIPS, Device Control	Optativa

Tabla 2.15. Licencia UTM SOPHOS 525 actualmente instalada[41]

Las principales características del firewall SOPHOS UTM son las siguientes:

Dispositivo de Hardware	UTM 525
Rendimiento del firewall	23 Gbps
Rendimiento de la VPN	4.2 Gbps
IPS throughput	8.8 Gbps
Antivirus throughput	1.7 Gbps
Conexiones concurrentes	4.5 millones
Interfaces Ethernet de cobre	8

[41] Información obtenida de: https://www.sophos.com/es-es/medialibrary/PDFs/factsheets/sophosutmoverviewdsna.pdf?la=es-ES

Interfaces Ethernet SFP	8

Tabla 2.16. Licencia UTM SOPHOS 525 actualmente instalada

2.25.1.10. Central Telefónica AVAYA IP OFFICE 500

Central telefónica que presenta desde 8 hasta 384 extensiones y 240 Líneas en un solo procesador, permite formar una red de comunicaciones con hasta 500 usuarios, presenta las siguientes características:

- Buzón de voz con mensaje personalizado por usuario.
- 4 módulos internos de 2 ó 8 extensiones analógicas.
- Soporta hasta 8 E1 (240 líneas) y hasta 128 canales en troncales SIP.
- Soporta administración WEB.

Figura 2.45. Central Telefónica AVAYA IP Office 500[42]

2.26. ANÁLISIS DE REQUERIMIENTOS

En base a la situación actual del MIES y al levantamiento de información realizado es necesario realizar cambios en la infraestructura física como lógica de la red, optimizando los recursos que actualmente posee el MIES, pensando en satisfacer las necesidades de los usuarios finales.

A continuación se presentan los requerimientos para el rediseño de la red del MIES integrando voz, datos y video:

[42] Imagen obtenida de: http://www.ip-office.es/

2.26.1. CABLEADO ESTRUCTURADO

Como se pudo observar en el levantamiento de información el cableado estructurado es una parte crítica de la actual infraestructura de red del MIES, ya que se ha instalado sin seguir las normas y estándares contemplados en ANSI/EIS-TIA, además de no presentar un correcto etiquetado para administrar la red y el tendido del cableado hacia los usuarios finales sin organizarlo en canaletas.

Para la infraestructura nueva de red del MIES se requiere lo siguiente:

- Mejorar el backbone de la actual infraestructura de red, ya que solo se presenta un hilo de fibra óptica conectado por piso de los dos hilos que posee cada piso.
- Los gabinetes de comunicaciones deben presentar mejor seguridad para que solo los administradores de red tengan acceso a los equipos de red.
- Mejorar el etiquetado tanto en los switches de acceso como en los patch panels.
- Mejorar la instalación de los equipos de red tanto en los gabinetes de comunicaciones como en el data center.
- Mejorar la climatización de los gabinetes de comunicaciones donde se encuentran los equipos de red para evitar exceso de temperatura donde los equipos no trabajan en condiciones normales.
- Mejorar la instalación de puntos de red para los usuarios finales basándose en normas de cableado estructurado.
- Mejorar el área donde se encuentran los gabinetes de comunicaciones, evitando utilizar el área como bodega de cada piso.

2.26.2. LAN

PARA LA LAN DEL MIES SE REQUIERE LO SIGUIENTE:

- Mejorar el equipamiento de equipos de red, principalmente los switches de acceso que no son administrables.
- Implementar redundancia en la red del MIES para evitar caídas de servicio al momento de falla de uno de los equipos.

- Implementar políticas de seguridad tanto en la red pasiva, equipos activos y usuarios finales.
- Incrementar equipos de red que complementen los actuales pensando en un crecimiento de la Institución.

2.26.3. CENTRAL TELEFÓNICA IP

La central telefónica IP que posee actualmente la institución fue instalada en el año 2013, se tenía una central 3COM la cual presentaba limitadas extensiones asociadas al chasis del equipo, por lo cual la Institución optó por integrar una nueva central telefónica, AVAYA Office 500, la cual amplió la cantidad de extensiones complementando las que tenía la central 3COM. En total las dos centrales telefónicas cuentan con 554 extensiones telefónicas: 384 extensiones la central AVAYA y 170 extensiones la central 3COM, lo cual es suficiente para la cantidad de usuarios que requieren el servicio de telefonía y pensando en un crecimiento a 5 años.

Por lo cual no se tomará en cuenta en el rediseño la inclusión de una nueva central telefónica.

2.26.4. VIDEOVIGILANCIA

Cada piso del edificio del MIES desde la planta baja al décimo piso cuenta con dos cámaras de vigilancia, la primera colocada en la entrada de los ascensores y la segunda en el pasillo principal al lado de las gradas, en los subsuelos se cuenta con dos cámaras de video una colocada en el estacionamiento y la siguiente en la entrada a cada estacionamiento.

No es necesaria la colocación de una mayor cantidad de cámaras de seguridad ya que las cámaras que actualmente se encuentran instaladas cubren las necesidades de cobertura del edificio.

CAPÍTULO 3

REDISEÑO DE LA RED DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL (MIES)

3.1. INTRODUCCIÓN

El Ministerio de Inclusión Económica y Social (MIES) cuenta actualmente con una infraestructura de red física que no cumple con ningún estándar tanto de cableado estructurado como de un modelo de red escalable.

Además no se tuvo la planificación necesaria del crecimiento de usuarios y por ende la infraestructura de la red, ya que se han realizado varios cambios en la estructura organizacional del MIES, a tal punto que se mantuvo la infraestructura de red desde que se llamó Ministerio de Bienestar Social hasta el actual Ministerio de Inclusión Económica y Social (MIES).

Como parte de la reestructuración del MIES, el presidente de la República, Rafael Correa firmó el Decreto Ejecutivo Nro. 1356, con el cual dispone que, el Instituto de la Niñez y la Familia (INFA) y el Programa de Protección Social (PPS) se integren al Ministerio de Inclusión Económica y Social (MIES).

3.1.1. NÚMERO DE USUARIOS ACTUALES

El Ministerio de Inclusión Económica y Social ha presentado varios cambios estructurales y organizacionales en los últimos años, lo que ha llevado a que su red presente inconvenientes tanto en la administración como en la parte física y lógica, entre los principales inconvenientes que presenta la red del MIES se pueden indicar los siguientes:.

- El cableado estructurado no fue diseñado correctamente para el crecimiento que ha tenido el Ministerio.
- Se han colocado nuevos puntos de datos sin ninguna planificación ni organización, de tal manera que la mayoría del cableado de los nuevos puntos no pasan por ninguna canaleta.

- Tanto los cuartos de telecomunicaciones como los gabinetes de comunicaciones no se encuentran ubicados en sitios aptos para su correcto funcionamiento.
- El montaje de los access point principalmente los que se encuentran en el quinto piso no es el correcto, los access point deben ser colocados en el techo para que su lóbulo de radiación permita la mayor cobertura posible a los usuarios, pero como se puede verificar los access point se encuentran sobre escritorios o sobre cartones donde no se aprovecha las características de irradiación del equipo.
- La organización del cableado en los gabinetes de comunicación en la mayoría de los pisos del edificio dificulta la administración de los equipos de red, además de que no existe el respectivo etiquetado tanto en los switches como en los patch panels.
- No existe un sistema de disipación de calor en los gabinetes de comunicaciones, por lo que los equipos presentan una temperatura superior a la normal y esto puede provocar un mal funcionamiento de los mismos hasta el punto de daño.
- EL direccionamiento de las VLAN no se lo realizó de acuerdo a una cantidad estimada de usuarios ni a su crecimiento, cada piso presenta una VLAN diferente con una máscara de red clase C (255.255.255.0), es necesario realizar un subneteo de la red para distribuir de mejor manera el direccionamiento por cada VLAN.
- En la topología de red del Ministerio no se presenta alta disponibilidad en los equipos, ni redundancia en los enlaces, por lo que si se presenta la caída de un equipo de acceso todos los usuarios y switches conectados en cascada a dicho switch se quedarían sin servicio tanto de Internet como servicios de navegación.

Los inconvenientes presentados se deben en parte a los cambios estructurales del Ministerio como también a una mala planificación de la red actual, sin tomar en cuenta el crecimiento en el número de usuarios finales, además de soluciones que se consideraron temporales para cubrir requerimientos de acceso a la red pero hasta el momento no se realizaron los cambios respectivos para remediar

estos inconvenientes y se deriva de esto problemas en la red tanto físicos como lógicos y de administración.

Actualmente el Ministerio de Inclusión Económica y Social cuenta con trescientos noventa y tres usuarios en las instalaciones , de los cuales hace uso de la red tanto cableado como inalámbrica, además utilizan los servicios que brinda la LAN y dependiendo de los permisos que tienen realizan consultas y modificaciones a los servidores que se encuentran en la DMZ.

3.2. REESTRUCTURACIÓN DE LA RED DEL MIES

3.2.1. INTRODUCCIÓN

Se realiza el rediseño de un Sistema de Cableado Estructurado para la Matriz del Ministerio de Inclusión Económica y Social para superar las dificultades que se tienen con el actual sistema. En base a las observaciones realizadas a la actual infraestructura se han evidenciado los problemas que experimenta el actual sistema de cableado estructurado y se ha determinado que es necesario realizar un rediseño para cubrir las necesidades que se presentan actualmente y prever un correcto funcionamiento de éste en un plazo de entre 10 y 15 años con las características que permitan obtener el rendimiento más óptimo.

3.2.1.1. Antecedentes

- El Sistema de cableado estructurado usado actualmente en la Matriz del Ministerio de Inclusión Económica y Social no cumple con las normas necesarias para asegurar su correcto funcionamiento y desempeño. Se ha podido evidenciar que algunos factores han hecho de esta infraestructura un sistema poco fiable, entre las que se puede destacar:
- El sistema de cableado estructurado muestra señales de descuido y daño en varios puntos por varios cambios dentro de cada uno de los pisos de la institución.
- No existe uniformidad respecto al sistema de cableado estructurado actual. Se puede evidenciar la diferencia entre los puntos instalados por un proveedor y otros puntos instalados posteriormente desordenadamente. De

la información recibida por parte del personal de TI, se sabe que estas instalaciones se hacían sin coordinación por parte de otras dependencias de la institución. Por este motivo no existe una documentación ni las pruebas que certifiquen los puntos de red más recientes, ni se puede asegurar el uso de una sola categoría de los componentes instalados.

- No se dimensionó adecuadamente el cableado acorde a la cantidad de personal que labora en la institución. La cantidad de puntos de red es insuficiente en varios pisos, por lo que se han insertado conmutadores y equipos inalámbricos para aumentar la cobertura de la red, incluso sin coordinación con el área de Gestión Tecnológica. Los cambios de personal y de funciones dentro de la institución siguen siendo considerables, por lo que se debe revisar los espacios tengan la adaptabilidad a estas nuevas situaciones.
- Se han realizado cambios dentro de la infraestructura dentro del edificio sin considerar el recorrido del cableado, perjudicando varios puntos de red al punto de dejarlos completamente dañados e inutilizables. Aún en la actualidad se hacen cambios en los pisos sin medir claramente las consecuencias en el sistema de cableado estructurado.
- Algunos cambios de la infraestructura del edificio han dejado a la misma infraestructura de cableado como un obstáculo no previsto que requiere volver a hacerse

3.2.1.2. Consideraciones

Todas las circunstancias descritas anteriormente conllevan a realizar un rediseño del sistema de cableado estructurado desde el principio, teniendo presentes las consideraciones que permitan que la nueva instalación no tenga los mismos inconvenientes. Para ello se ha realizado las siguientes observaciones:

- Considerar el incremento de usuarios en cada piso en función los posibles espacios que éstos puedan ocupar. Si bien se considera el incremento en los sistemas de cableado estructurado como un espacio adicional en la canalización para instalar nuevos puntos de red cuando sea necesario, se utilizará el criterio de instalar puntos adicionales y/o salidas de

telecomunicaciones multiusuarios (MUTOA) donde se considere que el espacio puede ser requerido para el trabajo del personal de la institución.

- Realizar el enrutamiento de la nueva instalación cableado por espacios que sean permanentes, evitando paredes falsas o separadores de cubículos que puedan ser cambiados a corto plazo con el fin de asegurar que la nueva instalación no se dañe en caso de que haya cambios dentro de la institución. En este sentido se ha tomado las paredes extremas del edificio y paredes fijas como las rutas principales, dando mayor protagonismo el extremo noreste del edificio para este propósito.
- El análisis y diseño de cableado estructurado contempla solamente la Planta baja y los pisos del 1 al 8. No se consideraron los pisos 9 y 10 para el rediseño porque la información al respecto es restringida por seguridad del ministerio. Los datos proporcionados por el personal de Dirección Tecnológica indican que estos pisos fueron levantados hace pocos años, y que se consideraron en su momento el diseño incluyendo cuartos de telecomunicaciones y cableado para el personal destinado a trabajar en dichas áreas. Debido a que se encuentran personas altos mandos el número de usuarios es relativamente pequeño y el dimensionamiento actual contempla su funcionamiento en el presente y el futuro.
- En el presente rediseño se usará cable UTP y demás componentes para el sistema de cableado estructurado con categoría 6A, cuyas características permiten trabajar con un ancho de banda de 500 MHz y alcanzar la velocidad de transmisión de 10 Gbps. El rediseño se acoge a la norma ANSI EIA/TIA 568-C.0.
- Se ha sacado provecho de algunos componentes del actual sistema de cableado estructurado para su reutilización con el fin de disminuir costos alterar en la menor medida de lo posible los espacios que se usan actualmente por parte del personal de la institución. No todos los subsistemas del cableado estructurado tienen problemas. En este caso los problemas tienen mayor relevancia con el cableado horizontal y las áreas de trabajo.

3.2.1.3. Distribución de puntos actual de red

La Matriz del Ministerio de Inclusión Económica y Social se encuentra conformada por once plantas (incluyendo la planta baja) y dos pisos en el subsuelo. Los servicios de la red llegan únicamente a las plantas superiores a través de un sistema de cableado estructurado en topología de estrella. El cuarto de equipos donde se concentran las conexiones del sistema de cableado estructurado se encuentra en el quinto piso. En cada piso se encuentra un gabinete de telecomunicaciones que contiene las terminaciones del cableado horizontal que se extiende hacia las estaciones de trabajo de cada área organizativa de cada piso conformada por varias personas.

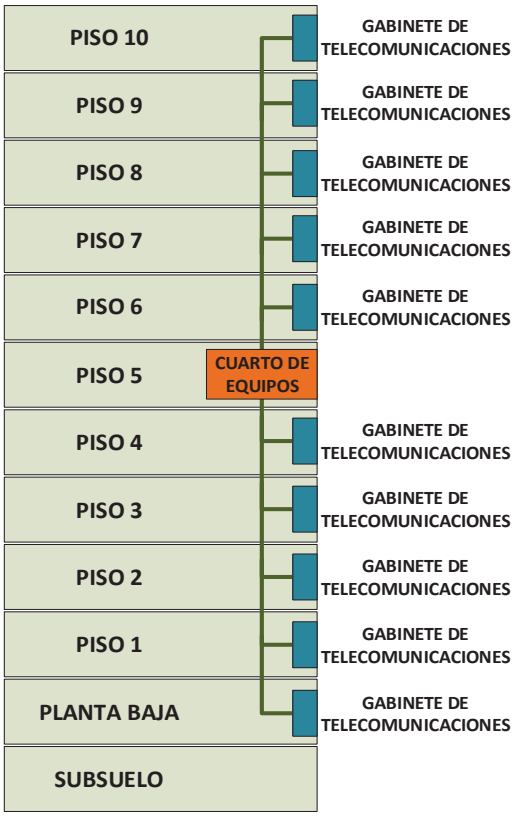

Figura 3.1. Distribución de cuarto de equipos y gabinete de telecomunicaciones en el edificio del MIES

Normalmente el número de usuarios puede variar relativamente rápido, pero el número de estaciones de trabajo y los dispositivos que se conectan a la red a través de estos puntos gozan de una mayor estabilidad numérica. La tabla

anterior describe la cantidad de puntos por piso. Cabe aclarar que algunos de estos puntos se encuentran a medio camino con conmutadores que permiten que uno o más usuarios puedan acceder a la red.

PISO	Estaciones de trabajo	Teléfonos	Impresoras y otros equipos de red	Access Points	Cámaras
Planta Baja	28	20	3	2	4
Piso 1	38	27	6	1	2
Piso 2	40	28	2	1	2
Piso 3	35	25	2	1	2
Piso 4	34	24	2	0	2
Piso 5	25	18	2	2	2
Piso 6	49	34	6	1	2
Piso 7	35	25	5	1	2
Piso 8	49	34	4	1	2
Piso 9	45	32	-	1	2
Piso 10	15	11	-	3	2

Tabla 3.1. Número de equipos finales por piso

Adicionalmente se debe aclarar que se tiene un solo punto de red por usuario en la gran mayoría de los casos. Los teléfonos se usan como puentes entre el punto de red y el computador del usuario. No todos los usuarios disponen de teléfono, lo que evidencia que el número de estaciones de trabajo sea mayor que el de teléfonos.

3.2.2. REDISEÑO DE LA RED PASIVA

3.2.2.1. Áreas de trabajo

En función de las actividades de cada usuario se contemplan para los espacios de cada usuario al menos dos salidas de telecomunicaciones para satisfacer la

necesidad de datos y telefonía. El esquema que se ha manejado hasta el momento ha permitido que los usuarios con teléfonos IP puedan conectarse a un solo punto de red utilizando al dispositivo como puente, logrando que la estación de trabajo pueda conectarse a la red. Sin embargo se debe considerar que estos equipos limitan la velocidad de conexión de la estación de trabajo dependiendo de sus características (por ejemplo cuando se conecta un teléfono que transmite a 100 Mbps cuando el punto de red maneja velocidades de transmisión de 1 Gbps o 10 Gbps), además limita la adquisición de modelos de teléfonos que permitan trabajar como puentes con mayores costos añadidos, y aún más costosos para que se ajusten a la velocidad de transmisión de la red. Estos inconvenientes se superan destinando una salida de telecomunicaciones para el dispositivo de telefonía.

La distribución de las estaciones de trabajo en los pisos varía considerablemente dependiendo del área organizativa que trabaja en cada piso, por este motivo el número de usuarios no es uniforme; mientras en unos pisos existe alguna holgura en el espacio de trabajo en otros hay muchos usuarios trabajando uno muy cerca del otro hasta donde es permisible el espacio. Se han notado casos de áreas destinadas a los usuarios convertidas en bodegas o archivos y viceversa en el transcurso del tiempo, por lo tanto se integrará en el nuevo diseño los puntos de red necesarios para que las áreas puedan ser usadas por usuarios en caso de que dejen de usarse en otros propósitos. Esto lleva a que en cada piso haya una distribución única de cableado estructurado. La distribución de las paredes que dividen las áreas en cada piso también es diferente. Un único diseño no basta para cubrir las necesidades de todos los pisos.

La cantidad de crecimiento de usuarios de la red se encuentra contemplada en función del espacio disponible por piso que puede ser ocupado a futuro. De la experiencia obtenida relacionada a la cantidad de usuarios se ha determinado que existe una gran rotación de personal y un incremento gradual de usuarios, lo que ha obligado a hacer constantes cambios en la distribución de cada piso.

Se destinarán salidas dobles en los espacios no ocupados donde se estima que un nuevo usuario puede integrarse y se dedicará una toma simple en los espacios donde se ha determinado que los usuarios requieren de otros dispositivos como

impresoras, copiadoras, escáner, proyectores, etc. Estos espacios están en función de las necesidades previstas por cada área administrativa.

3.2.2.1.1. Configuración de los conectores

Las salidas de telecomunicaciones se ubicarán en tomas de pared (simples y dobles) junto a las estaciones de trabajo, a 40 cm sobre el nivel del suelo.

Las tomas estarán compuestas por cajetines sobrepuestos en la pared, las terminaciones del cableado horizontal en jacks keystone 110-RJ45 y face plates de una o dos salidas para acoplar los jacks según corresponda.

Los cajetines tendrán un espacio adecuado para colocar las etiquetas que permitan identificar cada salida de telecomunicación con respecto al estándar EIA/EIA 606A.

Las estaciones de trabajo se conectarán a las tomas o puntos de red utilizando patch cords de 7 pies (2.13 m), a menos de que se encuentren a una distancia más alejada, en cuyo caso no deberá sobrepasar los 20 m.

La disposición de los hilos para cada cable UTP se realizará como se indica en las normas ANSI EIA/TIA 568-A y 568-B.

3.2.2.1.2. Cableado por zona

La distribución de algunas estaciones de trabajo alejadas de los puntos de red requiere que se concentren salidas de telecomunicaciones en sus proximidades con el fin de otorgar la flexibilidad necesaria. Para este propósito se han dispuesto de salidas de telecomunicaciones multiusuarios (MUTOA) en los puntos donde se aglutinan las estaciones de trabajo existente o donde se prevé que se dispondrán nuevas estaciones de trabajo.

En casi todos los casos se ha dispuesto que se dé servicio a cuatro estaciones de trabajo mediante el uso de MUTOA, con excepción de una salida de seis salidas, en cualquier caso se encuentra por debajo de las 12 salidas máximas permitidas.

Las distancias de los patch cords extendidos desde las MUTOA hacia las estaciones de trabajo no sobrepasan los 20 metros. Los cables se colocarán en

canaletas para piso en el trayecto comprendido entre la MUTOA y la estación de trabajo.

3.2.2.1.3. Dimensionamiento

La cantidad de puntos en función de las salidas de telecomunicaciones y el crecimiento respecto a la cantidad de puntos actuales se muestra en la siguiente tabla:

Tomas dobles para estaciones de trabajo	Puntos de red simples (impresoras, etc.)	Access Points	Cámaras	MUTOAs	Total de puntos previstos	% de crecimiento
40	12	2	4	2	110	42,86
46	18	3	3	2	111	21,05
46	10	2	3	2	107	15,00
51	6	3	3	2	116	45,71
49	14	2	3	3	119	44,12
33	22	3	3	1	94	32,00
61	13	2	3	2	137	24,49
44	14	3	3	2	108	25,71
55	15	2	3	3	142	12,24

Tabla 3.2. Número de salidas de telecomunicaciones previstas

El diseño de los puntos de red por piso se encuentra en el anexo 36.

3.2.2.2. Cableado horizontal

El subsistema de cableado horizontal es la parte del sistema de cableado que une las salidas de telecomunicaciones de las áreas de trabajo con el gabinete de telecomunicaciones (en este caso) de cada piso.

La conexión de cada punto de red con el gabinete de telecomunicaciones por medio del cableado horizontal define una topología de estrella.

Según la norma ANSI EIA/TIA 568-C.1 se limita la longitud máxima que puede tomar el recorrido del cableado horizontal a 90 metros. En el caso del diseño del cableado para la Matriz del Ministerio de Inclusión Económica y Social se ha determinado que la distancia máxima es de 72 metros, correspondiente a una

toma doble de telecomunicaciones para una estación de trabajo ubicada en el segundo piso.

3.2.2.2.1. Cálculo de la cantidad de cable

Para el cálculo de rollos de cable necesario para cada piso se deberán considerar las distancias más largas y más cortas de cada uno respectivamente. Adicionalmente se requiere conocer la cantidad de puntos de red presentes en cada piso. A continuación se realizará como ejemplo el cálculo de los rollos de cable para el primer piso:

1. Mediante los datos del diseño en el plano se determina el punto de red más cercano al gabinete dmin y el más lejano dmax respectivamente, además de la cuenta de salidas de telecomunicaciones (p). En este caso los datos son:

$$d_{min} = 3.50\ m$$

$$d_{max} = 62\ m$$

$$p = 110\ salidas$$

2. Determinar la distancia media dp en función de las distancias encontradas en el paso anterior:

$$d_p = \frac{3.50 + 62}{2}\ m$$

$$d_p = 32.75m$$

3. Añadir un valor del 10% para holgura D a la distancia promedio encontrada en el paso anterior:

$$D = 32.75 \times 1.1\ m$$

$$D = 36.03\ m$$

4. Calcular el número de corridas por rollo cr como la división entre la longitud total del cable que contiene un rollo (305 m) y la distancia promedio con holgura D del paso anterior. Aproximar el resultado al valor entero inferior:

$$cr = \frac{305\ m}{D}$$

$$cr = \frac{305\ m}{36.03\ m}$$

$$cr = 8.46\ \approx 8\ corridas\ por\ rollo$$

5. Con el número de corridas por rollo calcular la cantidad de rollos de la división entre el número de salidas de telecomunicaciones p y el número de corridas cr. El valor obtenido debe aproximarse al entero superior:

$$Rollos = \frac{p}{cr}$$

$$Rollos = \frac{110\ puntos}{8\ corridas\ por\ rollo}$$

$$Rollos = 13.75 \approx 14\ rollos$$

En el presente ejemplo se obtuvo el valor de 14 rollos de cable para el caso del primer piso. En la siguiente tabla se detallan estos valores para todos los pisos:

PISO	DISTANCIA MÍNIMA	DISTANCIA MÁXIMA	DISTANCIA MEDIA	DISTANCIA MEDIA +10%	NUMERO DE PUNTOS DE RED	CORRIDAS POR ROLLO	ROLLOS DE CABLE
PB	3,50	62,00	32,75	36,03	110	8	14
P1	3,50	62,00	32,75	36,03	111	8	14
P2	4,75	72,00	38,38	42,21	107	7	16
P3	4,20	60,50	32,35	35,59	116	8	15
P4	4,00	66,50	35,25	38,78	119	7	17
P5	6,50	66,50	36,50	40,15	94	7	14
P6	4,60	67,00	35,80	39,38	137	7	20
P7	5,50	61,00	33,25	36,58	108	8	14
P8	4,80	61,50	33,15	36,47	142	8	18

Tabla 3.3. Cantidad de rollos por piso

3.2.2.2.2. Enrutamiento horizontal

Se considera dentro de la norma TIA/EIA 569, y se define por todos los elementos que sean necesarios para poder distribuir el cableado en el mismo piso. En las instalaciones de la Matriz del MIES deben considerarse los siguientes aspectos para la decisión de los elementos a utilizar:

- No se dispone de cielo raso y la altura de cada piso no es apropiada para instalar cielo falso, en caso de instalar escalerillas quedarían visibles y expuestas.

- En este espacio se encuentran las lámparas, por lo que debe evitarse en lo posible que las rutas para el cableado atraviesen el techo por cualquier sitio. Se puede encaminar la instalación por lugares que no interrumpan con las luminarias ni otros dispositivos instalados en el techo como sensores de humo o de movimiento.
- El uso de canaleta es la mejor opción, porque la densidad de usuarios es relativamente baja, la ubicación es permanente y no se requiere más flexibilidad que la que ofrecen las MUTOAs. Los puntos dispuestos en el diseño se encuentran relativamente cerca y las distancias no llegan a más de 72 metros.

La mejor opción para la ruta del cableado horizontal es bordear en cada piso todas las instalaciones y estaciones de trabajo. Las canaletas no deberán obstaculizar puertas y accesos, y deberán establecerse sobre paredes fijas evitando paredes falsas o paredes temporales que limitan las oficinas para asegurar de la mejor manera que no se retiren junto con el cableado realizado en algún momento en que se reorganicen las áreas administrativas de cada piso. La posición en la parte inferior de la pared es la más apropiada debido a que la parte superior se compone de ventanas que llegan a la altura del techo.

3.2.2.2.3. Calculo de canaletas

En este punto se calcularán el número de canaletas a usarse en función de las dimensiones que éstas tienen y su relación con el área transversal de los cables que ocuparán este espacio. Las consideraciones de la norma EIA/TIA 569-A establecen que los conductos por donde se extiende el cableado horizontal debe llenarse entre el 30% al 60% de su capacidad en función del radio de curvatura del conductor, por lo que sólo debe usarse un porcentaje de su capacidad real.

Para el presente diseño de la instalación del cableado estructurado se ha considerado un crecimiento en promedio del 30% a nivel global considerando los puntos adicionales de cableado, por lo que el área usada será del 60% para la práctica.

Así, por ejemplo, una canaleta de 100mm x 45mm tiene una superficie de 4500 mm2 y un cable UTP categoría 6A de 9mm tiene una superficie de 63.62mm2. El

resultado de dividir la superficie de la canaleta para la del cable nos da como capacidad un total de 70 cables. El 60% de la capacidad calculada corresponde a un total de 42 cables.

La siguiente tabla muestra la capacidad de las canaletas considerando un 60% de llenado:

ALTO [mm]	ANCHO [mm]	SUPERFICIE [mm^2]	60% DE LA SUPERFICIE [mm^2]	CANTIDAD DE CABLES UTP 6A
100	45	4500	2700	42
60	40	2400	1440	22
40	25	1000	600	9
32	12	384	230,4	3
20	12	240	144	2

Tabla 3.4. Cantidad de cables UTP cat. 6A para distintos tamaños de canaleta al 60% de capacidad

La siguiente tabla enumera la cantidad de canaletas, uniones, derivaciones para la implementación del cableado horizontal en función del diseño.

Cada canaleta cubre una distancia de dos metros. El primer valor corresponde al número de canaletas, el segundo a las uniones y el tercero a las derivaciones:

PISO	100x45mm			60x40 mm			40x25 mm			32x12 mm			20x12 mm		
PB	46	2	12	28	7	9	21	9	2	0	0	0	13	0	2
P1	36	10	5	27	3	12	20	1	1	5	1	0	6	1	1
P2	35	10	5	27	3	12	20	1	1	5	1	3	6	1	1
P3	38	11	6	30	4	14	22	2	2	6	2	1	7	2	2
P4	39	12	7	31	5	15	23	3	3	7	3	2	8	3	3
P5	31	10	6	25	4	12	19	3	3	6	3	2	7	3	3
P6	46	15	9	37	6	18	28	5	5	9	5	1	11	5	5
P7	37	12	8	30	5	15	23	4	4	8	4	2	9	4	4

P8	49	16	11	40	7	20	31	6	6	11	6	4	12	6	6

Tabla 3.5. Cantidad de canaletas, uniones y derivaciones para implementación de cableado horizontal

3.2.2.3. Cableado Vertical (Backbone)

Corresponde al subsistema de cableado estructurado que permite la conexión de los gabinetes de telecomunicaciones con el cuarto de equipos, además de permitir la entrada de servicios desde la acometida.

En la instalación actual se dispone de un backbone de fibra de dos hilos que parte de cada piso hacia el cuarto de equipos. Para el propósito de brindar conexión a cada piso sólo se hace uso de una fibra, la segunda se encuentra como respaldo ante un daño en la principal. La instalación de backbone se encuentra en buen estado, por lo que se reutilizará para la implementación del nuevo sistema de cableado estructurado.

3.2.2.3.1. Medio utilizado

La fibra óptica utilizada es multimodo tipo OM3 50/125um. La velocidad de transmisión que soporta este medio es de 10 Gbps, con una distancia máxima de 300 m de longitud. Al disponer de dos hilos de fibra óptica por piso, se prevé aumentar a dos hilos por cada switch de acceso que se encuentre en el Gabinete de telecomunicaciones.

El número de equipos por gabinete de telecomunicación es de 3 por piso, quedando como resultado la cantidad de 6 hilos por piso. El total de hilos que se concentrarán en el cuarto de equipos es de 60.

3.2.2.3.2. Enrutamiento vertical

La ruta que toman los hilos de fibra óptica que conforman el backbone comprende una canalización en conduit en el extremo noreste del edificio de la Matriz del Ministerio de Inclusión Económica y social. La ubicación de los gabinetes de telecomunicaciones de encuentran en el trayecto del backbone, lo que facilita que ingresen a los gabinetes de manera segura. Las terminaciones se implementarán con conectores de tipo LC.

Los extremos del backbone que se agrupan en el cuarto de equipos se canalizan mediante una tubería metálica hasta alcanzar el rack de telecomunicaciones. El rack se ubica aproximadamente en el centro geométrico del cuarto de equipos.

3.2.2.4. Armario de telecomunicaciones

Constituye el subsistema que interconecta el cableado vertical y el cableado horizontal donde se alberga las terminaciones del cableado horizontal, equipos activos de telecomunicaciones y cableado de interconexión.

3.2.2.4.1. Consideraciones

Lo recomendable es destinar para este propósito un cuarto exclusivo dedicado para colocar todos estos elementos, conocido como cuarto de telecomunicaciones. Dadas las características de las instalaciones del edificio sólo se dispone de un espacio de estas características en los pisos 9 y 10.

El resto de los pisos dispone de gabinetes en el extremo noreste del edificio. Dado este espacio destinado a las instalaciones de telecomunicaciones; las áreas administrativas han dispuesto sus estaciones de trabajo para realizar sus actividades sin considerar un lugar exclusivo para albergar los equipos, lo que supone complicaciones adicionales el disponer de nuevos espacios.

En tal situación la posibilidad más viable para la instalación este subsistema es a través de gabinetes cerrados de telecomunicaciones en el espacio donde se encuentran los actuales, pudiendo contemplarse la reutilización de los mismos.

Se ha dispuesto un gabinete por piso para satisfacer las necesidades de todos los usuarios que se encuentren en él. Según la norma EIA/TIA 569-A se establece que debe colocarse un armario adicional cuando se superen los 90 metros de distancia, lo cual no es necesario considerando que el cableado horizontal maneja una distancia máxima de 72 metros en el peor de los casos.

Las prevenciones para mantener seguras las instalaciones serán las siguientes:

- Mantener bajo llave el gabinete para prevenir la manipulación del cableado y equipos.
- Mantener la ventilación permanente del equipo.

- Proveer la alimentación desde el cuarto de equipos con UPS para mantener la actividad de los equipos durante fallas eléctricas.
- Aterrizar correctamente la estructura de los gabinetes, debido a que son estructuras metálicas tal como se estipula para los cuartos de telecomunicaciones.
- Mantener un equipo contra incendios lo suficientemente cerca para sofocar el fuego en caso de un incendio.

3.2.2.4.2. Dimensionamiento

El dimensionamiento de los gabinetes estará en función de los equipos activos y los patch panels donde terminan los cables horizontales y del espacio que ocupen otros dispositivos o accesorios como es el caso de organizadores para cables o las regletas eléctricas para alimentar a los switches. La medida utilizada para este dimensionamiento está expresado en unidades de rack (UR), cada una de éstas corresponde a 4.45 cm. Los equipos y dispositivos que se coloquen dentro del gabinete tienen medidas expresadas en unidades de rack.

