UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA: "DISEÑO E IMPLEMENTACIÓN DE UNA RED DE DATOS Y CONTROL DE ACCESO BIOMÉTRICO EN EL EDIFICIO DE LA CÁMARA DE COMERCIO DE LA CIUDAD DE OTAVALO"

AUTORA: MARCELA ELIZABETH LÓPEZ HUERA.

DIRECTOR: ING. CARLOS PUPIALES.

IBARRA-ECUADOR

2017

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

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

IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar de este proyecto para lo cual pongo a disposición el siguiente trabajo:

DATOS DE CONTACTO	
Cédula de identidad	100359767-9
Apellidos y nombres	López Huera Marcela Elizabeth
Email	melopez@utn.edu.ec
Teléfono	(2) 558-392 / 0990680772

DATOS DE LA OBRA	
Título	Diseño e Implementación de una Red de Datos y Control de Acceso Biométrico en el edificio de la Cámara de Comercio de la Ciudad de Otavalo.
Autor (a)	López Huera Marcela Elizabeth
Fecha	
Programa	Pregrado
Título por el que opta	Ingeniera en Electrónica y Redes de Comunicación
Director	Ing. Carlos Pupiales.

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, MARCELA ELIZABETH LÓPEZ HUERA, con cédula de identidad Nro. 1003597679, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior artículo 144.

3. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y sela desarrolló sin violar derechos de autor por terceros, por lo tanto la obra es original y es titular de los derechos patrimoniales, por lo que se asume la responsabilidad del contenido de la misma y saldré en defensa de la universidad en caso de reclamación por parte de terceros.

En la ciudad de Ibarra,

Marcela Lopez H.

.....

Marcela Elizabeth López Huera

Autora

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

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

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

Yo, MARCELA ELIZABETH LÓPEZ HUERA, con cédula de identidad Nro. 100359767-9, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado: "DISEÑO E IMPLEMENTACIÓN DE UNA RED DE DATOS Y CONTROL DE ACCESO BIOMÉTRICO EN EL EDIFICIO DE LA CÁMARA DE COMERCIO DE LA CIUDAD DE OTAVALO", que ha sido desarrollado para optar por el título de Ingeniera en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la universidad facultada para ejercer los derechos concedidos anteriormente. En mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....Marcela López H.....

Marcela Elizabeth López Huera

100359767-9

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

DECLARACIÓN

DECLARACIÓN

Yo, Marcela Elizabeth López Huera, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamento y Normatividad vigente de la Universidad Técnica del Norte.

Marcela López H.

Marcela Elizabeth López Huera

100359767-9

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Marcela Elizabeth López Huera, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamento y Normatividad vigente de la Universidad Técnica del Norte.

Marcela López H.

Marcela Elizabeth López Huera

100359767-9

VI

V

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis: "DISEÑO E IMPLEMENTACIÓN DE UNA RED DE DATOS Y CONTROL DE ACCESO BIOMÉTRICO EN EL EDIFICIO DE LA CÁMARA DE COMERCIO DE LA CIUDAD DE OTAVALO" ha sido realizada en su totalidad por la señorita MARCELA ELIZABETH LÓPEZ HUERA portadora de la cédula de identidad Nro. 100359767-9.

.....

Ing. Carlos Pupiales.

AGRADECIMIENTO

A Dios y a mi familia. A Dios por brindarme la fortaleza para continuar y seguir adelante; a mis padres Marcelo y Marcia, por ser los pilares fundamentales en mi vida, ya que sin ellos no me hubiese sido posible alcanzar esta meta.

A mis hermanos Silvia y Ariel por siempre brindarme su apoyo incondicional y ser mi dulce compañía a cada segundo, a mi tía Cecy por ser parte indispensable de mi vida y apoyarme en todo momento.

A mis abuelos Luis, Bertha y Cecilia por sus sabios consejos y siempre haber confiado en mis habilidades.

A mis maestros a lo largo de mi carrera, a quienes les debo los conocimientos adquiridos, gracias por su paciencia y entrega en cada clase; especialmente a mi tutor de tesis Ing. Carlos Pupiales, quien me acompañó durante todo el proceso de realización de este trabajo de grado.

Finalmente agradezco a mi querida Universidad Técnica del Norte por permitirme formar parte de esta gran familia, preparándome con valores y conocimientos hacia el mundo laboral.

Marcela

DEDICATORIA

Este proyecto está dedicado principalmente a mi familia, que siempre ha estado apoyándome en cualquier circunstancia.

A mis padres Marcelo y Marcia, que con su tenacidad y lucha insaciable han hecho de ellos mi gran ejemplo a seguir.

Mis hermanos Silvia y Ariel, por ser mi alegría y apoyo incondicional.

A mi tía Cecy por ser mi mejor amiga y guía en todo momento; y a mis abuelos por sus sabios consejos.

A mis queridos maestros que han contribuido al desarrollo y finalización de este trabajo, Ing. Carlos Pupiales, Ing. Fabián Cuzme, Ing Jaime Michilena e Ing. Edgar Maya, aportándome sus ideas, conocimientos y sobretodo su valioso tiempo.

A todo el personal de la Cámara de Comercio de Otavalo, especialmente al Lic. Robert Cadena, por abrirme las puertas del establecimiento y brindarme su apoyo.

Marcela

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

PRESENTACIÓN

El trabajo de grado "DISEÑO E IMPLEMENTACIÓN DE UNA RED DE DATOS Y CONTROL DE ACCESO BIOMÉTRICO EN EL EDIFICIO DE LA CÁMARA DE COMERCIO DE LA CIUDAD DE OTAVALO" está compuesto por los siguientes capítulos:

CAPÍTULO I: Contiene la formulación del tema, objetivos, alcance y justificación.

CAPÍTULO II: Abarca la fundamentación teórica sobre redes, clasificación, medios de transmisión, servicios, cableado estructurado y seguridad.

CAPÍTULO III: Se plantea un estudio de la situación actual de la infraestructura del edificio tomando en cuenta el estado de la red y del cableado existentes.

CAPÍTULO IV: Se detalla el diseño de la red: sistema de cableado estructurado, topología física y lógica, enrutamiento y segmentación en vlans, con los requerimientos de usuario obtenidos.

CAPÍTULO V: Se evidencia la implementación de la red y los pasos que se siguieron para lograrlo.

CAPÍTULO VI: Se realiza el análisis costo beneficio con las variables económicas.

RESUMEN

El edificio de la Cámara de Comercio fue diseñado hace más de 40 años cuando la tecnología y escalabilidad no eran los principales parámetros de construcción, por lo que carece de una infraestructura tecnológica adecuada que contribuya a mejorar la productividad y el cumplimiento de los objetivos planteados por la organización como por ejemplo el brindar capacitaciones en línea, ferias de productos o servicios, así como también el mantener comunicación en red con otras organizaciones.

Este proyecto abarca desde el análisis hasta la implementación de la red de datos del lugar, incluyendo un Sistema de Control de Acceso biométrico cuyo objetivo principal fue conseguir una mejora tecnológica en la infraestructura del edificio, lo cual permitió aumentar la capacidad de conexión de los usuarios, con velocidades elevadas, instalación de switches y soporte para los requerimientos actuales y futuros considerando servicios de seguridad.

Se contempló el estudio de la infraestructura actual con el cual se determinó el enrutamiento del cableado tomando en cuenta la norma ANSI/TIA/EIA 568-B y la norma ANSI/TIA/EIA-569A. Una vez realizado el diseño se ejecutó la instalación y configuración de los equipos de redes y biométricos incluyendo la colocación del cableado, rack, face plates, enrutamiento del par trenzado, segmentación de la red, servidor proxy y manual de políticas de acceso.

Es así que, se logró implementar la Red de Datos y Control de Acceso biométrico en base a los requerimientos planteados, mejorando la infraestructura tecnológica del edificio de la Cámara de Comercio, y proporcionando niveles de seguridad que mejorarán la productividad y eficiencia de sus usuarios.

ABSTRACT

The building of the Chamber of Commerce was designed more than 40 years ago when technology and scalability were not the main parameters of construction, so it lacks an adequate technological infrastructure that contributes to improve productivity and the fulfillment of the objectives raised by The organization such as providing online trainings, product fairs or services, as well as maintaining network communication with other organizations.

This project ranges from analysis to implementation of the site's data network, including a biometric Access Control System whose main objective was to achieve a technological improvement in the infrastructure of the building, which allowed to increase the capacity of connection of the users , With high speeds, installation of switches and support for current and future requirements considering security services.

It was considered the study of the current infrastructure with which wire routing was determined taking into account ANSI / TIA / EIA 568-B and ANSI / TIA / EIA-569A. Once the design was carried out, the installation and configuration of the network and biometric equipment were implemented, including wiring, rack, face plates, twisted pair routing, network segmentation, proxy server and access policy manual.

Thus, it was possible to implement the Biometric Access Control and Data Network based on the requirements, improving the technological infrastructure of the building of the Chamber of Commerce, and providing levels of security that will improve the productivity and efficiency of its users..

CAPÍTULO I

1.1. TEMA

Diseño e Implementación de una Red de Datos y Control de Acceso Biométrico en el edificio de la Cámara de Comercio de la Ciudad de Otavalo

1.2. PROBLEMA

La Cámara de Comercio de la Ciudad de Otavalo es una entidad no gubernamental que agrupa a empresarios o dueños de negocios pequeños, medianos o grandes que tienen por objetivo incrementar la productividad de sus empresas cuidando sus intereses y teniendo como base la mutua cooperación. Tiene sus instalaciones en la Calles García Moreno 7-43 y Modesto Jaramillo de la ciudad; lleva operando desde el año 1975 y su edificio es considerado Patrimonio Cultural.

Este edificio de tres plantas fue construido hace más de cuarenta años, cuando la tecnología distaba mucho de la actual, por lo que su arquitectura no fue diseñada para alojar redes de datos ni mucho menos sistemas automatizados; únicamente cuenta con instalaciones eléctricas.

El inmueble involucrado tiene solamente una conexión directa desde el proveedor de servicios de internet hacia el router localizado en la oficina central mediante el enlace ADSL, tal y como son las conexiones en los hogares, por lo que para tener acceso a la red hay dos posibilidades: conectar el dispositivo final a través de un patch cord directamente al router o realizarlo de manera inalámbrica.

La Cámara de Comercio impulsa el seguimiento de talleres y capacitaciones para sus afiliados y demás gente interesada; por lo que la Sala de Seminarios es considerada un centro de

transferencia de información en donde se debe dotar el servicio de internet para cada equipo que ingrese allí. Esta sala tiene capacidad para cincuenta personas. Adicionalmente están las dependencias de arrendamiento en donde también se necesitan puntos de conexión para los clientes que lo soliciten.

La directiva actual lleva el registro de eventos que se llevan a cabo en este lugar, estimando que al día se recibe la visita de veinte socios y se realizan alrededor de cuatro seminarios al mes con una duración promedio de tres días y la asistencia de veinticinco a cincuenta personas adicionales a los afiliados y empleados que trabajan en las dependencias, por lo que en los días de mayor ajetreo donde se concentran casi cien usuarios y en los que se requiere conexión a la red, se ha optado por improvisar un Cableado sin el cumplimiento de ninguna norma específica lo que limita el acceso de estos usuarios a la red, generando insatisfacción en ellos y propiciando un ambiente poco adecuado para este tipo de eventos.

De igual forma no existen Políticas de Seguridad de Acceso Físico, ni ningún sistema capaz de controlar el ingreso del personal a ciertas estancias o detectar intrusos, siendo este edificio vulnerable a cualquier tipo de inseguridad. Y debido a la información de suma importancia que se maneja en la Cámara de Comercio es fundamental conocer qué persona debe o no tener acceso físico a los dispositivos o datos que manejan estos.

En base a estos antecedentes se plantea como solución la implementación de un Red de Datos lo suficientemente flexible para el lugar, que pueda integrar todas las dependencias de la Cámara de Comercio levantando Políticas de Seguridad de Acceso que permitan brindar conexión a todos los usuarios que la requieran, con un Sistema de Cableado Estructurado apto para transmitir a velocidades GigabitEthernet soportando aplicaciones tales como telefonía, PoE,

video on demand o video en alta definición; así como también la instauración de un Sistema de Acceso Biométrico que proporcione seguridad a las personas y bienes que se alojan en el edificio, por un tiempo estimado de hasta veinte años, convirtiendo al lugar en una infraestructura abierta y escalable encaminada al concepto de edificio inteligente.

1.3.OBJETIVOS

Objetivo general

Implementar una Red de Datos y Control de Acceso biométrico en base a los requerimientos necesarios para tener una red convergente que permita interconectar sus áreas y mejorar las condiciones de seguridad en la infraestructura de la Cámara de Comercio de la Ciudad de Otavalo.

Objetivos específicos

- Estudiar los protocolos de red, normativas de cableado estructurado y sistemas de seguridad actuales que posibiliten un servicio eficiente de comunicaciones y seguridad en el edificio de la Cámara de Comercio.
- Analizar la situación de la infraestructura vigente y de los requerimientos actuales y futuros de los datos que se manejan en la Cámara de Comercio de Otavalo.
- Diseñar la Red acorde al análisis realizado previamente, con una topología adecuada para cubrir las necesidades de capacidad, cobertura y seguridad.
- Implementar la Red en base a las normas de cableado estructurado ANSI/TIA/EIA 568-B y 569-A, con Políticas de Seguridad de Acceso físico y lógico y los protocolos internacionales de red y seguridad, con el financiamiento de SEDYM CIA LTDA DE SEGURIDAD de OTAVALO.

- Realizar el análisis Costo-Beneficio del proyecto de Red de Datos planteado.

1.4. ALCANCE

Este proyecto abarca desde el análisis hasta la implementación de la red propuesta, incluyendo un Sistema de Control de Acceso biométrico, por lo que en primer lugar se estudiarán los Protocolos de Red, Normativas de Cableado Estructurado y Sistemas de Seguridad Actuales para obtener el fundamento teórico indispensable al momento de diseñar la red.

El objetivo principal es conseguir una mejora tecnológica en la infraestructura del edificio de la Cámara de Comercio de Otavalo que permita contar con mayor capacidad de crecimiento, conexiones a velocidades elevadas, instalación de switches y soporte para los requerimientos actuales y futuros considerando servicios de seguridad.

Para su desarrollo es necesario determinar la situación actual del edificio, sus instalaciones y la cantidad de usuarios posibles que necesiten conexión a la futura red y acceso mediante biométricos.