Al espacio ocupado por los equipos y patch panels se debe añadir un espacio de holgura para permitir el crecimiento a futuro. Se prevé un valor del 30% de crecimiento. La tabla XXX muestra los valores para los gabinetes de telecomunicaciones tomando en cuenta las unidades de rack que ocupa cada uno:

PISO	SWITCHES (1U)	PATCH PANELS 24 PUERTOS (1U)	ORGANIZADORES (2U)	TOMAS ELECTRICAS (1U)	TOTAL UNIDADES DE RACK	CRECIMIENTO DEL 30%
PB	3	5	5	1	19	25
P1	3	5	5	1	19	25
P2	3	5	5	1	19	25
P3	3	5	5	1	19	25
P4	3	5	5	1	19	25
P6	3	6	6	1	22	29
P7	3	5	5	1	19	25
P8	3	6	6	1	22	29

Tabla 3.6. Dimensionamiento de los gabinetes de telecomunicaciones por piso

De los valores obtenidos nótese que en la mayoría de los casos un gabinete con capacidad de 20 unidades de rack es suficiente para satisfacer las necesidades de cada piso, inclusive en el caso del piso 6 y 8 puede optarse por colocar racks de 20 unidades de rack, debido a que el diseño contempla el crecimiento de la cantidad de usuarios al colocar salidas adicionales donde van a existir más usuarios, reduciendo las posibilidades de incrementar cables o equipos adicionales.

La distribución de los dispositivos dentro de los gabinetes de telecomunicaciones tendrá la apariencia que se muestra en la siguiente figura:

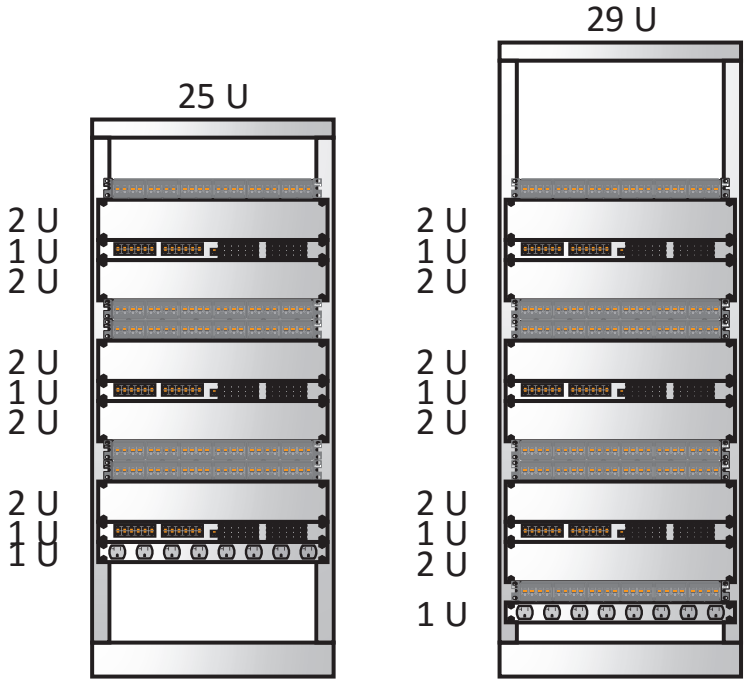

Figura 3.2. Distribución de los equipos dentro de los gabinetes de telecomunicaciones

3.2.2.5. Cuarto de equipos

La Matriz del Ministerio de Inclusión Económica y Social cuenta con un cuarto de equipos ubicado en el quinto piso en el extremo noreste. Hace aproximadamente tres años sufrió una remodelación en su infraestructura para poder albergar mejores equipos bajo mejores prácticas en su diseño y funcionamiento.

3.2.2.5.1. Instalaciones eléctricas

En lo que se refiere a energía eléctrica cuentan con entradas de voltaje reguladas y aseguradas mediante 2 UPS de 60KVA. Se añaden a los dispositivos 8 bancos de batería cambiables en caliente para suplir energía a los equipos de telecomunicaciones y a servidores que se encuentran instalados. El equipo tiene un grado de utilización promedio del 28% y 17% respectivamente. El respaldo ante los cortes de energía eléctrica permite que los equipos operen durante 2,5 horas.

Se dispone de una planta generadora para el edificio que requiere 30 segundos para funcionar y conectarse a las instalaciones eléctricas del edificio.

3.2.2.5.2. Sistema contra incendios

Disponen de sistema contra incendios con gases limpios. Las características de estos sistemas permiten activar el sistema en un tiempo menor a 10 segundos ante la detección de fuego. Su acción es efectiva ante el fuego pero es inocua para las personas y equipos, lo que permite que sigan operando sin dificultades después de su activación. Al final de la operación no quedan residuos de la descarga del gas.

3.2.2.5.3. Temperatura

El cuarto de equipos se encuentra cerrado herméticamente y su ingreso se realiza mediante un sistema electrónico, a través de una tarjeta que posee exclusivamente el personal de TI. Para regular la temperatura se cuenta con un sistema de aire acondicionado de precisión, que mantiene una temperatura estable por debajo de 18 OC y su funcionamiento es permanente.

3.2.2.5.4. Superficie

El espacio destinado al cuarto de equipos tiene un área actual de 22.75 metros cuadrados. El número de estaciones de trabajo actual es de 393 y se prevé que lleguen a 425 en el nuevo diseño.

El área recomendada por la norma ANSI EIA/TIA 569 es de 74 metros cuadrados cuando se dispone de un rango entre 401 y 800 estaciones de trabajo, sin

embargo la construcción de este espacio se realizó para mantenerse fija con las características necesarias para su funcionamiento, lo que incluye la iluminación, el aire acondicionado, el sistema anti-incendios y el cableado eléctrico. El uso de servidores tipo cuchilla (blade) ha permitido manejar una holgura considerable dentro del cuarto de equipos, por lo que se evidencia que el espacio es adecuado a pesar de la recomendación de la norma.

3.2.2.6. Acometida

La entrada de los servicios de telecomunicaciones al edificio se realiza desde la planta baja a través de la canalización metálica hasta el cuarto de equipos. Los hilos de fibra de los operadores llegan hasta el 5 piso donde reposan los equipos de telecomunicaciones.

3.2.2.7. Puesta a tierra

Siguiendo con la norma TIA/EIA-607 se requiere de una instalación de puesta a tierra. En el caso del edificio matriz del MIES se dispone de una malla de puesta a tierra bajo toda la edificación. La salida de la conexión a tierra está colocada en la planta baja.

Desde este punto se tomará una unión vertical para telecomunicaciones TBB, con un conductor de cobre de 3 AWG. La canalización deberá adecuarse a la par con la que contiene el backbone. Al recorrer en línea recta por el extremo noreste del edificio pasará por todos los gabinetes de telecomunicaciones en cada uno de los pisos conectándose directamente a una TGB.

La TGB es una barra de conexión que permite unir los equipos al TBB. Se conectan directamente los chasis de los equipos y al cuerpo de los gabinetes de telecomunicaciones.

3.2.2.8. Administración

Por medio del estándar TIA/EIA se establecen procedimientos para identificar y registrar los elementos del sistema de cableado estructurado correspondientes a patch panels, patch cords, gabinetes de telecomunicaciones, backbone, salida de

telecomunicaciones. La identificación de los elementos se realiza siguiendo un esquema de numeración que permite asociar los elementos por piso y hacia donde se encuentran conectados.

3.2.2.8.1. Identificadores de salida de telecomunicaciones

La identificación de los puntos de red tendrá la forma F-AXX y se realizará considerando los siguientes identificadores:

- F = Piso donde se encuentra localizado el punto, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.
- A = Letra que identifica al patch panel donde está conectado.
- XX = número de puerto del patch panel donde se encuentra conectado el punto.

Por ejemplo, un punto de red ubicado en el tercer piso, en el puerto 18 del patch panel B, tendría el identificador 3P-B18.

3.2.2.8.2. Identificador del patch panel

La identificación del patch panel tendrá la forma F-A, donde se tendrán los siguientes identificadores:

- F = Piso donde se encuentra localizado el patch panel, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.
- A = Letra que identifica al patch panel.

3.2.2.8.3. Identificador de la puesta a tierra

La identificación de la puesta a tierra tendrá la forma F-TGBXX, donde se tendrán los siguientes identificadores:

- F = Piso donde se encuentra localizado la toma de puesta a tierra, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.
- XX = número que identifica a la TGB del piso. En todos los casos será 01 porque sólo se instalará una por piso.

3.2.2.8.4. Identificador de las MUTOA

La identificación de las MUTOA tendrá la forma F-MTXX, donde se tendrán los siguientes identificadores:

- F = Piso donde se encuentra localizado el MUTOA, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.
- XX = número que identifica a la MUTOA por piso del resto, no se considera el patch panel a la que se encuentra conectada porque puede ser a más de uno.

3.2.2.8.5. Identificador de los gabinetes de telecomunicaciones

La identificación de los gabinetes de telecomunicaciones tendrá la forma F-GTXX, donde se tendrán los siguientes identificadores:

- F = Piso donde se encuentra localizado el gabinete de telecomunicaciones, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.
- XX = Letra que identifica al gabinete de telecomunicaciones. En este caso sólo puede ser 01 porque sólo hay un gabinete de telecomunicaciones por piso.

3.2.2.8.6. Identificador del rack de telecomunicaciones

La identificación del rack de telecomunicaciones del cuarto de equipos tendrá la forma F-RKXX, donde se tendrán los siguientes identificadores:

- F = Piso donde se encuentra localizado el RACK, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.

XX = Letra que identifica al rack de telecomunicaciones. En este caso sólo puede ser 01 porque sólo hay un rack de telecomunicaciones en el quinto piso.

3.2.2.8.7. Identificador del backbone

La identificación de las conexiones de backbone tendrá la forma FCE-FGT-XX, donde se tendrán los siguientes identificadores:

- FCT = Piso donde se encuentra localizado el cuarto de equipos. En este caso sólo puede tomar el valor 5P.

- FGT= Piso donde se encuentra localizado el gabinete de telecomunicaciones, pudiendo tener los valores de P1, P2, P3, P4, P5, P6, P7, P8 o PB.
- XX = Letra que identifica el número de cable.

3.2.3. REDISEÑO DE LA RED ACTIVA

Tomando en cuenta que la red debe soportar tráfico tanto de voz, datos y video, la propuesta de la red debe ser robusta, administrable y escalable para las nuevas tecnologías que se pueden presentar a futuro.

3.2.3.1. Equipos terminales

Los equipos terminales que actualmente se tiene en la red del MIES son:

- Computadoras de escritorio
- Computadoras portables personales
- Computadoras portables Ministeriales
- Smartphones
- Impresoras
- Teléfonos IP
- Cámaras de seguridad IP

3.2.3.2. Equipos de conectividad

Los equipos que se van a integrar a la red del MIES son en su gran mayoría switches de capa dos, los cuales van a ayudar a cubrir los requerimientos de acceso a la red a los usuarios actuales y a futuros usuarios.

Además se van a integrar nuevos equipos para la red inalámbrica, para cubrir las necesidades de acceso a la red desde cualquier dispositivo que maneje tecnología wireless.

Los equipos de conectividad deben soportar tecnologías Fast Ethernet y Gigabit Ethernet para realizar la conexión entre equipos del mismo tipo y hacia los equipos terminales.

3.2.3.3. Servidores

Los servidores que actualmente posee el MIES fueron redimensionados migrados y reconfigurados dependiendo de las características y necesidades del Ministerio.

Como parte de un proceso de actualización el MIES dispuso la reestructuración, actualización y redimensionamiento de los servidores con los que trabaja. Actualmente los servicios que brinda el MIES tanto a usuarios internos como a usuarios externos no presentan inconvenientes al ingresar a los respectivos servicios dentro de la DMZ de la Institución. La solución ya implementada de los servidores fue realizada pocos meses antes de la propuesta de rediseño de la red.

Debido a esto y al excelente estado de los servidores no se tomará en cuenta para el presente proyecto el redimensionamiento de los servidores del MIES.

A continuación se detallan las características de los servidores actualmente instalados en el Ministerio de Inclusión Económica y Social:

Sistema Operativo	Procesador	Memoria RAM	Disco Duro	Servicio	Plataformas
Windows 2003 Server	2 (3Ghz)	4 GB	200 GB	Domain Controler Secundario	Controlador de Dominio, DHCP
Windows 2003 Server	2 (3Ghz)	4 GB	300 GB	Servidor de Base de Datos SQL Server 2000	SQL Server 2000
Windows 2003 Server	2 (3Ghz)	4 GB	600 GB	Servidor de Antivirus Kaspersky	Sql Server 2008 Standart, Servidor de Administración Kaslab 8
Windows 2008 Server	2 (3Ghz)	4 GB	33.3 GB	Servidor de Impresión	Plataforma de Impresión Lexmark
Suse	1 (3 Ghz)	2 GB	2 TB	Sistema de Planificación	Apache Tomcat, My SQL
Centos 5.4	2 (5.86 Ghz)	6 GB	500 GB	Sistema de Talento Humano	Jboss, Apache

Centos	2 (5.86 Ghz)	4 GB	500 GB	Servidor Web MIES Backup	Joomla, My SQL
Red Hat	6 (17.4 Ghz)	12 GB	38 GB	Mail Server Zimbra	Zimbra 7.1, My SQL, Posfix
Windows 2008 Enterprise	24 (57.6 Ghz)	45 GB	180 GB	DNS Primario inclusión.gob.ec	Políticas de Administración de Dominio
Centos 5.4	8 (23.2Ghz)	12 GB	80 GB	Servidor de Aplicaciones	My SQL, Apache, PHP
Windows 2003 Server	2 (4.8 GHZ)	6 GB	180 GB	Sistema de Talento Humano (Ex Infa)	Apache, My SQL
Suse	1 (3 Ghz)	8 GB	600 GB	Sistema de Proyectos Planificación	Postgress9, ApacheTomcat

Tabla 3.7. Características de los servidores MIES[43]

3.2.3.3.1. Dimensionamiento de los Servidores

3.2.3.3.1.1. Servidor de Directorio Activo

El servidor de Directorio activo alberga a todos los usuarios que se encuentran dentro del dominio mies.gob.ec, en el cual no solo constan los usuarios de la matriz central del MIES, sino también de las instituciones que forman parte del MIES como son: INFA (Instituto de la Niñez y la Familia), IEPS (Instituto de Economía Popular y Solidaria), entro otros.

El cálculo del servidor se basa principalmente en el parámetro del número de usuarios, ya que a partir de los usuarios se crean bases de datos asociadas a cada cuenta, el cálculo se lo realizará a partir de la siguiente tabla:

Minimum Hardware Requirements by Domain Controllers (GC)			
User per domain in a site	Minimum number of domain controllers required per domain in a site	Minimum memory requirements per domain controller	Minimum disk requirements per domain controller
1–499	One – x64 Single Processor	512 MB	40 GB
500–999	One – x64 Dual Processors/Cores	1 GB	40 GB
1,000–2,999	Two – x64 Dual Processors/Cores	2 GB	40 GB
3,000–10,000	Two – x64 Quad Processors/Cores	4 GB	45GB
10,000–15,000	Three – x64 Quad Processors/Cores	8 GB	50 GB
15,000–20,000	Two – x64 Octo Processors/Cores	16 GB	70 GB
20,000–30,000	Four – x64 Octo Processors/Cores	32 GB	100 GB

Tabla 3.8. Cálculo del servidor de Directorio Activo[44]

[43] Información obtenida del Departamento de Tecnologías de la Información del MIES

De acuerdo a la tabla anterior y por el número de usuarios que maneja el MIES en sus diferentes instituciones adscritas que llegan alrededor de 2600 usuarios, se requiere un servidor con las siguientes características para su correcto funcionamiento:

Número de Usuarios	Número de Controladores de Dominio Requeridos por Sitio	Memoria requerida por Controlador de Dominio	Mínimo disco requerido por Controlador de Dominio
1,000 - 2,999	2 – X64 Dual processors/core	2 GB	40 GB

Tabla 3.9. Características actuales del servidor de Directorio Activo

Se puede concluir que el servidor el Directorio Activo se encuentra dimensionado correctamente de acuerdo a los requerimientos mínimos para su correcto funcionamiento.

3.2.3.3.1.2. Servidor de Correo Electrónico

Debido a la variedad de configuraciones, perfiles de usuario y número de usuarios es complicado determinar con precisión los requerimientos de hardware para un servidor de correo electrónico.

A presar de esto se puede dimensionar un servidor de correo electrónico con los siguientes parámetros:

- Número de usuarios totales con cuenta de correo
- Acceso concurrente al servicio de correo

Uso de CPU: la utilización del CPU viene dado por la siguiente operación

$$Uso_{CPU} = Velicidad_{CPU} \times Número_{CPU} \times Disponibilidad_{CPU}$$ [45]

$$Uso_{CPU} = 2000\ [MHz] \times 1 \times 0,95 = 1900\ [MHz]$$

Se utilizará un servidor que cuente con un procesador mínimo de 2 GHZ.

---

[44] Información obtenida de: https://social.technet.microsoft.com/Forums/es-ES/8708b2cd-e2f3-429b-8a83-e71e7435e762/dimensionar-servidor-para-adds-windows-server-2008-r2?forum=wsades

[45] Información obtenida de: http://docplayer.es/902900-Universidad-tecnica-del-norte.html

Parámetro	Descripción
Procesador	Mínimo Intel/AMD 2.0 GHz, de preferencia implementarlo en sistemas operativos de 64 bits.
Memoria RAM	Mínimo 2 GB (recomendado 4GB).
Capacidad de Almacenamiento	10 GB de espacio libre para software y logs. Espacio adicional para almacenamiento de correo: zimbra-store requiere 5 GB, adicionalmente el espacio para almacenamiento de correo; el resto de componentes de la arquitectura de zimbra requieren 100 MB.

Tabla 3.10. Características mínimas de funcionamiento del servidor de correo

Disco Duro: bajo las recomendaciones Zimbra para ambientes en los que se maneja alrededor de 3000 usuarios se debe tomar en cuenta las siguientes recomendaciones del tamaño de disco duro:

Parámetro	Tamaño en disco recomendado
Espacio para logs y software	10 GB
Zimbra Store	5 GB
Almacenamiento de correo	60 GB
Componentes de Zimbra	100 MB
Total	65,1 GB

Tabla 3.11. Cálculo de disco duro para el servidor Zimbra

Se toma en cuenta 3000 usuarios pensando en un crecimiento a 5 años de alrededor del 15% con un máximo de almacenamiento por usuarios de 20 MB.

Memoria RAM: se utilizará la memoria recomendada por Zimbra (4 GB).

El servidor Zimbra del MIES presenta características superiores a las descritas en las buenas prácticas de la marca.

3.2.3.4. Conectividad de la red

3.2.3.4.1. *Switches de acceso*

Se van a reutilizar los switches de acceso excepto los que no son administrables como entre los cuales tenemos:

- Switch DLINK DES-1008d 8 puertos.
- Switch DLINK DES-1024R 24 puertos.
- Switch TPLINK TL sg 1008d 8 puertos.
- Switch TPLINK TL sf 1008d 8 puertos.

Una de las principales características que se necesita saber para dimensionar un switch tanto de acceso como de núcleo es la cantidad de información procesada por lo que se necesita conocer la velocidad de backplane y throughput de cada switch, donde las velocidades se calculan de la siguiente manera:

$$V_{Backplane} = \text{Cantidad de puertos} * 2(velocidad\ de\ puertos)$$

$$V_{Backplane} = [(48 * 100) + (2*1000)] * 2 \text{ Mbps}$$

$$V_{Backplane\ 48P} = 13{,}6 \text{ (Gbps)}$$

$$V_{Backplane\ 24P} = 8{,}8 \text{ (Gbps)}$$

$$Throughput = \frac{puertos * velocidad}{paquete}$$

$$Throughput = \frac{2400\ (Mbps) * 2000(Mbps)}{64\ (bytes)}$$

$$Throughput = 8{,}6\ (Mbps)$$

Para cubrir las necesidades de los usuarios para la conexión a la red se necesita colocar un switch de acceso adicional por piso y reubicar otros, dependiendo de la siguiente tabla, se omiten los switches no administrables:

PISO	Número de usuarios proyectados	Actuales		Rediseño	
		Número de switches de 24 puertos	Número de switches de 48 puertos	Número de switches de 24 puertos	Número de switches de 48 puertos
PB	110	0	2	1	2
P1	111	0	2	1	2
P2	107	2	1	1	2

P3	116	0	2	1	2
P4	119	0	1	1	2
P5	94	0	2	0	2
P6	137	0	2	0	3
P7	108	0	2	1	2
P8	142	0	1	0	3
P9	45	1	1	1	1
P10	15	1	1	1	1

Tabla 3.12. Cálculo de switches de acceso por piso y por número de puertos

Las principales características que se necesita para los switches adicionales son las siguientes:

SWITCHES DE ACCESO: CAPA 2 DE 24 PUERTOS 10/100/1000	
Cantidad:	5 (cinco)
Throughput mínimo	8.6 Mbps
Tipo de equipo	De configuración fija, apto para montaje en rack estándar de 19”, debe ocupar una sola unidad de rack (1 RU). El equipo debe ser capaz de integrar un stack, mediante la adición futura de un módulo intercambiable en caliente (hot swappable). En un stack de este tipo de equipos debe ser factible lo siguiente: Administrar todo el stack como una sola entidad lógica con una sola dirección IP. El stack debe utilizar puertos especializados para el efecto.
Densidad de puertos	24 puertos de acceso 10/100/1000, con conector RJ-45, con negociación automática de la velocidad y del modo dúplex de operación. 4 slots de tipo SFP en los que se puedan instalar transceivers a 1Gbps. 1 puerto de consola
Seguridad	Funcionalidad para evitar que usuarios maliciosos finjan ser servidores DHCP y asignen direcciones IP arbitrarias.
Estándares	Per VLAN Spanning Tree IEEE 802.1D Spanning Tree Protocol IEEE 802.1Q 4096 VLAN

soportados:	Soporte configuración de Voice VLAN para simplificar las instalaciones de telefonía al mantener el tráfico de voz en una VLAN separada para facilitar la administración y el troubleshooting Soporte autenticación TACACS+ y RADIUS
Administración	Soporte Telnet Soporte SSH Soporte SNMPv1, v2c y v3 Soporte NTP Soporte TFTP para upgrades de software Soporte almacenamiento USB para respaldo (backup) y distribución de archivos.
Condiciones ambientales	Temperatura de operación: -5 a 45°C
Fuente de poder	100 – 240 VAC 5 - 2 A 50 – 60 Hz

Tabla 3.13. Requerimientos switches de acceso 24 puertos

SWITCHES DE ACCESO: CAPA 2 DE 48 PUERTOS 10/100/1000	
Cantidad:	4 (cuatro)
Throughput mínimo	13.28 Mbps
Tipo de equipo	De configuración fija, apto para montaje en rack estándar de 19”, debe ocupar una sola unidad de rack (1 RU). El equipo debe ser capaz de integrar un stack, mediante la adición futura de un módulo intercambiable en caliente (hot swappable). Administrar todo el stack como una sola entidad lógica con una sola dirección IP. El stack debe utilizar puertos especializados para el efecto.
Densidad de puertos	48 puertos de acceso 10/100/1000, con conector RJ-45, con negociación automática de la velocidad y del modo dúplex de operación. 4 slots de tipo SFP en los que se puedan instalar transceivers a 1Gbps. 1 puerto de consola
Seguridad	Funcionalidad para evitar que usuarios maliciosos finjan ser servidores DHCP y asignen direcciones IP arbitrarias.
Estándares	Per VLAN Spanning Tree IEEE 802.1D Spanning Tree Protocol

soportados:	IEEE 802.1Q 4096 VLAN Soporte configuración de Voice VLAN para simplificar las instalaciones de telefonía al mantener el tráfico de voz en una VLAN separada para facilitar la administración y el troubleshooting Soporte autenticación TACACS+ y RADIUS
Administración	Soporte Telnet Soporte SSH Soporte SNMPv1, v2c y v3 Soporte NTP Soporte TFTP para upgrades de software Soporte almacenamiento USB para respaldo (backup) y distribución de archivos.
Condiciones ambientales	Temperatura de operación: -5 a 45°C
Fuente de poder	100 – 240 VAC 5 - 2 A 50 – 60 Hz

Tabla 3.14. Requerimientos switches de acceso 24 puertos

3.2.3.4.2. Switch de núcleo

Actualmente el switch de núcleo con el que trabaja el MIES es un switch marca Cisco modelo Catalyst 6509-E, el cual tiene muy buenas características para equipo de core, se lo reutilizará para permitir redundancia a nivel de núcleo por lo que se sugiere la adquisición de un equipo con las siguientes características:

- Que contenga diversos tipos de interfaces para redes LAN, WAN y MAN.
- Número variable de puertos Ethernet de 10/100/1000 Mbps.
- Módulos Fast Ethernet (IEEE con 802.3af Power over Ethernet [PoE])
- Módulos de 10 Gigabit Ethernet
- Throughput mínimo de 135 Mbps
- Módulo de Servicios Firewall: Cada módulo a 4 Gbps y 100.000 conexiones por segundo, con inspección integrada hasta de capa 7.
- Multi-Gigabit servicios de los módulos (servicios de contenido, firewall, detección de intrusos, seguridad IP (IPSec), VPN, análisis de redes, y Secure Sockets Layer (SSL) aceleración.
- Doble fuente redundante de 3000 W.

- Supervisor Engine 720-3B, puerto de consola, puerto RJ-45 10/100/1000 Ethernet (con LED indicativo del link).
- Ejecuta protocolos: Spanning-Tree, Per VLAN Spanning-Tree, CDP y VTP.
- Maneja Protocolos y servicios: HTTP, Telnet, SNMP

3.2.3.4.3. Controladora de Red Inalámbrica

Debido a la falta de cobertura de red inalámbrica en los once pisos del edificio del MIES se ve la necesidad de aumentar la cantidad de equipos inalámbricos para tener una cobertura total de las instalaciones, para ello las características de las controladoras de access point deben tener las siguientes características:

CONTROLADOR DE RED INALÁMBRICA	
Cantidad:	1 (UNO)
Tipo de equipo	De configuración fija. Apto para montaje en rack estándar de 19". Debe ocupar máximo 1 RU. El equipo debe permitir la configuración de toda la red inalámbrica de manera centralizada. El equipo debe controlar los recursos de radio de toda la red inalámbrica. El equipo debe manejar el roaming entre APs de manera eficiente.
Cantidad de Access Points soportados	El controlador inalámbrico debe tener licencia para administrar mínimo 27 access points. El controlador inalámbrico debe tener la capacidad de administrar mínimo 500 clientes. Para incrementar el número de APs administrados, debe ser necesario simplemente adquirir una licencia de software, sin necesidad de modificar el hardware del equipo.
Densidad de puertos:	Incluir 4 transceivers con 1 puerto 10/100/1000 (RJ-45) cada uno. 1 puerto de consola
Administración RF	Debe integrarse de manera nativa con una tecnología en los Access Points, que provea información en tiempo real e histórica de interferencia de RF que impacte en la red inalámbrica.
Seguridad de extremo a extremo	Debe ofrecer encripción DTLS que cumpla con CAPWAP – (Control And Provisioning of Wireless Access Points); para garantizar encripción de línea completa entre Access Points y el controlador, pasando por enlaces LAN o WAN.

Estándares inalámbricos soportados:	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n
Estándares soportados	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.1Q VLAN tagging IEEE 802.1AX Link Aggregation
Estándares de seguridad	Wi-Fi Protected Access (WPA) IEEE 802.11i (WPA2)
Encripción	WEP y TKIP-MIC: RC4 de 40, 104 y 128 bits (tanto con claves estáticas como compartidas) AES: CBC, CCM, CCMP DES: DES-CBC, 3DES SSL y TLS: RC4 de 128 bits y RSA de 1024 y 2048 bits DTLS: AES-CBC IPSec: DES-CBC, 3DES, AES-CBC
Administración	Soporte Telnet Soporte SSH Soporte SNMPv1, v2c y v3 Soporte gestión vía web (HTTP y HTTPS) Soporte TFTP para upgrades de software Soporte RMON

Tabla 3.15. Requerimientos Controladora Inalámbrica

3.2.3.4.4. Access Point

Los access point existentes no se reutilizarán en la matriz ya que en algunos casos son equipos tipo home y se los reubicará en los edificios zonales del MIES.

Se realizó un site survey (revisar Anexo 21 y Anexo 37) en las instalaciones del edificio matriz del MIES para verificar el estado actual de la cobertura wireless y se llegó a la conclusión que es necesario colocar entre dos y tres access point por cada piso para tener una cobertura total de las instalaciones, de tal manera que la distribución de los access point quedaría de la siguiente manera:

PISO	NÚMERO DE ACCESS POINT
Planta Baja	2
Primer Piso	3
Segundo Piso	2

Tercer Piso	3
Cuarto Piso	2
Quinto Piso	3
Sexto Piso	2
Séptimo Piso	3
Octavo Piso	2
Noveno Piso	3
Décimo Piso	2
TOTAL	27

Tabla 3.16. Puntos de acceso necesarios por piso

Los puntos de acceso inalámbricos que van a estar bajo el mando de la controladora wireless deben tener las siguientes características

ACCESS POINTS PARA INTERIORES	
Cantidad:	27 (veinte y siete)
Tipo de equipo:	Para interiores con antenas internas. El equipo debe ser compatible con el controlador inalámbrico. El access point deberá poder operar en modo autónomo o bajo el manejo de una controladora.
Densidad de puertos:	2 puertos 10/100/1000BASE-TX (RJ45). El equipo debe poder recibir alimentación eléctrica, de acuerdo al estándar 802.3at PoE+. 1 puerto de consola RJ-45
Interfaz inalámbrica	El equipo debe operar tanto en la banda de los 2,4GHz, como en la banda de los 5GHz
Bandas de Frecuencia y Canales de operación de 20Mhz	2.412 a 2.462GHz; 11 canales 5.180 a 5.320GHz; 8 canales 5.500 a 5.700GHz; 8 canales (se excluye la banda de 5.600 a 5.640GHz) 5.745 a 5.825GHz; 5 canales
Estándares inalámbricos soportados:	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n
Seguridad	IEEE 802.11i Wi-Fi Protected Access 2 (WPA2) WPA 802.1x AES TKIP

Tabla 3.17. Requerimientos puntos de acceso inalámbricos

3.2.3.4.5. Equipo de administración de la Red

Con el fin de evaluar, analizar, configurar y monitorizar los equipos activos de la red se ve la necesidad de instalar un equipo de administración y gestión de la red con el fin de estudiar el desempeño de la red, poder evaluar y tomar decisiones oportunas para reducir costos, mejorar la velocidad y calidad del servicio de la red del Ministerio.

Para lograr estos objetivos las características de un sistema de administración de la red debe tener las siguientes características enfocadas a las necesidades de la red del MIES:

SISTEMA DE ADMINISTRACIÓN DE RED	
Cantidad:	1 (UNO)
Licenciamiento:	Debe permitir administrar infraestructura de red. Debe incluirse licenciamiento para gestionar al menos 125 dispositivos de red.
Protocolos de gestión soportados:	SNMPv1, v2c, v3, TACACS+.
Importación de archivos:	Debe soportar la importación de archivos de tipo PNG, JPEG, y AutoCAD (DXF y DWG).
Tipo de solución:	Debe ser factible montarla sobre máquinas virtuales o sobre appliances físicos.
Hardware requerido:	Características de hardware mínimas: Dos procesadores Quad Core Intel 2.4GHz Xeon E5620. 16GB de memoria RAM. 4 discos duros de 300GB operando en RAID5.
Administración simplificada y convergente del ciclo de vida de la red	Debe automatizar varias tareas del día a día, que permitan mantener y administrar infraestructura de red. Debe ofrecer herramientas de apoyo para: Diseño Despliegue Operación Reportería
Administración de red inalámbrica	Debe ofrecer herramientas para administración de RF, visibilidad de usuarios, reportería, troubleshooting, incluyendo: descubrimiento, inventario, configuración y administración de imágenes.

Tabla 3.18. Requerimientos software de administración de la red

3.2.3.4.6. Seguridad Perimetral

El equipo de seguridad perimetral que actualmente opera en el MIES cumple con las necesidades de los administradores de red para un correcto funcionamiento de la misma, entre los principales requerimientos se tiene:

- Características de Firewall.
- Características de Control de contenido.
- Características de Filtrado de contenido.
- Permitir realizar VPNs tanto SSL como IPsec
- Que permita una característica de Antivirus dentro del mismo appliance
- Características de IPS (Sistema de prevención de Intrusos), con la actualización de la base de firmas automáticamente y periódicamente.
- Que permita la creación de objetos para ser utilizados en las diferentes reglas.
- Que permita generar reportes de los features activos en el equipo y además permita exportar a formatos como: PDF y WORD.
- Que permita la configuración de clúster entre equipos del mismo fabricante para garantizar disponibilidad del servicio.

Como complemento a la seguridad de la red se ve la necesidad de establecer políticas de seguridad físicas y lógicas de información en la red del MIES, las cuales se puede observar en el Anexo 35.

3.2.3.4.7. Direccionamiento de la LAN

Al momento de realizar la reestructuración de los servidores en el año 2013 se aprovechó la oportunidad de la ventana de mantenimiento para realizar la reestructuración del direccionamiento de la LAN del MIES, ya que antes se tenía una red plana donde se utilizaba un segmento diferente para la red de servidores.

Toda la red LAN cableada como inalámbrica se encontraba en la VLAN 1 y se presentaban problemas de tormentas de broadcast, lo que obligó a los administradores realizar una segmentación de VLAN.

De tal manera el direccionamiento en la parte de la LAN se seguirá utilizando de la misma manera, tal como se presenta en la siguiente tabla.