Posteriormente se realizará el diseño de la Red de Datos y Control de Acceso Biométrico en base a los requerimientos y al análisis realizado acerca de usuarios e instalaciones respectivamente, aquí se considerará la topología, el medio de transmisión, distancias, interfaces de conexión, ubicación de los dispositivos, puntos de voz y datos y zonas de mayor extensión que requieran más puntos de conexión, dependencias que requieren biométricos, tomando en cuenta la norma ANSI/TIA/EIA 568-B para saber cómo instalar el cableado y la norma ANSI/TIA/EIA-569 A para el respectivo enrutamiento en los recorridos y los protocolos de seguridad.

Después se realizará la instalación y configuración de los equipos de redes y biométricos que incluye la colocación del cableado, rack, face plates y otros dispositivos que se podrían beneficiar en esta implementación.

Luego, se procederá a empezar con la debida puesta en marcha de acuerdo a las especificaciones de diseño y en concordancia con la persona encargada por parte de la Cámara de Comercio, para que una vez terminadas todas las configuraciones se pueda ejecutar pruebas de monitoreo a través de aplicaciones que permitan capturar los paquetes y verificar el correcto funcionamiento.

Finalmente, se realizará la documentación pertinente después de implementado este proyecto dejando recomendaciones para que los usuarios futuros puedan hacer uso de ellas.

1.5. JUSTIFICACIÓN

El proyecto propuesto será fácilmente adaptable a las operaciones que efectúa la Cámara de Comercio de la Ciudad de Otavalo, lo que ocasionará una notable mejora en relación a la calidad y cantidad de información que atravesará la Red Local.

Será posible administrar la red en su totalidad, optimizando los procesos que se llevan a cabo y ahorrando tiempo cuantiosamente.

En base a un análisis porcentual realizado acerca de los dispositivos que necesitan conexión, tomando en cuenta a veinte miembros de la Cámara de Comercio (usuarios que acuden al lugar en un día normal), de los cuales el 50% utiliza más de un dispositivo que requiere acceso a la red entre los que destacan: computadoras y Smartphones se constató que únicamente se pueden conectar cuatro computadoras directamente a los puertos del router , el resto de dispositivos deben hacerlo mediante la red inalámbrica proporcionada por este.

El acceso a la red inalámbrica lo lograron 8 dispositivos mientras que los demás tenían acceso limitado, o por el contrario no pudieron establecer su dirección ip necesaria.

En conclusión, el 60% de los dispositivos de usuario no pudieron acceder a la red mientras que el 40% restante lo hizo, pero con una velocidad mínima.

Un estudio realizado en Lima-Perú titulado "Tecnologías de información y comunicaciones en las Empresas" mostró que el 85.7% de empresas de ese país ya cuenta con tecnología en red pero aún queda más del 14% que debe integrarse a esta tecnología ya que constituye una herramienta básica para las empresas a efectos de mejorar la gestión empresarial en todos sus aspectos, solucionando inconvenientes de producción, información, ventas, entre otros.

El estudio también demuestra que las empresas que disponen de una Red de Área Local son el 40% más eficientes que las que no tienen conectividad en red, ya que son capaces de incrementar el flujo de la información induciendo una reducción de los costos de transacción como también pueden generar una difusión acelerada de la información acrecentando la eficiencia de los mercados, generando así beneficios directos e indirectos para la economía.

El presente proyecto permitirá proteger el activo más importante de esta entidad, la información, así como también los bienes que se alojan en el edificio y brindar seguridad a sus empleados, a través del Control de Acceso que limite la entrada de las personas a ciertos lugares; dado que en los últimos años se han registrado robos de equipos de valor, debido a la carencia de un Control de Acceso que ha dejado el libre ingreso a personas no autorizadas, no obstante la pérdida de información es lo que más se lamenta cuando se suscitan este tipo de eventos.

La integración tecnológica del edificio mediante la red local y control de acceso busca crear una edificación con infraestructura que provea a sus usuarios y dispositivos que allí se localizan,

un ambiente flexible y seguro mejorando la funcionalidad del mismo al ser capaz de transferir información a mayor velocidad, utilizar aplicaciones de videoconferencia, controlar intrusiones e interceptar el tráfico TCP/IP.

CAPÍTULO II

FUNDAMENTO TEÓRICO

2.1. CONCEPTOS DE REDES

2.1.1. Definición de Red

Una red es un conjunto de dispositivos conectados mediante un cableado físico o de forma inalámbrica que comparten información, servicios u otros recursos. El objetivo de una red es que cada dispositivo que se encuentre conectado a ella pueda acceder a la información de cualquier otro dispositivo en la red sin tomar en cuenta la ubicación física de estos. (Stallings, 2014)

2.1.2. Topologías de Red

La topología de una red es la manera física en que se conectan los dispositivos de red sobre un medio de comunicación y pueden tener diferentes configuraciones: bus, anillo, estrella, malla, entre otras. (Rivera, 2016)

2.1.2.1.Topología de bus

En este tipo de topología la red posee un solo canal de comunicaciones, denominado bus troncal o backbone que es el que se encarga de interconectar todos los dispositivos como se evidencia en la figura 1. Una de las ventajas de este tipo de topología es su fácil implementación, no obstante algún inconveniente en el bus troncal puede disminuir el desempeño de la red. (Tanenbaum, 2012)

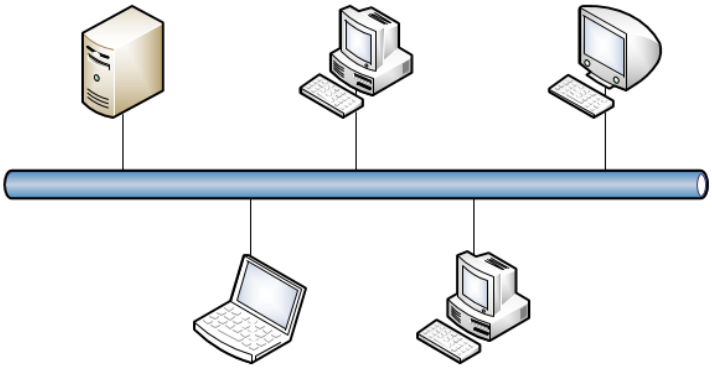


Figura 1. Topología tipo bus. Microsoft Office Visio 2013.
Fuente: El autor.

2.1.2.2. Topología en estrella

Existe un nodo central en el que se conectan todas las estaciones, esta configuración tiene la ventaja de que si algún nodo llega a fallar, la red seguirá funcionando correctamente ya que dicho nodo no interfiere con los demás. (Katz, 2013) En la figura 2 se puede apreciar el gráfico.

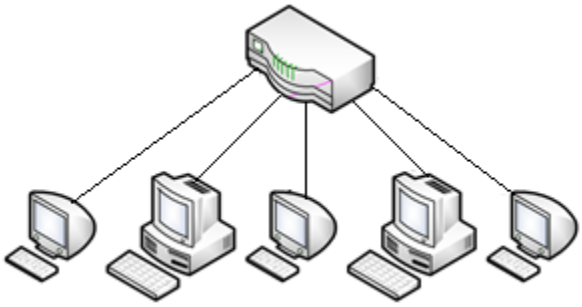


Figura 2. Topología en estrella. Microsoft Office Visio 2013.
Fuente: El autor.

2.1.2.3.Topología en árbol

Tiene un nodo de enlace troncal a partir del cual sobresalen ramificaciones donde se conectan los nodos en forma jerárquica asemejándose a un árbol, como se observa en la figura 3. Se la puede considerar como una variación de la topología en estrella con la diferencia de que no existe un nodo de enlace central. Su cableado es punto a punto. (Tanenbaum, 2012)

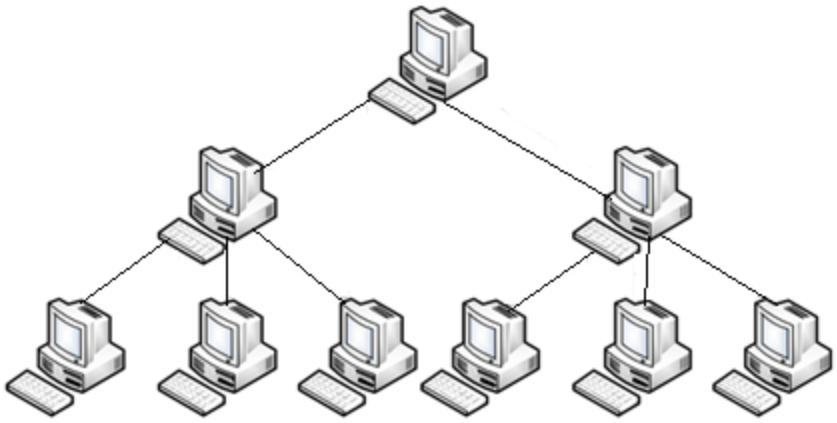
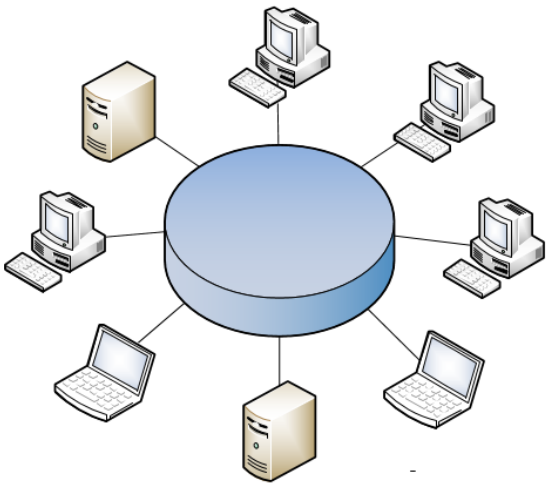


Figura 3. Topología de árbol. Microsoft Office Visio 2013.
Fuente: El autor.

2.1.2.4. Topología en anillo

Topología en la cual los nodos se interconectan formando un anillo. Cada estación actúa como receptor y transmisor con el fin de pasar la señal a la estación siguiente, la comunicación se realiza mediante un token (sólo la estación que lo posea podrá transmitir la información). Es posible generar redundancia con esta topología al utilizar una configuración de anillo doble. (Soto Gil, 2015). Véase figura 4.



*Fig**ura** 4.* Topología en anillo**.** Microsoft Office Visio 2013.
Fuente: El autor.

2.1.2.5. Topología en malla

Topología en la cual cada estación se conecta con las demás estaciones generando una especie de malla puesto que la información puede ser transmitida por diferentes rutas lo que da lugar a una red redundante, sin embargo su costo al momento de implementar puede resultar elevado. La figura 5 indica su configuración. (Plevyak, 2015)

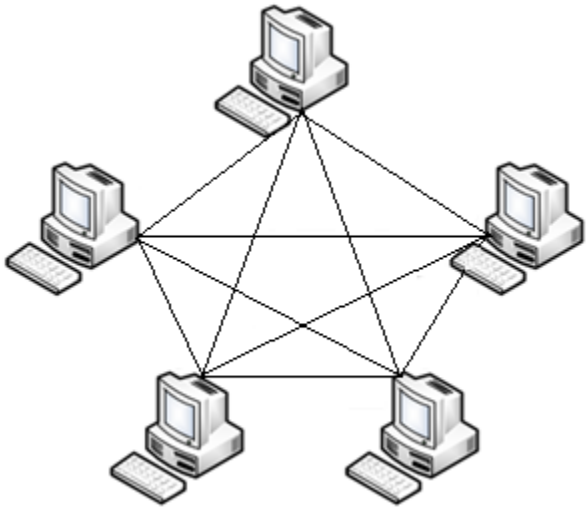


Figura 5. Topología de malla. Microsoft Office Visio 2013.
Fuente: El autor.

2.1.3. Clasificación de las Redes

2.1.3.1. Por su tamaño y extensión

- **Redes PAN (Personal Area Network)**

  Esta red se conforma únicamente por los dispositivos cercanos a su usuario, siendo una red pequeña de entorno local como se muestra en la figura 6. (Tanenbaum, 2012)

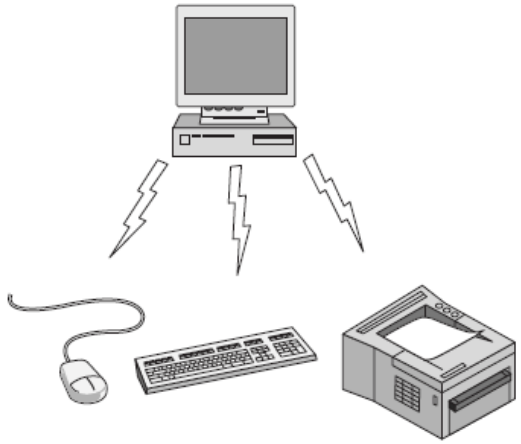


Figura 6. Esquema de Red de Área Personal. Tanenbaum, 2012. Pág 16.
Redes de Computadoras, 5ta Edición.

- **Redes LAN (Local Area Network)**

Su extensión varía de entre 10 metros a 1 kilómetro. Debido a su tamaño suelen ser redes de velocidad rápida en donde las estaciones se encuentran cerca una de la otra. Este tipo de red incrementa la eficiencia en oficinas, edificios o pequeñas empresas. La figura 7 identifica el esquema de este tipo de red. (Rivera, 2016)

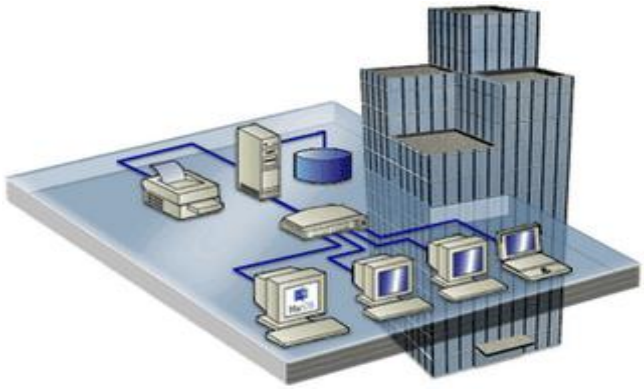


Figura 7. Esquema de Red de Área Local. CISCO, 2014.
Recuperado de http://www.cisco.com

- **Redes MAN (Metropolitan Area Network)**

Como se puede observar en la figura 8, una red MAN comprende una cobertura superior a los 4 kilómetros y puede llegar a cubrir una distancia de 10 kilómetros o incluso más con repetidores, ya que unifica varias redes LAN proporcionando un medio de transmisión de larga distancia que puede ser par trenzado o fibra óptica. (Tanenbaum, 2012).

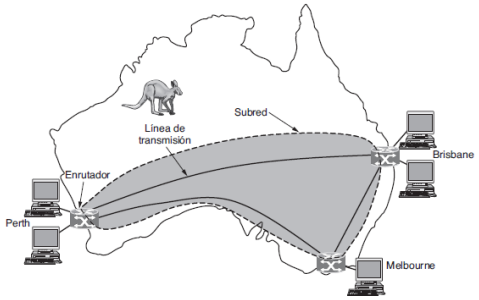


Figura 8. Esquema de Red de Área Metropolitana. Tanenbaum, 2012. Pág 22. Redes de Computadoras, 5ta Edición.

- **Redes WAN (Wide Area Network)**

Este tipo de red usualmente se encarga de conectar países ya que consiste en un conjunto de redes LAN interconectadas por otra subred. Su tamaño varía de entre 100 y 1000 kilómetros. (Tanenbaum, 2012) .Observe la ilustración de la figura 9.

Figura 9. Esquema de Red de Área Extensa. INFORMATICAHOY, 2016 Recuperado de http://www.informatica-hoy.com.ar/redes/LAN-WAN-MAN-WLAN-WMAN-WWMAN-SAN-PAN.php

2.1.3.2.Por la tecnología de transmisión

- **Redes tipo Broadcast**

  Son redes en las que la información es recibida por todas las estaciones pertenecientes a esta debido a que comparten un mismo canal de comunicaciones.

- **Redes Punto a Punto**

  Son redes en donde cada canal de comunicaciones solamente interconecta dos nodos, es decir las estaciones resultan pares entre sí pudiendo actuar en una relación maestro-esclavo.

2.1.3.3. Según el tipo de transferencia de datos

- **Redes de transmisión Símplex**

  La información se transmite en un solo sentido.

- **Redes de transmisión Half-Dúplex**

  La información viaja en ambos sentidos pero no al mismo tiempo.

- **Redes Full-Dúplex**

  Los datos se transmiten en ambos sentidos simultáneamente.

2.1.4. Dispositivos de Red

Comprende el hardware que se conecta a la red para permitir la comunicación entre estaciones. Estos pueden ser dispositivos finales y dispositivos intermedios.

2.1.4.1. Dispositivos finales o de usuario

Son aquellos dispositivos que interactúan directamente con el usuario final como se aprecia en la figura 10: computadoras, impresoras, teléfonos IP, entre otros. A todos estos dispositivos se les suele llamar “hosts”. (Reid & Lorenz, 2016)

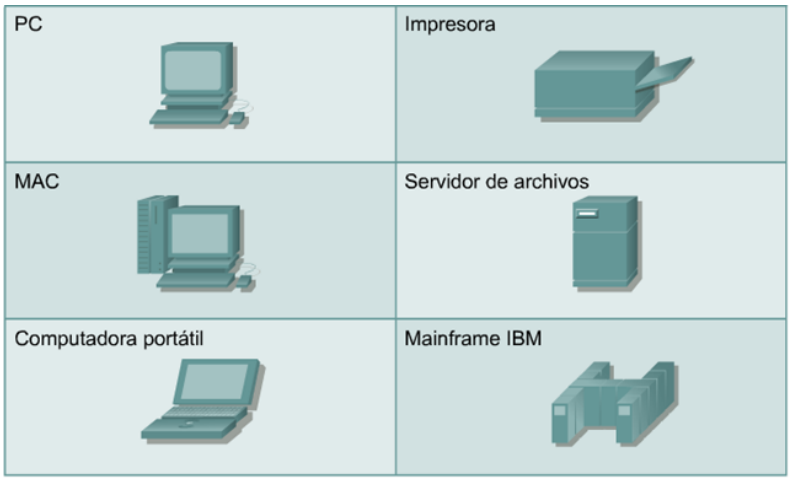


Figura 10. Dispositivos finales. Cisco Networking, 2011. Recuperado de http://aspectosbasicosdenetworking.blogspot.com/2011/03/dispocitivos-finales-y-su-papel-en-la.html

2.1.4.2. Dispositivos intermediarios

Estos dispositivos son los que conectan a la red con los dispositivos finales, o bien con otras redes, algunos ejemplos se muestran en la figura 11. (Reid & Lorenz, 2016). Y pueden ser:

- **Dispositivos de acceso a la red**

  Permiten la comunicación de lo hosts con su red, aquí se ubican los hubs, switches o puntos de acceso inalámbricos.

- **Dispositivos de internetwork**

  Se encargan de la conexión de una red con otra. Por ejemplo: routers.

- **Dispositivos de seguridad**

  Se encargan de la protección de la red en base a un análisis de su tráfico. Un claro ejemplo es un firewall.

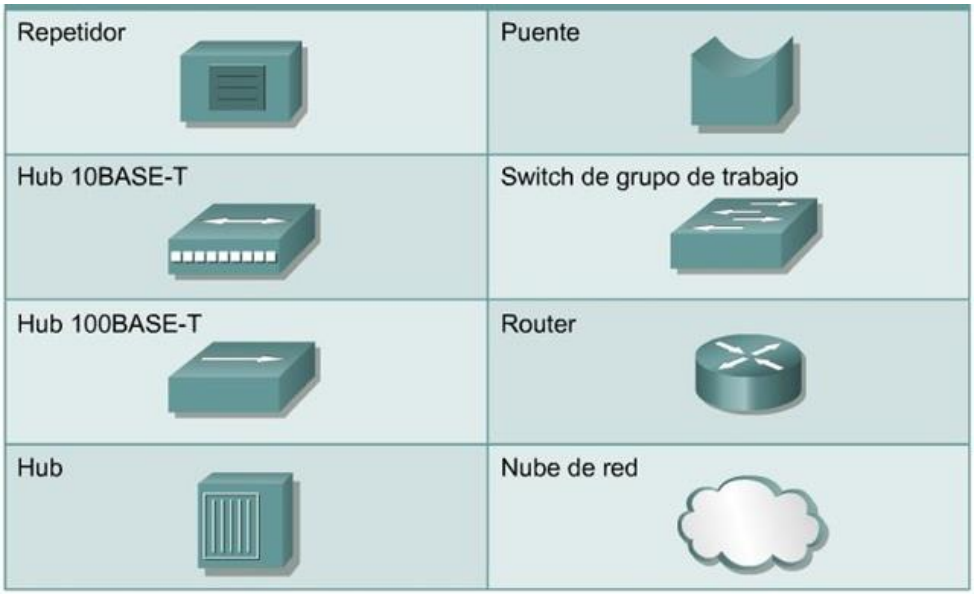


Figura 11. Dispositivos intermediarios de red. . Cisco Networking Academy Program, 2017. Recuperado de https://mind42.com/public/4766a894-0d91-4cbc-bbd0-0e3c06eabe01

2.1.5. Medios de transmisión

Constituye el canal por el cual se establece la comunicación.

2.1.5.1. Medios de transmisión guiados

Son aquellos que utilizan componentes físicos o cables para el "guiado" o conducción de las ondas. Estos pueden ser: cable coaxial, par trenzado y fibra óptica.

Las características de estos medios de transmisión tales como: velocidad de transmisión, ancho de banda se encuentran dadas por el propio medio dependiendo de la distancia entre los terminales u otros factores. (Stallings, 2014)

- **Cable coaxial**

Es un cable que consta de dos conductores concéntricos: el núcleo y la malla o blindaje como se muestra en la figura 12, en medio de estos se localiza un aislante, al igual que en su cobertura, por protección.

Inicialmente estos cables eran los utilizados en redes locales por su capacidad y resistencia frente a interferencias, actualmente se ha desestimado su uso con la llegada del par trenzado y fibra óptica.

Existen dos tipos de cable coaxial, el grueso y el delgado. El primero era utilizado en la mayoría de redes locales transmitiendo acorde a 10 Base 2, mientras que el segundo se empezó a utilizar con el fin de reducir costes en la implementación de redes siendo acorde a la norma 10 Base 5.

Son utilizados normalmente para transmitir señales de TV o datos de alta velocidad, esta varía en un promedio de 100 Mbits/seg.

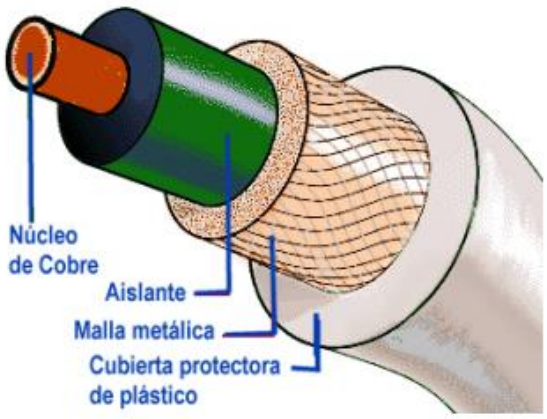


Figura 12. Partes de un cable coaxial. Soto Gil, 2015
Recuperado de http://www.portatiles-pcs.net/files/documents/
MANUAL-PARA-EL-CURSO-DE-DISE%C3%91O-DE-REDES-2015.pdf

- **Par trenzado**

El cable de par trenzado es un conjunto de hilos de cobre que se entrelazan entre sí con el fin de minimizar la interferencia electromagnética.

Se dice que a mayor número de cruces se reduce el inconveniente de diafonía (interferencia electromagnética). El par trenzado puede ser apantallado y no apantallado.

- **Par trenzado no apantallado o cable UTP**

Son cables sin apantallar (figura 13) que se suelen utilizar con mayor frecuencia debido a su bajo coste.

Figura 13. Cable UTP. Aguilar, 2015. Pág 7.
Recuperado de http://en.calameo.com/read/004695317c67cf139fd84

Categorías de cable UTP

Dependiendo de la velocidad de transmisión los cables se clasifican de acuerdo a la tabla 1, siendo reconocidos por la EIA/TIA (Alianza de Industrias Electrónicas/ Asociación de la Industria de Telecomunicaciones) a partir de la categoría 3.

Tabla 1

Categorías de cable UTP

Categoría	Velocidad de transmisión	Ancho de Banda
1	-	1 MHz
2	-	4 MHz
3	10 Mbps	16 MHz
4	20 Mbps	20 MHz
5	100 Mbps	100 MHz
5e	1000 Mbps	100 MHz
6	1 Gbps	250 MHz
6a	10 Gbps	hasta 500 MHz

Stallings, 2014. Pearson Education. Data and computer communications

- **Par trenzado apantallado o cable STP**

En este tipo de cables, cada par trenzado está cubierto por una malla conductora como se muestra en la figura 14, que actúa como pantalla frente a la interferencia electromagnética.

Debido a esta malla su nivel de protección frente a perturbaciones es bastante superior que el del cable UTP. Se utiliza generalmente en redes Ethernet o Token Ring.

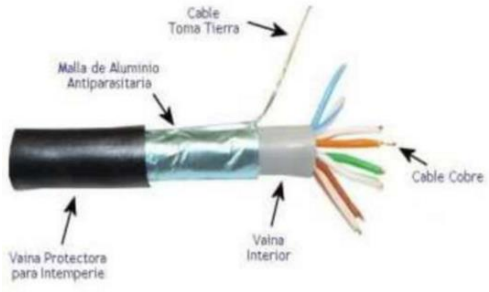


Figura 14. Partes de un cable STP. Aguilar, 2015. Pág 10.
Recuperado de http://en.calameo.com/read/004695317c67cf139fd84

- **Par trenzado con pantalla global o cable FTP.**

  Similar al par trenzado UTP con la diferencia de que posee un apantallamiento que recubre todos los pares. Véase en la figura 15.

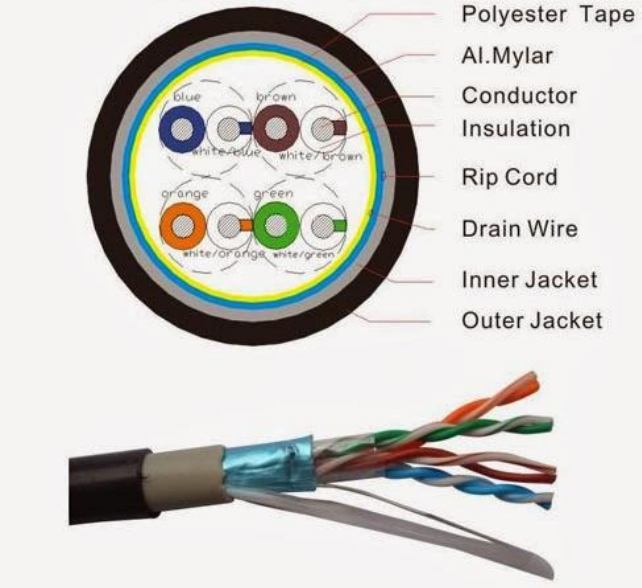


Figura 15. Partes de un cable FTP. Tipos de cable de red, 2014. Recuperado de http://k4b135.blogspot.com/

2.1.5.2. Medios de transmisión no guiados

Son aquellos que transmiten ondas a través del aire o del vacío. Constituyen medios sin cable que se utilizan en lugares donde los medios guiados no llegan o resulta más costoso realizarlo.

Su transmisión se realiza mediante antenas receptoras y transmisoras, y según su frecuencia pueden ser: ondas de radio, microondas, infrarrojas, entre otras.

2.1.6. Servicios de una Red

2.1.6.1. Telefonía IP

La telefonía IP o Voz sobre IP es una tecnología que permite combinar los servicios de voz y datos en la misma red, haciendo que la señal de voz viaje mediante Internet utilizando el

protocolo IP. Los elementos que permiten una comunicación por Voz IP son: la central IP, el Gateway IP y por supuesto teléfonos que soporten este servicio. (Lamus, 2014)

La principal ventaja de este servicio es la reducción de infraestructura que requiere ya que al integrar los servicios mencionados anteriormente se puede obtener un Sistema Unificado de Telefonía con funciones avanzadas.

2.1.6.2. Correo electrónico

Permite a un usuario enviar mensajes hacia otro, mediante dispositivos como computadoras o celulares independientemente de su ubicación. (Ardita, 2012)

Para utilizar este servicio se necesita un buzón de correo en un servidor que normalmente es físico propiedad del ISP, y el programa de correo comercial en el cual el usuario escribe su mensaje.

2.1.6.3. Impresora en red

Una de las principales ventajas de utilizar impresoras en red es la reducción de recursos ya que en muchas ocasiones resulta muy costoso adquirir una impresora dedicada para cada estación de trabajo en un determinado lugar.

Consiste en conectar varias computadoras o hosts y una o más impresoras en la misma red con el fin de que todos estos puedan tener acceso al servicio de impresión. Actualmente estas impresoras permiten inclusive la recepción de mails para lograr una impresión remota. (Windows, 2012)

2.1.6.4. Fax

Es un servicio en el cual se escanean los documentos en el dispositivo denominado “fax” y se los transmiten a través de la línea telefónica hacia otro fax conectado como salida. El fax de salida replica la imagen escaneada y la imprime en papel. Este tipo de servicio se encuentra casi obsoleto debido al triunfo de la tecnología actual como es el correo electrónico o el internet. (Coopersmith, 2015)

2.1.6.5.Videovigilancia IP

La videovigilancia en red es la combinación entre los Circuitos Cerrados de Televisión CCTV y las redes de comunicación, con el objetivo de observar imágenes y escuchar sonido de manera local o remota. Dependiendo del hardware que se utilice, es posible también sincronizar aplicaciones que permitan reconocimiento facial o de otro tipo. (EC&M, 2016).