ID de VLAN	NOMBRE DE LA VLAN	DIRECCIÓN DE RED	PUERTA DE ENLACE
3	Wireless	192.168.3.0/23	192.168.3.1
10	Planta Baja	192.168.10.0/24	192.168.10.1
11	Piso 1	192.168.11.0/24	192.168.11.1
12	Piso 2	192.168.12.0/24	192.168.12.1
13	Piso 3	192.168.13.0/24	192.168.13.1
14	Piso 4	192.168.14.0/24	192.168.14.1
15	Piso 5	192.168.15.0/24	192.168.15.1
16	Piso 6	192.168.16.0/24	192.168.16.1
17	Piso 7	192.168.17.0/24	192.168.17.1
18	Piso 8	192.168.18.0/24	192.168.18.1
19	Piso 9	192.168.19.0/24	192.168.19.1
20	Piso 10	192.168.20.0/24	192.168.20.1
21	Servidores	192.168.21.0/28	192.168.21.1
22	Impresoras	192.168.22.0/26	192.168.22.1
23	Cámaras de video	192.168.23.0/27	192.168.23.1
24	Biométricos	192.168.24.0/28	192.168.24.1
25	Telefonía IP	192.168.25.0/24	192.168.25.1
26	Videoconferencia	192.168.26.0/27	192.168.26.1

Tabla 3.19. Direccionamiento VLAN

3.3. DIMENSIONAMIENTO DEL TRÁFICO

A pesar de que en el año 2013 fueron dimensionados los servicios del MIES (servicio WEB, descarga de archivos, correo electrónico, videoconferencia, videovigilancia), es necesario comprobar que el ancho de banda que actualmente posee la Institución pueda asegurar que los servicios el correcto desempeño de la red.

3.3.1. ANCHO DE BANDA DEL SERVICIO WEB

Par realizar el cálculo de una forma más precisa del peso de la página web del MIES existe una herramienta que nos facilita el cálculo preciso y a partir de este peso se va a calcular y dimensionar el tráfico de la red del MIES.

Se define que el personal del MIES accede en promedio a 80[46] páginas web en una hora, dato que se obtiene por medio de la reportería del firewall SOPHOS.

Para calcular el peso exacto de la página web del MIES ingresamos a la siguiente dirección electrónica: http://tools.pingdom.com/fpt/

La cual nos dio como resultado que la página web del MIES tiene un peso de: 3.1 MBytes, como se muestra en la siguiente figura:

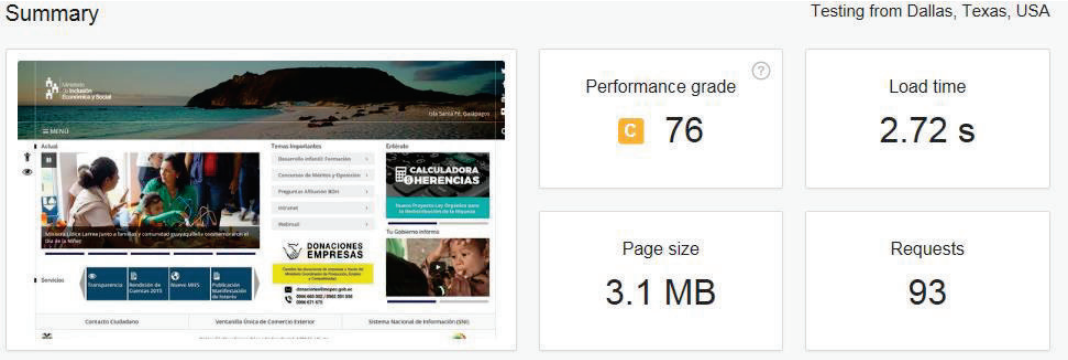

Figura 3.3. Peso de la página web del MIES

Con esta información se puede calcular el ancho de banda para el servicio web definido de la siguiente manera:

$$AB_{web} = \frac{3.1 MBytes}{página} * \frac{8\ bits}{1\ byte} * \frac{500\ páginas}{3600\ segundos}$$

$$AB_{web} = 3{,}44\ Mbps$$

3.3.2. ANCHO DE BANDA PARA TRANSFERENCIA DE ARCHIVOS

Un archivo desde Internet tiene un promedio de peso de 1 Mbyte descargado en 40 segundos[47].

Para el cálculo del ancho de banda para transferencia de archivos tenemos el siguiente cálculo.

$$AB_{T.archivos} = \frac{1024 KBytes}{1\ archivo} * \frac{8\ bits}{1\ byte} * \frac{1\ archivo}{40\ segundos}$$

[46] Información obtenida del personal de Tecnologías de la Información del MIES, no fue posible adjuntar la captura ya que por políticas de la Institución la información del Firewall es restringida
[47] Información obtenida de. http://computopractico.blogspot.com/2009/10/ccna-1-226-calculo-de-la-transferencia.html

$$AB_{T.archivos} = 204{,}8\ Kbps$$

3.3.3. ANCHO DE BANDA PARA CORREO ELECTRÓNICO

El tamaño promedio de un correo electrónico en la actualidad es de 75 KBytes[48], tomando en cuenta que cada usuario envía un promedio de 13 correos electrónicos en una hora el ancho de banda que se necesita es el siguiente:

$$AB_{correo} = \frac{75KBytes}{correo\ electr.} * \frac{8\ bits}{1\ byte} * \frac{1000\ correo\ electr.}{3600\ segundos}$$

$$AB_{correo} = 166{,}66\ Kbps$$

3.3.4. ANCHO DE BANDA PARA VIDEOCONFERENCIA

El servicio de videoconferencia no es una aplicación muy utilizada en el MIES, de acuerdo a la información obtenida por parte del administrador de la red de la Institución se realiza una videoconferencia en promedio por semana, la videoconferencia cuenta con un máximo de 5 personas.

Para una conexión de videoconferencia con compartición de audio, video, archivos y chat; se estima que lo mínimo recomendado para una sesión de videoconferencia es de alrededor de 400Kbps[49] por usuario.

$$AB_{videoconferencia} = \frac{400Kbits}{segundo} * 5\ usuarios$$

$$AB_{videoconferencia} = 2\ 000\ Kbps$$

El equipo que reserva el ancho de banda por usuario dedicado para la videoconferencia es el SOPHOS (Firewall perimetral), actualmente se dispone de 2 Mbps por usuario dedicados para cada videoconferencia.

3.3.5. DIMENSIONAMIENTO DE LA WAN

Para dimensionar la WAN del MIES es necesario conocer el ancho de banda de las aplicaciones que se transmiten por el enlace, por lo que el estimado de ancho de banda de la WAN es el siguiente:

---

[48] Información obtenida de: https://medium.com/@raindrift/how-big-is-email-305bbdb69776#.qkedm0r1r

[49] Información obtenida de: https://www.saba.com/us/apps/collaboration/

$$AB_{Total} = AB_{web} + B_{T.archivos} + AB_{correo} + AB_{videoconferencia} + AB_{otros\ servicios}$$

$$AB_{Total} = 3{,}44\ Mbps + 204{,}8\ Kbps + 166{,}66\ Kbps + 2\ 000\ Kbps + 1024\ Kbps$$

$$AB_{Total} = 6835{,}46\ \text{Kbps}$$

3.4. REESTRUCTURACIÓN DE LA RED TOTAL

Una vez realizado el levantamiento de información y estructurada de mejor manera la red tomando en consideración los requerimientos y necesidades tanto de los usuarios como de los administradores de red, se puede visualizar en la figura anterior cómo quedaría la red del MIES con sus modificaciones respectivas.

Se ha tomado en cuenta principalmente la redundancia de los equipos de red, principalmente para que cuando se genere una falla en uno de los equipos de red de acceso no se pierda conectividad y sea transparente para los usuarios finales.

3.5. CONSUMO DE ANCHO DE BANDA POR LOCALIDAD

EL MIES brinda diferentes servicios tanto a los usuarios internos como a la comunidad en general, para ofrecer un buen servicio es necesario asegurar que los servicios brindados dispongan de un ancho de banda adecuado dependiendo del servicio y la concurrencia de los usuarios.

Actualmente el MIES dispone un excelente ancho de banda, ya que como se pudo calcular la red del MIES necesita alrededor de 6.9 Mbps, para los servicios que ofrece como se puede observar en la siguiente tabla:

No.	PROVINCIA	CIUDAD	Ancho de Banda
1	Pichincha	Quito	200 Mbps
2	Cotopaxi	Latacunga	3 Mbps
3	Bolívar	Guaranda	3 Mbps
4	Chimborazo	Riobamba	3 Mbps
5	Tungurahua	Ambato	4 Mbps

6	Guayas	Guayaquil	4 Mbps
7	Manabí	Portoviejo	3 Mbps
8	Cañar	Azogues	3 Mbps
9	Azuay	Cuenca	3 Mbps
10	Esmeraldas	Esmeraldas	3 Mbps
11	Imbabura	Ibarra	3 Mbps
12	Carchi	Tulcán	3 Mbps
13	El Oro	Machala	3 Mbps
14	Loja	Loja	3 Mbps
15	Zamora	Zamora Chinchipe	3 Mbps
16	Sucumbíos	Lago Agrio	3 Mbps
17	Orellana	El Coca	3 Mbps
18	Los Ríos	Babahoyo	3 Mbps
19	Napo	Tena	3 Mbps
20	Pastaza	Puyo	3 Mbps
21	Santa Elena	Santa Elena	3 Mbps
22	Santo Domingo de los Tsáchilas	Santo Domingo de los Tsáchilas	3 Mbps
23	Galápagos	Puerto Baquerizo Moreno	3 Mbps
24	Morona Santiago	Macas	3 Mbps

Tabla 3.20. Ancho de banda actual dedicado por ciudad

A pesar de tener 200 Mbps de ancho de banda para el personal del edificio Matriz se puede observar que el enlace está ocupado hasta en un 10% en el tráfico de salida y un 60% en el tráfico que ingresa a la Matriz.

No existen reglas para bloquear el acceso a aplicaciones que consumen gran ancho de banda como son páginas de descarga, streaming de audio, streaming de video, páginas de juegos online, etc.

Como no se puede observar saturación del canal no se registran reglas de control de ancho de banda y las únicas páginas que se bloquean para la navegación para todos los usuarios del Ministerio.

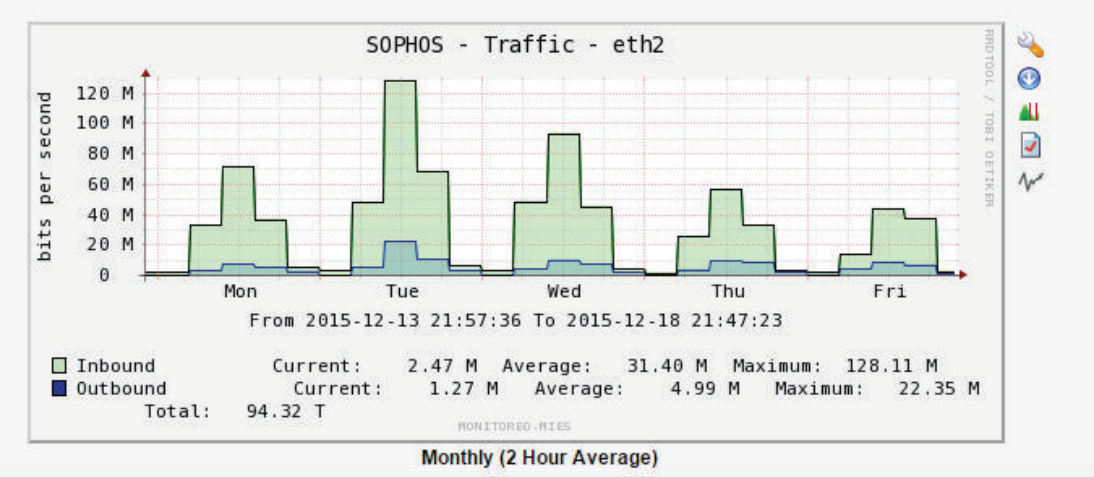

Tabla 3.21. Consumo de ancho de banda salida hacia Internet desde el Firewall SOPHOS[50]

Como se observa en la anterior tabla se puede llegar a la conclusión que no se utiliza ni la mitad de ancho de banda que tiene el canal de Internet, pero se registran picos de consumo de ancho de banda en el tráfico que ingresa a la red, la tabla 3.21 fue obtenida en horas pico donde el consumo de ancho de banda es mayor durante todo el día.

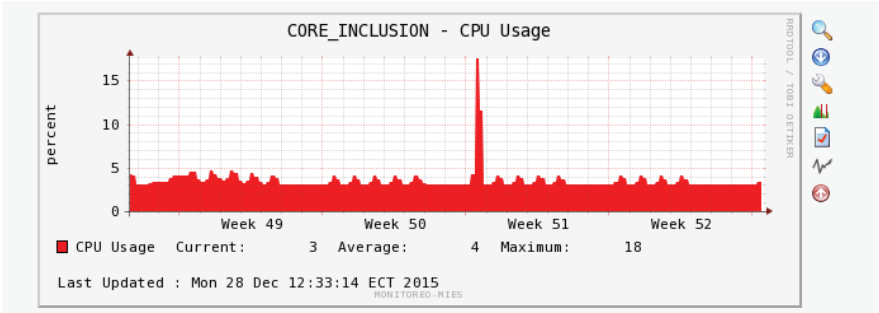

Tabla 3.22. Procesamiento del actual switch de núcleo del MIES Planta Central

El gráfico anterior muestra la utilización de CPU del switch de núcleo en hora pico, se puede observar que no presenta saturación, pero no tiene un equipo que permite realizar redundancia.

[50] Información obtenida por el Departamento de Tecnologías de la Información del MIES

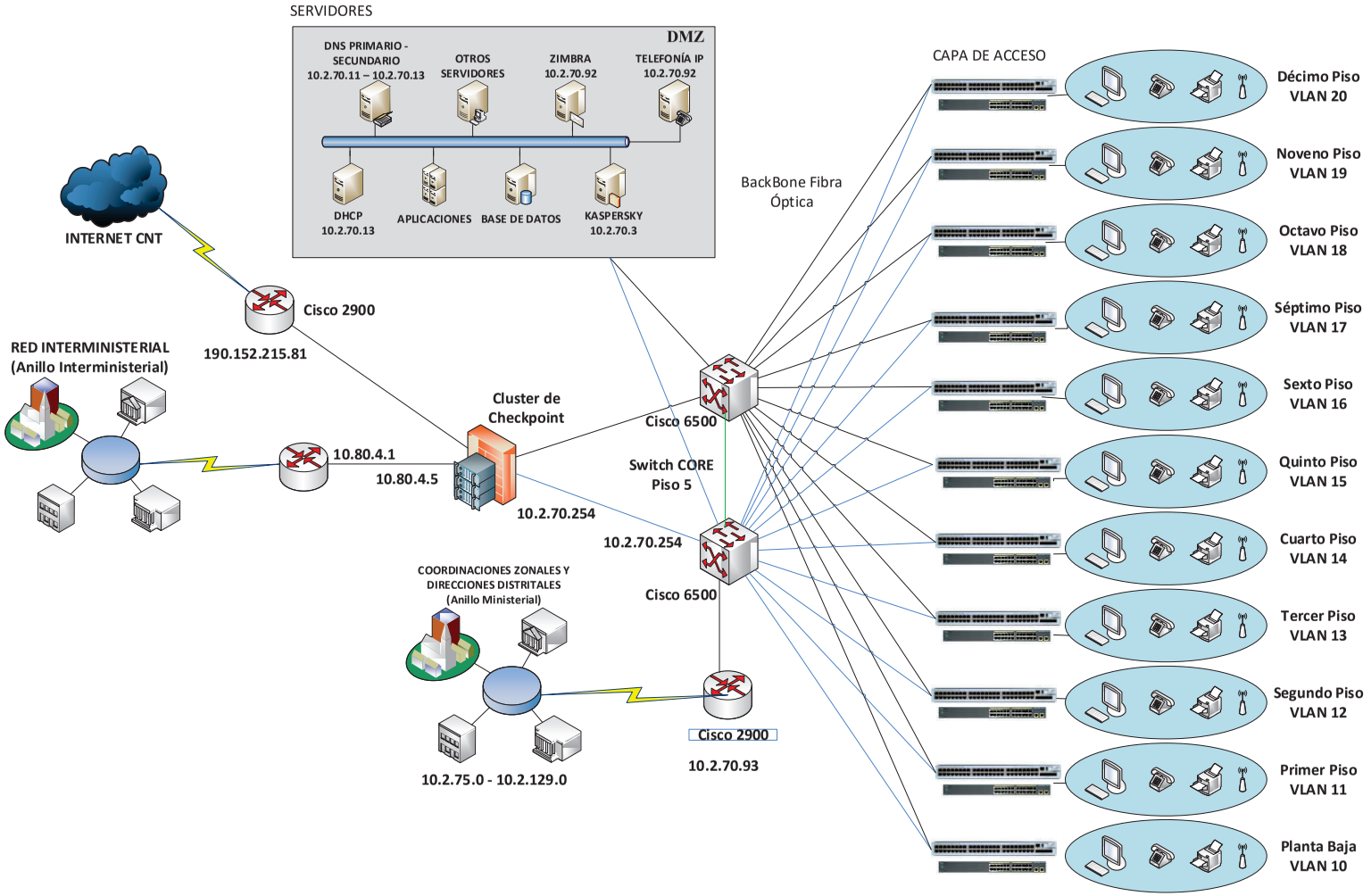

Figura 3.4. Diagrama de red del MIES rediseñado

3.6. JUSTIFICACIÓN DE LA ELECCIÓN DE EQUIPOS

3.6.1. SWITCHES

Para la elección de los switches de acceso presentamos a continuación las siguientes opciones:

3.6.1.1. Switch HP 3100-24 v2 SI

Switch de acceso completamente gestionable, trabaja en la capa de acceso, ideal para medianas empresas, se los puede encontrar en modelos de 8,16 y 24 puertos, puertos con enlaces Gigabit Ethernet.

Entre las principales características se tiene:

Características de Switch HP 3100-24 v2 SI	
Puertos y slots	2 dual-personality 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASET/ 100BASE-TX: half or full; 1000BASE-T: full only 24 autosensing 10/100 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX); Duplex: half or full
Puertos adicionales	Puerto de consola RJ-45
Memoria y Procesador	128 MB SDRAM, 16 MB flash; tamaño del buffer: 384 KB
Administración	IMC—Intelligent Management Center; Línea de comandos; Web browser; SNMP Manager
Throughput	8.6 Mbps
Protocolos Generales	IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3i 10BASE-T IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP

Tabla 3.23. Características Swicth HP 3100

3.6.1.2. Switch Cisco Catalyst 2960X-24TS-LL

Los Switch Cisco Catalyst 2960X-24TS-LL son equipos Gigabit Ethernet apilables, que ofrecen conectividad en capa acceso para grandes y medianas empresas, el cual cuenta con las siguientes características:

Característica Switch Cisco Catalyst 2960X-24TS-L	
Puertos	24 x 10/100/1000 + 2 x Gigabit SFP
Rendimiento	Capacidad de conmutación : 100 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 68.5 Mbps
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, HTTP, TFTP, SSH, CLI
Memoria RAM	512 MB
Memoria Flash	64 MB
Interfaces	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x consola - RJ-45 - gestión 1 x consola - mini USB tipo B - gestión 1 x USB - Type A 1 x 10Base-T/100Base-TX - RJ-45 - gestión 2 x SFP (mini-GBIC)
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 802.3ae, IEEE 802.1ae, IEEE 802.3az, IEEE 802.1AX

Tabla 3.24. Características Switch Cisco 2960X

3.6.1.3. TP-LINK JetStream Gigabit Switch manejable L2 TL-SG3424

TP-LINK JetStream Gigabit Switch manejable L2 TL-SG3424 en un equipo que ofrece 24 puertos 10/100/1000, equipo dedicado para el alto rendimiento en la red empresarial, presenta funciones de seguridad robusta y fácil administración, entre las principales características tenemos:

CARACTERÍSTICAS TP-LINK JetStream Gigabit Switch manejable L2 TL-SG3424

Interface	24 puertos RJ45 a 10/100/1000 Mbps (Negociación automática, MDI/MDIX automático) 4 slots SFP combo a 100/1000 Mbps* 1 puerto de consola
Security	Vinculación IP-MAC-puerto-VID Autenticación según puerto IEEE 802.1X/MAC, Radius, VLAN para invitados Defensa contra ataques DoS Inspección ARP dinámica (DAI) SSH v1/v2 SSL v2/v3/TLSv1 Funcionalidad Port Security Función Storm Control broadcast/multicast/unicast desconocido
Management	Interface de usuario basado en web y gestión mediante línea de comando SNMP v1/v2c/v3, compatible con MIBs públicas y MIBs privadas de TP-LINK RMON (grupos 1, 2, 3, 9) Cliente DHCP/BOOTP, snooping DHCP, opción DHCP Monitorización del procesador Duplicación de puertos (Port Mirroring) Configuración de la hora: SNTP Función integrada NDP/NTDP Actualización de firmware: TFTP y vía web Diagnóstico del sistema: VCT SYSLOG y Public MIBS
Medios de Red	10BASE-T: Cable UTP categoría 3, 4, 5 (100 metros máximo) 100BASE-TX/1000Base-T: cable UTP categorías 5, 5e o superior (máximo 100 m) 100BASE-FX:MMF,SMF 1000BASE-X: MMF, SMF
VLAN	Soporte IEEE802.1Q con 4000 grupos VLAN y 4000 VIDs VLAN basada en puerto/MAC/protocolo GARP/GVRP

Tabla 3.25. Características Switch TPLink TL-SG3424

3.6.1.4. Elección del Switch del acceso

La elección de los switches de acceso para complementar la solución que actualmente tiene el Ministerio va en función de las características de rendimiento, velocidad, disponibilidad y costos.

Debido a que los equipos de las marcas seleccionadas tienen características similares se debería seleccionar el switch Cisco Catalyst 2960X-24TS-L por presentar características más robustas, pero por las diferencia de precios entre los equipos se aconseja la elección del switch HP 3100-24 v2 SI, ya que presenta características que cubren la necesidad de la red del MIES, a continuación se puede observar en la siguiente tabla la diferencia de precios entre estos dos equipos:

Comparación de costos de los switches elegidos	
Equipo	***Costo***
Cisco Catalyst 2960X-24TS-L	$ 1.240,00
HP 3100-24 v2 SI	$ 1 080,00
TP-LINK JetStreamGigabitSwitch manejable L2 TL-SG3424	$ 439,00

Tabla 3.26. Comparación de costos de switches

3.6.2. CONTROLADORA WIRELESS

Para la controladora de puntos de acceso inalámbricos se ha tomado en consideración los siguientes equipos:

3.6.2.1. AIR-CT2504-25-K9

La controladora de acceso Cisco 2504 proporciona la comunicación en tiempo real entre equipos Cisco para el despliegue y cobertura de los puntos de acceso inalámbricos, permitiendo la administración centralizada de políticas y configuraciones de cada uno de los equipos. Las principales características de la controladora se presentan a continuación:

CARACTERISTICAS CONTROLADORA CISCO AIR-CT2504-25-K9	
Cantidad de puertos	4
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet

Protocolo de conmutación	Ethernet
Número de access point soportados	Desde 5 hasta 75
Red / Protocolo de transporte	P/IP, UDP/IP, ICMP/IP, IPSec, ARP, BOOTP, DHCP
Protocolo de gestión remota	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH
Características	Soporte de DHCP, soporte BOOTP, soporte ARP, soporte VLAN, soporte para Syslog, soporte IPv6, Sistema de prevención de intrusiones (IPS), soporte SNTP, soporte Wi-Fi Multimedia (WMM), soporte de Trivial File Transfer Protocol (TFTP), Quality of Service (QoS), CAPWAP
Algoritmo de cifrado	DES, Triple DES, RSA, RC4, MD5, WEP de 128 bits, WEP de 40 bits, IKE, SSL, TLS, SHA-1, TLS 1.0, WEP de 104 bits, TKIP, WPA, WPA2, PKI, AES-CCMP, AES-CCM, AES-CBC
Método de autentificación	RADIUS, certificados X.509, TACACS, Extensible Authentication Protocol (EAP)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, IEEE 802.11h, IEEE 802.11e, IEEE 802.11n

Tabla 3.27. Características Controladora Wireless cisco 2504

3.6.2.2. Hp msm720 wireless Controller

La controladora HP MSM Controller ofrece compatibilidad en el diseño de redes de baja y mediana capacidad de usuarios inalámbricos, soporta los estándares IEEE 802.11a/b/g/n, las principales características que presenta la controladora HP son las siguientes:

CARACTERÍSTICAS CONTROLADORA WIRELESS Hp msm720	
Puertos y Slots	4 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T)

Características generales	IEEE 802.11 a/b/g/n and .11ac hasta 40 access points IEEE 802.3ad Link Aggregation Control Protocol (LACP) Soporta hasta 40 access point 250 usuarios invitados simultáneos Plug-and-play AP management Acceso de invitados Portal cautivo Roaming avanzado Mobility Traffic Manager (MTM)
Entorno de administración	IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1D (STP) RFC 1155 Structure of Management Information RFC 1157 SNMPv1 RFC 1212 Concise MIB definitions RFC 1215 Convention for defining traps for use with the SNMP RFC 1901 SNMPv2 Introduction RFC 2578 SMIv2
Security	RFC 1321 The MD5 Message-Digest Algorithm RFC 1851 ESP Triple DES Transform RFC 2104 Keyed-Hashing for Message Authentication RFC 2246 Transport Layer Security (TLS) RFC 2401 Security Architecture for the Internet Protocol RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)

Tabla 3.28. Características Controladora Wireless HP msm720

3.6.2.3. Ruckus ZoneDirector 3050

La controladora Ruckus provee un servicio de administración de equipos wireless centralizada, permitiendo el control y configuración de los access point desde una consola gráfica de administración, presenta las siguientes características:

CARACTERÍSTICAS CONTROLADORA RUCKUS ZONE DIRECTOR 3050	
Características de software	Administra hasta 500 access point Funcionalidades de DHCP Soporta hasta 1024 WLAN

	Control de usuarios en tiempo real Calidad de servicio con priorización de WLANs Portal Cautivo Base de datos de autenticación local Soporta asociación con Active Directory Vista de mapa gráfico y detección de AP rogué Monitoreo y estadísticas del rendimiento
Alimentación	Suministro de potencia interna de 220 watts Conector 320 IEC, 100 – 250 V CA Universal
Puertos Ethernet	2 puertos, auto MDX, detección automática 10/100/1000 Mbps, RJ-45
Estándares	WPA, WPA2, 802.11i

Tabla 3.29. Características Controladora Ruckus ZoneDirector 3050

Comparación de costos de las controladoras de access point	
Equipo	***Costo***
Controladora Wireless Hp msm720	$ 1.440,00
CISCO AIR-CT2504-25-K9	$ 1.675,00
Ruckus ZoneDirector 3050	$ 1.370,00

Tabla 3.30. Comparación de costos Controladoras de access point

3.6.3. PUNTOS DE ACCESO INALÁMBRICO

3.6.3.1. Access point Cisco AIR-CAP702W-A-K9

Equipo de acceso inalámbrico ideal para empresas de mediana y baja cantidad de usuarios, compatible con todas las controladoras Cisco y presenta las siguientes características:

CARACTERÍSTICAS ACCESS POINT CISCO AIR-CAP702W-A-K9	
Algoritmo de encripción	AES, TKIP, WPA, WPA2

Cantidad de antenas	4
Tasa de transferencia	300 Mbps
Tecnologías Cisco	Flex connect Clean Air
Protocolo de enlace de datos	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Estándares complementarios	IEEE 802.11a, IEEE 802.3at, IEEE 802.11b, IEEE 802.11e, IEEE 802.11g, IEEE 802.11h, IEEE 802.11i, IEEE 802.11n, IEEE 802.1x, IEEE 802.3af
Protocolo de administración remota	Telnet, SSH
Tecnología Clean Air	SI

Tabla 3.31. Características Access Point 702W

3.6.3.2. Access point HP MSM410

Puntos de acceso de banda dual que trabajan con las controladoras HP, los cuales ofrecen una solución de alto rendimiento y cobertura en comunicaciones de voz y datos, las principales características tenemos:

CARACTERÍSTICAS ACCESS POINT HP MSM410	
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n (draft 2.0)
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n (draft 2.0)
Algoritmo de cifrado	MS-CHAP v.2
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11d, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, IEEE 802.11h, IEEE 802.11n (draft 2.0)
Tecnología de conectividad	Inalámbrico, cableado

Tabla 3.32. Características Access Point HP MSM410

3.6.3.3. Access point ZoneFlex R700

Access point con características específicas para usuarios de medianas empresas, con antenas internas direccionales, presentan las siguientes características:

CARACTERÍSTICAS ACCESS POINT RUCKUS ZONEFLEX R700	
Alimentación	12 VDC 1.5A PoE: 802.3af
Radio Frecuencia	Ganancia de antenas internas 3dBi
Puertos	2 ports, auto MDX, auto-sensing 10/100/1000 Mbps, RJ-45 Power over Ethernet (802.3af)
Usuarios concurrentes	Arriba de 500
Canales en los que opera	IEEE 802.11ac: 5.15 – 5.85 GHz IEEE 802.11a/n: 5.15 – 5.85 GHz IEEE 802.11b: 2.4 – 2.484 GHz

Tabla 3.33. Características Access Point Ruckus Zone Flex R700

Comparación de costos puntos de acceso inalámbricos	
Equipo	***Costo***
HP MSM410	$ 461,97
AIR-CAP702W-A-K9	$ 495,00
Ruckus Wireless ZoneFlex R700	$ 539,00

Tabla 3.34. Comparación de costos access point

3.6.3.4. Elección de la controladora wireless y puntos de acceso inalámbricos

Para la elección de la controladora de puntos de acceso y sus respectivos access point podemos observar que los precios son muy parejos entre las tres soluciones propuestas.

Se recomienda la adquisición de la solución completa la cual consta de la controladora junto con los access point, o la posibilidad de adquirir solo los access point para que trabajen de forma independiente y no tengan una administración centralizada.

La elección de los access point desde el punto de vista económico es similar, pero podemos indicar que la tecnología de Cisco, tecnología clean air propia de la marca permite realizar ajustes para optimizar la cobertura inalámbrica permitiendo superar los problemas de interferencia. Además con la tecnología Flex Connect permite a los access point seguir operando una vez que la controladora wireless falle.

3.6.4. SWITCH DE NÚCLEO

Para reutilizar el switch de núcleo que actualmente posee el MIES se recomienda la adquisición de un segundo switch de núcleo, el cual permita realizar redundancia entre los equipos para asegurar el servicio a los usuarios en caso de la falla de uno de los equipos de núcleo.

Se ha tomado en cuenta los equipos Cisco para realizar la redundancia, ya que si bien es cierto se necesita que el equipo que realice la redundancia necesita trabajar con el protocolo GLBP (Gateway Load Balancing Protocol) o HSRP (Hot Standby Router Protocol), es aconsejable colocar un equipo de la misma marca para no tener inconvenientes con la redundancia de con equipos de otras marcas, por lo que se recomienda adquirir el siguiente switch:

3.6.4.1. Switch Catalyst 4500E

CARACTERÍSTICAS SWITCH CATALYST 4500E	
Puertos y conmutación	Capacidad de conmutación de 800 Gbps
	10/100/1000 RJ-45 y el puerto de la consola de gestión
Hardware	Hardware dinámico asignaciones reenvío de mesa para facilitar la

	migración de IPv4 a IPv6
Enrutamiento	Enrutamiento escalable (IPv4, IPv6 y multicast), Capa 2 y Capa 3, y ACL y calidad de servicio (QoS)
Puertos	48 puertos 10/100/1000 PoEP
Tecnologías de redundancia	HSRP, VSS, GLBP

Tabla 3.35. Características switch Cisco 4500E

3.6.5. SOFTWARE DE ADMINISTRACIÓN DE RED

Para realizar la administración y gestión de la red del MIES se ha tomado en cuenta el software que cumple con los requerimientos de:

- Monitoreo de equipos de red.
- Descubrimiento periódico de dispositivos.
- Almacenamiento de logs
- Posibilidad de extraer back ups de equipos integrados al software de monitoreo
- Que permita ingresar a los equipos ya sea por CLI o browser, dependiendo del dispositivo,
- Generación de alarmas.
- Envío de mensajes por medio del protocolo SMTP.
- Trabajar con el protocolo SNMP V1, V2C, V3.

Entre el software elegido podemos tener los siguientes:

3.6.5.1. SolarWinds

Software que permite graficar el diagrama de red una vez descubiertos los equipos, administra y gestiona la red desde un solo equipo de administración, además presenta las siguientes características:

- Monitoreo y gestión de la red.
- Acceso remoto por SSH V1, SSH V2, http, https,
- Descubrimiento calendarizado de la red.
- Generación de alarmas

- Envío de alarmas y mensajes por SMTP
- Trabaja con el protocolo SNMP V1, V2C, V3.

3.6.5.2. WhatsUP Gold

Con la licencia WhatsUp Gold Basic permite administrar de manera centralizada 484 dispositivos de red, permite gestionar equipos de red desde su consola via browser,

- Generación de reportes.
- Permite administrar equipos virtualizados y realiza operaciones básicas a los hosts virtuales: encendido, apagado, suspensión.
- Permite monitorear el ancho de banda en equipos que se pueda configurar comandos de QoS o Netflow.
- Envío de mensajes de alertas.
- Grafica la red desde el descubrimiento de los equipos de red.
- Presenta la topología en tiempo real, además de generar alarmas gráficas.
- Trabaja con el protocolo SNMP V1, V2C, V3.

3.6.5.3. PRTG

Software de monitoreo que permite administrar de manera continua la LAN y WAN, utilizando el protocolo SNMP en sus diferentes versiones.

- Permite administrar la red desde un navegador compatible con la versión del software instalado.
- Trabaja con el protocolo SNMP V1, V2C, V3
- Genera reportería
- Genera alarmas.
- Envío de alarmas al correo.

Comparación de costos Software de Administración	
Equipo	***Costo***
Solarwinds	$ 9.995,00

WhatsUpGold	$ 9.344,00
PRTG	$ 1.600,00

Tabla 3.36. Comparación de costos Software administración de red

3.6.5.4. Elección del software de gestión de red

La administración de red es un punto importante en el rediseño de la red, como WhatsUp Gold es una de las herramientas que se posiciona entre una de las mejores de administración y gestión de red, además de presentar una administración sencilla e intuitiva, se recomienda la adquisición de este software, además permite la integración de dispositivos de diferentes marcas, modelos y tiene una base de datos especializada para cada dispositivo descubierto, de esta manera gestiona de mejor manera dichos dispositivos.