2.1.6.6.Internet

Actualmente uno de los principales objetivos de las redes de datos es conectarse a internet; es decir, formar parte de la gran red global que enlaza continentes con el fin de compartir información a nivel mundial. En esta “red de redes” participan hosts de diferentes tipos, desde sistemas robustos hasta modelos personales. En la red se dan citas instituciones oficiales, gubernamentales, educativas, científicas y empresariales que ponen a disposición de millones de personas su información. (Plaza & Janés, 2013).

2.1.1.1.Servicios de la intranet

La intranet constituye una red dentro de una organización, es decir se accede de manera privada, y no pública como sucede con el internet. (Martínez Ferreira, 2014). En esta se pueden encontrar o alojar diversos servicios como por ejemplo:

- Telnet (Telecommunication Network): se refiere al acceso remoto que se puede obtener de una máquina a otra, generalmente a través del puerto 23.
- SSH (Secure Shell): también se refiere a conexión remota, sin embargo ssh utiliza métodos de cifrado por lo que resulta más seguro que telnet.
- FTP (File Transfer Protocol): software para compartir e intercambiar información de un computador a otro, este intercambio se realiza en texto plano por lo que es vulnerable si se lo ataca. Utiliza el puerto 20 y 21.
- WEB: software que utiliza el protocolo http para almacenar archivos y emitirlos a través de la red hacia los usuarios que lo soliciten.

2.2. Modelos de red

Explican la comunicación desde un host hacia otro para lo cual se han dividido en capas para un mejor entendimiento.

Para que la información se transfiera de un extremo a otro es necesario que todos los dispositivos manejen un mismo protocolo o idioma, entendiéndose como protocolo como el conjunto de normas que establecen el formato y transmisión de paquetes. (Tanenbaum, 2012)

2.2.1. Modelo OSI (Interconexión de Sistemas Abiertos)

Desarrollado por la Organización Internacional de Normalización (ISO) con el objetivo de lograr la compatibilidad de redes entre fabricantes. No es una arquitectura de red puesto que no especifica los protocolos y servicios de cada capa. (Rivera, 2016). Es un modelo de 7 capas:

- **Capa física**

  Establece la relación entre el medio de transmisión y un dispositivo, para lo cual es necesario conocer características eléctricas, físicas y mecánicas de estos.

- **Capa de enlace de datos**

  Sus funciones son: framing, direccionamiento físico, control de flujo, control de errores y control de acceso.

- **Capa de Red**

  Se encarga de encaminar la información hacia su destino (direccionamiento lógico). Los routers son los que trabajan en esta capa.

- **Capa de Transporte**

  Proporciona una transferencia de datos confiable para las capas superiores, sin duplicidad y sin errores.

- **Capa de Sesión**

  Esta capa controla las conexiones entre los hosts, es decir establece, administra y termina las conexiones.

- **Capa de Presentación**

  Se encarga de la sintaxis de los datos, es decir los traduce en la forma que la aplicación lo requiere, pudiendo cifrarlos para su envío mediante internet.

- **Capa Aplicación**

  Esta capa abarca todas las aplicaciones de red y servicios de internet que puede utilizar un usuario.

2.2.2. Modelo TCP/IP

Mientras el modelo OSI se encarga únicamente de la estandarización de redes, el modelo TCP/IP ya constituye una arquitectura que incluye además el stack de protocolos de las

diferentes capas del modelo OSI. Los protocolos más relevantes son el TCP (Protocolo de Control de Transmisión) y el IP (Protocolo de Internet). (Hidrobo Moya, 2015)

El protocolo IP envía los paquetes basado en la dirección destino desde una estación a otra mientras que el TCP verifica que esta información sea entregada correctamente.

TCP/IP está formado por cuatro capas:

- **Capa Acceso a la Red**

  Esta capa precisa las características de hardware de red. TCP/IP proporciona libre elección del protocolo y medio de transmisión a utilizarse describiendo estándares de hardware como IEEE 802.3.

- **Capa Internet o Red**

  Recibe y transfiere paquetes para la red. Abarca los siguientes protocolos:

- IP (Internet Protocol): se ocupa de las direcciones IP, formato y fragmentación de paquetes.
- ICMP (Internet Control Message Protocol): detecta las condiciones de error como por ejemplo fallos de conectividad o paquetes que llegan muy rápido que no se pueden procesar.
- IGMP (Internet Group Management Protocol): permite que los hosts soliciten la recepción de tráfico de multidifusión. (Hidrobo Moya, 2015)

- **Capa Transporte**

  Se ocupa de la comunicación extremo a extremo. Los protocolos pueden ser:

- UDP (User Datagram Protocol): es un protocolo no orientado a conexión que por lo tanto no es confiable debido a que envía la información pero no garantiza la adecuada recepción.
- TCP (Transmission Control Protocol): protocolo orientado a conexión que garantiza que los datos lleguen en una secuencia correcta y libre de errores.

- **Capa de Aplicación**

Esta capa opera con protocolos de alto nivel como:

- Transferencia de archivos: TFTP, FTP, HTTP.
- Correo electrónico: SMTP, POP3.
- Administración de red: SNMP.
- Administración de Nombres: DNS.

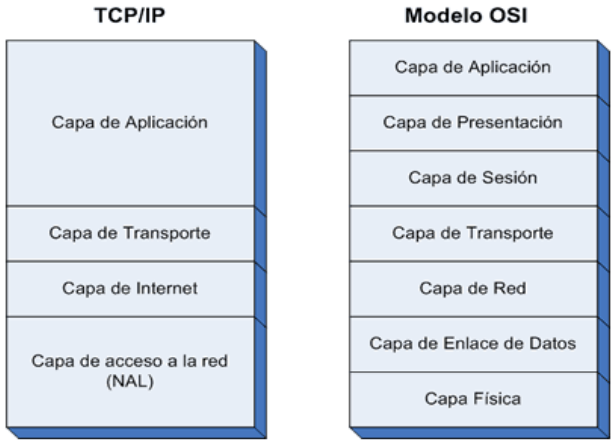


Figura 16. Modelo OSI y Modelo TCP/IP. CISCO, 2014. Internet of everything. Recuperado de http://www.cisco.com

En la figura 16 se pueden observar las capas del modelo OSI y su equivalente en TCP/IP.

2.3. Redes LAN

Red de Área Local o LAN constituye un conjunto de dispositivos, en su mayoría computadoras conectadas a través de un medio de transmisión guiado con el fin de compartir recursos de hardware o software optimizando su desempeño. (Reid & Lorenz, 2016). Las principales funciones de una red LAN en una empresa son:

- Transferencia de archivos: es posible compartir aplicaciones de software para que todos los empleados de la empresa puedan tener acceso a los archivos creados por otros, como si estos estuviesen almacenados en su propia máquina.
- Control de dominio: permite verificar la autenticidad del usuario mediante un username y password, siendo posible permitir o denegar la utilización de ciertos recursos dependiendo de la jerarquía del usuario, lo que proporciona un nivel de seguridad más elevado.
- Correo electrónico.

2.3.1. Sistema de Cableado Estructurado de una red LAN

Un Sistema de Cableado de Estructurado consiste en el tendido de cable dentro de un edificio con el objetivo de levantar una red de área local.

2.3.1.1. Organismos que rigen las normas de Cableado Estructurado

- **ANSI (American National Standards Institute)**

  Organización fundada en el año de 1918 encargada de supervisar el sistema de estandarización voluntaria en el sector privado de los Estados Unidos. (ANSI, 2016)

- **EIA (Electronics Industry Association)**

  Organismo conformado por empresas y organizaciones de alta tecnología pertenecientes a los Estados Unidos que fomentan el desarrollo del mercado referente a electrónica del consumidor. (EIA, 2016)

- **TIA (Telecommunications Industry Association)**

  Principal asociación comercial fundada en 1985 que se dedica a la elaboración de normas de cableado estructurado para muchos productos de las telecomunicaciones. (TIA, 2016)

- **ISO (International Standards Organization)**

  Es el mayor desarrollador de normas internacionales voluntarias a nivel mundial.

  (ISO, 2016)

- **IEEE (Instituto de Ingenieros Eléctricos y de Electrónica)**

  Es la asociación más grande de profesionales relacionados con la tecnología en el mundo. Es la responsable de las especificaciones de redes LAN como token ring, Ethernet y gigabit Ethernet. (IEEE, 2016)

Figura 17. Organismos que rigen el Cableado Estructurado. Frazer, 2013.
Structured cabling comes of age.

Los logotipos de las organizaciones que rigen las normas de cableado estructurado se pueden observar claramente en la figura 17.

2.3.1.2.Normas de Cableado Estructurado

Con la finalidad de evitar seguir las reglas de algún proveedor en especial se han creado normativas para cableado estructurado referentes a tipos de cable, conectores, topologías, distancias y otros parámetros. Las normas que destacan son:

- ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales sobre cómo instalar el Cableado.
    - TIA/EIA 568-B1 Requerimientos generales
    - TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado
    - TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.
- ANSI/TIA/EIA-569-A: Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado.
- ANSI/TIA/EIA-570-A: Normas de Infraestructura Residencial de Telecomunicaciones.
- ANSI/TIA/EIA-606-A: Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-607: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-758: Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones. (Anixter, 2015)

ANSI/TIA/EIA-568-B

Cableado de Telecomunicaciones en Edificios Comerciales que trata sobre cómo instalar el Cableado. Se divide en ANSI/TIA/EIA-568-B.1, ANSI/TIA/EIA-568-B.2 y ANSI/TIA/EIA-568-B.3

Su propósito es:

- Instaurar una norma genérica con soporte a aplicaciones de diferentes vendedores.
- Instalar y planificar el cableado estructurado en edificios comerciales.
- Establecer el criterio técnico para las configuraciones del SCE.

ANSI/TIA/EIA-568-B.1: Requerimientos Generales

De acuerdo a este estándar, el SCE se divide en seis subsistemas: facilidades de entrada, cuarto de equipos, cableado vertical o backbone, cuarto de telecomunicaciones, cableado horizontal y las áreas de trabajo.

- **Facilidades de entrada (Acometida):** se refiere al hardware que se requiere para la interconexión de los proveedores externos de servicio con el SCE del cliente, siendo el punto de demarcación aquel que delimita las responsabilidades entre proveedor y cliente. Este punto puede localizarse en cuartos de otros servicios como por ejemplo agua potable o energía eléctrica.
- **Cuarto de equipos:** constituye el centro de la red, aquí se localizan todos los equipos de telecomunicaciones como: routers, switches, servidores, centrales PBX. Puede incluir áreas de trabajo para los encargados.

- **Cuarto de telecomunicaciones:** concentra las terminaciones del cableado horizontal con los cables de backbone con el objetivo de brindar el servicio a las áreas de trabajo. Se recomienda un cuarto de telecomunicaciones por piso mientras no se sobrepase los 90 metros.

  Si se trata de una infraestructura pequeña es posible utilizar montantes de pared o gabinetes encerados.

- **Cableado vertical o backbone:** interconecta los cuartos de telecomunicaciones, los cuartos de equipos y las acometidas de un SCE incluyendo también el tendido de cable entre edificio.

  - Los cables reconocidos por la norma son:
  - Cable par trenzado 100 ohmios
  - Fibra multimodo 50/125micras o 62.5/125micras.
  - Fibra monomodo.

  En la norma se definen dos niveles de conexión que se evidencian en la figura 18:

  - Conexión directa entre cuarto de equipos y cuartos de telecomunicaciones.
  - Conexión mediante un cuarto intermedio.

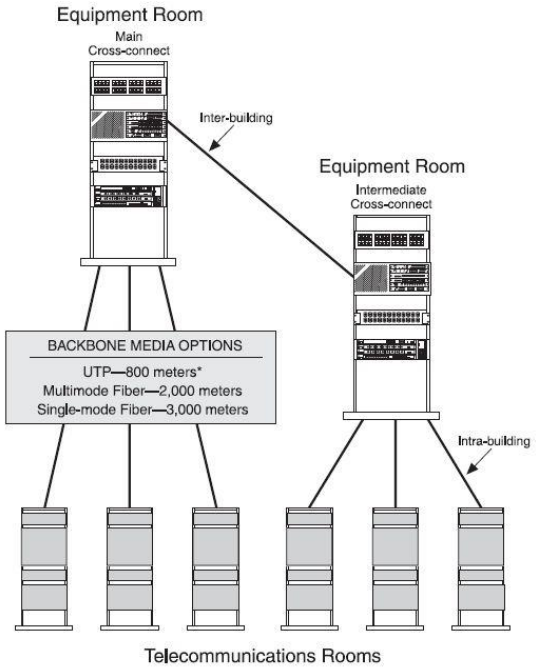


Figura 18. Niveles de conexión del cableado vertical. Cableado Estructurado, 2012. Recuperado de http://cableado-horizontal.blogspot.com/2011_08_01_archive.html.

Según el medio de transmisión se puede determinar la máxima distancia a utilizarse acorde a la tabla 2:

Tabla 2

Distancias máximas para el cableado vertical

Tipo de medio	Conexión cruzada principal a horizontal	Conexión cruzada principal a intermedio	Conexión cruzada intermedia a horizontal
Cobre	800m	500m	300m
Fibra multimodo	2000m	1700m	300m
Fibra monomodo	3000m	2700m	300m

Equipo de redes/Cableado esttructurado. 2011. Recuperado de https://es.slideshare.net/equipoderedes/cableado-estructurado-8803415

- **Cableado horizontal:** conecta las áreas de trabajo con los cuartos de telecomunicaciones incluyendo patch cords, salidas de telecomunicaciones y las terminaciones en los patch panel con una topología en estrella. Su distancia máxima hasta la salidas de telecomunicaciones es de 90 metros como se observa en la figura 19.

  Los cables reconocidos por la norma son:

- Cable de cobre 4 pares UTP 100 ohmios o STP.
- Fibra óptica multimodo de 62,5/125 o 50/125 micras.

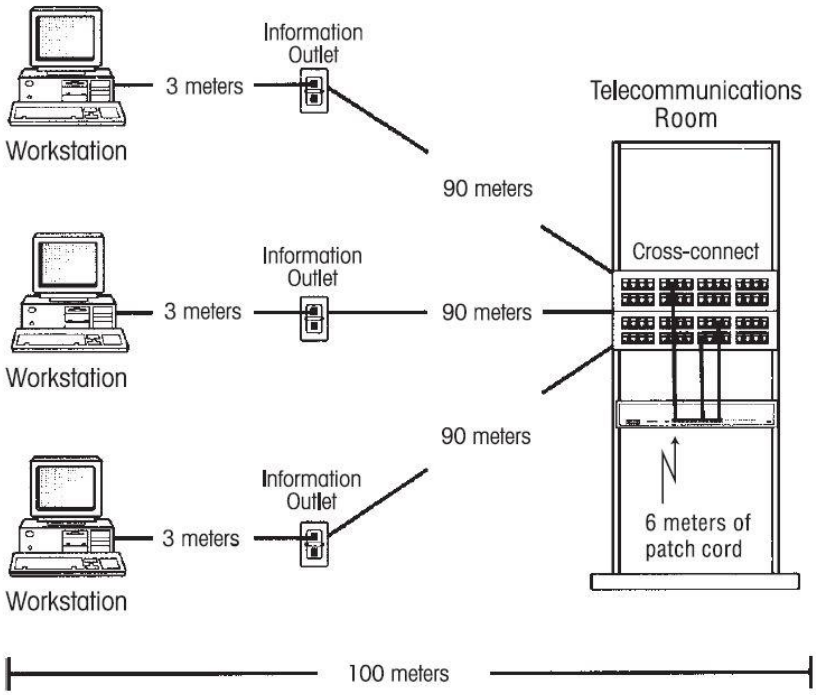


Figura 19. Distancia máxima del cableado horizontal. Cableado Estructurado, 2013. Recuperado de http://2.bp.blogspot.com/-oLdlbNFhW6c/UWrRbw7IBKI/AAAAAAAAAAs/Ul9byZ1fbHc/s1600/ca.jpg

- **Área de Trabajo:** es aquella que se extiende desde la salida de telecomunicaciones hasta el equipo de trabajo. El cableado en las áreas de trabajo generalmente no es permanente por lo que debe resultar fácil de cambiar. El patch cord empleado en el área de trabajo tiene una longitud máxima de 3m.

Cada área de trabajo deberá tener al menos dos salidas de telecomunicaciones, como lo muestra la figura 20, una para voz y otra para datos. Una salida será cable UTP de 100 ohmios categoría 3 o superior, mientras que la otra será par trenzado o fibras multimodo. (Stallings, 2014)

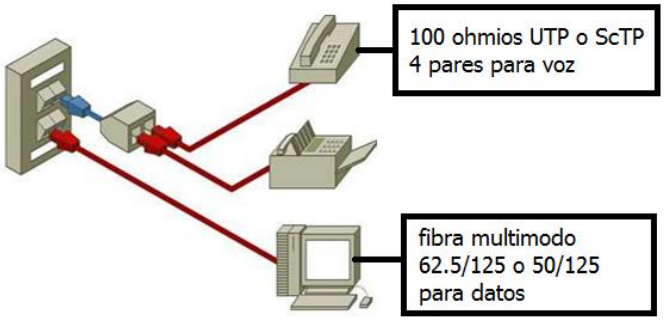


Figura 20. Salidas de telecomunicaciones. Manual de Cableado Estructurado, 2015. Pág 272. Recuperado de http://dgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

En ambientes de oficinas abiertos el estándar reconoce dos opciones de instalación como salidas de telecomunicaciones:

- **MUTOA (Multi-user Telecommunications Outlet):** conecta un máximo de 12 usuarios a una misma columna o mobiliario de forma permanente.

  Véase el esquema en la figura 21.

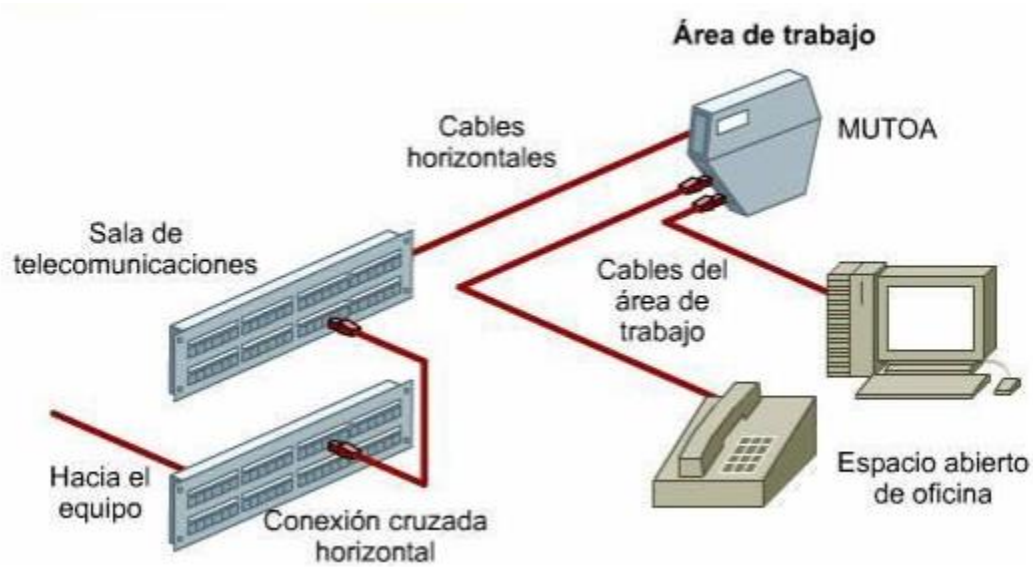


Figura 21. Salida de Telecomunicaciones para Múltiples Usuarios. Manual de Cableado Estructurado, 2015. Pág 273. Recuperado de dgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

De acuerdo a la figura 21 se plantea la tabla 3 que indica las distancias que debe tener el cableado estructurado horizontal hacia las áreas de trabajo.

Tabla 3

Distancias del cableado en el Área de Trabajo

Conexión Cruzada	Cuarto de telecomunicaciones - MUTOA	MUTOA-Dispositivo Área de Trabajo	TOTAL
5	90	5	100
5	85	9	99
5	80	13	98
5	75	17	97
5	70	22	97

Manual de Cableado Estructurado, 2015.
Recuperado de rddgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

- **Punto de consolidación:** la diferencia con el MUTOA es que necesita una conexión extra en el trayecto del cableado horizontal como se observa en la figura 22.

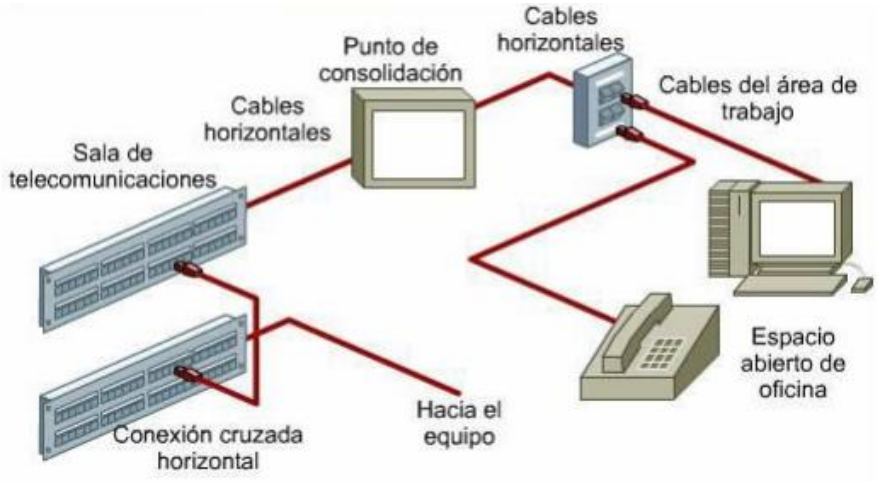


Figura 22. Punto de consolidación. Manual de Cableado Estructurado, 2015. Pág 275.
Recuperado de rddgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

La distribución de pines en los conectores y jacks puede ser según la normas T568A o T568B definiendo un cable directo si ambos extremos se distribuyen con la misma norma, y un cable cruzado si cada extremo cumple con diferente norma como se observa en la figura 23.

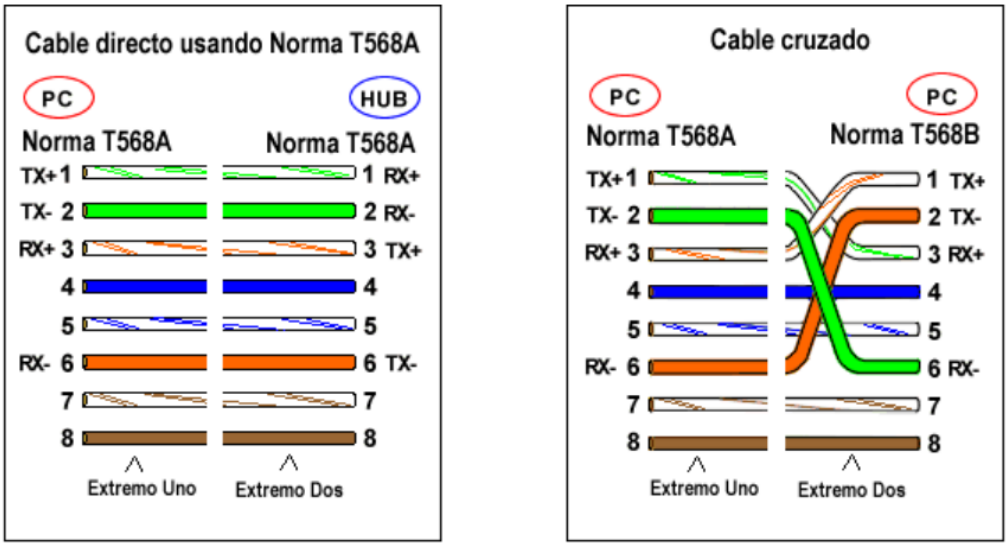


Figura 23. Distribución de pines en los conectores. Soto Gil, 2015
Recuperado de http://www.portatiles-pcs.net/files/documents/
MANUAL-PARA-EL-CURSO-DE-DISE%C3%91O-DE-REDES-2015.pdf

ANSI/TIA/EIA-568-B.2: Componentes del Par Trenzado Balanceado UTP

La norma ANSI/TIA/EIA- 568-B.2 describe los parámetros en cuanto a transmisión de los cables de par trenzado, refiriéndose a los diferentes tipos de ruidos o diafonías que estos pueden producir.

Requerimientos del cable horizontal: este estándar muestra los parámetros que debe cumplir el cable horizontal categoría 3 y categoría 5e para una distancia de 100 metros según la tabla 4:

Tabla 4

Parámetros de rendimiento del par trenzado categoría 3 y 5e

Par Trenzado	Frecuencia	Pérdida de inserción (dB)	NEXT (dB)	PSNEXT (dB)	ELFEXT	PSELXT	Pérdida de retorno	Tiempo de propagación (ns)	Diferencia en tiempo o propagación (ns)
Categoría 3	16	13.1	23.2	23	-	-	-	545 (10Mhz)	45
Categoría 5e	16	8.2	47.2	44.2	37.8	24.8	25.0	-	-
	100	22.0	35.3	32.3	23.8	20.8	20.1	538	45

Manual de Cableado Estructurado, 2015. Recuperado de ddgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

Parámetros del cableado

- Mapa de cableado: evidencia los cortocircuitos, pares cruzados, pares invertidos, divididos y cualquier otro fallos.
- Pérdida de inserción: pérdida en dB, que es diferente según la categoría.
- NEXT (Near End Crosstalk): es el ruido que induce un par transmisor a un receptor vecino.
- PSNEXT (Power Sum NEXT): mide el crosstalk en el extremo más cercado (near end), considerando los efectos de los otros 3 pares.
- ELFEXT (Equal Level Far End Crosstalk): mide la relación entre el crosstalk en el extremo lejano y la atenuación.
- PSELFEXT (Power Sum Equal Level Far End Crosstalk): está dado por el ELFEXT de cada par que interfiere en la señal transmitida por el par de señal útil.
- Pérdida de retorno: medida dada por las reflexiones de la señal.

- Tiempo de propagación: es el tiempo que se demora la señal en pasar de un extremo a otro.
- Diferencia en tiempo de propagación: mide la diferencia de velocidad entre el par más rápido y el par más lento del cable.

ANSI/TIA/EIA-568-B.2-1: Componentes del Par Trenzado balanceado categoría 6

Debe tener compatibilidad con las categorías 3 y 5e, y para el cableado de backbone y vertical se toman en cuenta los parámetros de la tabla 5:

Tabla 5

Parámetros de Rendimiento de Par Trenzado Cat.6

Cableado de backbone y vertical a una distancia de 100 metros							
Frecuencia (MHz)	Pérdida de inserción (dB)	NEXT (dB)	PSNEXT (dB)	ELFEXT (dB)	PSELFEXT (dB)	Pérdida de Retorno (dB)	FEXT (dB)
250	32.8	38.3	36.3	19.8	16.8	17.3	-
Accesorios de conexión							
250	0.32	46.0	-	-	-	16.0	35.1
Enlace Permanente							
250	31.1	35.3	32.7	16.2	13.2	10.0	-
Enlace de Canal							
250	35.9	33.1	30.2	15.3	12.3	8.0	-

Manual de Cableado Estructurado, 2015.
Recuperado de rddgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

Existe un adendum de este estándar, en donde se describen los parámetros del par trenzado categoría 6 aumentada, que se describen en la tabla 6:

Tabla 6

Parámetros de rendimiento para Par Trenzado Cat. 6

Current ISO Cat-6 Channel Specifications								
frecuencia (MHz)	PS Atenuación (dB)	pr-pr NEXT (dB)	PS NEXT (dB)	pr-pr ELFEXT (dB)	PS ELFEXT (dB)	Pérdida retorno (dB)	Retraso Fase (ns)	Retraso Torc. (ns)
1	2,2	72,7	70,3	63,2	60,2	19,0	580,0	50,0
4	4,2	63,0	60,5	51,2	48,2	19,0	563,0	50,0
10	6,5	56,6	54,0	43,2	40,2	19,0	556,8	50,0
16	8,3	53,2	50,6	39,1	36,1	19,0	554,5	50,0
20	9,3	51,6	49,0	37,2	34,2	19,0	553,6	50,0
31,25	11,7	48,4	45,7	33,3	30,3	17,1	552,1	50,0
62,5	16,9	43,4	40,6	27,3	24,3	14,1	550,3	50,0
100	21,7	39,9	37,1	23,2	20,2	12,0	549,4	50,0
125	24,5	38,3	35,4	21,3	18,3	11,0	549,0	50,0
155,52	27,6	36,7	33,8	19,4	16,4	10,1	548,7	50,0
175	29,5	35,8	32,9	18,4	15,4	9,6	548,6	50,0
200	31,7	34,8	31,9	18,4	15,4	9,0	548,4	50,0
250	36,0	33,1	30,2	17,2	14,2	8,0	548,2	50

Recuperado de http://www.monografias.com/trabajos93/cable-categoria-5/image004.png

ANSI/TIA/EIA-569-A

Norma de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado.