3.7. VALOR TOTAL DEL REDISEÑO DE LA RED DEL MIES

El valor total del rediseño de la red del MIES consta a continuación en la siguiente tabla:

Valor de la implementación de la red del MIES	
Ítem	***Valor***
Cableado estructurado 6A	$ 280.287,03
Equipos de red	$ 44.774,00
Mano de obra especializada	$ 9.600,00
Total	$ 334.661,03

Tabla 3.37. Valor del rediseño de la red del MIES

CAPÍTULO 4

IMPLEMENTACIÓN DEL PROTOTIPO, PRUEBAS Y RESULTADOS

4.1. INTRODUCCIÓN

La implementación del prototipo que se describe a continuación tiene como objetivo realizar las pruebas de todo los criterios expuestos anteriormente, con el equipamiento más básico que permita obtener los servicios planteados en el plan de este proyecto.

A grandes rasgos, se pretende implementar servicios de correo electrónico, telefonía IP, alojamiento y compartición de archivos, videovigilancia, directorio activo, videoconferencia, control de navegación y seguridad perimetral. El despliegue de los servicios contará con la agrupación del tráfico de la red activa a través del uso de VLAN.

4.2. CONSIDERACIONES

En vista de la cantidad de servicios que requieren ser levantados, se ha segmentado la funcionalidad del prototipo en siete servidores. A grandes rasgos, la mayor parte de los servidores usa software libre tanto como sistema operativo, así como paquetes de software que permiten instalar y levantar los servicios deseados.

La excepción dentro del diseño se encuentra en el servidor de Directorio Activo, sistema operativo para servicio de videovigilancia y el Firewall. El motivo que impulsa a resolverse por usar software propietario[51] en estos servicios es la seguridad que ofrecen en comparación a soluciones libres y la compatibilidad del software con la cámara de videovigilancia empleada en el presente prototipo que no se acopló a una solución de software totalmente libre.

---

[51] Al contrario del software libre, el software propietario no cumple con alguna o varias de las libertades que permite al usuario del mismo; que en resumen consisten en el acceso a su código,

Haciendo una reseña del decreto 1014 que obliga a las instituciones públicas como es el caso del Ministerio de Inclusión Económica y Social, también se considera que su uso se hará siempre y cuando éste no ponga en riesgo la seguridad de la Institución. Las buenas prácticas referentes a la implementación de seguridad sugieren de manera estricta usar soluciones certificadas (y en la gran mayoría de los casos propietarias) en los puntos más vulnerables de la red de datos debido al soporte efectivo que tienen estas soluciones. En este caso se consideró al Firewall y al Directorio Activo como puntos que requieren de mayor seguridad dentro del diseño propuesto.

4.2.1. DIAGRAMA DEL PROTOTIPO

El diagrama para el prototipo a realizarse se muestra en la figura 4.1. Sobre el gráfico se muestran las direcciones IP principales a usarse en el diseño. Tanto el Switch 1 como el Switch 2 representan los switches de acceso a los puntos de red del primer y quinto piso. El Switch 3 concentra el tráfico de la Zona Desmilitarizada (DMZ) y el tráfico pasa a través del Firewall entre la LAN y la DMZ. Las VLAN se gestionan en el switch de núcleo, el cual concentra el tráfico de los segmentos de red descritos.

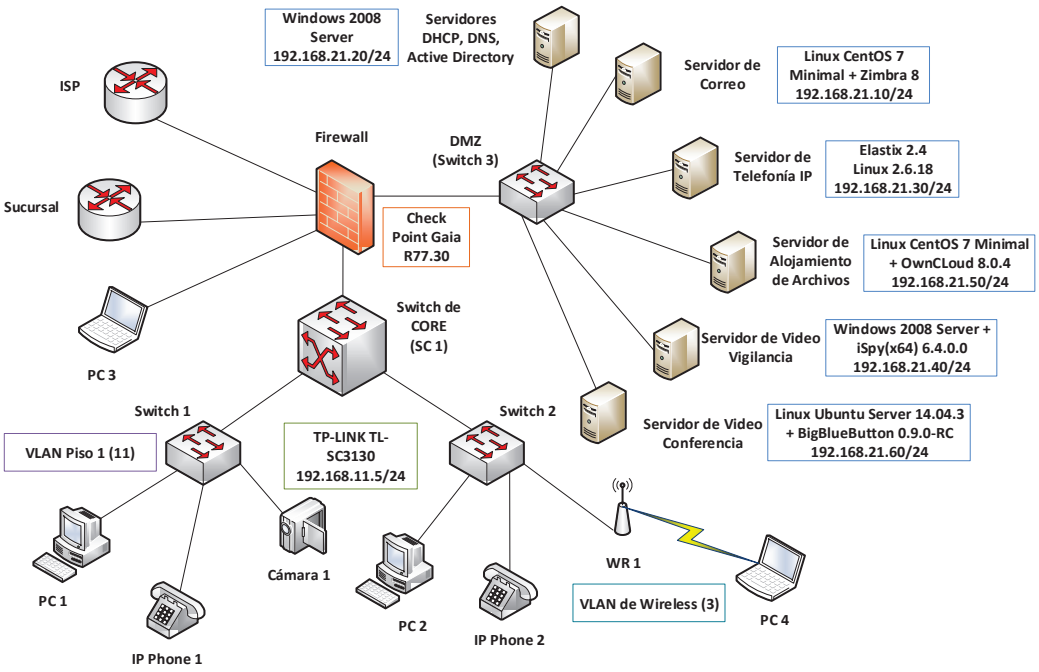

Figura 4.1. Diagrama del prototipo

4.2.2. EQUIPOS DE RED

4.2.2.1. Esquema general

Los equipos de red a utilizarse el prototipo, permiten delimitar tres zonas principales: el segmento de la LAN que permite la comunicación entre los usuarios conectados al switch 1 con el switch 2, el segmento de la zona desmilitarizada y un segmento externo donde el Firewall controla el tráfico generado interna y externamente. Los conmutadores de laboratorio y/o simulación del prototipo, independientemente de la marca y modelo, deberán estar en la capacidad de soportar la norma IEE 802.1Q para permitir el tráfico de VLAN.

4.2.2.2. VLAN

Las VLAN y su respectivo direccionamiento para cada una de ellas, se definen en la tabla 4.1. Las direcciones de los servidores y de los computadores están realizadas en base a dicha tabla. Los scripts de configuración de los equipos de la red del prototipo se adjuntan en el Anexo 5.

ID de VLAN	NOMBRE DE LA VLAN	DIRECCIÓN DE RED	PUERTA DE ENLACE
3	Wireless	192.168.3.0/24	192.168.3.1
10	Planta Baja	192.168.10.0/24	192.168.10.1
11	Piso 1	192.168.11.0/24	192.168.11.1
12	Piso 2	192.168.12.0/24	192.168.12.1
13	Piso 3	192.168.13.0/24	192.168.13.1
14	Piso 4	192.168.14.0/24	192.168.14.1
15	Piso 5	192.168.15.0/24	192.168.15.1
16	Piso 6	192.168.16.0/24	192.168.16.1
17	Piso 7	192.168.17.0/24	192.168.17.1
18	Piso 8	192.168.18.0/24	192.168.18.1
19	Piso 9	192.168.19.0/24	192.168.19.1
20	Piso 10	192.168.20.0/24	192.168.20.1

21	Servidores	192.168.21.0/29	192.168.21.1
22	Impresoras	192.168.22.0/26	192.168.22.1
23	Cámaras de video	192.168.23.0/27	192.168.23.1
24	Biométricos	192.168.24.0/28	192.168.24.1
25	Telefonía IP	192.168.25.0/24	192.168.25.1

Tabla 4.1. Numeración y direccionamiento de las VLAN

4.2.2.3. Access Point (Punto de acceso) [PW2]

Para el presente prototipo se dispone de un Access Point marca Cisco modelo AIR-LAP 1131AG-A-K9, de la serie Cisco Aironet 1130AG. Este dispositivo puede optar entre dos modos de operación, el primero, llamado *lightweight mode* que consiste en la operación del punto de acceso bajo el mando de un dispositivo controlador centralizado (que simplifica la aplicación de configuraciones) dentro de la red como parte de un conjunto de puntos de acceso con características y funcionalidades comunes, mientras que el segundo modo consiste en la operación autónoma, independiente de otros dispositivos controladores. La diferencia entre uno u otro modo depende básicamente de la imagen (sistema operativo del dispositivo) que se encuentre funcionando en el punto de acceso. Dadas las necesidades y características del prototipo, el dispositivo en cuestión trabajará en modo autónomo.

4.2.2.3.1. Características del Access Point

Las principales características de este dispositivo se listan a continuación:

- Soporta los estándares 802.11a y 802.11g.
- Ajuste de transmisión de potencia variable.
- Cobertura omnidireccional.
- Cifrado AES por asistido por hardware.
- Autenticación WPA y WPA2.
- Compatible con alimentación eléctrica a través de Ethernet (802.3af).

Además de todas estas características, dispone de un puerto de consola por donde se puede configurar a través de comandos simples o puede realizarse la

configuración a través de un navegador entrando a la página web de configuración del dispositivo.

Las capturas que muestran la imagen del dispositivo y sus respectivos puertos se muestran en la figura 4.2, nótese que se encuentran de izquierda a derecha los puertos de alimentación, de red y de consola. También se encuentra un botón llamado “MODE”. Para acceder a esta vista es necesario deslizar la tapa del dispositivo.

Figura 4.2. Puertos del Access Point

Cuando el dispositivo se encuentra en operación se puede verificar los indicadores luminosos activos de Ethernet y Radio respectivamente. Cuando se cierra la tapa superior se ocultan los puertos y los indicadores, pero se puede comprobar el estado de la operación del equipo mediante un indicador externo circular. En la figura 4.3 se puede observar al equipo en operación con el indicador en verde.

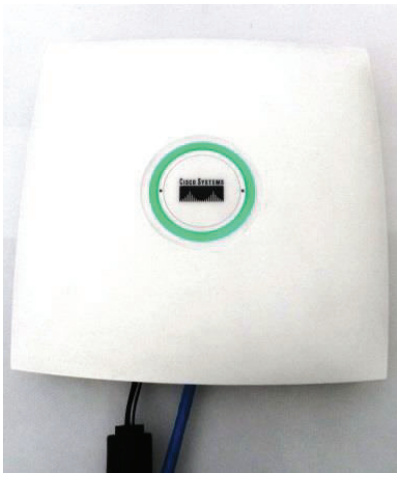

Figura 4.3. Access Point en operación

4.2.2.3.2. Configuración del Access Point

Por defecto, el access point está configurado para operar en modo ligero mediante una controladora de WLAN centralizada. Para entrar en operación autónoma se requiere el cambio de imagen. Ese procedimiento se realiza mediante un servidor TFTP en el cual se aloja la imagen para que el equipo la copie desde su interfaz Ethernet durante el arranque.

El procedimiento a seguir consiste en configurar el servicio TFTP con la imagen requerida y se inicia el access point con el botón MODE presionado. La interfaz del computador que tiene configurado el servicio TFTP debe tener una dirección IP entre 10.0.0.1 y 10.0.0.50. El access point buscará la imagen guardada en el computador a través de su interface Ethernet, luego la imagen es copiada y se descomprime para inicializarse. El procedimiento de copia se muestra en la figura 4.4:

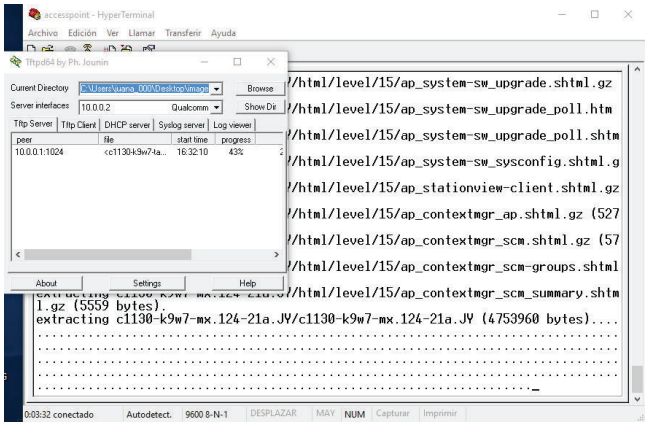

Figura 4.4. Copia de imagen al Access Point

Lo siguiente consiste en configurar la interface del access point para poder continuar la configuración vía web. El procedimiento se realiza inicialmente a través de consola, y los comandos utilizados se describen a continuación:

```
ap>enable
Password: <Password>
ap#configure terminal
ap(config)#interface bvi1
ap(config-if)#ip address <Dirección IP> <Máscara de red>
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#exit
ap#write
```

Los campos <*Dirección IP*> se refieren a la dirección que se le asigna a la interface Ethernet con su respectiva máscara de red identificada en el campo <*Máscara de red*>. La dirección por donde se ingresará vía web posteriormente es a la dirección configurada en este campo, y la contraseña para acceder estará especificada por lo que se coloque en el campo <*Password*>. En la figura 4.5 se muestra la captura del ingreso a la página de configuración del access point.

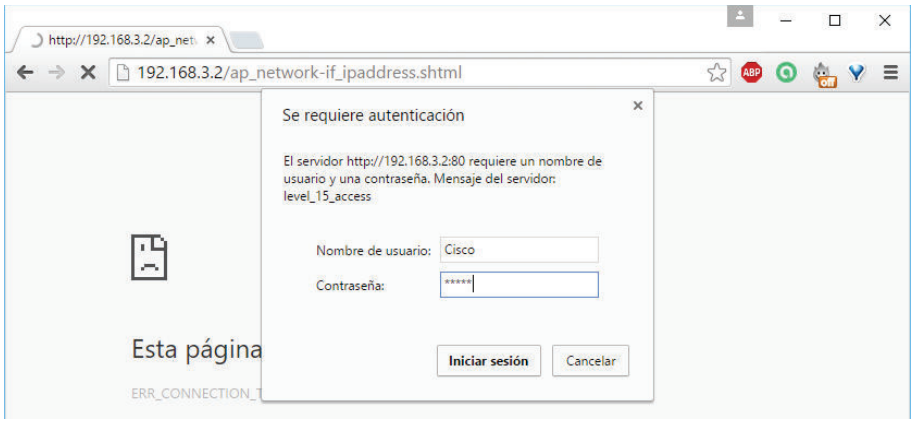

Figura 4.5. Ingreso a configuración del AP

Al ingreso correcto de las credenciales de autenticación se mostrará la pantalla de estado del dispositivo junto con un menú en el lado izquierdo para realizar todas las configuraciones requeridas. La figura 4.6 muestra una captura de la pantalla de estado del dispositivo. Las configuraciones adicionales se detallan en el Anexo 6.

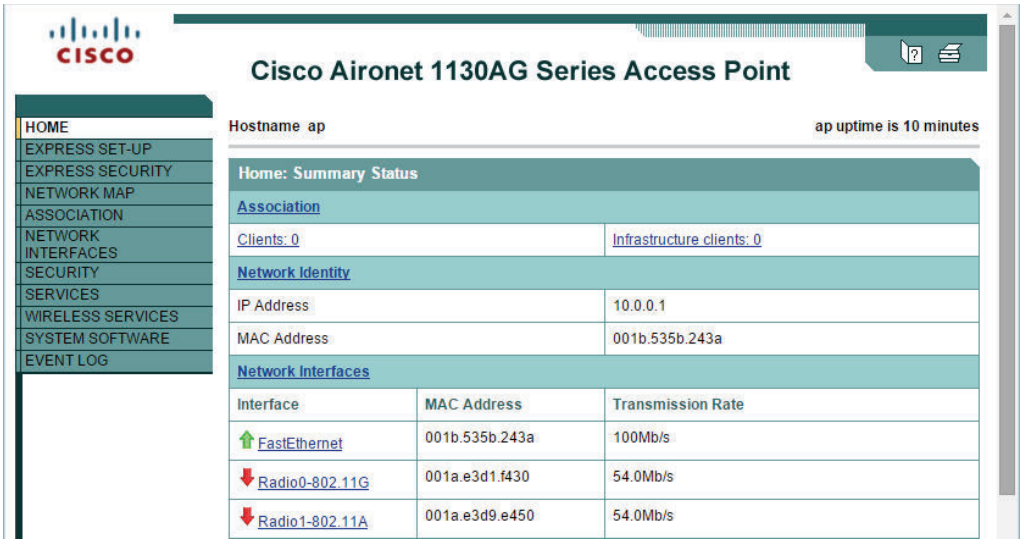

Figura 4.6. Pantalla de estado del AP

4.2.3. SERVIDORES

Para brindar los servicios de la red, se disponen de cinco servidores. La lista de características usadas para la implementación del prototipo se detalla en la tabla 4.2. El servidor de telefonía IP dispone además de un equipo que le permite comunicarse a la PSTN. Dicho equipo contiene un puerto FXO por medio del cual tiene la capacidad de conectarse a una línea analógica y un puerto de red en que permite conectarse a la central telefónica dentro de la red.

Servidor	Sistema Operativo	Paquete/Software	Procesador	Código abierto	Dirección IP
Correo electrónico	Linux Centos 7 Minimal 1503-01	Zimbra Collaboration Suite 8.6.0	x64	Sí	192.168.21.10/24
Directorio Activo, DNS, DHCP	Windows 2008 Server Standard	Servicios propios de Microsoft	X86	No	192.168.21.20/24
Central telefónica	Kernel Linux 2.6.18	Elastix 2.4.0	X86/x64	Sí	192.168.21.30/24
Video vigilancia	Windows 2008 Server Standard	iSpy 64 v6.4.0.0	x64	Sí (servicio) No (S.O.)	192.168.21.40/24
Alojamiento de archivos	Linux Centos 7 Minimal 1503-01	OwnCloud 8.0.4	x64	Sí	192.168.21.50/24
Videoconferencia	Linux Ubuntu Server 14.04.3	BigBlueButton 0.9.0-RC	x64	Sí	192.168.21.60/24
Firewall	Check Point Gaia OS R77.30	Check Point R77.30	X86/x64	No	10.2.70.254

Tabla 4.2. Listado de servidores

La implementación del Firewall así como del resto de servidores no se realizará en dispositivos dedicados (*appliances*). Tanto la instalación y configuración de los sistemas operativos a usar, así como los paquetes de software usados se detallará posteriormente para cada caso.

4.2.3.1. Instalación de Windows Server 2008

En el servidor que contiene Windows Server 2008 se realizará el levantamiento de los servicios de DNS, DHCP y Active Directory. Para tales propósitos se detalla

los pasos a seguir y las principales configuraciones del sistema operativo Windows Server 2008 en el Anexo 7.

4.2.3.2. Instalación de Linux CentOS 7 Minimal 1503-01

Los servidores a cargo de ofrecer correo electrónico con Zimbra, alojamiento y compartición de archivos a través de OwnCloud y las primeras pruebas de videovigilancia con ZoneMinder estarán configurados sobre el sistema operativo Linux CentOS 7 Minimal 1503-01.

Los detalles de la instalación y configuraciones básicas se describen en el Anexo 8.

4.2.3.2.1. Instalación de Webmin 1.75

Webmin es una aplicación que permite administrar el servidor con ambiente web. Es muy útil para cambiar algunos parámetros que son menos sencillos de hacer cuando se hace a través de archivos de configuración del sistema operativo, o sencillamente no se conoce mucho acerca de los servicios instalados, entonces Webmin los reconoce y permite su administración con una interfaz amigable para cada uno de ellos.

La explicación de la instalación y configuraciones básicas de Webmin se detalla en el Anexo 9.

4.2.3.3. Instalación de Linux Ubuntu Server 14.04.3

El servidor de videoconferencia basado en BigBlueButton requiere de manera exclusiva para su correcto funcionamiento trabajar sobre el sistema operativo Linux Ubuntu Server y exclusivamente sobre la versión 14.04.3, según la página de los desarrolladores del software. Por este motivo los pasos para la instalación y configuraciones básicas de este sistema operativo e detallan en el Anexo 10.

4.2.4. FIREWALL

Para el propósito de instalar el Firewall, se optó por usar el software de Check Point en un servidor. El software se llama Check Point Gaia R77.30 el cual es un sistema operativo que contiene las funcionalidades del Firewall - UTM (Gestión

Unificada de Amenazas). Las particularidades de este componente se detallan en al Anexo 11.

4.2.4.1. Pruebas del firewall

El objetivo del firewall es la de gestionar, supervisar y tomar las medidas necesarias en base a las políticas programadas en el equipo entre la red externa y la red interna para brindar seguridad ante el tráfico entrante y saliente de la red. Las configuraciones incluyen políticas a nivel de qué puertos están habilitados al tráfico, que direcciones de destinos u orígenes deben restringirse y qué políticas respecto a la visitas de páginas web deben permitirse o bloquearse al usuario final. El firewall en este caso tiene que inspeccionar las direcciones de los paquetes, e incluso más detalladamente el contenido para encontrar código o palabras clave (llamadas expresiones regulares) para permitir o impedir el tránsito de los mismos.

Por ejemplo, en la figura 4.7 se muestra la restricción ante el intento de navegación en la popular página de YouTube, la regla determina este comportamiento porque es de interés prohibir páginas que consuman mucho ancho de banda, como sucede en este caso. En el ejemplo el firewall bloquea el tráfico que incluso posee contenido cifrado que se dirige al puerto 443 (https) del destino. También se aprecia que se mantiene registrado al usuario con nombre y dirección IP de origen, de esta manera se alerta al usuario acerca de la política, quién está a cargo, además de llevar un registro de los intentos de navegación.

Figura 4.7. Ejemplo de restricción de firewall Check Point

4.3. SERVIDOR DE DIRECTORIO, DNS Y DHCP

El conjunto de los tres servidores se instalarán sobre Windows 2008 Server. Los procesos de instalación en los tres casos son relativamente sencillos, por lo que se adjuntan en el Anexo 12 una serie de capturas en cada caso, para indicar los pasos que se siguieron para levantar cada uno de ellos. En cambio los servicios levantados alternativamente en Linux para este mismo propósito se encuentran en el Anexo 13 con un mayor grado de explicación, puesto que no es muy evidente su configuración.

4.3.1. SERVICIO DNS [PW20]

Este servicio permite hacer resolución de nombre en direcciones IP de manera bidireccional. Su razón de ser es mantener una jerarquía en el dominio de la red, y permitir resolver los nombres a direcciones para que sea más fácilmente accedido por el usuario final.

A continuación se describen los pasos para levantar y configurar estos servicios en Windows y Linux.

4.3.1.1. Pruebas del servicio de DNS

En este punto la comprobación se realiza haciendo una búsqueda del nombre de host en base a las configuraciones realizadas. En el caso del servidor de correo electrónico se le ha asignado la dirección 192.168.21.10 y el nombre a resolverse es correo.mies.com. En el caso de la comprobación mediante consola en sistemas operativos Linux se realiza con los comando *hostname* y *dig* tal como se muestra en los siguientes ejemplos:

```
# hostname

correo.mies.com

# dig mies.com mx

; <<>> DiG 9.9.4-RedHat-9.9.4-18.el7_1.1 <<>> mies.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51040
```

```
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mies.com.                      IN      MX

;; ANSWER SECTION:
mies.com.               38400   IN      MX      10
correo.mies.com.

;; AUTHORITY SECTION:
mies.com.               38400   IN      NS      correo.mies.com.

;; ADDITIONAL SECTION:
correo.mies.com.        38400   IN      A       192.168.21.10

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mié jun 17 11:12:47 ECT 2015
;; MSG SIZE  rcvd: 90
```

En el caso de Windows se puede comprobar de manera muy fácil la resolución de las direcciones cuando se usa un navegador para resolver el nombre del host. En este caso la figura 4.8 nos muestra que somos capaces de obtener respuesta del servidor de correo electrónico (el cual se explicará más adelante) con solo ubicar la dirección https://correo.mies.com.

Figura 4.8. Resolución del servidor DNS

4.3.2. ACTIVE DIRECTORY[PW12]

El servicio de Active Directory permite crear un directorio para administrar los elementos de la red como objetos con propiedades y permisos específicos. Los usuarios y los grupos, por ejemplo, son conjuntos de elementos que disponen de permisos para iniciar sesiones, acceder a archivos, incluso integrarse con otros servicios y sistemas. En el Anexo 12 se muestra una guía gráfica de la instalación y configuración del servicio.

4.3.2.1. Pruebas de Active Directory

Para estas pruebas se realizará el inicio de sesión en un sistema operativo Windows XP Professional luego de conectarse al dominio. Tras arrancar la sesión se comprueba que efectivamente las credenciales fueron aceptadas por el controlador de dominio, por lo tanto se permite el inicio de sesión. En la figura 4.9 se muestran los usuarios que se configuraron para las pruebas. La figura 4.10 muestra la configuración de DHCP en el host cliente donde se va a hacer la prueba.

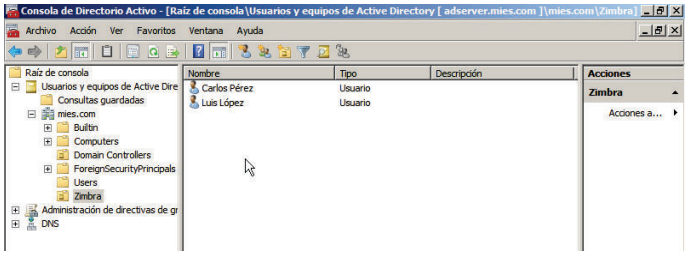

Figura 4.9. Usuarios creados en el directorio activo

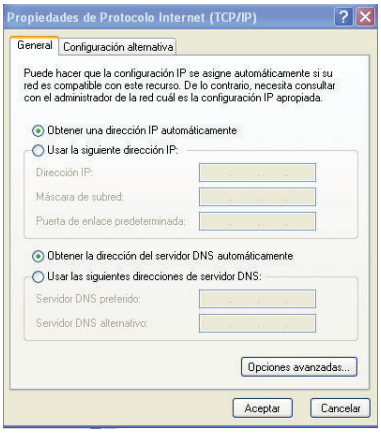

Figura 4.10. Configuración DHCP en cliente

Los pasos realizados para probar que las configuraciones están funcionando correctamente se describen a continuación en el siguiente orden:

- Figura 4.11: El equipo se configura para que se una al dominio mies.com.
- Figura 4.12: Se solicitan las credenciales con las que se une al dominio.
- Figura 4.13: Se da mensaje de bienvenida una vez que el host se autenticó al Active Directory.

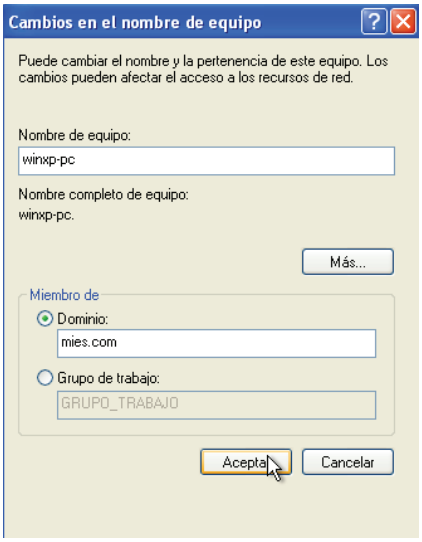

Figura 4.11. Unión de host cliente al dominio

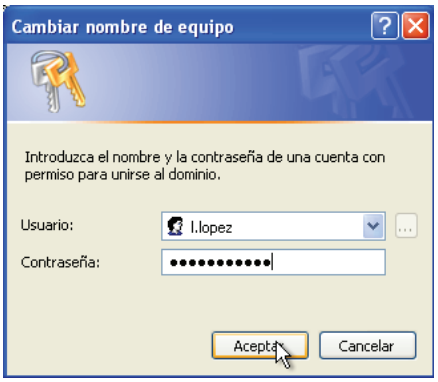

Figura 4.12. Cambios de dominio con credenciales de AD

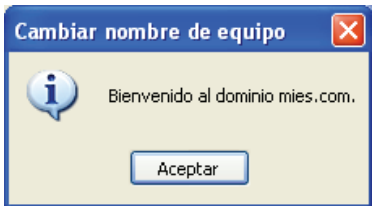

Figura 4.13. Mensaje de bienvenida al dominio

En el siguiente reinicio de la sesión se puede utilizar las credenciales guardadas en Active Directory en el dominio en el que nos unimos en los pasos anteriores. La figura 4.14 muestra el inicio. En la figura 4.15 tenemos como resultado el nombre del usuario en la barra de inicio de Windows tal como se configuró en el directorio activo.

Figura 4.14. Inicio de sesión con credencial definida

Figura 4.15. Sesión iniciada con éxito

En la figura 4.16 se puede verificar que la resolución de nombres del DNS permite conectar a los servidores de correo y almacenamiento usando sus nombres en los navegadores y en vez de sus direcciones IP, además de que el host previamente recibió la dirección IP a través de DHCP. La carpeta del usuario también se

encuentra dentro del dominio. En el mismo ejemplo se puede comprobar que los servicios de DNS, DHCP, Active Directory y el almacenamiento de archivos se encuentra gestionado en el mismo servidor.

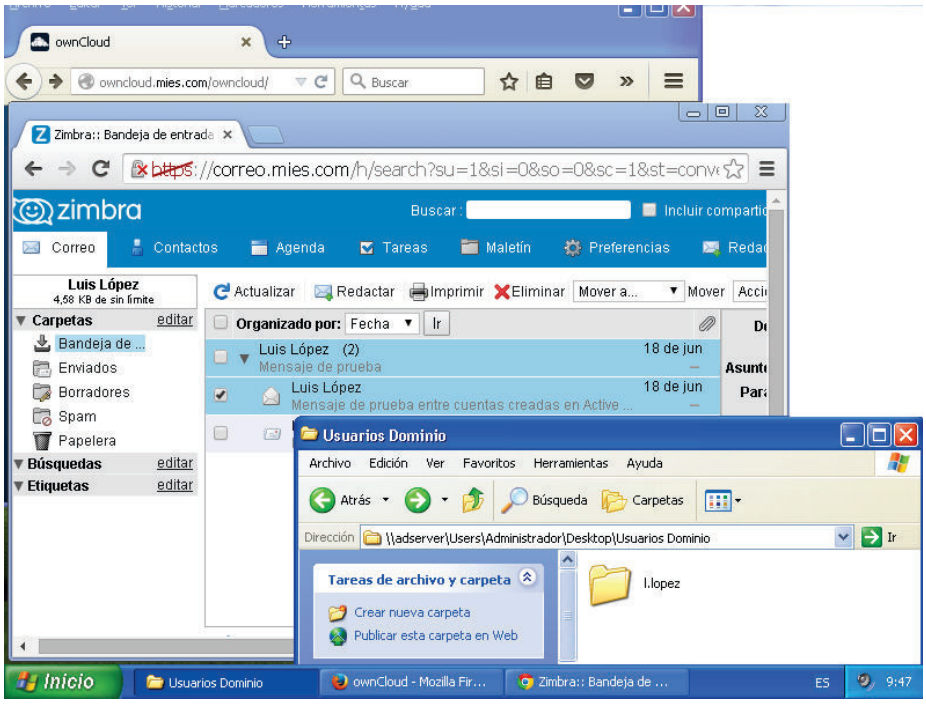

Figura 4.16. Inicio de sesión en Zimbra con usuario de AD

4.3.3. SERVICIO DHCP

Para este servidor se crea uno o varios ámbitos para la asignación de direcciones dinámicas a los computadores que soliciten alguna dentro de la red. La configuración que se muestra a continuación permite definir un POOL de direcciones para ser prestadas. Sin embargo el ámbito solo presta direcciones dentro del mismo segmento lógico de red. Para las VLAN que tienen otras direcciones, los equipos de red deben realizar un procedimiento de *DHCP Relay Agent.* El objetivo es que las peticiones de direcciones pasen de una VLAN a otra.

En equipos Cisco, el comando debe configurarse en el modo de configuración de interfaz, por medio del comando `#ip helper-address <IP del servidor DNS>` en la interfaz por donde recibe las peticiones de DNS. Se comporta como un puente en estos casos.

La configuración de DHCP se detalla en el Anexo 12.

4.4. SERVIDOR DE CORREO ELECTRÓNICO

En esta sección se detallan los pasos para la instalación del servidor de correos. Debido a la exigencia de utilizar software libre en el sector público (el cual consta en el decreto 1014, tal como se explica en el Capítulo 1) se mantendrá para este prototipo el mismo software para servidor de correo que se usa en la institución: Zimbra. La exigencia respecto al uso de correo institucional implica un buen desempeño, en cuyo caso, Zimbra tiene muy buenas prestaciones en lo que refiere a soluciones de código abierto para servicio de correo.

Zimbra permite ingresar a los buzones de correo vía web (a través de un navegador de Internet por medio del puerto 443 – https, aunque también puede configurarse para usar el puerto 80 como un servicio http sin encripción) y también permite integrar un cliente de correo para escritorio. Zimbra también posee un cliente de escritorio, pero también es compatible con otras soluciones de código abierto, como por ejemplo Mozilla Thunderbird.

4.4.1. ZIMBRA COLLABORATION OPEN SOURCE EDITION [PW13] [PW14]

Zimbra Collaboration Open Source Edition es una suite de proyectos de código abierto colaborativos, los cuales en conjunto dan forma a un servicio de correo con utilidades adicionales como (entre algunas) calendario y manejo de contactos y búsqueda avanzada. La funcionalidad completa le permite trabajar como servidor IMAP y POP3.

Actualmente, Zimbra Inc. (la compañía creadora del servidor de correo Zimbra) fue comprada por Telligent. Antes de su venta en julio del 2013 era propiedad de VMware. Desde su fundación, la suite se creó y ha permanecido como una distribución colaborativa de código abierto. En base a este proyecto también se han lanzado al mercado otras distribuciones privadas con funcionalidades extras de manera comercial.

Para el presente prototipo se realizará la implementación de un servidor de correo con la versión colaborativa de Zimbra. La versión a utilizarse es la 8.6.0 GA Release. La instalación se la realizará en el sistema operativo Linux Centos 7 Minimal 1503-01. El objetivo de usar esta distribución es la de instalar la menor

cantidad de componentes del sistema operativo para enfocar los recursos de hardware al óptimo desempeño del servidor de correo, y en cumplimiento con el uso de software libre en organismos gubernamentales.

4.4.1.1. Instalación de Zimbra

Los detalles de la instalación de Zimbra ZCS 8.6.0 sobre Linux CentOS 7 Minimal se encuentran en el Anexo 14.

4.4.1.2. Configuración de Zimbra

Se ingresa con el usuario administrador en la pantalla de *login* en un navegador apuntando a la dirección IP del servidor, a través del puerto 7071, tal como se muestra en la figura 4.17.

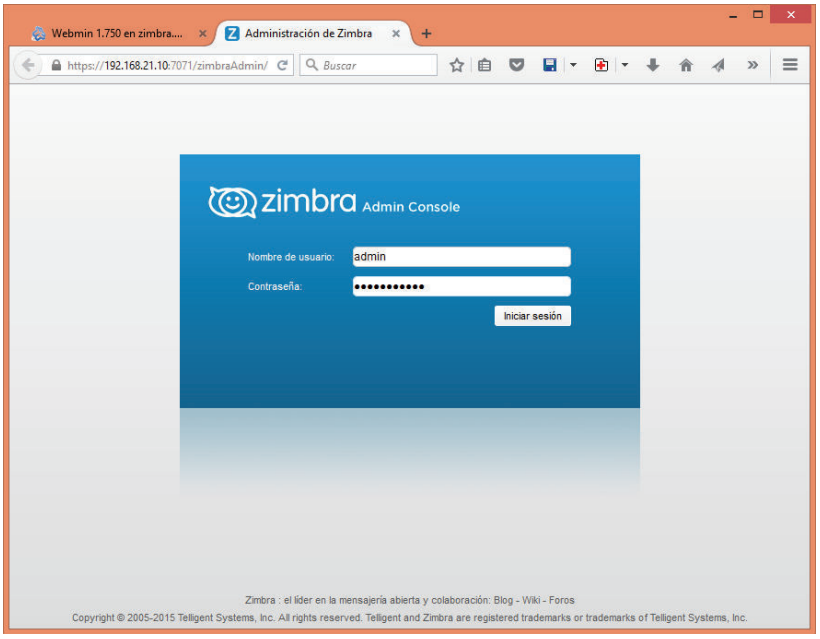

Figura 4.17. Ingreso a Zimbra como administrador

Una vez dentro de la interfaz de administración del correo, tal como lo muestra la figura 4.18, se debería comprobar que todos los servicios se encuentren levantados mediante un visto en el lado izquierdo de cada uno. Normalmente basta que uno de los servicios esté parado para que el comportamiento del correo sea anormal o totalmente disfuncional. En otras palabras, el hecho de entrar a la consola de administración no es garantía de que la totalidad del servicio se

encuentre bien. El resto de configuraciones para crear usuarios se detallan en el Anexo 14.

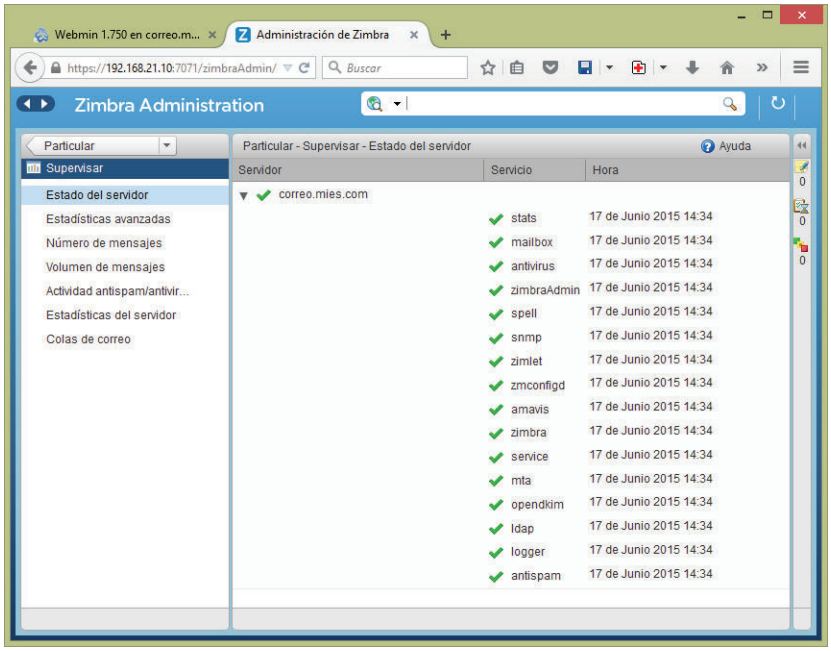

Figura 4.18. Consola de administración de Zimbra

4.4.1.3. Pruebas preliminares

Para el ingreso de los usuarios normales se debe ingresar por la dirección del servidor, sin el número del puerto como es el caso de la consola de administración. En este caso la dirección es https://192.168.21.10 como se muestra en la figura 4.19. Se está utilizando un usuario creado en Zimbra para el ejemplo.

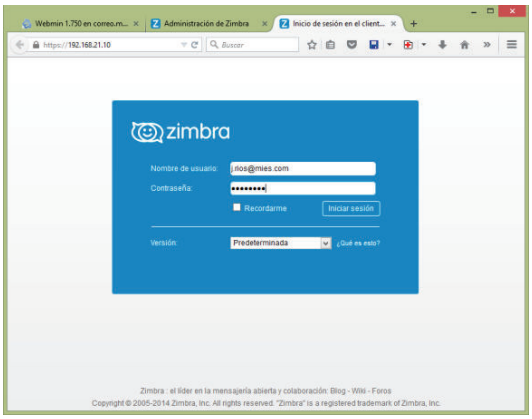

Figura 4.19. Ingreso de usuarios comunes a Zimbra

El primer ingreso a la pantalla de la cuenta se muestra como la figura 4.20.

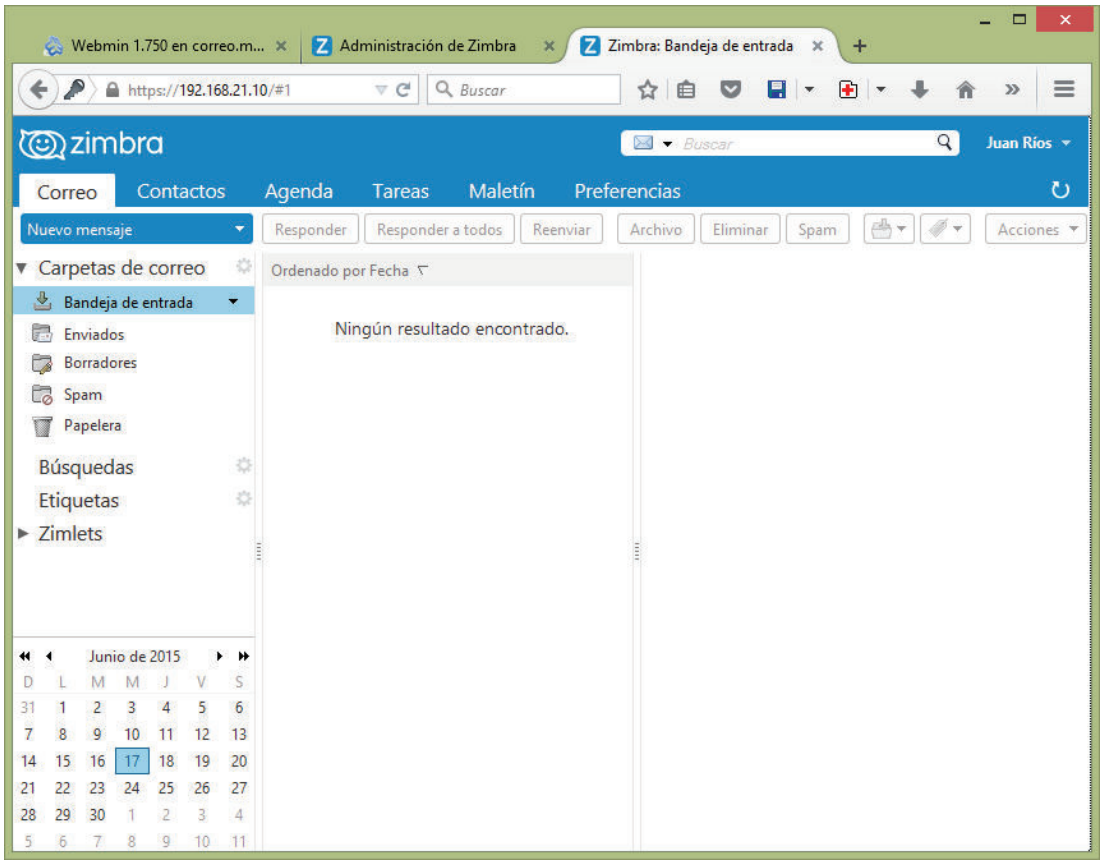

Figura 4.20. Buzón del usuario vacío

Al tratar de editar el mensaje y dirigirlo a un contacto automáticamente dará como resultado el nombre más aproximado, tal como se visualiza en la figura 4.21 en donde se lista otro usuario creado en el sistema.

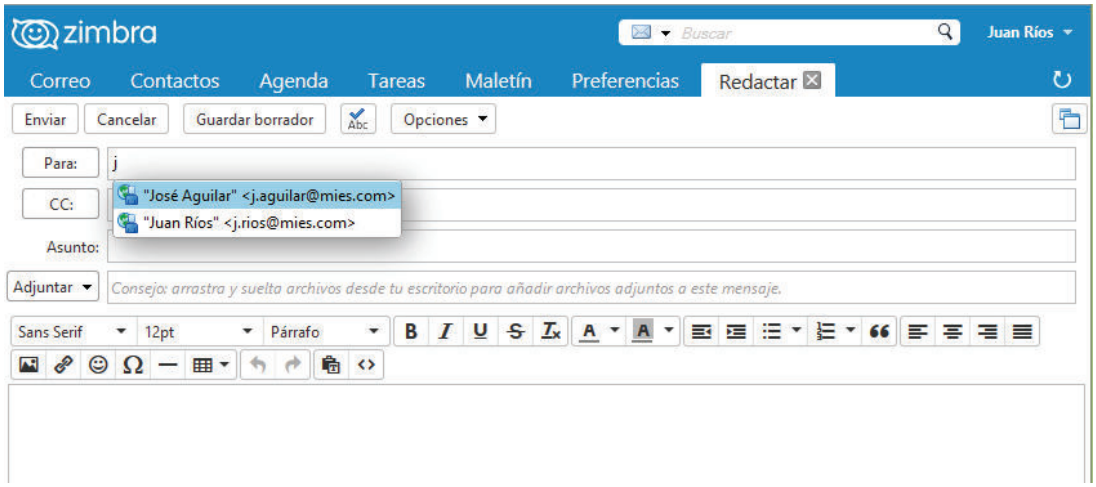

Figura 4.21. Destinatario de correo

A continuación se ha editado un correo de prueba para ser enviado y comprobar que los módulos de Zimbra se encuentran operando con normalidad y que no exista ningún impedimento a nivel de puertos, como se ilustra en la figura 4.22.

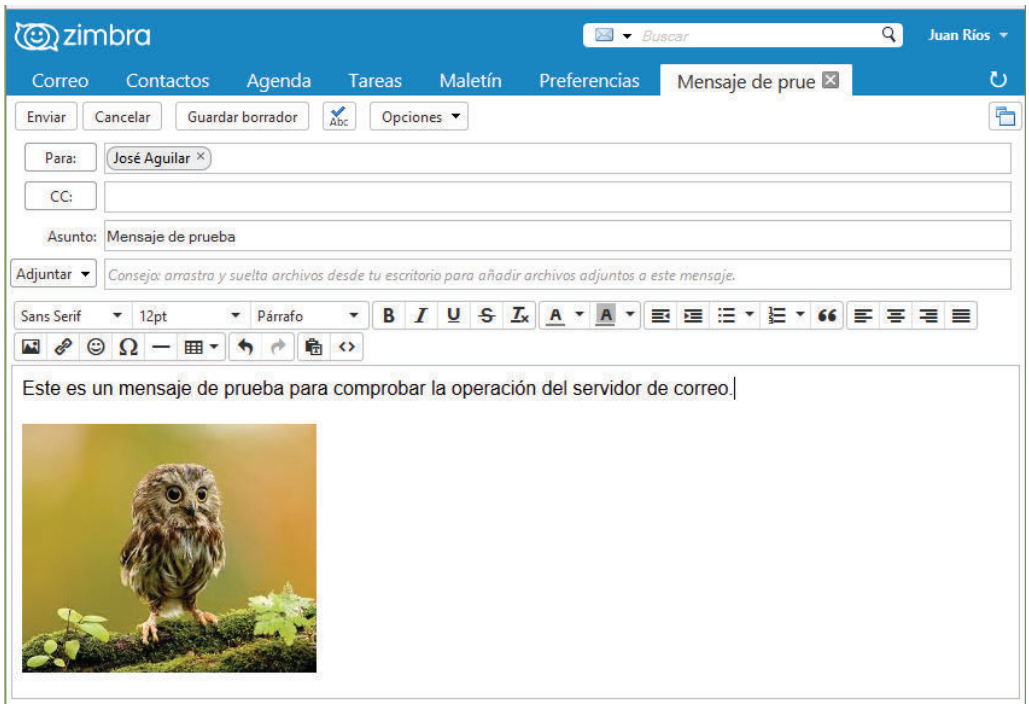

Figura 4.22. Edición de mensaje de prueba

El mensaje es correctamente almacenado en la bandeja de enviados, como se muestra en la figura 4.23. La siguiente comprobación consiste en verificar la llegada del mensaje en el buzón del usuario destino, dicha comprobación se verifica en la figura 4.24.

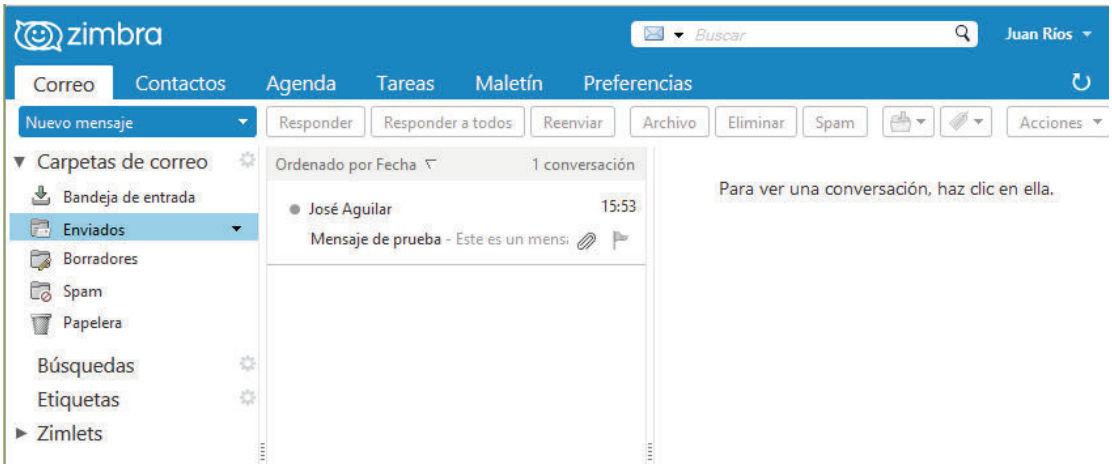

Figura 4.23. Bandeja de mensajes enviados

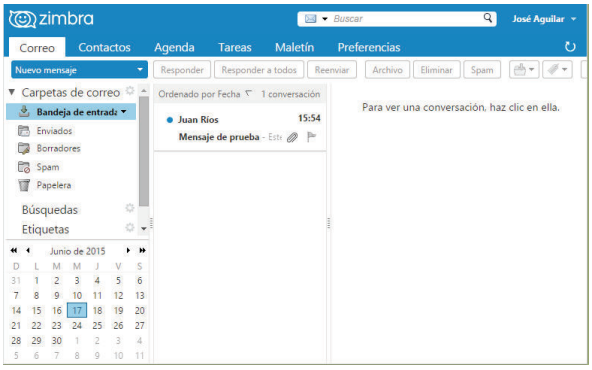

Figura 4.24. Mensaje recibido en la bandeja del destinatario

Al abrir el mensaje se despliega la información enviada por el primer usuario junto con la imagen añadida, como se muestra en la figura 4.25.

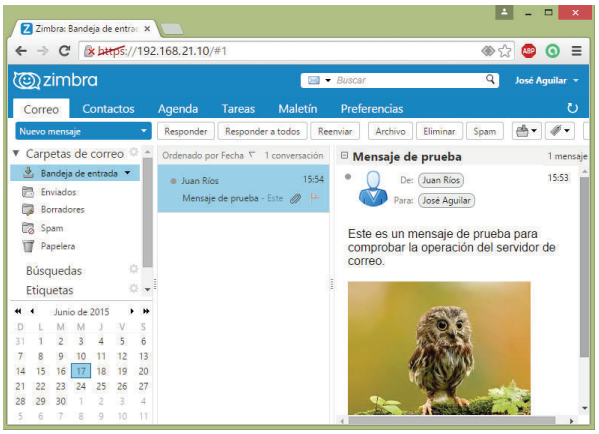

Figura 4.25. Mensaje mostrado en el receptor

El cuerpo del mensaje puede ser revisado en la opción de “Mostrar Original” dentro de las opciones del mensaje recibido en el menú de “Acciones”, tal como se detalla en la figura 4.26.

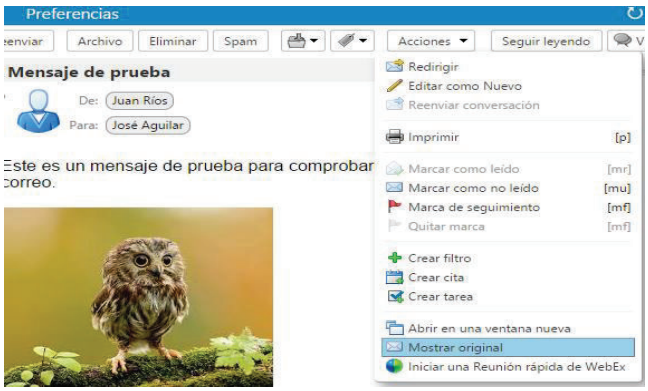

Figura 4.26. Acceso al cuerpo original del mensaje

El cuerpo del mensaje tiene información del trayecto del mensaje en su cabecera. Hay información de las direcciones, dominios y banderas de SPAM. Este control permite a Zimbra trabajar con valores numéricos para determinar mediante una calificación si un mensaje es seleccionable como SPAM o peligroso. La calificación se realiza en base a varios parámetros relacionados a la reputación de las direcciones que se encuentran en listas blancas y negras, entre otros aspectos. La figura 4.27 muestra el cuerpo del mensaje del ejemplo anterior.

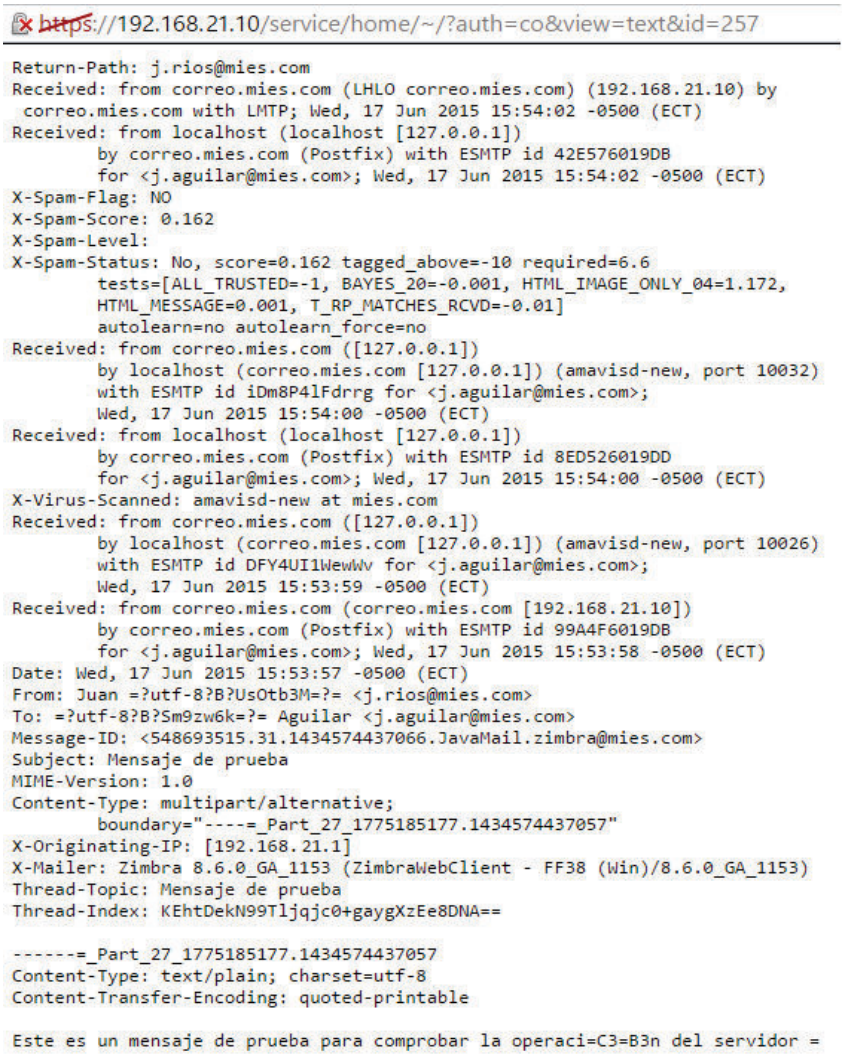

Figura 4.27. Cuerpo original del mensaje

4.4.2. PRUEBAS DEL SERVICIO DE CORREO ELECTRÓNICO

Las pruebas del servicio de correo mostradas en el apartado anterior detallan pruebas con usuarios locales creados y configurados en Zimbra. Lo que se

pretende a continuación es realizar pruebas con usuarios creados en Active Directory y sincronizados con Zimbra.

Los pasos realizados para sincronizar los dos servicios se detallan en el Anexo 14 junto con todas las configuraciones anteriores.

En la figura 4.28 se está realizando el ingreso al correo electrónico en Zimbra con las credenciales de un usuario del directorio activo. El usuario creado se llama “Luis López” y su nombre de usuario es l.lopez.

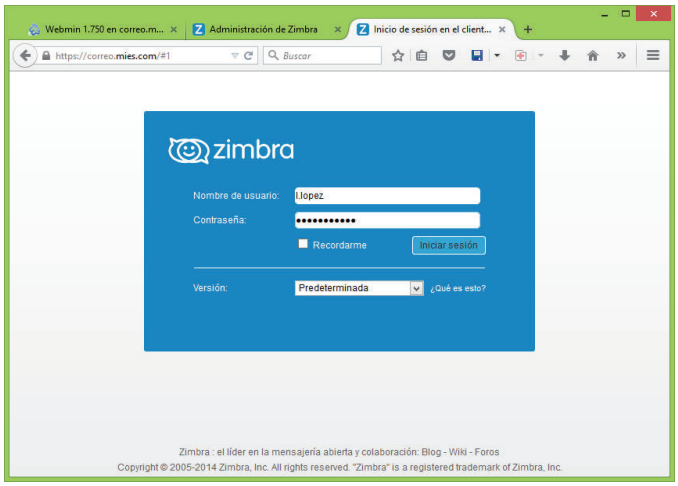

Figura 4.28. Usuario de AD en Zimbra

La figura 4.29 muestra al usuario creando un mensaje de correo. Como destinatario Zimbra aún conserva los usuarios creados en su propio sistema.

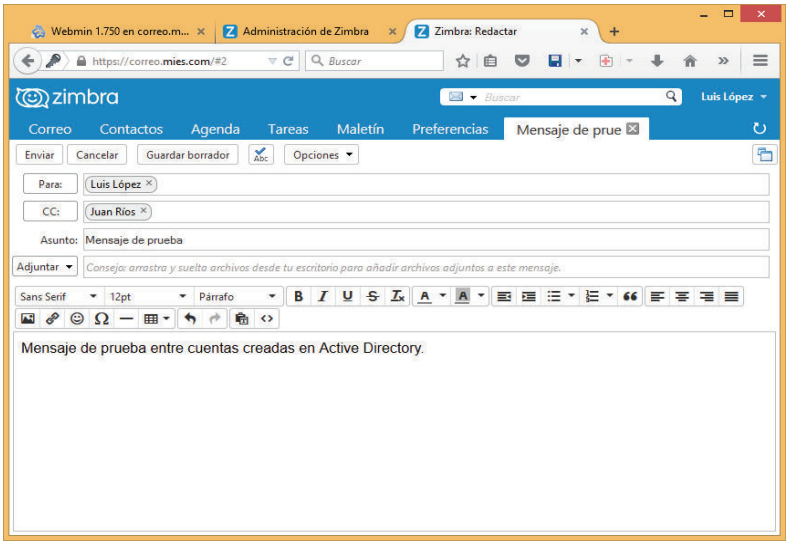

Figura 4.29. Mensaje de prueba de usuario de AD

Finalmente el mensaje es enviado a su propio correo y puede ser recuperado de la bandeja de entrada. La figura 4.30 demuestra que el usuario creado a partir de la integración de Zimbra con Active Directory tiene la msima funcionalidad que los usuarios creados inicialmente en el sistema como ocurrión con los ejemplos anteriores.

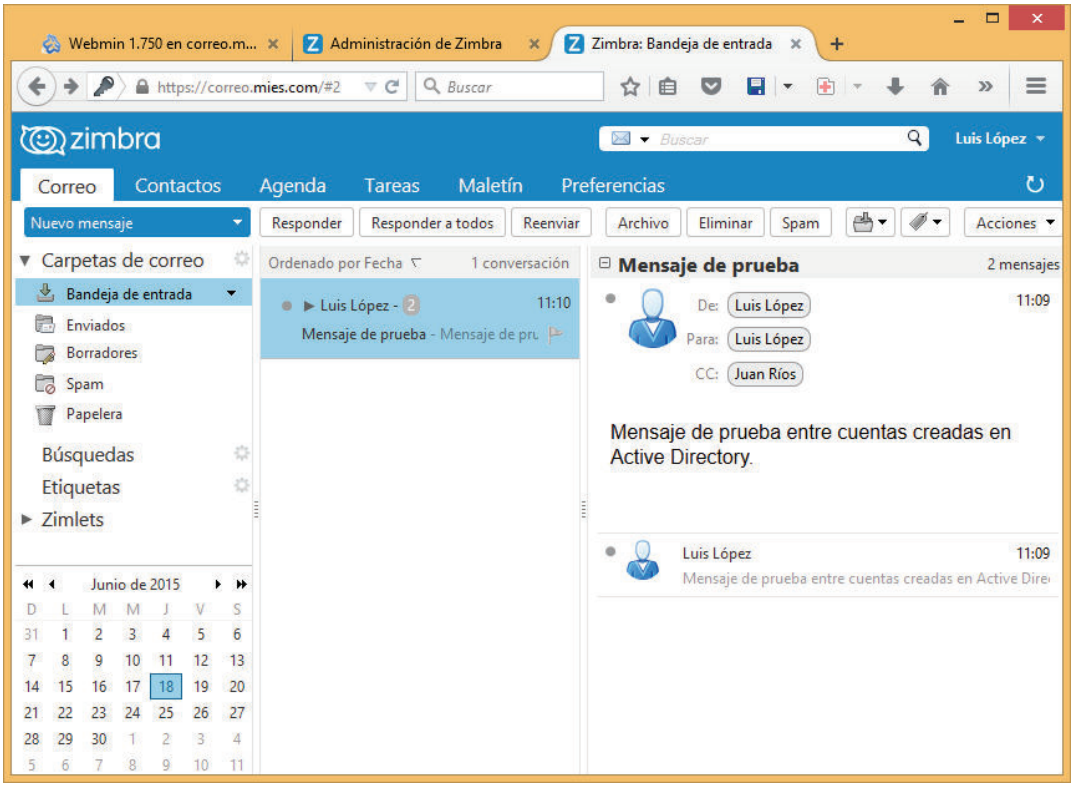

Figura 4.30. Usuario de AD recibe mensaje satisfactoriamente

4.5. SERVIDOR DE TELEFONÍA IP

El servicio de telefonía, utiliza el protocolo IP para transmitir la voz a través de paquetes por la red de área local. A diferencia con tecnologías antiguas, la infraestructura para telefonía IP es la misma que la de datos.

Las soluciones comerciales basan la gran mayoría de sus productos en un núcleo de software libre llamado Asterisk (desarrollado por la empresa Digium), el cual tiene la funcionalidad de una central completa, pero cuya administración se realiza a través de archivos de texto plano. Esto permite la proliferación de soluciones basadas en su núcleo.

4.5.1. SOFTWARE DE PBX IP ELASTIX

Consiste en una solución de software libre auspiciada por la empresa ecuatoriana Palosanto Solutions y se conoce en el mercado como Elastix. El giro de negocio entorno a esta solución permite (al igual que Zimbra) tener una solución gratuita a cargo de una comunidad y una versión pagada soportada por los desarrolladores. Esta solución también incorpora Aterisk en su núcleo, y añade algunas funcionalidades que le permiten tener servicios adicionales como correo electrónico, por ejemplo.

En este ejemplo se utilizará la distribución comunitaria, en la versión 2.4.0. La lista de las versiones de los componentes que incluye esta solución se lista en la figura 4.31.

Detalles de las versiones de los paquetes

(Modo Texto)

Name	Package Name	Version	Release
Kernel			
	Linux(x86_64)	2.6.18	371.1.2.el5
Name	**Package Name**	**Version**	**Release**
Elastix			
	elastix	2.4.0	8
	elastix-a2billing	1.9.4	5
	elastix-addons	2.4.0	10
	elastix-agenda	2.4.0	14
	elastix-asterisk-sounds	1.2.3	1
	elastix-email_admin	2.4.0	6
	elastix-endpointconfig2	2.4.0	2
	elastix-extras	2.4.0	5
	elastix-fax	2.4.0	4
	elastix-firstboot	2.4.0	4
	elastix-framework	2.4.0	19
	elastix-im	2.4.0	2
	elastix-my_extension	2.4.0	6
	elastix-pbx	2.4.0	18
	elastix-portknock	0.0.1	0
	elastix-reports	2.4.0	10
	elastix-security	2.4.0	9
	elastix-system	2.4.0	13

Figura 4.31. Versión de Elastix

4.5.1.1. Instalación de Elastix

Elastix usa como base el sistema operativo Linux CentOS. La instalación no es muy diferente a la descrita en el Anexo 8. Debido a que se usan versiones más antiguas, los menús para configuración de hora, zona horaria, dirección IP y nombre de host son parecidos a lo explicado en el caso del sistema operativo CentOS 7. La instalación y configuraciones básicas de este software se detallan en el Anexo 15.

4.5.2. GATEWAY GRANDSTREAM HT503

Provee un puerto FXO para poder transmitir las comunicaciones generadas por la IP PBX hacia la PSTN. Posee un puerto adicional para hacer un puente y permitir el paso de la llamada hacia un puerto FXS a manera de puente. También puede configurarse para usar su puerto FXS como un punto adicional y permitir la conexión de un teléfono analógico a la IP PBX. Ninguna de las dos últimas opciones será usada en este diseño.

El dispositivo físico es relativamente pequeño. Las figuras 4.32 y 4.33 muestran la parte frontal y posterior del dispositivo:

Figura 4.32. Gateway Grandstream HT503 – Vista frontal

El puerto FXO corresponde al puerto marcado como “LINE”, mientras que el puerto FXS está marcado como “PHONE”, éste no será usado. Además posee un puerto LAN, un puerto WAN, un botón RESET y un puerto de alimentación.

Figura 4.33. Gateway Grandstream HT503 – Vista Posterior

En la figura 4.34 se muestra el equipo en operación. Los indicadores luminosos muestran que puertos físicos están siendo usados. Esto incluye los puertos FXO y FXS.

Figura 4.34. Gateway Grandstream HT503 en funcionamiento

4.5.2.1. Configuración de puerto FXO

Las configuraciones de este dispositivo se realizan en un ambiente web mediante el uso de un navegador.

Cuando se encuentra el equipo con las opciones de fábrica tras un *reset*, es necesario configurar la IP y hostname para continuar con el resto de configuraciones. Todas las configuraciones aplicadas en el dispositivo, tanto las básicas como las necesarias para que el equipo pueda comunicarse adecuadamente con la central se detallan en el Anexo 16.

4.5.3. SOFTPHONES

Para el presente prototipo se ha usado un softphone diseñado para Windows, llamado Zoiper. La versión más básica (freeware) permite registrar dos cuentas SIP. Otras características más avanzadas se obtienen con la versión pagada.

Tras la instalación del software se inicia una ventana que tiene aspecto de teléfono. Entre sus principales funciones dispone de un espacio para almacenar contactos, un historial de marcado, una pantalla parecida al teclado de un teléfono y un historial de llamadas, tal como se muestra en la figura 4.35. El software puede configurarse para iniciar en tiempo de arranque.

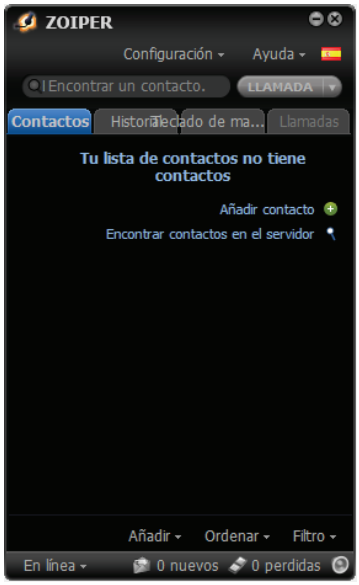

Figura 4.35. Pantalla principal de Zoiper

Las configuraciones básicas permiten ingresar la dirección IP de la PBX, el nombre de usuario, la contraseña y el nombre con el que quiere registrarse el usuario para detectar al originario durante una llamada. La figura 4.36 muestra estos campos.