- **Facilidades de Entrada**

  Deben ubicarse en lugares libres de humedad, cercanos a las canalizaciones de backbone.

- **Cuarto de Equipos**

  Se debe evitar la humedad y tener fácil acceso para equipos grandes. El tamaño mínimo recomendado es 13.5 metros cuadrados, es decir un espacio de 3.7x3.7 metros.

- **Canalizaciones de bakcbone**
    - Pueden ser internas o externas al edificio. En caso de tratarse de canalizaciones externas se distinguen cuatro tipos:
    - Canalizaciones subterráneas: consiste en ductos de 100mm de diámetro mínimo.
    - Canalizaciones directamente enterradas: los cables deben tener la protección respectiva ya que quedan totalmente bajo tierra.
    - Canalizaciones aéreas: los cables deben contar con protecciones mecánicas para soportar los cambios climáticos.
    - Canalizaciones tipo túnel: se crea un túnel exclusivamente para el cableado aislándolo de otros servicios para evitar interferencias.

Ahora bien, si las canalizaciones son internas pueden ser ductos, bandejas, portacables, entre otros. Este cableado puede ser vertical u horizontal.

- Canalizaciones verticales: ductos, bandejas verticales o escalerillas. No se permite la utilización de ductos en ascensores.
- Canalizaciones horizontales: en caso de que los cuartos o armarios de telecomunicaciones no se encuentren alineados se debe usar tramos de cableado horizontal que se pueden localizar debajo del piso, en las paredes o cielorraso.

- **Cuarto o armario de telecomunicaciones**

  Se recomienda que haya almenos un armario por piso a menos que el área a servir exceda los 1000 metros cuadrados.

- **Canalizaciones horizontales**
  - Su diseño debe soportar los cables especificados en la norma TIA-568B además de estar lo suficientemente distanciados del cableado de energía. Los tipos de canalizaciones pueden ser:
  - Ductos bajo el piso: forman parte de la obra civil.
  - Ductos bajo el piso elevado: bajo el piso falso es posible instalar el sistema de cableado de telecomunicaciones.
  - Ductos aparentes: metálicos o de PVC, no es recomendable ductos flexibles.
  - Bandejas: estructuras sólidas que generalmente se instalan sobre el cielorraso y pueden o no tener tapa.
  - Ductos sobre cielorraso: deben estar fijos al techo.
  - Ductos perimetrales: se usan para alcanzar las áreas de trabajo, deben colocarse de forma estética. (Anixter, 2015)
- **Áreas de trabajo**

Se asume áreas de trabajo de 10 metros cuadrados, es decir 3x3.

2.4. Seguridad en redes

Es necesario crear medidas y políticas que permitan tener cierto nivel de seguridad dentro y fuera de una red, es decir, controlar y restringir el acceso para prevenir y actuar correctamente cuando se suscite algún evento. (Plevyak, 2015)

2.4.1. Seguridad Física

La seguridad física consiste en la protección física de los equipos de hardware mediante la utilización de barreras tangibles y procedimientos de control como medida para evitar pérdida de información y daño a los equipos. (Escrivá Gascó & Romero Serrano, 2013)

2.4.1.1. Políticas de seguridad

Es un documento que detalla las directrices para los usuarios, personal y demás personas que puedan tener acceso a los recursos de la empresa.

En este documento también se deben incluir las acciones a tomar en caso de presentarse alguna emergencia que ponga en riesgo la seguridad física de la organización, por lo que todos los involucrados deberían tomarse el tiempo de leer estos parámetros y de ser necesario proporcionar sugerencias con el fin de mejorarlo. . (Ardita, 2012)

La RFC 1244 define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán. (RFC, 1244).

Al momento de levantar políticas en una institución se debe tomar en cuenta que la seguridad empieza y termina con personas, por lo que deben ser:

- Holísticas.
- Acorde a las necesidades (no excederse).
- Atemporal (Independiente del tiempo en que se aplique).
- Estratégicas (Poseer alternativas en caso de emergencias.)

Las políticas de seguridad deben contemplar aspectos esenciales tales como integridad, disponibilidad, privacidad y, adicionalmente, control, autenticidad y utilidad.

No debe abarcar sanciones sino más bien descripciones justificadas de lo que se desea proteger y porqué. (Ardita, 2012)

2.4.1.2. Sistemas de control de acceso

Es importante resguardar el área de acceso a los equipos de hardware, evitando el hurto de estos, para que únicamente el personal autorizado pueda hacer uso de este.

Uno de los principales controles de acceso consiste en la utilización de lectoras biométricas, que son las que se encargan de la recepción de datos de los usuarios que requieran acceso. Existen varios tipos de lectoras:

- **Lectoras de teclado:** es el mecanismo más básico ya que recibe la información mediante un teclado únicamente
- **Lectoras de proximidad:** el usuario debe poseer una tarjeta de control de acceso, que dependiendo del tipo y energía que esta utilice permitirá o no una mayor distancia.
- **Lectoras biométricas:** se considera una medida de seguridad bastante avanzada ya que el dispositivo lector se encarga del escaneo de alguna parte física del usuario como por ejemplo: rostro, huella dactilar, iris.

Las lectoras enunciadas en este apartado pueden ser combinadas con el fin de proporcionar mayor seguridad, es decir pueden ser lectoras biométricas con teclado o de proximidad.

2.4.2. Seguridad Lógica

Este tipo de seguridad es la que se encarga de filtrar el acceso a los recursos de la red, protegiendo la información que contiene el hardware. (Katz, 2013)

2.4.2.1. Firewall

Es un dispositivo configurado para permitir o bloquear el acceso a ciertas páginas o servicios basado en normas y criterios definidos con anterioridad. Los firewall pueden implementarse en harware o software, y se utiliza frecuentemente en usuarios de internet, evitando que estos ingresen a páginas no autorizadas. El firewall intercepta todas las peticiones, examinándolas para bloquear o no su paso. (Katz, 2013)

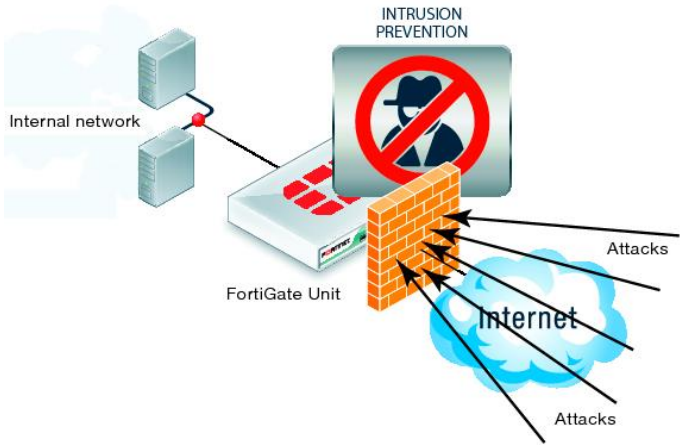


Figura 24. Esquema de protección de un firewall. Katz, 2013.
Redes y seguridad, apoyo en la web, Alfaomega.

2.4.2.2.Antivirus

Es un software con el que actualmente, ya cuentan la mayoría de computadoras, su funcionamiento varía dependiendo del tipo de antivirus que se utilice, no obstante, se basan en reconocer los virus de acuerdo a una lista en su base de datos y analizarlos para luego seleccionar una acción en contra de estos. (Katz, 2013)

De acuerdo a un artículo publicado por la revista PC Magazine, en mayo de 2016, los mejores antivirus son:

- Webroot
- McAfee
- BitDefender
- Kaspersky UK
- AVAST Software
- Amazon
- ESET North America
- F-Secure UK
- Panda Security
- MSRP. (PC Magazine, 2016)

2.4.2.3. Filtros MAC

Consiste en crear un listado con las direcciones MAC de los dispositivos que se desea tengan acceso a la red. La dirección MAC o dirección física, es un identificador único a un dispositivo de red, tiene 48 bits, los primeros 24 dados por el fabricante mientras que los restantes corresponden la parte específica del equipo. Mientras no se encuentre la MAC en la lista no se podrá acceder a los recursos de la red. (Reid & Lorenz, 2016)

2.4.2.4. Redes LAN virtuales (VLAN)

Constituye una red de área local que agrupa dispositivos de red de manera lógica y no física. La implementación de VLANs incrementa la seguridad de una red, debido a que si se produce un ataque a una de ellas, las demás no se verán afectadas. (Reid & Lorenz, 2016)

Las VLAN pueden asignarse de forma manual o dinámica. Manualmente quiere decir que se asigna el puerto a una determinada VLAN sin que intervenga el host final, mientras que dinámicamente, el dispositivo final o de usuario, de acuerdo a su MAC es asociado a una VLAN. Véase figura 25.

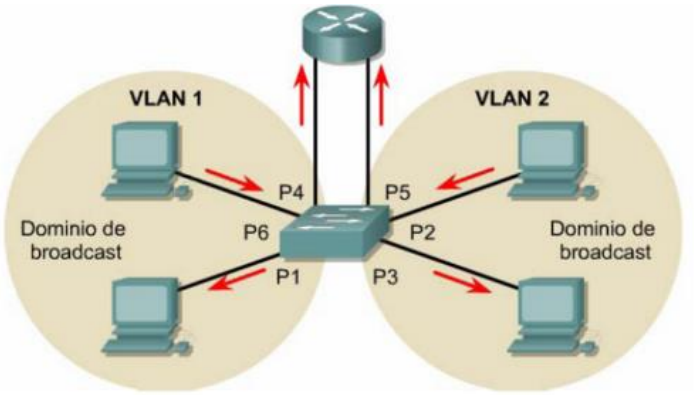


Figura 25. Esquema de segmentación de las VLANS. CISCO, 2014. Internet of everything. Recuperado de http://www.cisco.com.

2.4.2.5.Redes privadas virtuales (VPN)

La figura 26 muestra el esquema de una VPN que corresponde a un túnel entre el usuario y la red que se quiere alcanzar a través de internet, es decir, crea una extensión de una red privada sobre una pública Todo el tráfico que pasa a través de esta está protegido y asegurado.

Figura 26. Funcionamiento de una VPN. CISCO, 2016. Recuperado de http://www.cisco.com.

2.4.2.6.Servidor RADIUS (Remote Authentication Dial In User Service)

Un servidor RADIUS gestiona el acceso a la red mediante un servidor de acceso de red (NAS) basándose en el protocolo UDP, RADIUS se considera un servicio sin conexión, siendo un protocolo cliente/servidor.

El cliente RADIUS es generalmente un NAS y el servidor de RADIUS constituye un daemon (proceso) que se ejecuta en UNIX o una máquina del Windows.

El usuario comienza la autenticación PPP al NAS y este le solicita que ingrese nombre y contraseña, el usuario responde y el cliente envía esta información al servidor RADIUS, el cual finalmente responde con aceptar, rechazar o impugnar. (CISCO Web Support, 2012)

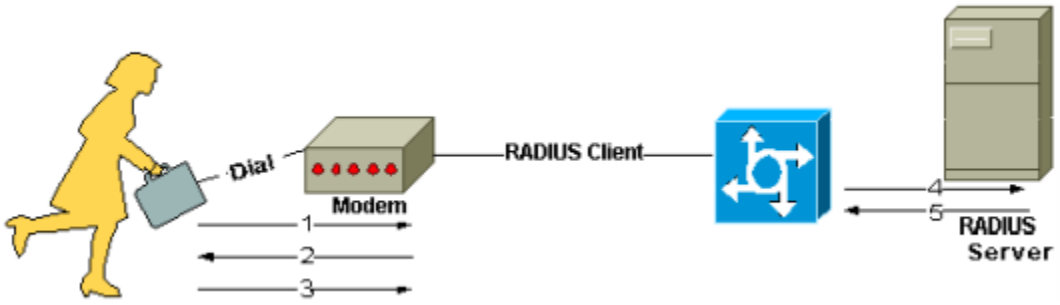


Figura 27. Funcionamiento del protocolo RADIUS. CISCO Web Support, 2012. Recuperado de http://www.cisco.com/cisco.

2.4.2.7.Portal cautivo

Un portal cautivo puede ser un software o hardware que se encarga de vigilar el tráfico haciendo que los usuarios atraviesen este filtro en caso de que quieran navegar a través de Internet. (Katz, 2013)

El portal cautivo es capaz de controlar o aplicar calidad de servicio al restringir el ancho de banda o tiempo brindado hacia el usuario.

Ejemplos de programas que implementan un portal cautivo por software:

- Chillispot (Linux)
- WifiDog (embedded Linux - OpenWRT, Linux, Windows)
- HotSpotSystem.com (embedded Linux, WRT54GL, Mikrotik, etc)
- m0n0wall (embedded FreeBSD)
- PfSense (FreeBSD)
- ZeroShell (Linux)

Ejemplos de dispositivos que implementan un portal cautivo por hardware:

- Cisco BBSM-Hotspot
- Nomadix Gateway
- Antamedia Hotspot Gateway
- Mikrotik RouterOS
- Warriors Labs WD Portal Cautivo
- Seeketing.

2.4.3. Sistemas de seguridad actuales

Según cifras de la Policía Nacional, desde enero hasta junio del 2015 se registraron 7 022 robos a domicilio y 2 467 a locales comerciales. Mientas que en el 2016, durante el mismo período, se contabilizaron 5 660 robos a domicilio y 2 296 a locales comerciales.

Por lo que, Carlos Castillo, director Ejecutivo de la Cámara de la Seguridad Privada del Ecuador (Casepec), afirma que la delincuencia ha aumentado en los últimos tres años; y por este motivo se ha incrementado la demanda de los productos y servicios para prevenir los problemas de la inseguridad. (Líderes, 2016).

De igual manera, no solamente existe delincuencia en bienes y productos, sino también a través de la red; tal fue el incidente suscitado en agosto de 2011 en el que el grupo denominado Anonymous se adjudicó la intrusión a la página de la empresa Hunter para Ecuador (http://www.hunter.com.ec) mostrando en su portada la imagen de personas enmascaradas con la leyenda "Somos Anonymous" (Telégrafo, 2011). Más tarde revelaron información personal a través de un boletín de pastebin.com que incluía nombres, apellidos, correos electrónicos, cargos, teléfonos y números de cédula, de varias personas que trabajaban en el Aeropuerto de Quito.

Y el más reciente fue el hackeo de la cuenta de twitter de la Federación Ecuatoriana de Fútbol (FEF) el pasado marzo de 2017, a través de la cual publicaron el mensaje "Gracias por sus comentarios, como nos quitaron la clasificación nosotros les quitamos sus cuentas...!!!". (El Universo, 2017).