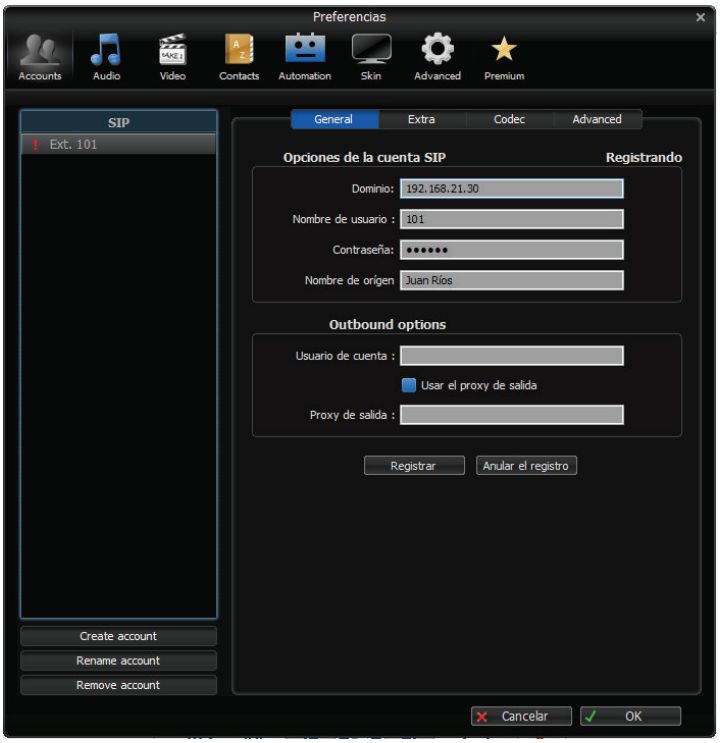

Figura 4.36. Configuración de Zoiper

Cuando la extensión ha sido registrada en la central tras la configuración, un visto aparece en la sección izquierda del menú tal como se muestra en la figura 4.37.

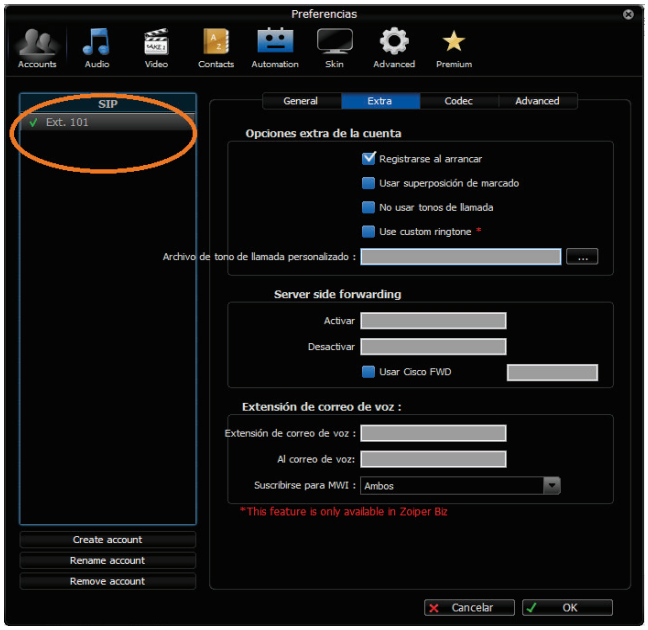

Figura 4.37. Registro de extensión en Zoiper

La pantalla estilizada del teléfono es amigable y fácil de usar, como si se tratara de un teléfono real. La figura 4.38 muestra una captura del mismo.

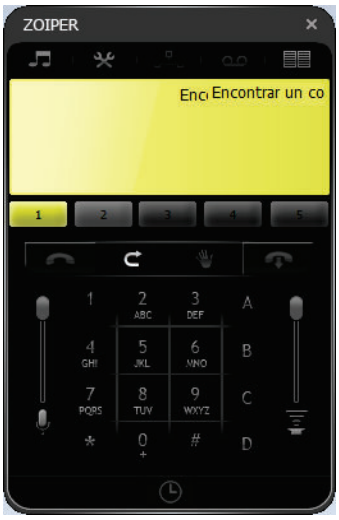

Figura 4.38. Pantalla del teléfono virtual Zoiper

4.5.4. PRUEBAS DEL SERVICIO DE TELEFONÍA IP

El softphone Zoiper también está disposible para smartphones, en este caso se instaló en un teléfono con sistema operativo Android. Similar al caso de los

softphones de PCs de escritorio también debe registrarse la extensión. La configuración se meustra en la figura 4.39.

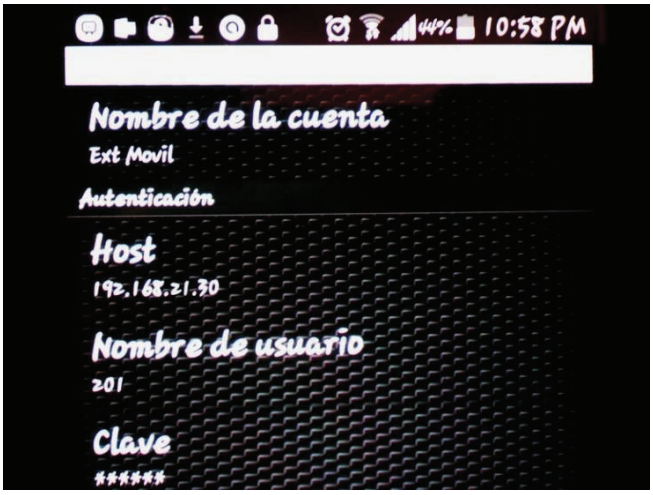

Figura 4.39. Configuración de Zoiper en smartphones

Una extensión registrada aparece con el mensaje en la pantalla, tal como en la figura 4.40:

Figura 4.40. Extensión registrada en smartphone

Haciendo una llamada entre los dos softphones, la llamada generada por el primer teléfono es registrada rápidamente por el segundo, tal como se muestra en la figura 4.41.

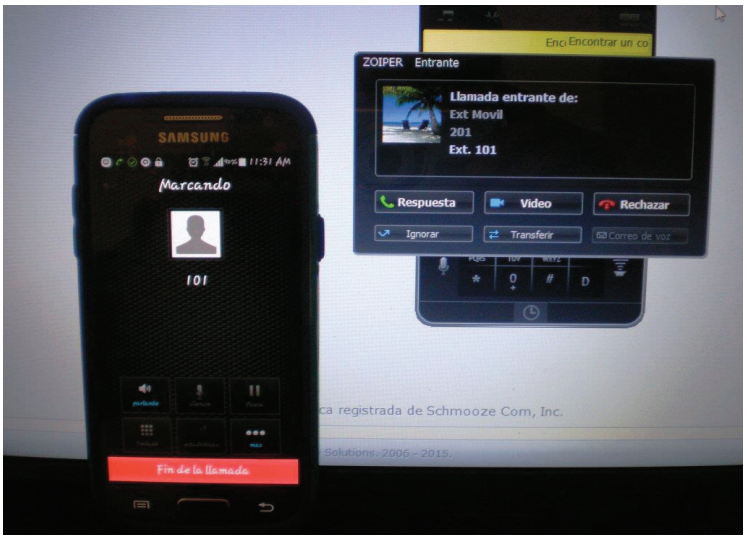

Figura 4.41. Llamadas entre dos extensiones

La llamada se registra en el teléfono, con el número de extensión y el nombre que se usó para registrar el teléfono. La figura 4.42 muestra el momento en que se recibe una llamada.

Figura 4.42. Recepción de llamada en Zoiper

De la misma manera, una llamada hecha desde el softphone del computador es registrada al ser recibida por el softphone en el teléfono. Se registra de la misma

manera el número de extensión y el nombre del usuario, tal como se muestra en la figura 4.43:

Figura 4.43. Recepción de llamada en Smartphone con Zoiper

4.6. SERVIDOR DE ALOJAMIENTO DE ARCHIVOS

El propósito de disponer de un servidor de almacenamiento de archivos es mantener el almacenamiento de archivos de una manera centralizada y ordenada. Dependiendo de las necesidades de la organización, los archivos deben permitir un manejo seguro, al cual se permite el acceso con el uso de contraseñas. Otra necesidad común es la de compartir archivos entre varios usuarios de la red de una manera eficiente. Además, en muchos casos es necesario tener un conjunto de archivos a los cuales pueda acceder el público. En cualquier escenario se requiere de un método para hacerlo.

Las propuestas que se plantean en los siguientes párrafos consisten en el manejo de dos soluciones. En el modelo de servidores que usan Windows este objetivo se logra a través de carpetas compartidas desde el servidor. En soluciones abiertas, como es el caso de OwnCloud, se puede almacenar y compartir archivos con mucha flexibilidad, también permite sincronizar archivos mediante una aplicación cliente que se sincroniza con el servidor.

4.6.1. CARPETAS COMPARTIDAS EN AMBIENTE WINDOWS

En apartados anteriores se muestra el uso del servidor de directorio activo de Windows Server. Dentro del mismo servidor se pueden crear directorios de almacenamiento a los cuales se pueden acceder mediante contraseñas. Los elementos dentro de estos directorios también se pueden compartir con otros usuarios dentro de la red. Básicamente esto es lo que hace un servidor de archivos.

Por ejemplo, el usuario Luis López puede acceder a una carpeta creada dentro del servidor, con su propia contraseña que ocupa para iniciar sesión se puede centralizar su uso, con lo cual se ofrece seguridad de los datos.

En la figura 4.44 se muestra la carpeta dentro del servidor:

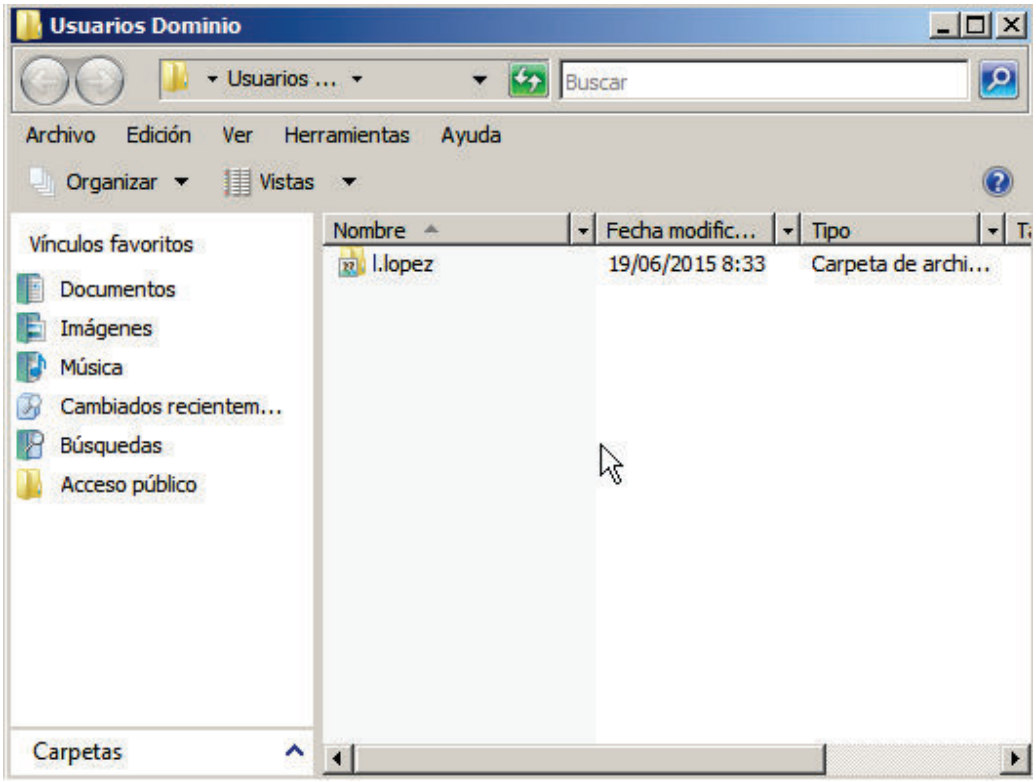

Figura 4.44. Carpetas compartidas en servidor Windows

La forma de asignar recursos compartidos en este ambiente es sencilla. Basta con compartir la carpeta y seleccionar con que usuario o grupo se desea hacer esta compartición, y asignar el nivel de permisos que se requiere para cada caso. La figura 4.45 refleja lo explicado:

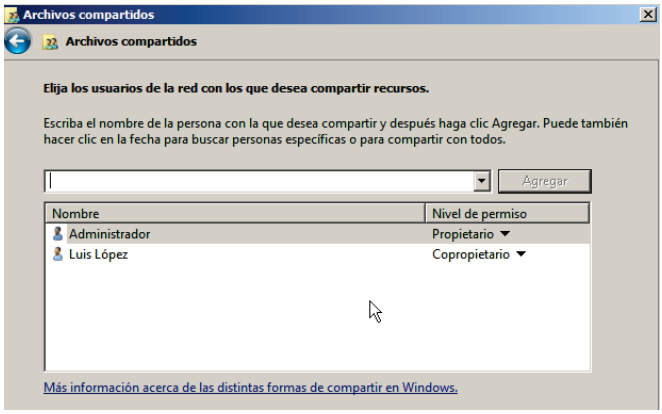

Figura 4.45. Compartición de una carpeta en ambiente Windows

Los usuarios dentro de la red pueden acceder a estos recursos apuntando a la dirección del mismo. Las políticas asignadas a dichos recursos permitirán que se pueda ingresar de manera simple o con contraseñas. Dependerá de eso también los permisos de lectura/escritura dentro de los directorios compartidos. En la figura 4.46 se observa el ingreso al recurso compartido de las figuras anteriores por parte del usuario autorizado para hacerlo.

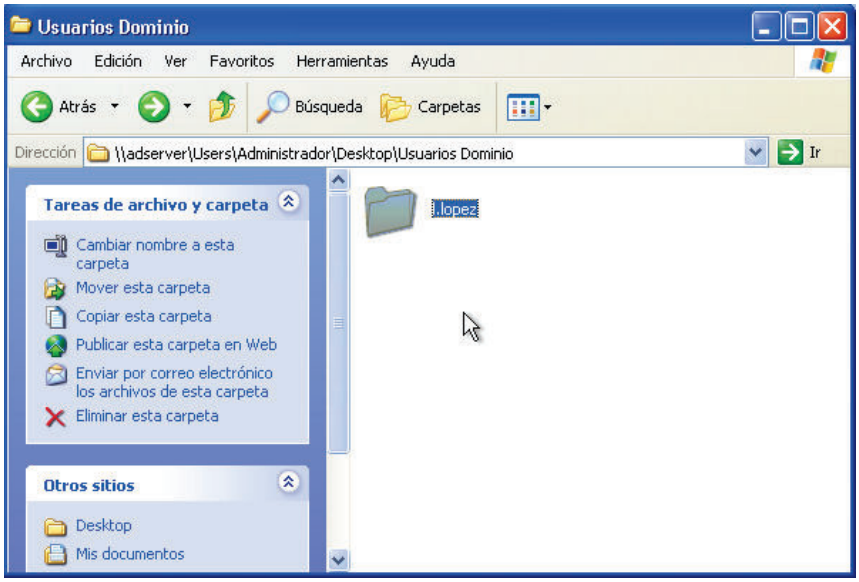

Figura 4.46. Ingreso a compartidas en Windows

4.6.2. OWNCLOUD SERVER [PW10] [PW21]

OwnCloud es una distribución de software libre con la capacidad de almacenar archivos y acceder a aplicaciones en una nube privada. Difiere de alternativas comerciales de este estilo con la facilidad de que el usuario haga su propia

instalación dentro de un servidor. Esta diferencia de paradigma ofrece al usuario final mayor seguridad y confidencialidad de su propia información.

Más adelante se explica cómo levantar este aplicativo en un servidor con Linux CentOS 7 Minimal, su integración con el servicio de directorio activo y la sincronización con un aplicativo “cliente” en el equipo del usuario final.

4.6.2.1. Instalación de OwnCloud Server

La instalación de OwnCloud varía entre cada sistema operativo y entre cada distribución. En un ambiente de consola como ocurre con CentOS Minimal se requieren seguir algunos pasos para asegurar la correcta configuración. Los detalles de la instalación y configuración se detallan en el Anexo 17.

4.6.3. PRUEBAS DEL SERVICIO DE ALOJAMIENTO DE ARCHIVOS

Para la realización de pruebas, primero se realizó la integración del servicio de OwnCloud con Active Directory. Al igual que el caso de Zimbra, OwnCloud posee su por defecto su propia administración de usuarios dentro de una base de datos, sin embargo, se usarán los usuarios creados para la integración con Zimbra explicados en apartados anteriores para demostrar la ventaja de disponer centralización de usuarios en un directorio activo así como la flexibilidad de OwnCloud. Los detalles de cómo configurar la integración de OwnCloud con Active Directory se detallan en el Anexo 17.

Los usuarios importados pueden acceder a través de un navegador web con sus respectivas credenciales usadas dentro del directorio activo, tal como se presenta en la imagen 4.47.

Figura 4.47. Inicio de sesión en OwnCloud

El usuario se encontrará con el mensaje de bienvenida al sistema:

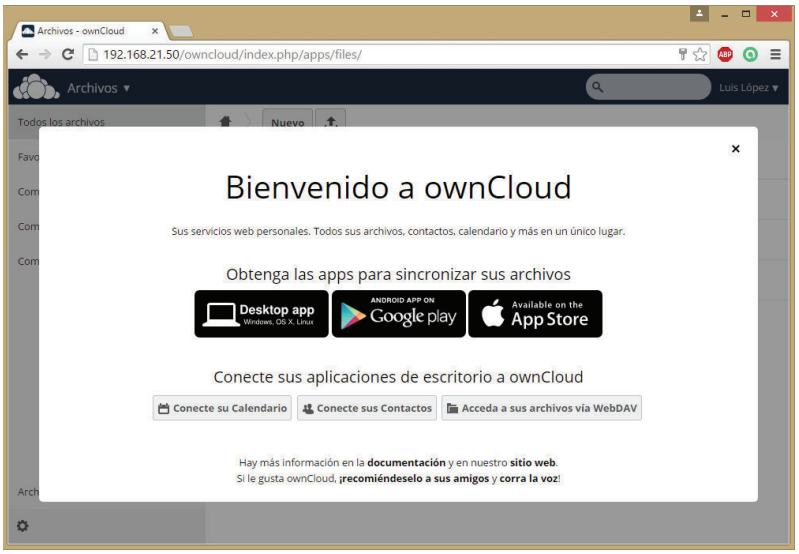

Figura 4.48. Pantalla de bienvenida en OwnCloud

Finalmente se encontrarán todos los archivos creados por defecto para el primer uso, así como un menú de los directorios y herramientas ubicadas a la derecha de cada archivo, como se describe en la figura 4.49.

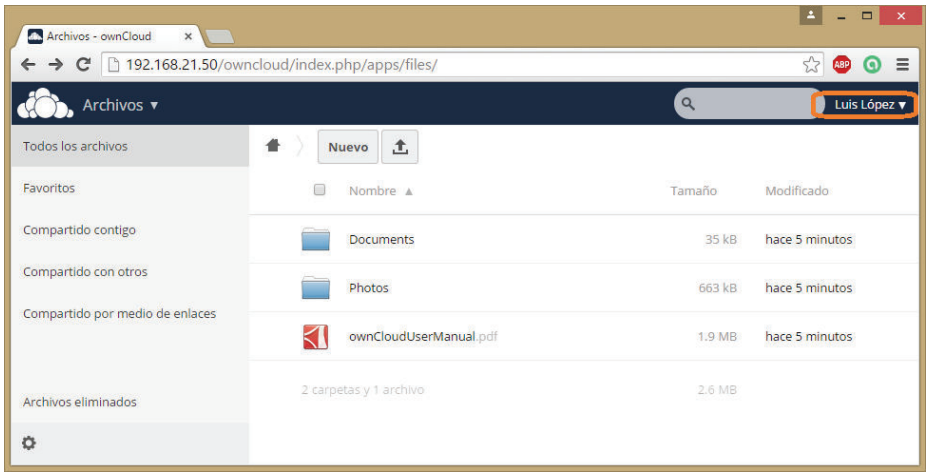

Figura 4.49. Listado de archivos almacenados en OwnCloud

4.6.3.1. Owncloud Client

OwnCloud Client es un aplicativo que permite la sincronización de los archivos que un usuario tiene en su cuenta con una carpeta en su computador. Esto presupone una ventaja añadida a la funcionalidad de cualquier servidor de

archivos: la capacidad de respaldar la información en su computador, o en varios equipos. El detalle de la instalación y configuración de OwnCloud Client se detalla en el Anexo 17.

El aplicativo una vez instalado muestra el status, la cuenta y la dirección del servidor con la que ocurre la sincronización como se puede apreciar en la figura 4.50.

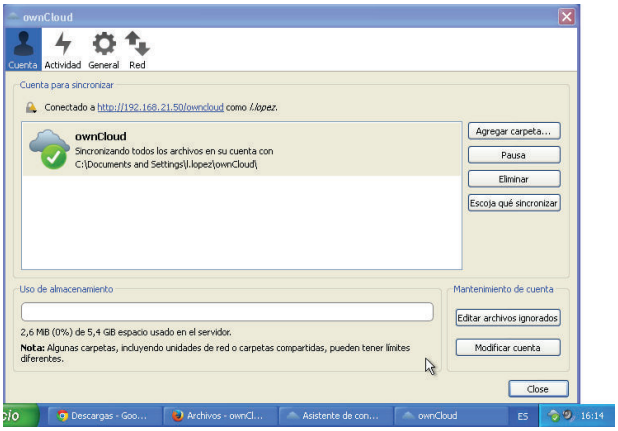

Figura 4.50. OwnCloud Client en sincronización con servidor

Al abrir el directorio hacia donde apunta el cliente de sincronización de Owncloud, los elementos que se encontraban en la cuenta también se encuentran en la carpeta. La figura 4.51 muestra los elementos que se han sincronizado entre la cuenta de OwnCloud en el servidor y la carpeta de sincronización del cliente OwnCloud.

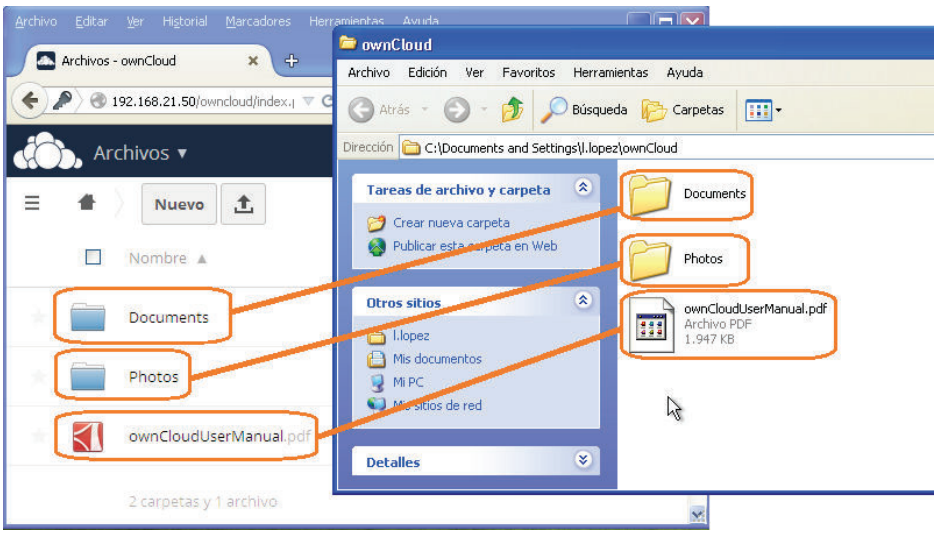

Figura 4.51. Sincronización de cuenta con carpeta

Cualquier nuevo archivo creado se sincronizará automáticamente, ya sea subido al directorio del computador o subido a través del navegador a la cuenta de OwnCloud, a continuación se puede verificar lo explicado en la figura 4.52:

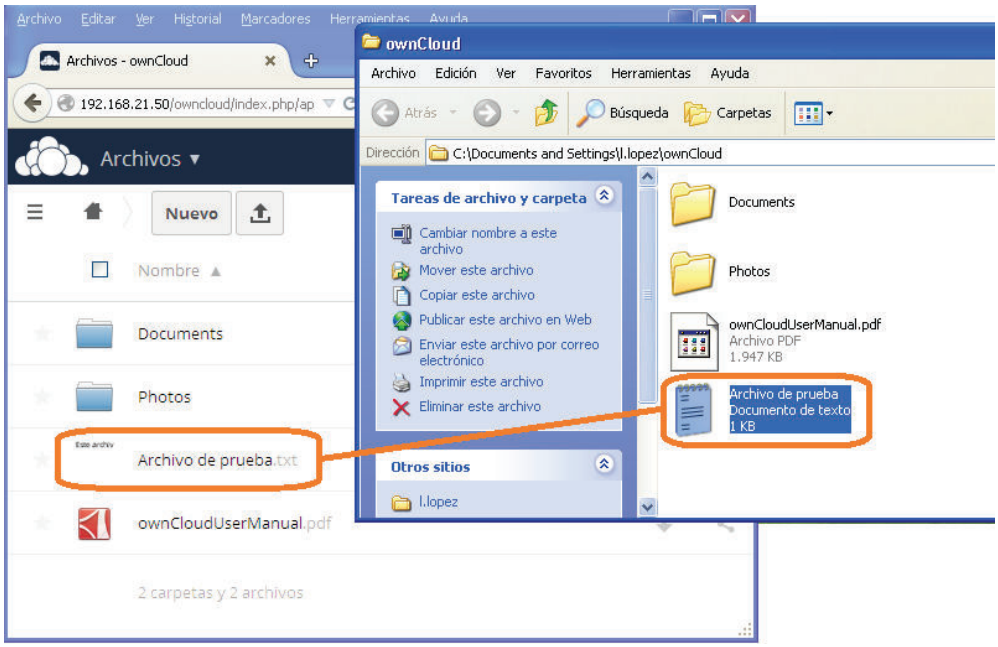

Figura 4.52. Ejemplo de sincronización cliente – servidor

4.7. SERVIDOR DE VIDEO VIGILANCIA

En esta sección se describirán los pasos a seguir para la implementación de un servidor de video vigilancia que puede concentrar una o varias cámaras IP. En este caso también se usará software libre para este propósito. Se evaluó por cuestiones de logística del prototipo dos posibles soluciones basadas en software libre; la primera puede trabajar sobre sistemas operativos Linux y el otro requiere del sistema operativo Windows.

En el primer caso se instaló en un servidor que tiene como sistema operativo CentOS 7 Minimal. El paquete de software que permite levantar el servicio de videovigilancia en este caso se llama ZoneMinder. La solución completa en este caso es completamente software libre por parte del software dedicado a esta tarea así como el sistema operativo en el que funciona. Sin embargo, no se pudo demostrar el funcionamiento de este paquete como se esperaba por la incompatibilidad de la cámara web usada con el software.

En el segundo caso se levantó el servicio de videovigilancia en un sistema operativo Windows. El paquete tiene versiones disponibles para cada distribución y para cada arquitectura (x32-x64). El paquete de software que levanta el servicio se llama iSpy64, el cual es software libre.

La cámara web usada en el prototipo corresponde al modelo TL-SC3130 de la marca TP-LINK, la cual permite ser administrada vía WEB (posee el software embebido para hacerlo) y se puede acoplarse, como en este caso, a servidores externos para sistemas de videovigilancia. Este modelo en particular permite tener dos vías de audio para envío y recepción. Adicional a la cámara IP se probaron alternativas de software para utilizar las cámaras WEB comunes de los equipos portátiles usados durante el prototipo como cámaras IP independientes.

4.7.1. CÁMARAS IP

4.7.1.1. Cámara WEB transformada a cámara IP mediante software WebcamX.

Se ha utilizado un paquete de software para transformar la utilidad de una cámara WEB común en una cámara IP configurada con dirección IP y puerto TCP para envío y recepción de información. WebcamX versión 5 es un freeware (no es Software Libre) que permite realizar este propósito. Al igual que sucede con una cámara IP, un servidor WEB le permite monitorizar la actividad en varias cámaras conectadas al computador.

El proceso de instalación del software es sencillo y similar a cualquier programa instalado en ambientes Windows. En la figura 4.53 se muestra la primera ventana de la instalación del software.

Figura 4.53. Instalación de WebcamXP 5

Una vez instalado, la pantalla principal permite escoger entre varios monitores donde cada uno representa a una cámara conectada al computador.

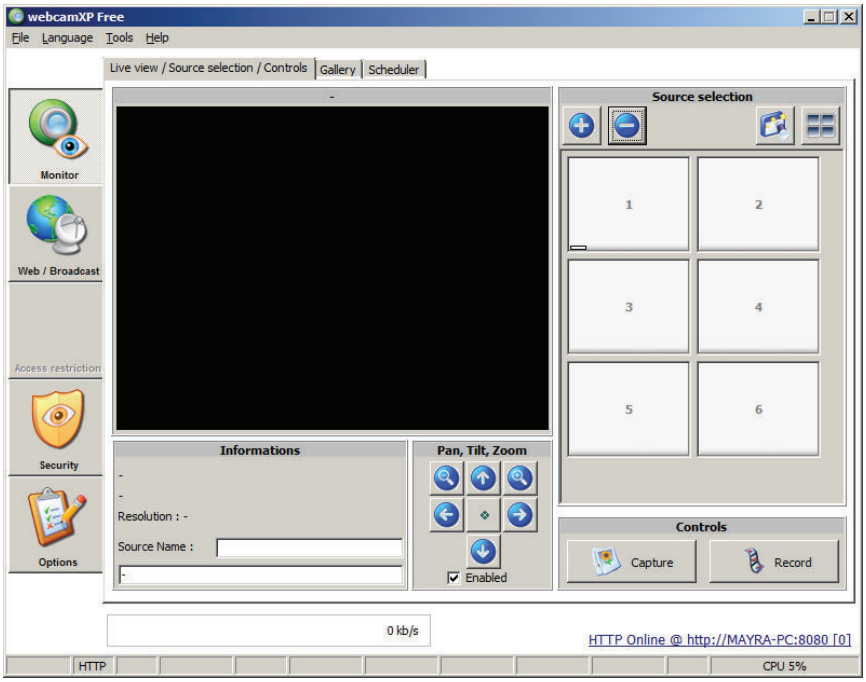

Figura 4.54. Monitores de WebcamXP

Para acceder a uno de estos monitores hay que dar clic derecho en el mismo y asociar la cámara que se desea integrar al sistema, como en la figura 4.55.

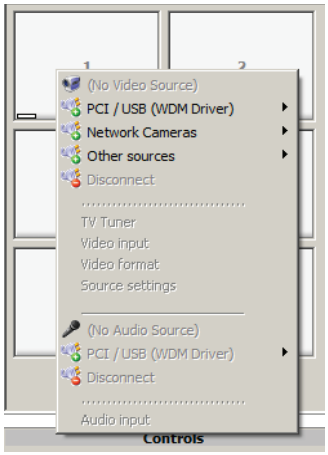

Figura 4.55. Asociación de cámara a monitor

En la figura 4.56 véase asociada la cámara capturando la imagen que se dispone en ese momento. Se va a realizar la prueba con un juguete de gran tamaño, para verificar que sigue siendo captado por la cámara de manera remota.

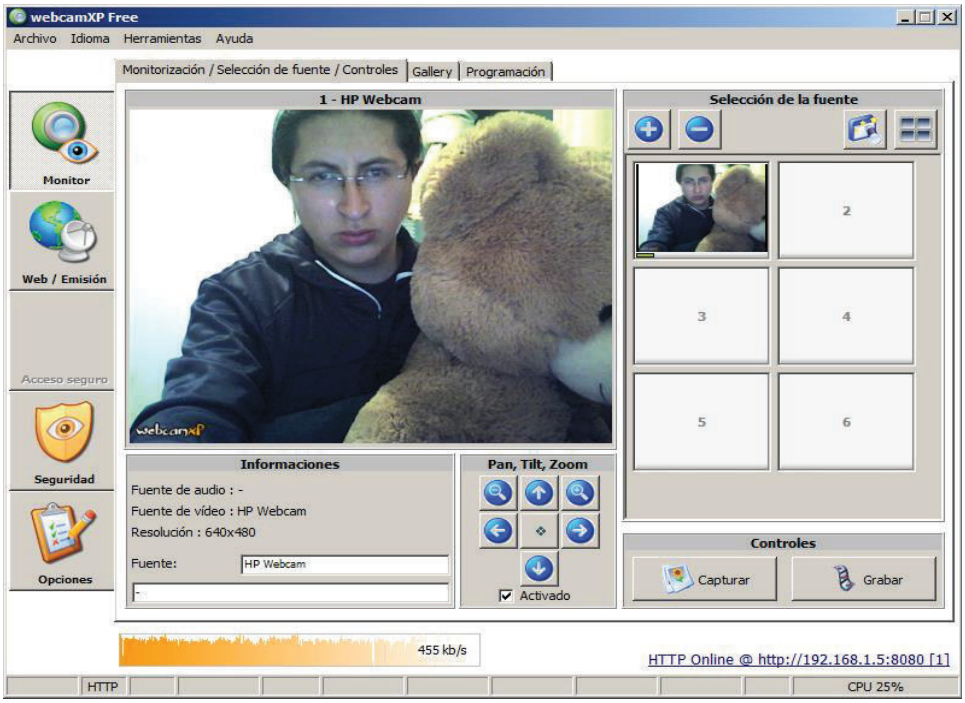

Figura 4.56. Prueba de imagen en WebcamXP

Antes de realizar el monitoreo remoto es necesario configurar la dirección IP y el puerto, tal como se aprecia en la siguiente figura. Con estos datos se puede acceder desde un navegador en otro computador de la misma red, o incluso desde otra red (o desde Internet) en caso de que se haya realizado un NAT a una dirección pública. Este no es el caso, porque solo se realizará vigilancia dentro de la red. Estas configuraciones se aprecian en la figura 4.57.

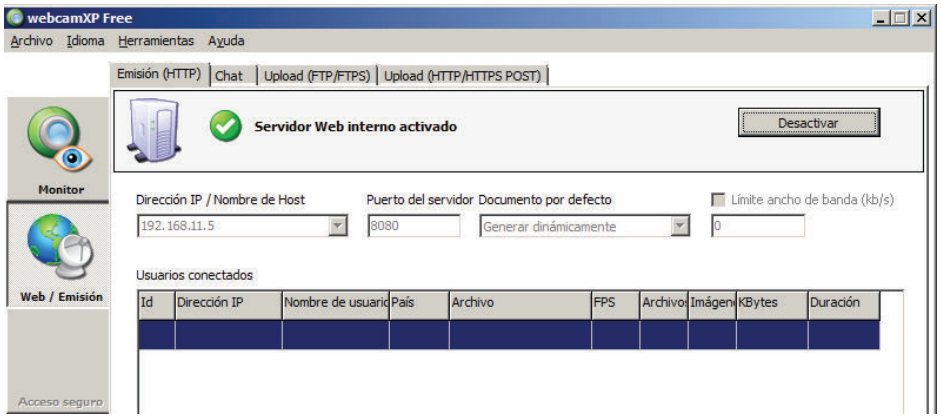

Figura 4.57. Configuración de dirección y puerto

Desde un navegador en otro computador de la red se puede constatar que el *streaming* de video está disponible para realizar un monitoreo. El programa tiene

su propia aplicación WEB que permite incluso utilizar algunos controles de movimiento de la cámara en tiempo real. En la figura 4.58 se puede ver la imagen que está siendo captada en ese instante:

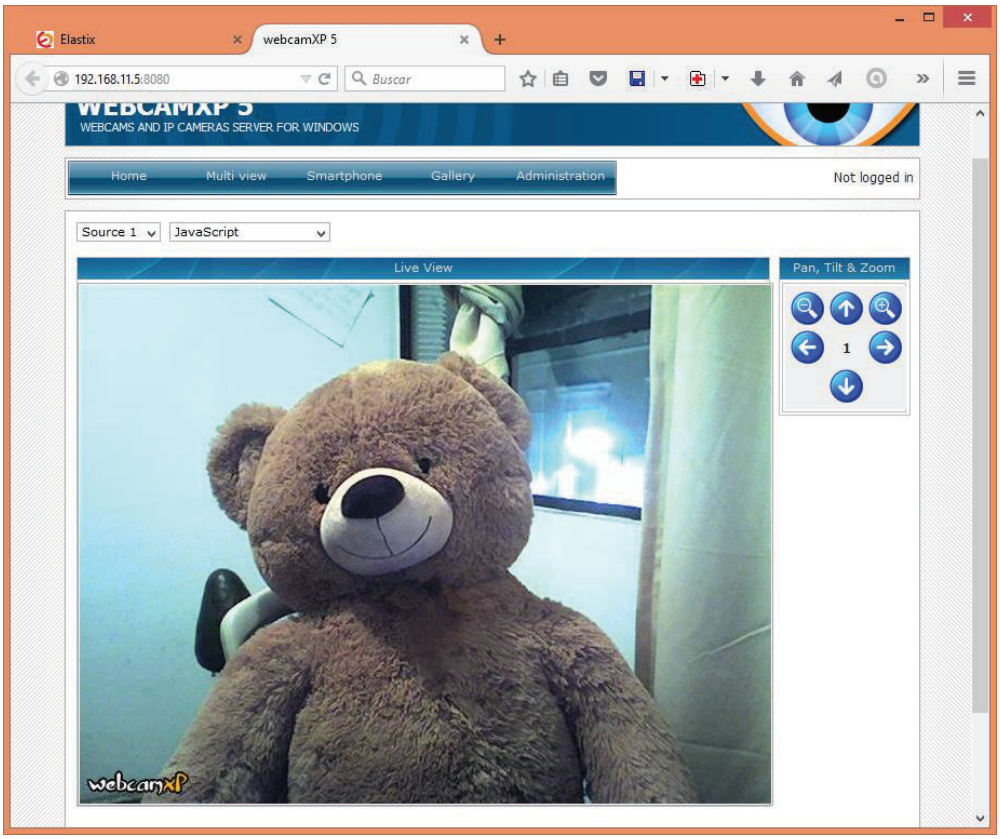

Figura 4.58. Imagen captada por la cámara

4.7.1.2. Cámara IP TP-LINK TL-SC3130

La alternativa en cámara IP (hardware) que se pudo disponer para este prototipo corresponde a la TP-LINK modelo TL-SC3130. Las características de este modelo son las siguientes:

- Modo de compresión MJPEG (sin pérdidas, pero mayor consumo de capacidad de canal) y MPEG-4 (con compresión) para envío de vídeo.
- Envío y recepción de audio. Posee un micrófono que permite registrar el sonido en tiempo real. También permite recibir audio en un parlante externo.
- Velocidad de fotogramas @30fps en resolución VGA (640 x 480).

Físicamente, el enfoque de la cámara se puede ajustar manualmente. Dispone de un puerto de red, una ranura de alimentación y una ranura para la conexión de un parlante para recepción de audio. También dispone de un botón de reset, tal como se aprecia en la figura 4.59 donde se aprecian todas las caras de la cámara:

Figura 4.59. Vistas de la cámara IP – Frontal, inferior y posterior

4.7.2. SERVIDOR DE CÁMARAS IP

4.7.2.1. ZoneMinder [PW11] [PW8]

ZoneMinder se conforma por un conjunto de paquetes de software libre que en conjunto permiten brindar un servicio de video vigilancia en ambiente Linux que soporten V4L (Video for Linux). Su funcionalidad permite integrar cámaras de seguridad, cámaras IP e incluso webcams.

Actualmente V4L se encuentra en su segunda versión (V4L2) y se integra al núcleo de las distribuciones de Linux. Para el caso explicado a continuación, el servicio de Video Vigilancia se levantará sobre la distribución de CentOS 7 Minimal.

Las instrucciones de la instalación se ofrecen en la página del aplicativo (wiki). El servicio prestado permite realizar vigilancia en tiempo real, realizar la grabación e incluye análisis de la imagen para detectar movimiento.

El procedimiento realizado se detalla en el Anexo 18.

Se lista la cámara como un dispositivo dentro de la lista. Desde este lugar puede hacerse pruebas y verificar que el servidor puede recibir la señal de video. El campo “Source” debería estar en color verde cuando la conexión es exitosa. En este caso el color rojo mostrado en la figura 4.60 indica que la cámara no está siendo reconocida. El hardware usado en este caso no dispone compatibilidad con ZoneMinder, por lo que se hizo las pruebas con otro servidor de videovigilancia. A estas alturas no se pudo comprobar la compatibilidad de este software ni con la cámara IP virtual WebcamXP ni con la cámara dedicada TP-LINK TL-SC3130.

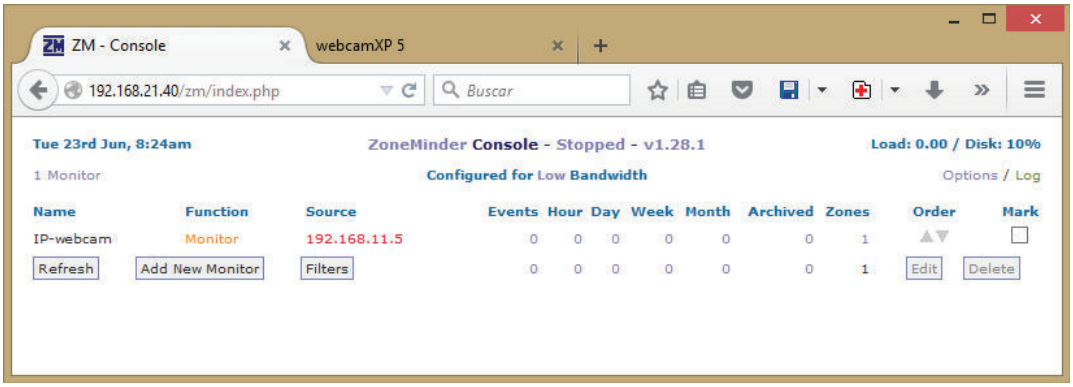

Figura 4.60. Lista de monitores en ZoneMinder

4.7.2.2. iSpy (iSpy64)

iSpy es un software de videovigilancia de código abierto para sistemas operativos Windows. Se seleccionó este software para el prototipo porque, en este caso, las pruebas de compatibilidad entre la cámara IP TPLINK TL-SC3130 y el programa de videovigilancia fueron exitosa a diferencia de lo sucedido con ZoneMinder.

Dentro de las principales características de iSpy tenemos las siguientes:

- Permite la captura de fuentes de video y sonido.
- Control de cámaras PTZ (pan-tilt-zoom). Este término se refiere a cámaras, normalmente de vigilancia, que permiten control remoto de movimiento, enfoque y disponen de sensibilidad a sonido y/o movimiento.
- Detección, resalte, rastreo y registro de movimiento.
- Conexión ilimitada de cámaras, lo que permite escalabilidad mientras las condiciones del servidor lo permitan.

- Puede integrarse el visor de iSpy en sitios web.
- Tiene la capacidad de transmitir video y audio en vivo o grabado a dispositivos móviles que soporten navegadores HTML5, así como alertas vía SMS y Twitter.
- Mediante *plugins* oficiales (con costo) se pueden añadir características adicionales al software, como por ejemplo reconocimiento de placas vehiculares para apertura de puertas de estacionamiento.

4.7.2.2.1. Instalación de iSpy (iSpy64)

Previo al proceso de instalación se requiere disponer de .Net Framework 4.0 o superior instalado en el sistema operativo Windows. Otros factores a consideración dependen de las necesidades de la aplicación, así por ejemplo, la cantidad de disco adicional en función del tiempo que se requiere mantener un registro de las grabaciones. En la página oficial del desarrollador se establece como requisitos mínimos 2GB de memoria RAM y 200GB en disco duro para soporte de 4 cámaras de 320x240.

La instalación de este software, al ser un instalador en un ambiente Windows, tiene similitud con la instalación de otros paquetes de software en los que se despliegan varias ventanas durante la instalación donde se aceptan paso a paso parámetros básicos como el directorio de instalación.

Las versiones del instalador dependerán de qué tipo de sistema operativo esté siendo usado; de 32 o 64 bits, ambas versiones pueden ser descargadas independientemente de la página web oficial. En el caso del prototipo se ha usado la versión de 64 bits. Se puede instalar la versión x86 en sistemas plataformas x64, pero el desempeño de CPU y memoria RAM puede verse disminuido, según se explica en la página oficial del desarrollador.

Las respectivas capturas de los pasos de instalación se detallan el Anexo 19.

4.7.2.2.2. Configuración de iSpy

La primera vez que se inicia la aplicación se selecciona el idioma antes de continuar con las primeras configuraciones, en este caso está soportado el español. A continuación se procede a asociar la cámara IP a través de la red en

base a un asistente sencillo proporcionado por el software. La captura se muestra en la figura 4.61:

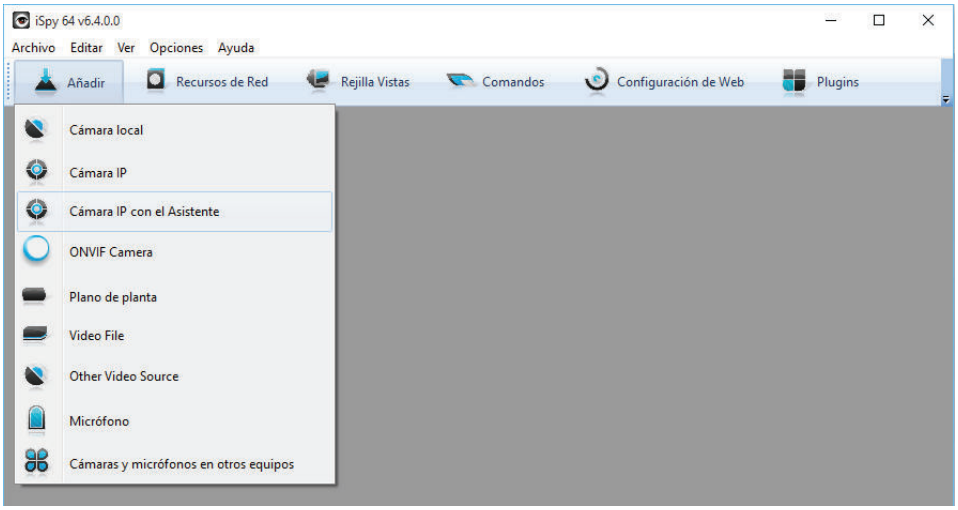

Figura 4.61. Asistente de adición de cámara IP

Posteriormente se debe seleccionar la marca y el modelo de la cámara IP del listado soportado por el software. A diferencia de ZoneMinder, iSpy muestra compatibilidad con el modelo 3130 de la marca TP-LINK. Por este motivo se decidió el uso de este programa para el prototipo. La figura 4.62 muestra la captura de pantalla de la marca y modelo.

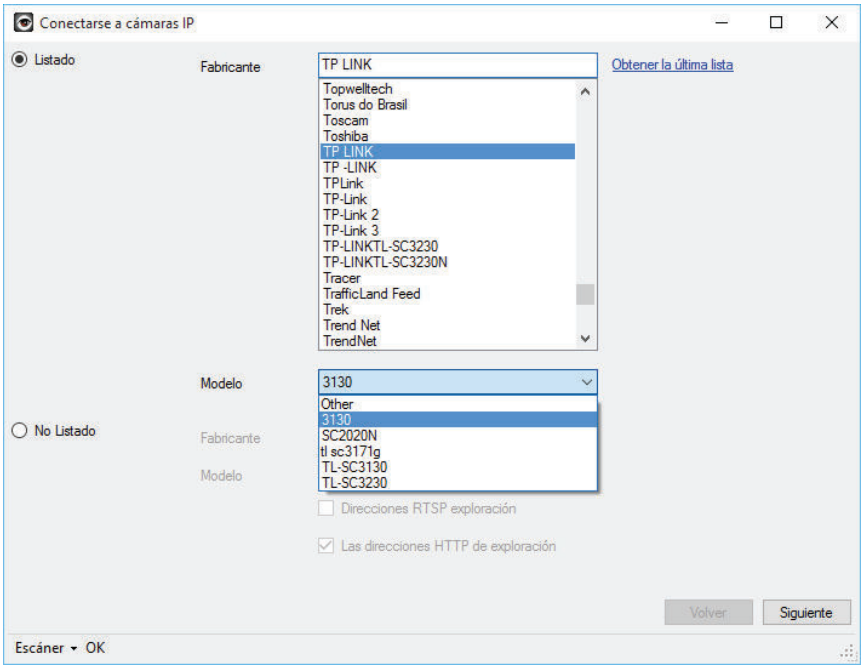

Figura 4.62. Modelos y marcas soportadas por iSpy

Luego se establecen los parámetros de usuario y contraseña para autenticarse a la cámara y se continúa hacia una ventana de detección de dispositivos y cámaras dentro de la red de área local. Con los parámetros indicados se despliega una lista de posibles dispositivos que pueden ser la cámara buscada, enfatiza en dispositivos que tengan habilitados los puertos 80 y 8080 para luego listarlo junto a su IP, MAC y versión de servidor web. La figura 4.63 ilustra la lista de los dispositivos (incluyendo la cámara IP) que se obtuvieron durante la prueba.

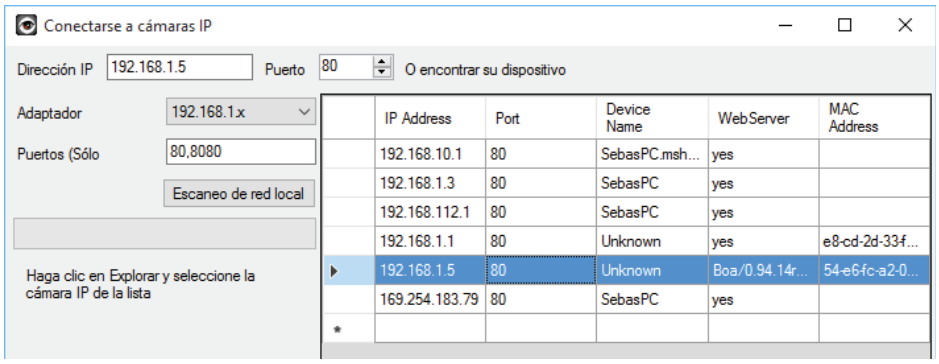

Figura 4.63. Listados de dispositivos en la LAN

Finalmente, la cámara se registra en iSpy y lo que resta es la configuración de los parámetros con los que va a funcionar la cámara posteriormente. Al tratarse de parámetros generales para cualquier modelo algunas características pueden no ser necesarias para algunos modelos de cámaras, como por ejemplo en este caso el control de movimiento no tiene ningún uso porque la cámara es estática y no posee ningún mecanismo PTZ remoto. Los parámetros que se deben configurar se detallan a continuación:

- Fuente de vídeo, micrófono y parlante.
- Configuración de detección de movimiento.
- Configuración de alertas ante un evento.
- Configuración de sensibilidad para la grabación.
- Configuración de PTZ (panning, tilt y zoom).
- Configuración de grabación de imágenes (con sensibilidad opcional).
- Configuración de grabación de imágenes en servidor FTP (con sensibilidad opcional).
- Configuración de almacenamiento en nube.

- Programación de funcionamiento de la cámara.
- Opciones para el almacenamiento en disco duro.

Las capturas de la configuración se detallan en el anexo “iSpy”.

4.7.3. PRUEBAS DEL SERVICIO DE VIDEO VIGILANCIA

En el caso de ZoneMinder no se pudo asociar la cámara correctamente al software. Al momento de intentar visualizar la imagen dentro de la página web sólo apareció una pantalla azul. El estado no mostraba ningún valor de fps (frames per second), evidentemente no se pudo obtener la señal de vídeo deseada. La figura 4.64 muestra la captura obtenida.

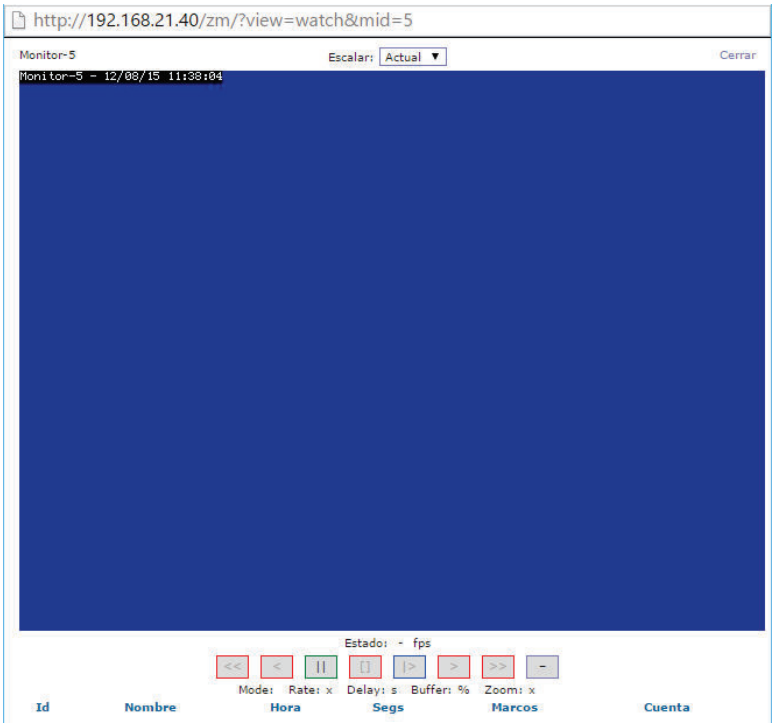

Figura 4.64. Pruebas con ZoneMinder

Las pruebas con iSpy, por el contrario, resultaron exitosas. En la figura 4.65 se puede apreciar una toma de un oso de peluche con luz artificial durante horas de la noche. El programa muestra la imagen captada en tiempo real en el recuadro central y permite manejar algunos controles en la parte inferior de la imagen para capturar una imagen estática o detener la captura de la cámara además de los registros de movimiento. Si se decide grabar, el vídeo sigue siendo almacenado en el disco duro.

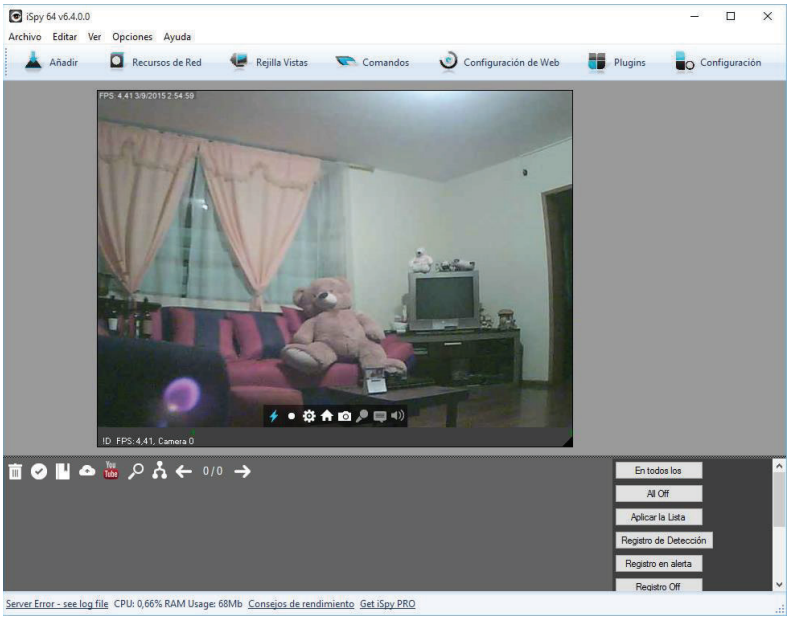

Figura 4.65. Toma en tiempo real de vídeo

La configuración por defecto permite que se grabe vídeo únicamente cuando la cámara detecte movimiento. En el ejemplo que se detalla en la figura 4.66 se observa la imagen casi estática de una puerta con tres grabaciones producidas en el instante en que la cámara detectó movimiento. Las grabaciones aparecen como pequeños recuadros bajo la toma en tiempo real de la imagen.

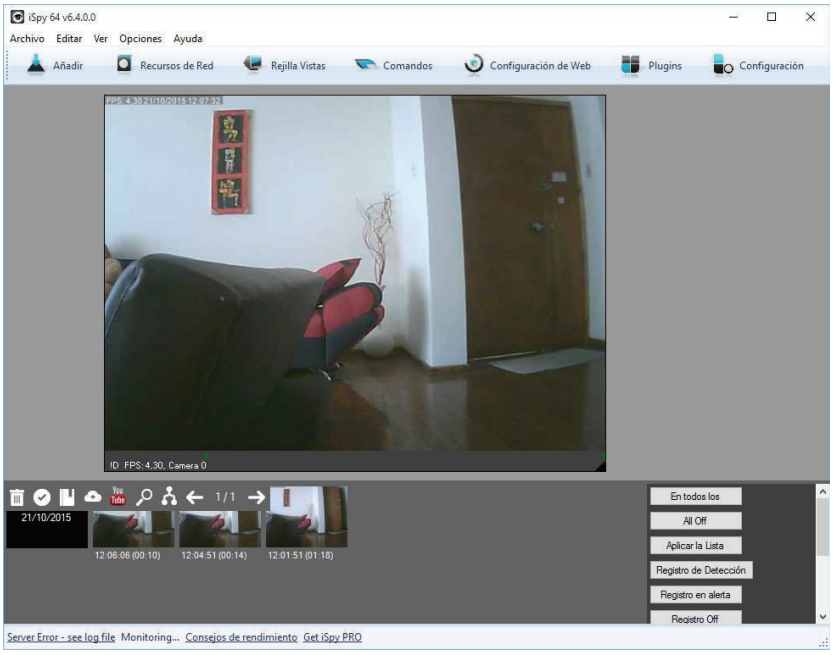

Figura 4.66. Registro de grabaciones

Cuando se reproducen los vídeos del registro de grabaciones se despliega un reproductor del programa donde se puede visualizar una línea de tiempo en la parte inferior del mismo. Las partes que contienen actividad o movimiento se oscurecen para que sea más fácil que el usuario que revise las grabaciones encuentre fácilmente el punto de movimiento. En la figura 4.67 se observan dos tomas en el reproductor de vídeo; una cuando la imagen permanece sin alteraciones a la izquierda y otra cuando se ha producido movimiento en la derecha. Se ha remarcado en color rojo la zona de la línea de tiempo del reproductor para denotar el periodo en que la cámara detecta la presencia de movimiento de una mano frente a la lente.

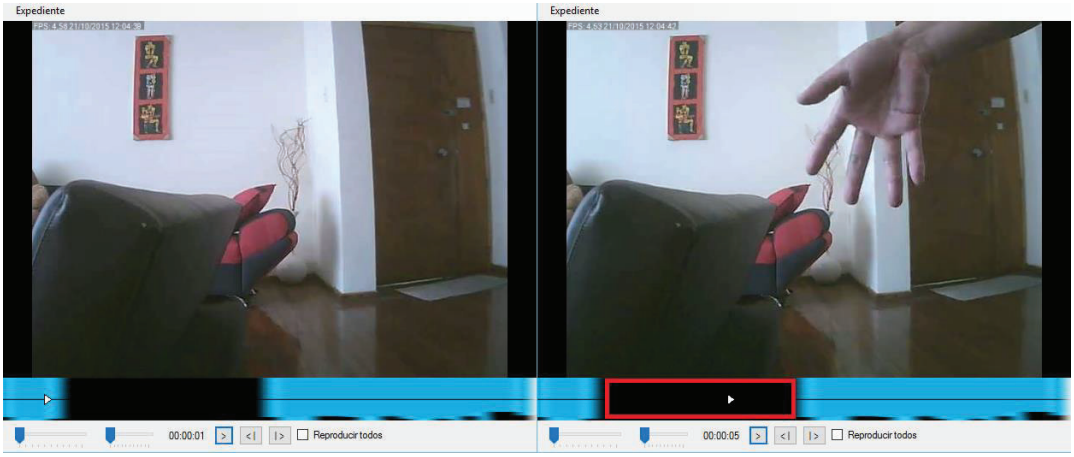

Figura 4.67. Reproductor de vídeo con línea de tiempo resaltada

En el ejemplo anterior se puede observar que el intervalo de tiempo que se muestra resaltado en el reproductor en color negro fue producido por la intromisión directa de una mano frente a la cámara. Durante este tiempo la mano se movió constantemente. Lo cambios mucho más imperceptibles como la cantidad de luz o pequeñas vibraciones se muestran como pequeñas manchas oscuras bajo la línea de tiempo del reproductor y no ameritan la atención del usuario durante su revisión.

Sin embargo pueden haber casos en que hayan pequeños cambios en la imagen, casi imperceptibles, pero que pueden denotar el inicio de un evento a ser registrado. En el siguiente ejemplo mostrado en la figura 4.68 se puede apreciar que el reproductor muestra un “pico” de actividad representado por una línea roja vertical antes de grabar la actividad generada al abrir la puerta que aparece en la

imagen y mostrar una mano agitándose posteriormente. Este registro corresponde a una pequeña sombra que se desliza bajo la hendija inferior de la puerta (debido a la presencia del sujeto que va a abrir la puerta) antes de que ésta fuera abierta desde la parte de afuera. Este detalle que puede pasar desapercibido por un usuario es registrado minuciosamente por el programa, lo cual es una valiosa ventaja cuando el usuario revise las grabaciones.

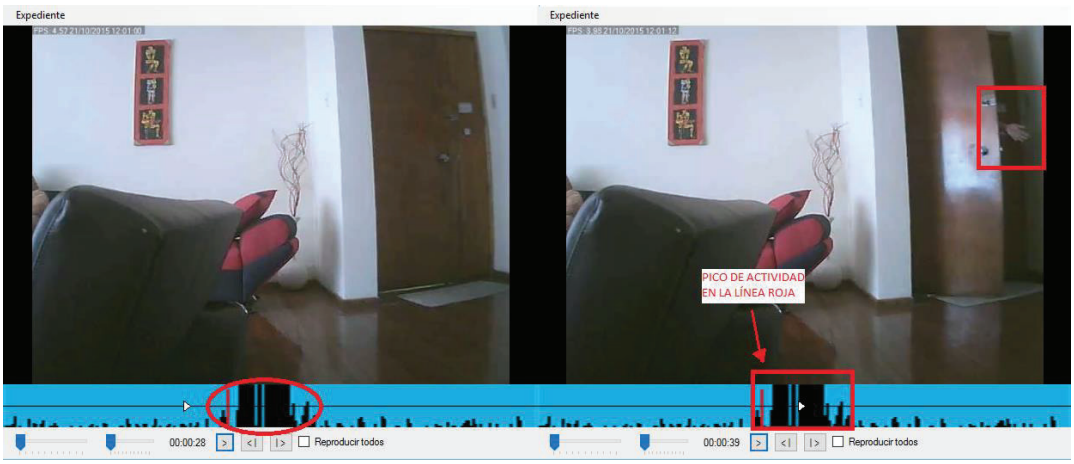

Figura 4.68. Registro de picos de actividad

El programa se ejecuta en segundo plano dentro del equipo, sea estación de trabajo o servidor, a menos que sea cerrado. En los momentos en que se ha realizado un registro de actividad por movimiento el sistema operativo lanza una notificación desde el área de notificaciones de la barra de tareas de Windows, alertando al usuario de un evento en registro.

Figura 4.69. Notificación de grabación

Las grabaciones almacenadas en disco duro pueden ser reproducidas desde la aplicación (con su respectivo reproductor con resalte de movimiento) o puede

reproducirse con cualquier reproductor que admita archivos con extensión .mp4 que es el tipo de archivos producidos durante la grabación.

El directorio de grabación puede ser configurado por el usuario. En la figura 4.70 se muestra el directorio usado en la prueba descrita en este apartado.

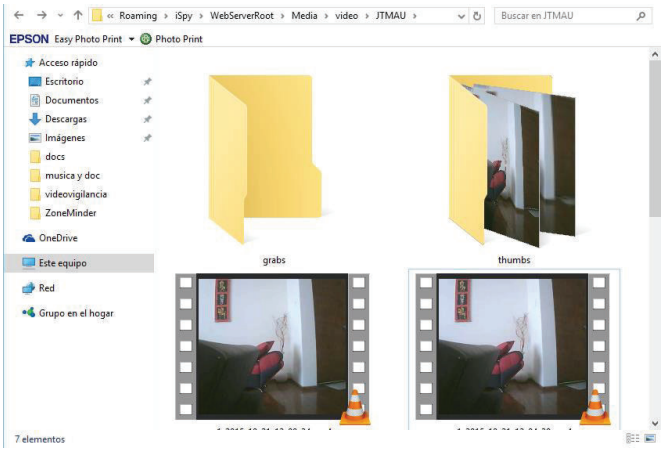

Figura 4.70. Directorio de grabaciones

4.8. SERVIDOR DE VIDEOCONFERENCIA

En este punto se decidió abordar la solución a la necesidad de videoconferencia a través de una solución de software libre que fue concebida con fines meramente educativos. La razón para decantarse por la elección de un software de esta naturaleza se justifica en la forma en como éste se utiliza y su similitud al ambiente que existe en una conferencia moderada y la facilidad de compartir imágenes de escritorio en tiempo real así como su posterior recuperación en forma de video en caso de ser necesario. En otras palabras, el software permite que un moderador presente una ponencia (o tema central en este caso) y que sea visto por varios usuarios participantes a través de video, así como también es factible compartir la imagen de los documentos de escritorio, la interacción con dichos documentos con herramientas de edición en tiempo real y la posibilidad clave de otorgar la palabra a los participantes de la videoconferencia de una manera controlada y ordenada donde todos pueden verse a través de video.

Básicamente se asemeja al ambiente de una clase magistral con participantes remotos, donde se puede dar mayor prioridad a los participantes para el desarrollo de la conferencia.

4.8.1. BIGBLUEBUTTON [PW9]

El software que brindará el servicio de videoconferencia se llama BigBlueButton. Este software de código abierto se encuentra disponible desde su sitio web oficial, lanzado por una comunidad que soporta el proyecto. Hasta el momento de las pruebas pertinentes la última versión estable fue la 0.9.0-RC.

Una peculiaridad de este paquete de software es que sólo funciona bajo la versión de Ubuntu Server 14.04 de 64 bits. No hay documentación oficial de cómo instalar en otras versiones de Ubuntu Server ni mucho menos de otras distribuciones de Linux. Durante el proceso de instalación se establece una lista de repositorios para la descarga del software.

Este software aplicado a una conferencia de personas con propósitos distintos a los educativos pueden contar con las mimas ventajas, por este motivo se eligió este software para el presente prototipo. Los participantes tienen la oportunidad de interactuar, compartir PDFs y documentos de Office, de ver todo el material de escritorio de quien hace de ponente y de mantener un equilibrio y orden respecto a sus intervenciones.

4.8.1.1. Características de BigBlueButton

Tal como se describió inicialmente, este software fue concebido con fines educativos en línea. De gran versatilidad; el software simula un ambiente de clases en tiempo real donde varios participantes con estaciones de trabajo equipadas con micrófono y cámara web inician sesión y son enlazados a una clase virtual donde un moderador (quien funge de profesor o ponente) utiliza una estación de trabajo de similares características para exponer en tiempo real al resto de participante su propia imagen y voz, con la posibilidad de mostrar documentos, presentaciones con diapositivas u otros elementos de escritorio (sistema operativo) simultáneamente. Adicional a estas características también posee la capacidad de otorgar la palabra a cualquiera de los participantes para interactuar durante la ponencia.

Esto le da permiso de decidir en función de la necesidad de la clase a quienes y en qué tiempo otorgar la palabra. El audio y video generado durante en la clase

es elegible de ser grabado para que esté disponible luego de la clase, de tal modo que los integrantes de la clase pueden acceder a éste posteriormente. Quienes cumplen el rol de estudiantes pueden recibir material PDF o documentos de Office, además pueden comunicarse a través de chat.

Las principales características que se citan por parte del equipo de desarrolladores en su página oficial son los siguientes:

- Grabación y reproducción de ponencias para los estudiantes.
- Función de pizarrón para anotaciones importantes.
- Compartición de escritorio (funciona en Mac, Unix y PC).
- Función integrada de VoIP para conferencia. Basta micrófono y parlantes.
- Presentación a partir de PDFs y documentos de Office.
- Compartición de cámaras web entre los participantes. No existe límites de simultaneidad más que por la capacidad del servidor a nivel de hardware.

Adicional a estas características la presente versión tiene mayor desempeño con navegadores Chrome y Firefox para comunicación en tiempo real (WebRTC).

El sistema puede agregarse como complemento a otras plataformas educativas como es el caso de Moodle. El material grabado puede añadirse al material de Moodle gracias a un *plugin* desarrollado para este objetivo.

4.8.1.2. Instalación de BigBlueButton

BigBlueButton tiene la particularidad de trabajar sobre Ubuntu Server 14.04 como único sistema operativo y única versión soportada por la comunidad a cargo del proyecto. La instalación del sistema operativo se detalla en el Anexo 7 mientras que los pasos que describen el proceso de instalación del software BigBlueButton se detallan en el Anexo 20.

Por cuestiones de desempeño se recomienda de manera especial desde su página oficial no instalar en ambientes virtualizados sino utilizar un servidor dedicado. Se recomienda utilizar un equipo con procesador de 4 núcleos de 2.6GHz o superior con al menos 4GB de memoria RAM.