Es así que, las empresas, compañías u organizaciones con grandes infraestructuras o aquellas que simplemente deseen proteger su hardware o software, se ven en la necesidad de implementar mecanismos que sean capaces de proteger su equipamiento físico así como también su

información, a continuación se mencionan algunos tipos de organizaciones que cuentan cierta seguridad.

2.4.3.1. Seguridad en Centros Comerciales

En los centros comerciales priman dos temas importantes cuando se habla de seguridad: proteger los bienes y proteger las personas, siendo el público una variable con constante rotación y concurrencia, sobretodo en horas pico y feriados. (Reisz, 2016). Entonces generalmente en estos espacios se tienen:

- Guardias de seguridad: capacitados en diferentes aspectos como trato con el público, derechos humanos, defensa, lenguaje corporal entre otros.
- CCTV (más entrenamiento a operadores).
- Alarmas contra desastres ambientales.
- Alarmas de robo
- Sistemas de control de acceso.
- Sistemas de observación y patrullaje.
- Sistemas de órdenes por altavoces.

2.4.3.2. Seguridad en Instituciones Bancarias

Los bancos o instituciones de este tipo, deben tomar en cuenta medidas de seguridad impuestas a nivel nacional que abarcan parámetros como:

- Cámaras de seguridad que capten movimientos sospechosos.
- Pulsadores de accionamiento de señales de alarmas.
- Controles de acceso individualizados para cada usuarios.

2.4.4. Soluciones de seguridad más utilizadas

En el país, compañías como GREENETICS SOLUCIONES S.A o GMS Seguridad de la Información, que prestan sus servicios de protección cibernética en niveles de seguridad perimetral o avanzada, utilizan los siguientes tipos de firewall/proxies:

2.4.4.1. Sophos

Sophos ofrece soluciones de seguridad de hardware y software que se encarga de la protección desde estaciones de trabajo hasta servidores. Por lo que sus funciones abarcan desde parámetros básicos como calidad de servicio (QoS) automático, Stateful Packet Inspection, VPN para acceso remoto(PPTP/L2TP), reportes y su administración es 100% gráfica. (Sophos, 2016).

2.4.4.2. FireEye

Fire Eye se encarga de los ataques de malware avanzado con soluciones de prevención de intrusiones, antivirus y puertas de enlace añadiendo también protección en varias fases contra amenazas multivectoriales. FireEye reúne información y la almacena en un banco de pruebas como dirección ip, protocolos y puertos que utiliza el atacante con el fin de bloquear la comunicación. (GMS, 2017)

2.4.4.3. Checkpoint

Checkpoint provee una amplia gama de equipos de seguridad de alta performance. Si bien es posible instalar el software de checkpoint sobre plataformas abiertas como Nokia y Crossbeam también se lo puede hacer sobre los equipos hardware propios de checkpoint, los cuales están construidos con una arquitectura de seguridad mucho más robusta que permite a las organizaciones realizar todos los parámetros referentes a la administración de seguridad mediante una consola unificada.

2.4.4.4. Cisco Asa

El Software Cisco Adaptive Security Appliance (ASA) es el sistema operativo que da origen a la familia Cisco ASA, ofreciendo funcionalidades de firewall de clase empresarial a equipos exclusivos de Cisco ASA, incluyendo tecnologías de seguridad críticas para brindar soluciones completas como: IPS, VPNs, routing dinámico, seguridad CiscoTrustSec y firewall basado en identidad. (CISCO Web Support, 2012).

CAPÍTULO III

SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA DEL EDIFICIO DE LA CÁMARA DE COMERCIO DE OTAVALO

3.1. Antecedentes

La Cámara de Comercio de la Ciudad de Otavalo alberga a empresarios o dueños de negocios pequeños, medianos o grandes que tienen por objetivo incrementar la productividad de sus empresas cuidando sus intereses y teniendo como base la mutua cooperación.

La arquitectura del edificio no fue diseñada para alojar redes de datos ni mucho menos sistemas automatizados; únicamente cuenta con instalaciones eléctricas, ya que su infraestructura existe desde hace más de 40 años.

De igual forma no existen Políticas de Seguridad de Acceso Físico, ni ningún sistema capaz de controlar el ingreso del personal a ciertas estancias o detectar intrusos, siendo este edificio vulnerable a cualquier tipo de inseguridad.

En base a estos antecedentes se plantea como solución la implementación de una Red de Datos lo suficientemente flexible para el lugar, que pueda integrar todas las dependencias de la Cámara de Comercio levantando Políticas de Seguridad de Acceso que permitan brindar conexión a todos los usuarios que la requieran, con un Sistema de Cableado Estructurado apto para transmitir a velocidades GigabitEthernet soportando aplicaciones tales como telefonía, PoE, video on demand o video en alta definición; así como también la instauración de un Sistema de Acceso Biométrico que proporcione seguridad a las personas y bienes que se alojan en el edificio.

3.2. Distribución departamental

La estructura organizacional de la Cámara de Comercio se divide en cuatro niveles:

a) Nivel Directivo:
    - Junta de socios
    - Directorio
    - Presidente
    - Vicepresidente
b) Nivel Ejecutivo:
    - Dirección ejecutiva
    - Dirección administrativa
    - Dirección financiera
    - Dirección de negocios y capacitación
c) Nivel Asesor:
    - Asesoría jurídica
d) Nivel Operativo:
    - Secretaria
    - Contabilidad

La figura 28 muestra el esquema jerárquico que se maneja en la Cámara de Comercio del cantón Otavalo.

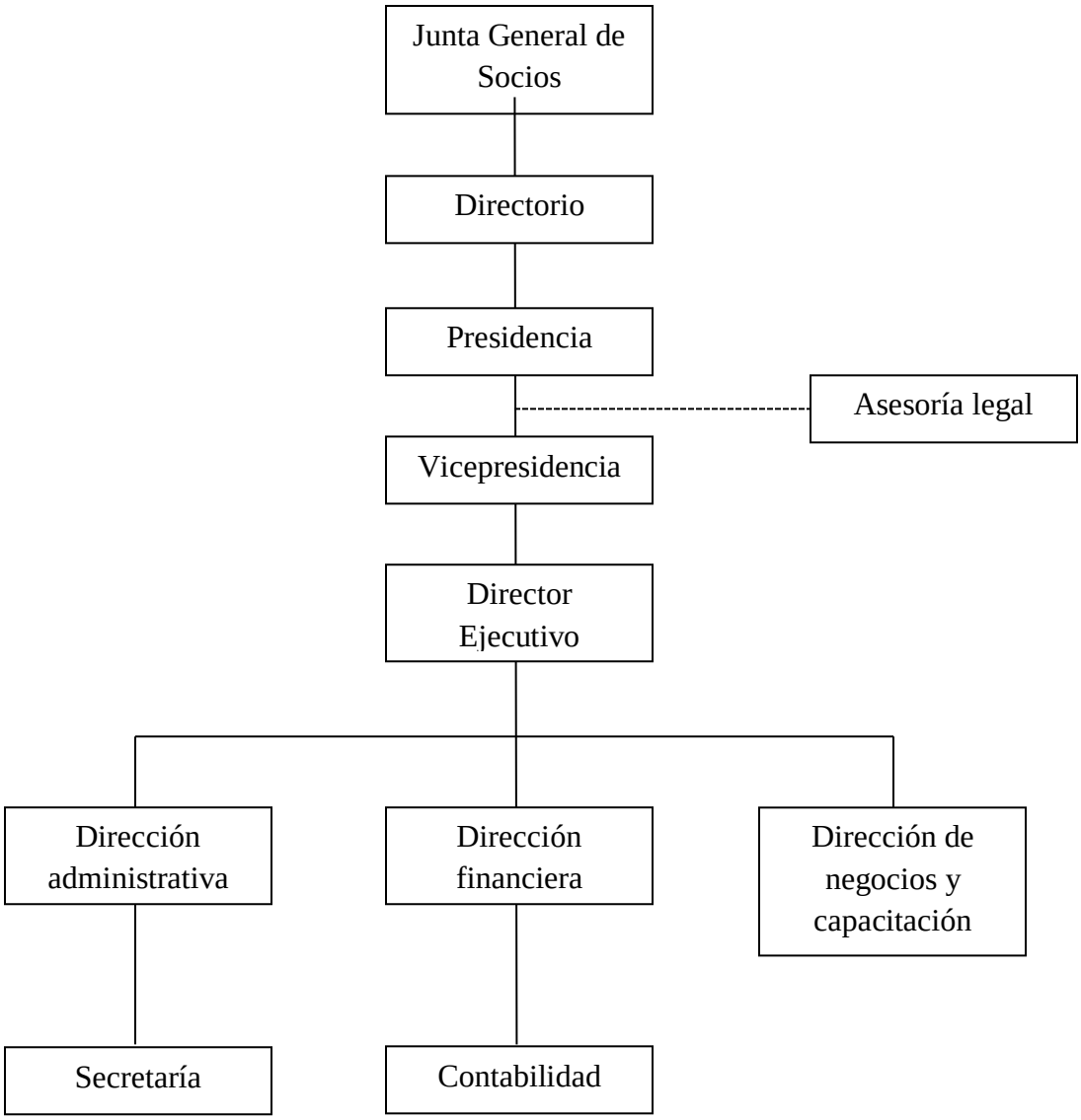


Figura 28. Diagrama jerárquico de la Cámara de Comercio de Otavalo. Manual de funciones por procesos para la Cámara de Comercio del Cantón Otavalo, 2014.
Fuente: Ing. Paola Andrade Sánchez.

3.3.Obra Civil

La Cámara de Comercio de la Ciudad de Otavalo cuenta con una infraestructura civil organizada de la siguiente forma:

- **Planta baja:** tiene una extensión de 260 metros cuadrados, las paredes son de hormigón, no tiene cielorraso ni piso flotante, por lo que no será posible el tendido de cables subterráneos.

  En esta planta funciona una pequeña sala de capacitación, tres cocinas con su respectivo comedor y departamentos en general. No cuenta con puntos de voz ni datos, solamente los tomacorrientes del sistema eléctrico. Véase figura 29.

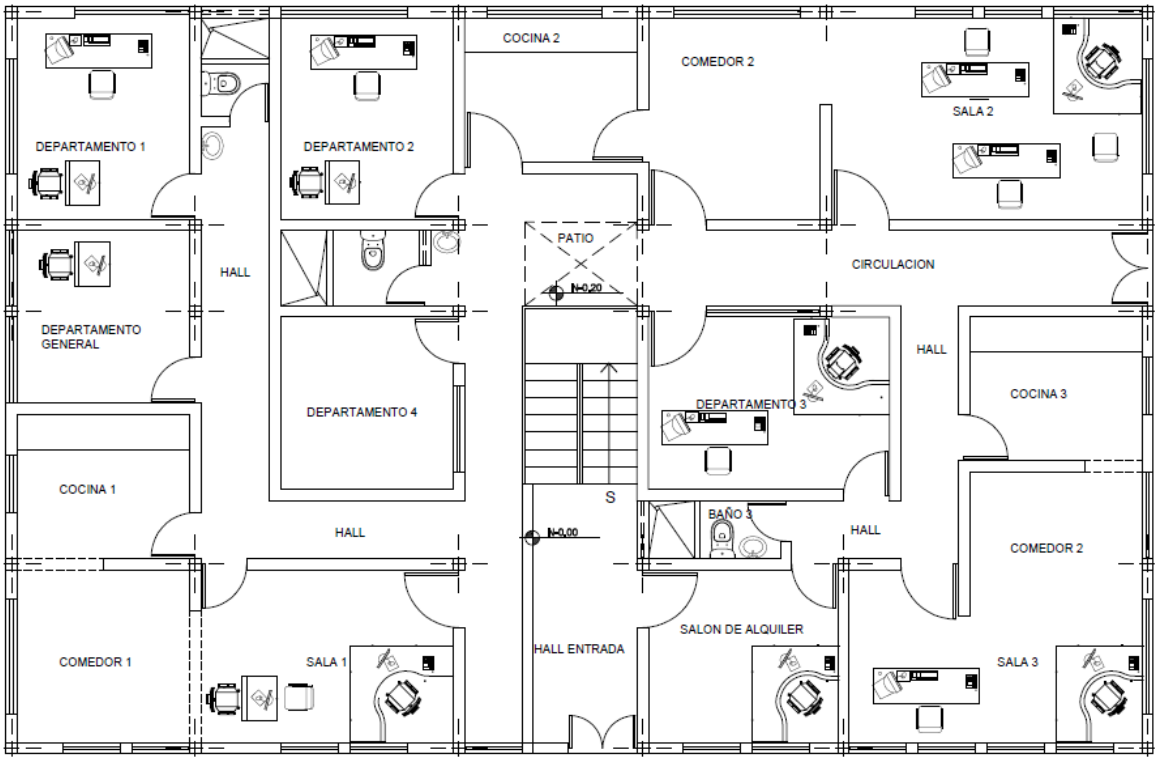


Figura 29. Plano Planta Baja de la Cámara de Comercio de Otavalo.
Fuente: El autor. Basado en planos originales. Archivo Cámara de Comercio 1988.

- **Primer piso:** constituye el espacio donde se localizan las oficinas de los socios, es de 260 metros cuadrados, las paredes son de hormigón y cuenta con divisiones entre oficinas, sin cielorraso ni piso flotante. Véase figura 30.

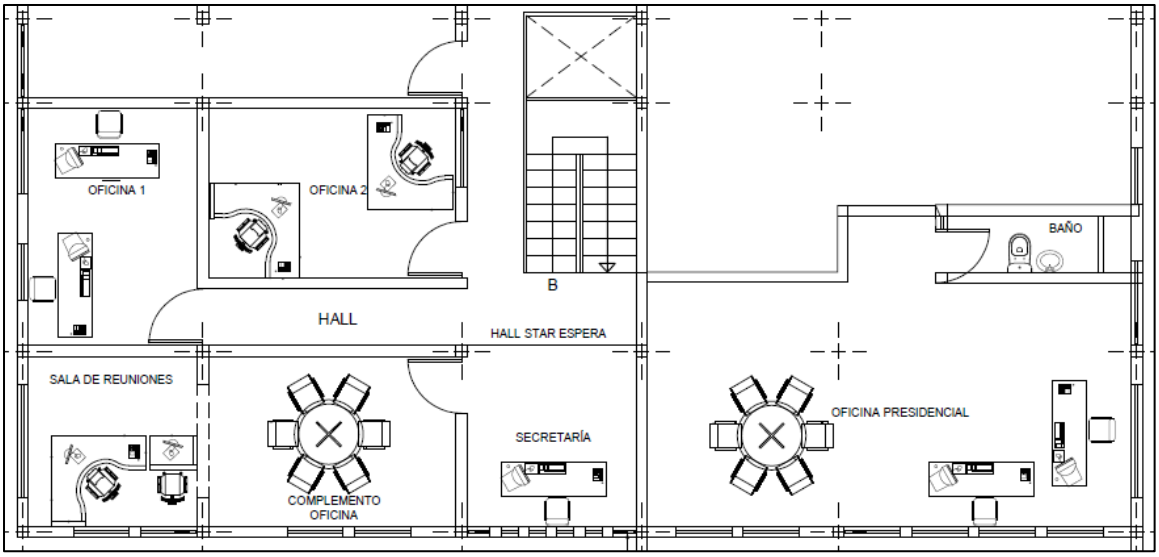


Figura 30. Plano Primer Piso de la Cámara de Comercio de Otavalo.
Fuente: el autor. Basado en planos originales. Archivo Cámara de Comercio 1988.