En lo que respecta a la configuración, tras la instalación se debe ingresar al programa mediante un navegador web a la dirección del servidor. La primera vez nos mostrará una página de bienvenida con la posibilidad de ingresar al demo del producto, además de algunos videos de cómo realizar las configuraciones iniciales. En la figura 4.71 se puede observar este ingreso:

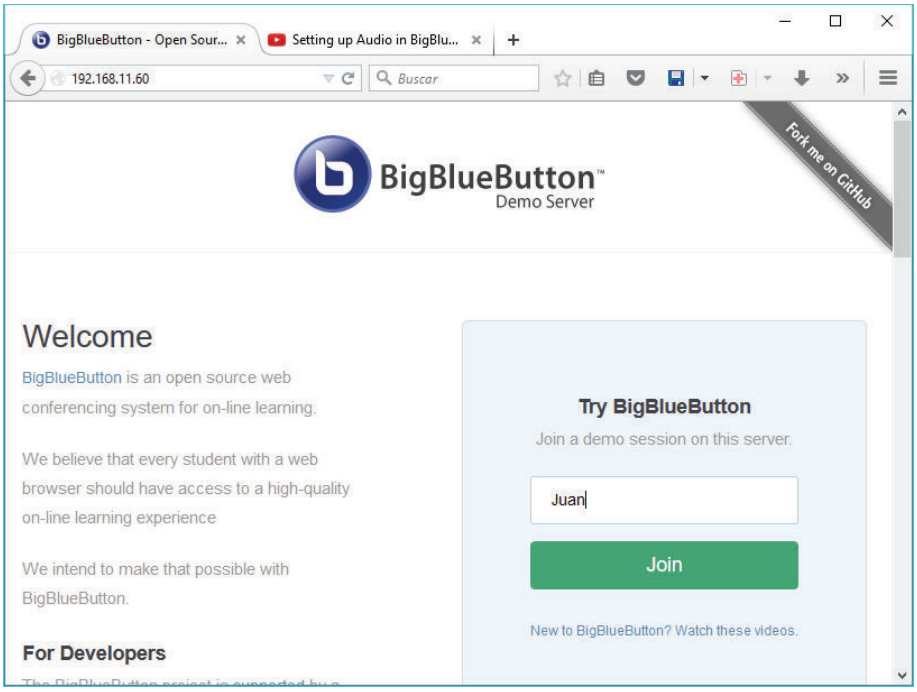

Figura 4.71. Ingreso a BigBlueButton

Posteriormente el software solicita la configuración de los dispositivos de audio y cámara. La prueba se hace con el retorno de lo que se diga en el micrófono, mientras que el video debe comprobarse corroborando que aparece la imagen del sujeto en la pantalla tras otorgar el permiso respectivo para su activación.

El primer ingreso al sistema conduce a una pantalla donde se puede visualizar tres secciones bien definidas: en el lado izquierdo se muestran la lista de todos los usuarios ligados al mismo espacio o clase, en la parte inferior de la lista se define la zona de video del sujeto. En el área central se muestra el espacio que el usuario comparte con los demás usuarios, el cual incluye sus propias herramientas de edición y anotación. Finalmente a la derecha se muestra un área de chat para interacción entre los usuarios. En la figura 4.72 se muestra una captura de lo descrito:

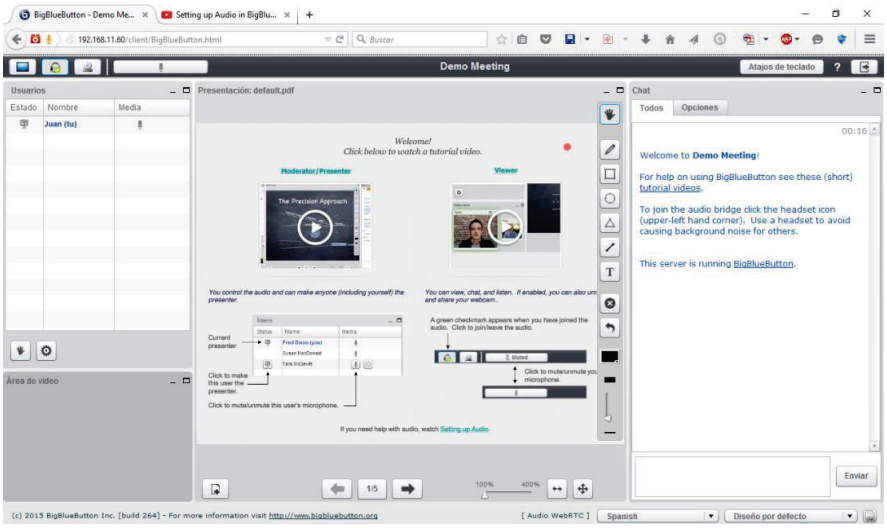

Figura 4.72. Primera pantalla en sesión BigBlueButton

4.8.2. PRUEBAS DEL SERVIDOR DE VIDEOCONFERENCIA

Una vez comprobado que el servidor está activo y que se puede registrar un usuario para el ingreso al demos del software, se realizará la respectiva prueba de sonido y de video. Las figuras 4.73, 4.74 y 4.75 muestran respectivamente la configuración de estos dos aspectos:

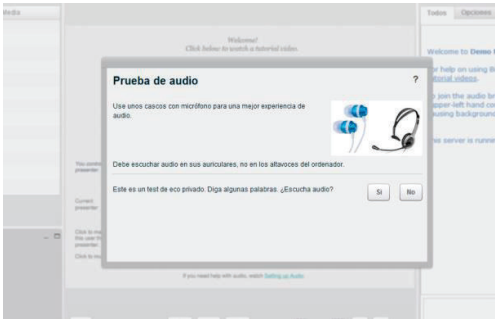

Figura 4.73. Configuración de audio en BigBlueButton

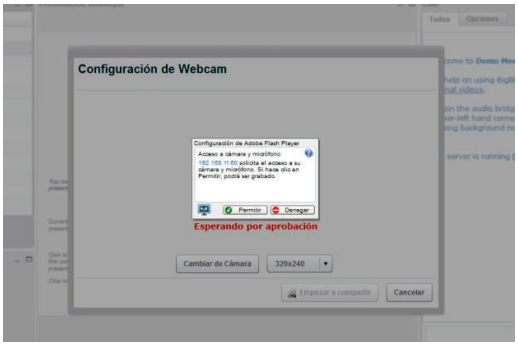

Figura 4.74. Requerimiento de configuración de vídeo en BigBlueButton

En la figura 4.75 se muestra la imagen del sujeto en caso de que se tenga correcto ingreso a la cámara web del paso de la figura 4.74. Las opciones que se dan al sujeto son las de cambiar la resolución en caso de que la cámara se lo permita y además se permite la compartición de su propia imagen con el grupo de personas que hayan ingresado en ese instante al sistema.

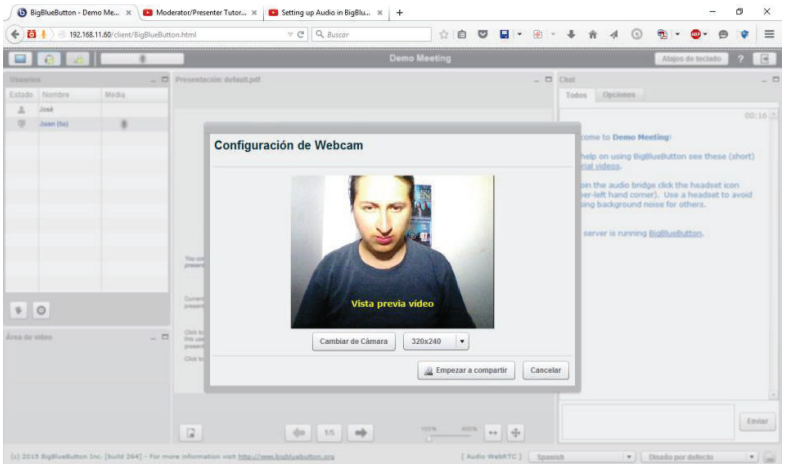

Figura 4.75. Prueba de webcam en BigBlueButton

Para este ejemplo se inició simultáneamente en el sistema una sesión con otro usuario - alumno en otro navegador. Se puedo evidenciar que el primer usuario ha compartido su webcam y puede visualizarse en el recuadro inferior izquierdo de la pantalla, tal como se aprecia en la figura 4.76.

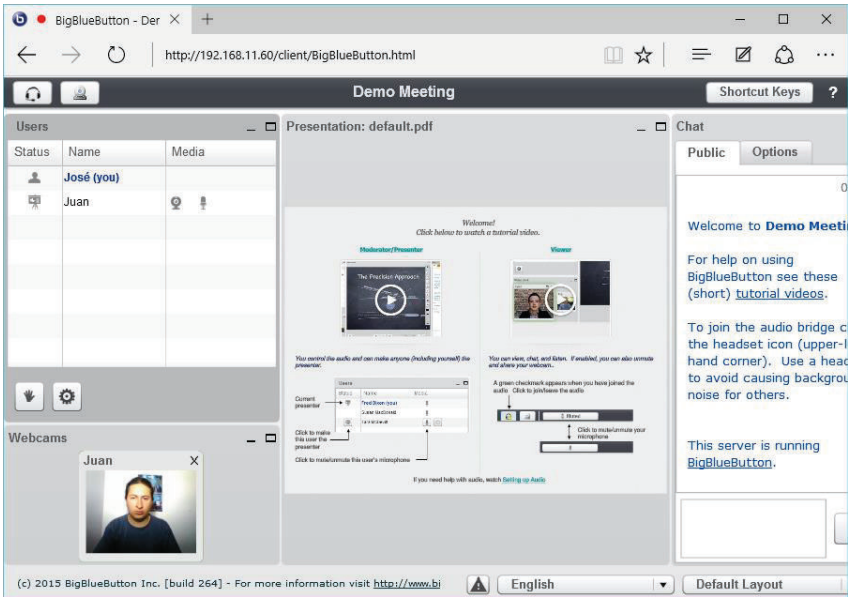

Figura 4.76. Perspectiva de usuario - alumno en BigBlueButton

En la figura 4.77 se puede observar la perspectiva del ponente y el usuario – alumno simultáneamente. Se observa que la misma imagen que proyecta el ponente es inmediatamente captada por quien funge de estudiante. Esto demuestra la rapidez y efectividad de la conferencia.

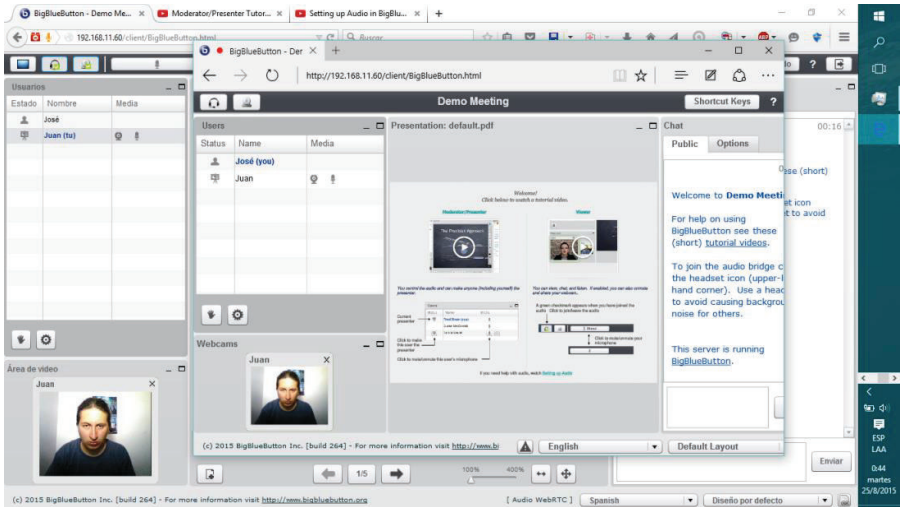

Figura 4.77. Perspectiva de dos usuarios en BigBlueButton

Las pruebas que se hicieron luego corresponden a la capacidad de usar la pantalla como un pizarrón. Encima de la presentación de prueba que viene por defecto el usuario ponente de la derecha de la figura 4.78 escribe mediante un cuadro de texto “Este es un texto de prueba”, lo que inmediatamente es visto desde la perspectiva del usuario – estudiante ubicado en el lado derecho de la figura, de manera transparente y sin la necesidad de ver el cuadro de texto, o en otras palabras, sólo ve el resultado de la interacción sin necesidad de ver la herramienta de edición.

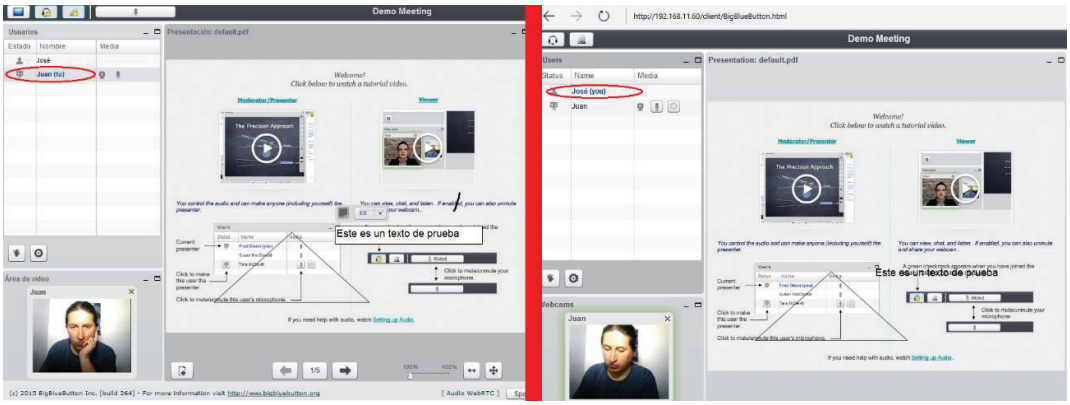

Figura 4.78. Escritura de texto en pizarra

En la figura 4.79 se observa el uso del pizarrón en una hoja vacía. Se aprecia de mejor manera el uso de las herramientas para dibujar figuras geométricas y colores que el usuario ponente usa para su presentación.

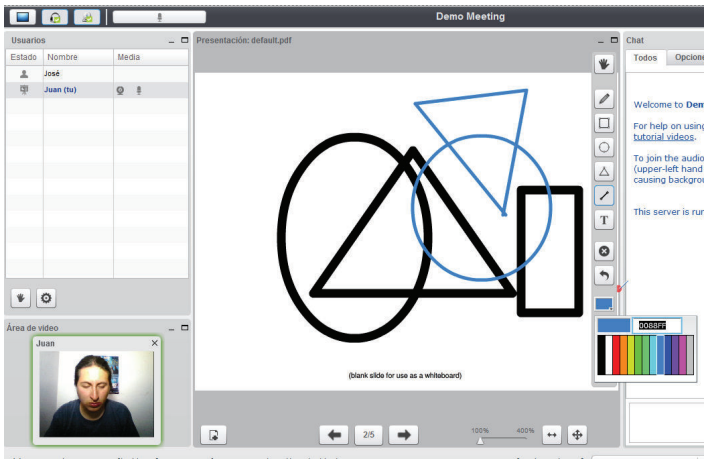

Figura 4.79. Edición de figuras en pizarra

Nuevamente el usuario – estudiante observa la creación de las figuras en la presentación en su panel central de manera transparente sin la necesidad de observar el conjunto de herramientas que generan el contenido tal como se puede apreciar en la figura 2.80. De esta manera se enfoca la atención en la explicación más que en la creación de los objetos usados para la explicación. Se puede observar a la par cómo se mantiene en el recuadro inferior izquierdo la imagen del usuario ponente mientras que también se observa la explicación en el recuadro central. Por esta facilidad se puede utilizar de mejor manera este software con el fin de realizar una conferencia con elementos explicativos sin tener que limitar su uso exclusivamente al ámbito educativo.

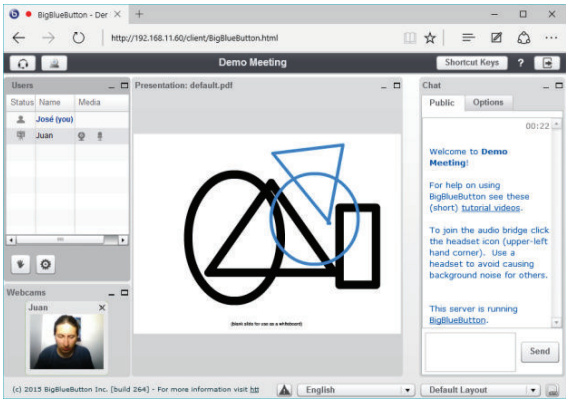

Figura 4.80. Perspectiva del usuario – estudiante de imágenes en pizarra

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Los constantes cambios que se realizan en el Ministerio de Inclusión Económica y Social crean la necesidad de tener una buena planificación para los administradores del Departamento de Tecnologías de la Información de la Institución, de tal manera que no se presenten los inconvenientes tanto en la infraestructura física de la red, administración de la misma y equipos activos de la red, para brindar un servicio de calidad a los usuarios finales.
- El levantamiento de información tanto de la parte activa como pasiva, además de realizar las prácticas pre profesionales en el MIES nos permitieron verificar los inconvenientes que presenta la red y el malestar de los usuarios finales por el mal funcionamiento y acceso a la red y a los servicios prestados.
- La reestructuración propuesta de la red permite integrar tecnologías existentes como futuras a altas velocidades sin tener problemas de inestabilidad o inconsistencia en la red, gracias al estudio realizado se espera una mejora tanto la disponibilidad de la red como también la administración por parte de la Dirección de Tecnologías de Información.
- El análisis de la situación actual del cableado estructurado del MIES proporciona la información necesaria para evidenciar los principales problemas que tiene la red, los cuales fueron estudiados en el Capítulo 2 y remediados en el Capítulo 3, lo cual permite a los administradores de red una mejor administración y gestión de la misma, además asegura un crecimiento organizado de la red aproximadamente a quince años sin tener los mismos problemas que actualmente poseen.
- El esquema de red propuesto para la reestructuración de la misma pretende organizar de mejor forma la infraestructura presente y la que se pretende implementar, aunque no sigue los lineamientos del esquema

jerárquico que expone Cisco el cual propone tres capas (acceso, distribución y núcleo), se plantea el modelo donde encontramos capa acceso y capa núcleo, con lo cual se cubren los requerimientos actuales y futuros de la red.

- La seguridad perimetral de la red es fundamental en cualquier tipo de infraestructura, debería existir una área de administración y monitoreo de la red en cada Institución que se dedique exclusivamente a la seguridad en redes, ya que en la actualidad se ha evidenciado la falta de políticas de seguridad en equipos perimetrales, lo cual ha llevado a realizar consultorías en las redes para mitigar los ataques generados y evidenciar los huecos de seguridad en la red.
- La colocación de switches en cascada a partir de los switches de acceso sin ningún tipo de estudio previo ni planificación puede resultar en una solución temporal que puede generar más problemas que beneficios a la red y a los administradores de red, ya que existe la posibilidad de que se generen bucles en la red ya que estos equipos en su gran mayoría no soportan protocolos que ayudan a mitigar este problema.
- El constante cambio que tiene el personal de las empresas públicas perjudica a la continuidad de los proyectos presentes en las Instituciones, ya que existen proyectos planificados y ejecutados con diferente personal a cargo, lo que conlleva a que se deba transferir la información nuevamente y se tengan que cambiar algunos parámetros ya establecidos anteriormente.
- La nueva infraestructura WLAN propuesta permitirá tener cobertura total en el edificio matriz del MIES, con puntos de acceso inalámbricos de características para cubrir las necesidades de los usuarios finales, de tal manera que los equipos sean colocados en puntos del edificio donde provean la máxima cobertura proveyendo el servicio de roaming sin perder la cobertura en ningún área de las instalaciones.
- La implementación de varios servicios puede centralizarse de mejor manera a través del uso de un servicio de directorio activo. Un gran porcentaje de las aplicaciones permite enlazar sus servicios con un único componente de administración. De esta forma se puede ahorrar tiempo de

administración en el área de TI, además de aplicar de mejor manera las políticas orientadas al usuario.

- Las aplicaciones y servicios más vulnerables dentro de la red requieren de un análisis minucioso antes de tomar la decisión de implementarlas. Pese a que el decreto 1014 pide el uso de software abierto en la mayor cantidad de aplicaciones posibles dentro de las instituciones de carácter público, no se debe olvidar que se limita su uso cuando se encuentre en riesgo de seguridad de la institución. Normalmente las soluciones pagadas relacionadas a la seguridad tienen mejores valoraciones técnicas que las soluciones de código abierto. Al no existir reglas generales y debido al ritmo cambiante de las tecnologías y las inseguridades intrínsecas que nacen de ellas es necesario tomar las decisiones correctas para evitar estar en riesgo.
- El mejoramiento de la red inalámbrica es fundamental para aplicaciones que pueden integrase de mejor manera a dispositivos móviles. Los servicios de telefonía y de *cloud computing* aprovechan mucho mejor la versatilidad que ofrecen los dispositivos móviles. Por este motivo se puede sacarle un mejor rendimiento a los dispositivos con las tecnologías que se manejen dentro de la institución. Por ejemplo, la cobertura inalámbrica puede permitir que los usuarios se conecten a la IP PBX de la institución, portando su extensión en su mismo teléfono a cualquier lugar con cobertura inalámbrica, permitiendo un mejor grado de servicio.
- Durante el diseño de cableado estructurado se pude prever la rotación de usuarios en las instalaciones que ocupan actualmente. La estrategia en este caso fue la colocación de nuevas salidas de telecomunicaciones en los lugares que podrían ser ocupados utilizando un enrutamiento de cableado sobre superficies que no sean removidas en el tiempo.

5.2. RECOMENDACIONES

- Una vez realizada la instalación de los elementos tanto activos como pasivos se debe realizar periódicamente un plan de mantenimiento, con el fin de realizar una depuración tanto física como lógica, de tal manera que

se pueda realizar una limpieza de las diferentes partes de los equipos, depuración de reglas y configuraciones e instalación de actualizaciones de los sistemas operativos de los equipos.

- El equipo que se plantea para sustituir el actual firewall tiene la capacidad de realizar filtrado por URLs de una manera más granular que cualquier otro equipo, por lo que se recomienda verificar la base tanto de grupos como aplicaciones que pueden ser vulnerables con los llamados Anonymizers, ya que Checkpoint actualiza su base periódicamente de posibles vulnerabilidades para las redes.
- Es recomendable limitar el ancho de banda en las aplicaciones que utilizan streaming tanto de audio como de video, ya que se pudo verificar que el consumo de ancho de banda para estas aplicaciones es exagerado por lo que el ancho de banda con el que trabaja el MIES tiene horas pico donde llega a saturar el enlace. Actualmente no existe un equipo que realice esta función por lo que no se puede controlar el consumo de ancho de banda.
- El personal de la institución requiere de un programa completo de capacitación en todas las actividades relacionadas con la seguridad informática. Las medidas tomadas para evitar problemas de seguridad son necesarias, pero deben complementarse estrictamente con el accionar del personal para prevenir estos problemas.
- Luego de la respectiva implementación se deberá solicitar al proveedor se registren y verifiquen los ATPs (protocolo de aceptación de pruebas), para verificar los procedimientos y configuraciones realizadas en cada equipo implementado, de esta manera se comprueba el correcto funcionamiento y configuración de los equipos.
- De la experiencia práctica, se recomienda que el uso de software libre sea licenciado en todos los casos que sea posible. Sin quitar méritos a la comunidad que trabaja constantemente en el desarrollo de más y mejores soluciones, es necesario reconocer que el software libre pagado se sujeta a contratos con tiempos de respuesta y niveles de servicio que permiten superar las dificultades en menor tiempo. Debe dejarse de lado el criterio que el software libre es siempre gratis y que no ofrece ninguna garantía.

- Es recomendable tener documentado la topología como la configuración y direccionamiento de los equipos, para tener respaldada la información en el caso que se presenten cambios de personal que administra la red, de tal manera que el traspaso de información sea más eficiente y real.
- Es recomendable tener un respaldo o backups periódicos de los equipos implementados, en caso de falla de algún equipo tener el respaldo oportuno y completo de cada equipo.
- Se recomienda considerar algunas de las políticas descritas en este proyecto para establecer un sistema de políticas formales que a posteriori permitan regular de mejor manera el uso de la red por parte de los usuarios, poniendo énfasis en las cuestiones relacionadas a la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

[L1] N. Oliva Alonso, M. Castro Gil, P. Losada de Dios, G. Díaz Orueta, *Sistemas De Cableado Estructurado*. España: RA-MA S. A., 2006.

[L2] M. Alboroz, C. Alfaraz, *Redes de conocimiento: construcción, dinámica y gestión*, Primera Edición. Argentina: RICYT, 2006.

[L3] J. Areitio Bertolín, *Seguridad de la información. Redes, informática y sistemas de información*.España: Editorial Paranifo, 2008.

[L4] A. Barba Marti, *Gestión de red*. España: Ediciones OPC, 2001.

[L5] Ministerio de Educación, *La información en Internet*. Primera Edición, Argentina: Publicación Buenos Aires, 2010.

[L6] T. Saydam, T. Magedanz, *Redes, gestión de redes y servicio de administración*, *Diario de Redes y Sistemas de Gestión*, Vol. 4, 1996.

FOLLETOS

[F1] P. Hidalgo, "Redes de Área Local", Escuela Politécnica Nacional, Año 2009.

[F2] S. Sinche, "Redes de Área Extendida", Escuela Politécnica Nacional, Año 2009.

[F3] J. Joskowicz, “Cableado Estructurado”, Universidad de la República, Montevideo, URUGUAY, Setiembre 2006, Versión 5.

PUBLICACIONES, PAPERS, REVISTAS

[P1] A. Lago Castillo, D. Mera Moreano, W. Medina, “Implementación virtual de redes LAN, enfocadas en el análisis comparativo de las ventajas y desventajas del uso y aplicación de las diferentes versiones del protocolo SNMP”, Escuela Superior Politécnica del Litoral (ESPOL), 2014.

TESIS

[T1] E. Pinto, “Rediseño de la red de comunicaciones de la “Cooperativa de Ahorro y Crédito Mushuc Runa” para manejar aplicaciones de voz y datos con calidad de servicio”, Escuela Politécnica Nacional, Quito, Ecuador, 2012.

[T2] M. Madrid, “Rediseño de la red de datos del Gobierno Autónomo Descentralizado Municipal del cantón Pujilí para el soporte de multiservicios y la interconexión de sus dependencias”, Escuela Politécnica Nacional, Quito, Ecuador, 2012.

[T3] E. Vizuete, “Rediseño de la red de datos cableada e inalámbrica, para permitir el funcionamiento de nuevas aplicaciones para el colegio militar no 10 Abdón Calderón”, Escuela Politécnica Nacional, Quito, Ecuador, 2014.

[T4] C. Barreiro, A. Herrera, “Reingeniería de la red de datos corporativa de la Administración Zonal Sur Eloy Alfaro del Municipio del Distrito Metropolitano de Quito”, Escuela Politécnica Nacional, Quito, Ecuador, 2012.

PÁGINAS WEB

[PW1] (Accesado Nov. 2015) "Decreto 1014 sobre Software Libre en Ecuador", [PDF en línea]:

http://www.estebanmendieta.com/blog/wp-content/uploads/Decreto_1014_software_libre_Ecuador.pdf

[PW2] (Accesado Sep. 2015) "To Convert Cisco a Lightweight AP to an Autonomous AP", [Vídeo en línea, YouTube]:

https://www.youtube.com/watch?v=QQ_NuxdRhQ4

[PW3] (Accesado Ago. 2015) “Suplemento sobre cableado estructurado”, [PDF en línea]:

http://www.espoch.edu.ec/Descargas/noticias/dacee2_CCNA1_CS_Structured_Cabling_es.pdf

[PW4] (Accesado Ago. 2015) “Gestión de red”, [Página Web]:

http://www.ramonmillan.com/tutoriales/gestionred.php

[PW5] (Accesado Sep. 2015) “Internetworking Technology Handbook”, [Página web]:

http://www.cisco.com/c/en/us/td/docs/internetworking/technology/handbook/ito_doc.html

[PW6] (Accesado Oct. 2015) "Precio de Cisco Catalyst 2960X-24TS-L", [Página web de Amazon]:

http://www.amazon.es/s/ref=nb_sb_noss?__mk_es_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&url=search-alias%3Dcomputers&field-keywords=Cisco+Catalyst+2960X-24TS-L&rh=n%3A667049031%2Ck%3ACisco+Catalyst+2960X-24TS-L

[PW7] (Accesado Oct. 2015) "Precio de TP-LINK TL-SG3424 - Switch (24 puertos, gestionado, montaje en rack)", [Página web de Amazon]:

http://www.amazon.es/TP-LINK-TL-SG3424-puertos-gestionado-montaje/dp/B005B7YVCK

[PW8] (Accesado Feb. 2015) "Cómo Configurar Sistema de Vigilancia Gratuito, Zoneminder" [Página web]:

http://www.eleinformatico.es/seguridad/23-como-configurar-zoneminder

[PW9] (Accesado Mar. 2015) "How to install BigBlueButton 0.81", [Página web]:

https://code.google.com/p/bigbluebutton/wiki/InstallationUbuntu

[PW10] (Accesado Mar. 2015) "The ultimate guide: Owncloud 8 on CentOS 7.x – step by step. Will work 100%", [Página web]:

http://reviews.myhken.com/the-ultimate-guide-owncloud-on-centos-7/

[PW11] (Accesado Mar. 2015) "Zmrepo - A ZoneMinder repository for RPM based distros", [Página web, Wiki]:

http://www.zoneminder.com/wiki/index.php/CentOS#Zmrepo_-_A_ZoneMinder_repository_for_RPM_based_distros

[PW12] (Accesado Mar. 2015) "Zimbra: Integración con Active Directory"; Jorge de la Cruz, [Página web]:

https://www.jorgedelacruz.es/2014/02/10/zimbra-integracion-con-active-directory/

[PW13] (Accesado Mar. 2015) "Zimbra Collaboration - Open Source Edition Documentation", [Página web]:

https://www.zimbra.com/documentation/zimbra-collaboration-open-source

[PW14] (Accesado Mar. 2015) "Instalar Zimbra 8.6 en Centos 7 desde Cero", [Página web]:

http://martinlugo.networksolutions-peru.com/?p=492

[PW15] (Accesado Feb. 2015) "Seguridad en redes"; Jaime Abraham Rivera, [Presentación Slideshare en línea]:

http://es.slideshare.net/JaimeACR/seguridad-en-redes-jacr

[PW16] Pello Xabier Altadill Izura (Accesado Mar. 2015) "IPTABLES - Manual práctico", [Página web]:

http://www.pello.info/filez/firewall/iptables.html

[PW17] (Accesado Mar. 2015) "¿Qué es el software libre? Definición de software libre", [Página web]:

https://www.gnu.org/philosophy/free-sw.es.html

[PW18] Paco Orozco (Accesado Mar. 2015) "GESTIÓN DE RED - del boli al SNMP", [PDF en línea]:

https://eetac.upc.edu/ca/fitxers/Gestion_de_red.pdf

[PW19] (Accesado Mar. 2015) "Introducción a la Gestión de Redes ", [PDF en línea]:

http://www.eslared.org.ve/walc2012/material/track3/gestion-de-redes.pdf

[PW20] (Accesado Mar. 2015) "ZIMBRA 8 MAIL - CONFIGURANDO EL DNS WINDOWS SERVER Y AUTENTICACION ACTIVE DIRECTORY part 3/3", [Vídeo en línea, YouTube]:

https://www.youtube.com/watch?v=QunxPaFIbws

[PW21] (Accesado Mar. 2015) "OwnCloud con Active Directory: Montando nuestro propio Dropbox", [Vídeo en línea, YouTube]:

https://www.youtube.com/watch

ANEXOS

- Anexo 1: Presupuesto referencial de Cableado Estructurado.
- Anexo 2: Presupuesto referencial de Check Point.
- Anexo 3: Cotización de switches de acceso Cisco.
- Anexo 4: Cotización de WRL Cisco.
- Anexo 5: Scripts de configuración de equipos de la red del prototipo.
- Anexo 6: Configuración de Access Point Cisco Aironet 1130AG Series.
- Anexo 7: Instalación de Windows 2008 server.
- Anexo 8: Instalación y configuración de Linux CentOS 7 1503-01.
- Anexo 9: Instalación y configuración de Webmin (en CentOS 7 Minimal).
- Anexo 10: Instalación y configuración de Ubuntu Server 14.04.3.
- Anexo 11: Instalación de Check Point Gaia R77.20.
- Anexo 12: Instalación de servicio DNS en Windows 2008 Server.
- Anexo 13: Instalación de servicio DNS en CentOS 7.
- Anexo 14: Instalación de Zimbra ZCS 8.6.0.
- Anexo 15: Configuración de PBX en Elastix.
- Anexo 16: Configuración de puerto FXO en equipo Grandstream HT503.
- Anexo 17: Instalación de OwnCloud Server.
- Anexo 18: Instalación del Servidor de Cámaras IP ZoneMinder.
- Anexo 19: Instalación de iSpy x64 en Windows.
- Anexo 20: Instalación de BigBlueButton 0.9.1 en Ubuntu Server 14.04.
- Anexo 21: Site Survey realizado en el Edificio Matriz del MIES.
- Anexo 22: Ubicación de los access point en el Edificio Matriz del MIES.
- Anexo 23: Cotización switch de acceso HP
- Anexo 24: Cotización switch de acceso TP-LINK
- Anexo 25: Cotización controladora Inalámbrica HP
- Anexo 26: Cotización controladora Inalámbrica Ruckus
- Anexo 27: Cotización access point HP
- Anexo 28: Cotización Controladora Inalámbrica Cisco
- Anexo 29: Cotización switch de acceso Cisco
- Anexo 30: Cotización access point Ruckus
- Anexo 31: Cotización access point Cisco
- Anexo 32: Cotización switch de núcleo C4510
- Anexo 33: Cotización Cableado Cat 6
- Anexo 34: Cotización Cableado Cat 6A
- Anexo 35: Políticas para la seguridad física y lógica de la información de la red de datos del Ministerio de Inclusión Económica y Social
- Anexo 36: Planos del edificio del MIES de la reestructuración del cableado estructurado.
- Anexo 37: Diagramas de calor de los access point que se deben instalar en el MIES para tener una óptima cobertura