- **Segundo Piso:** en esta planta se localiza el salón máximo que es donde se alberga la mayor cantidad de usuarios en caso de conferencias o capacitaciones y también cuenta con su cocina y balcón. Su extensión es de 200 metros cuadrados sin cielorraso ni piso flotante. Véase figura 31.

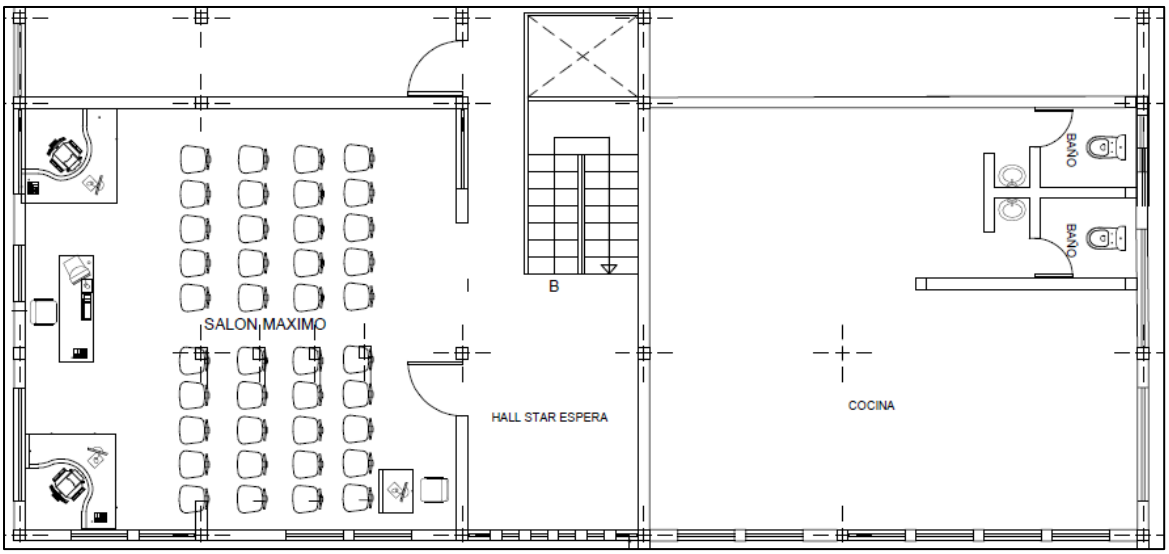


Figura 31. Plano Segundo Piso de la Cámara de Comercio de Otavalo.
Fuente: el autor. Basado en planos originales. Archivo Cámara de Comercio 1988.

Los puestos de trabajo de la Cámara de Comercio se distribuyen de acuerdo a la tabla 7:

Tabla 7
Total de puestos de trabajo de la Cámara de Comercio

Piso	Dependencia	Puestos de trabajo
Planta Baja	Departamento 1	2
Planta Baja	Departamento 2	2
Planta Baja	Departamento 3	2
Planta Baja	Departamento 4	-
Planta Baja	Departamento General	1
Planta Baja	Salón de Alquiler	1
Planta Baja	Sala 1	2
Planta Baja	Sala 2	3
Planta Baja	Sala 3	2
Primer Piso	Oficina presidencial	3
Primer Piso	Secretaría	1
Primer Piso	Complemento Oficina	2
Primer Piso	Sala de reuniones	2
Primer Piso	Oficina 1	2
Primer Piso	Oficina 2	2
Segundo Piso	Salón Máximo	4
	TOTAL	31

Fuente: el autor.

Al momento la Cámara de Comercio cuenta con computadoras independientes en las oficinas de usuario y las portátiles que cada usuario suele llevar.

Se piensa adquirir equipos de redes como routers, switch, NIC, tarjetas inalámbricas, entre otros, para lo cual se necesita una infraestructura cableada tomando en cuenta la proyección a futuro, que permita hacer uso óptimo de estos equipos.

3.4. Estado actual de la red y del sistema de cableado estructurado

El inmueble involucrado no tiene un sistema de cableado estructurado acorde a las normativas internacionales descritas en el capítulo anterior. El edificio cuenta con par trenzado UTP que se interconecta directamente al router, no siguiendo una ruta específica. Esta situación da lugar a la desconexión constante de los equipos, dañando el par trenzado y provocando pérdida de información. Obsérvese las imágenes en el ANEXO A.

La Cámara de Comercio necesita una red capaz de dar soporte a todos los usuarios de los diferentes puestos de trabajo; al momento el único router disponible es el proporcionado por el proveedor de servicios de internet que, solamente da cabida a cuatro equipos conectados directamente, y de manera inalámbrica se conectan ocho dispositivos, quedando sin acceso a la red los 28 hosts restantes.

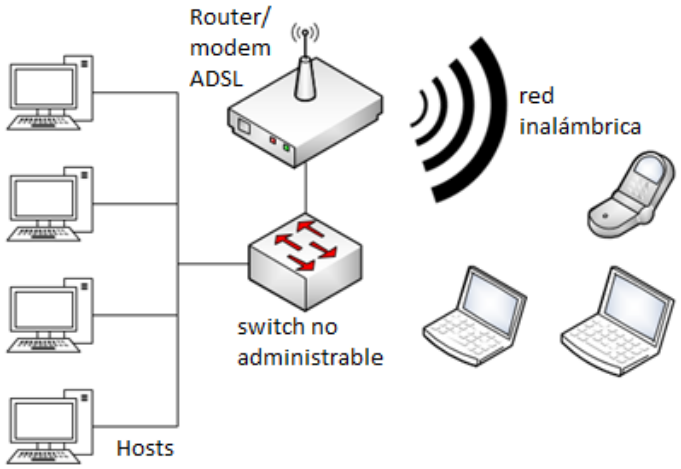


Figura 32. Esquema de la red actual.
Fuente: el autor.

El modem router proporcionando por CNT es un Wi-Fi Huawei Echolife HG520c, este dispositivo se encuentra diseñado para usuarios residenciales. Cuenta con interfaces ADSL y ADSL2+ de alta velocidad para lograr el acceso WAN externo. Además provee cuatro interfaces Ethernet y la antena para la WLAN con el protocolo 802.11g a 54 Mbit/s para ser utilizado como Access Point, soporta DHCP, filtrado MAC y traducción de direcciones NAT. (HUAWEI, 2013)

Figura 33. Router Huawei EchoLife HG520c. HUAWEI, 2013.
Recuperado de http://www.manualslib.com

3.5. Descripción de software

En la tabla 8 de este apartado se detallará el sistema operativo anfitrión que poseen los dispositivos que conforman la entidad en mención.

Tabla 8

Descripción de software

Sistema operativo	Licencia	Versión
Microsoft Windows XP	NO	Professional
Microsoft Windows 7	NO	Home Basic
Microsoft Windows 7	NO	Ultimate
Microsoft Windows 7	NO	Premium
Microsoft Windows 8	NO	
Microsoft Windows 10	NO	
Linux	GNU	CentOS 6.5

Fuente: El autor.

3.6. Descripción de hardware

En la tabla 9 se describirán las características que tienen los dispositivos del lugar.

Tabla 9

Descripción de hardware

Dependencia	Dispositivo	Marca	Características	Cantidad
Sala 1	PC portátil	Samsung	Dual Core con 2Gb de RAM	2
Sala 2	PC portátil	ACER	Dual Core con 4Gb de RAM	1
	PC portátil	Toshiba	Intel Core i5 con 4Gb de RAM	1

Oficina Presidente	Central telefónica híbrida TEA-308	Panasonic	Capacidad de 3 líneas externas y 8 extensiones híbridas. Compatible con teléfonos analógicos, faxes y terminales de datos.	1
	Teléfono Analógico KXT-SC11	Panasonic	Teléfono de mesa Identificación de llamada Memorias alfanuméricas Tecla de navegación	1
	PC escritorio	Samsung	CPU Intel Core Duo con monitor Samsung con 4Gb de RAM	2
	Impresora E-210	Lexmark	Compatible con Windows y Linux	1
Secretaría	PC escritorio	LG	CPU Intel Core Duo	1
	Teléfono Analógico KXT-SC11	Panasonic	Teléfono de mesa Identificación de llamada Memorias alfanuméricas Tecla de navegación	1
	Impresora MG3510	CANON	Multifunción compatible con Windows y MAC	1
Sala de	PC portátil	HP	Intel Core i3 con 4Gb de	1

reuniones			RAM	
	PC portátil	Sony Vaio	Intel Core i5 con 6Gb de RAM	1
Oficina 1	PC escritorio	LG	Intel Core i3 con 4Gb de RAM	1
	PC portátil	HP	Intel Core i5 con 4Gb de RAM	1
Oficina 2	PC portátil	HP	AMD Dual-Core de 4Gb de RAM	1
	PC portátil	HP	Intel Core i5 con 4Gb de RAM	1
Salón Máximo	PC escritorio	LG	CPU Intel Core i3 con 4Gb de RAM	1

Fuente: El autor.

3.7. Seguridad física del lugar

En la Cámara de Comercio no existe un mecanismo avanzado de seguridad física como protección del lugar, ya que se consideraba que cerrar las puertas con llave era un método válido de resguardar la información; no obstante, eventualmente existe personal de seguridad que vigila la entrada principal del lugar.

Sin embargo, al incrementarse el hardware y por ende la información, se hace evidente la necesidad de una mayor protección que garantice la seguridad de la organización.

CAPÍTULO IV

DISEÑO DE LA RED DE DATOS Y SISTEMA DE CONTROL DE ACCESO PARA EL EDIFICIO DE LA CÁMARA DE COMERCIO DE OTAVALO

En este capítulo se realizará el diseño de la red de datos y control de acceso considerando los parámetros enunciados por las normas ANSI/EIA/TIA 568B y 569. Este diseño abarca todos los subsistemas presentes para cableado estructurado así como también la ubicación de los equipos pasivos y activos que conformarán la red; indicando la topología física y lógica de cómo serán conectados.

De igual manera se enunciarán las políticas de acceso que se utilizarán, tomando en cuenta las restricciones para el acceso lógico así como también para el acceso físico por parte de los usuarios.

4.1. Requerimientos de usuario

Una red de datos es un activo muy importante dentro de cualquier organización, ya que, para el caso, algunas operaciones que se efectúan en este establecimiento dependen de esta. Sin embargo, al carecer de una red de datos se presentan varios inconvenientes como lo han manifestado sus afiliados y demás personas. Lo que se pretende lograr con el presente proyecto es el acceso a la red por parte de todos sus usuarios, mejorando así su desempeño, por lo que en la tabla 10 se enlistan los requerimientos, obtenidos mediante el análisis realizado en base a las encuestas ejecutadas como método de investigación. Véase ANEXO B.1.

La evaluación de resultados de las encuestas realizadas, arrojó las siguientes observaciones:

- El 70% de los usuarios afirma que no existe un método eficiente para compartir información dentro de la empresa, el 20% afirma en cambio, que hay una carencia total de este servicio, mientras que el únicamente el 10% considera que el servicio es aceptable.

- El 90% de los usuarios manifestaron que les gustaría compartir información mientras se movilizan dentro del edificio, además de hacerlo en su PC de escritorio.

- El 93% de los usuarios cree que la infraestructura física actual del edificio sí abastece a todos sus usuarios, el resto considera que el lugar es ideal para trabajar y hasta "sobra espacio."
- El 60% de los usuarios cree que su antivirus es totalmente negligente, el 26,7% piensa que su antivirus es medianamente aceptable; un 3,3% manifiesta que su software antivirus puede actualizarse para lograr resultados satisfactorios y un 1% no tiene antivirus.
- El 80% de los usuarios de la Cámara de Comercio considera que en el edificio no existe un método de control de acceso que regule la entrada mientras que el 16,7% manifiesta que la guardianía de seguridad que en ciertas ocasiones se contrata no es suficiente y el 3,3 considera que con este último método es suficiente para resguardar la seguridad del lugar.

Mediante esta recolección de datos también se detalla la importancia de un dispositivo que controle el acceso a ciertos sitios para hacer un uso eficiente del ancho de banda; sin embargo la explicación y configuración detallada se muestra en el apartado de Políticas de Seguridad que se encuentra más adelante.

Tabla 10

Requerimientos de usuarios de la Cámara de Comercio

Observación	Requerimiento	Característica	Consideraciones
Servicio de compartición de datos ineficiente.	RED DE DATOS ESCALABLE	La red debe ser capaz de dar soporte a todos sus usuarios actuales y futuros	• Puntos de red para los puestos de trabajo actuales y su proyección a futuro. • Puntos de red dobles para voz y datos respectivamente.
Conexión mientras hay movilidad	CONEXIÓN MÓVIL	Puntos de red localizados en lugares estratégicos	• Puntos de red para access points.
Software antivirus ineficiente	PREVENCIÓN DE MALWARE	Implementación de programas capaces de evitar la descarga de software malicioso en los hosts de la red	• Antivirus
Optimizar el acceso a la red.	CONTROL DE CONTENIDOS WEB	Se debe filtrar el acceso a páginas inadecuadas.	• Firewall Proxy
Carencia de			• Controles de Acceso

un método de seguridad de acceso.	SEGURIDAD FÍSICA	Los equipos de red deben estar bajo protección física para evitar el acceso o incluso robo, por parte de intrusos.	Biométricos

Fuente: El autor.

4.1.1. Análisis de la cantidad de puntos de red necesarios.

Actualmente se necesitarían 31 puntos de red para cada puesto de trabajo, no obstante, considerando el incremento de personal y socios, de los últimos años como se evidencia en la tabla 11, se deduce que, hubo un crecimiento del 1,37% aplicando la fórmula de la ecuación (1) , en base a los archivos proporcionados por la Cámara de Comercio que dado que son confidenciales no se los puede publicar.

Tabla 11

Cantidad de usuarios por año

Año	Número de usuarios
2012	29
2013	29
2014	30
2015	31
2016-2017	31

Obtenido de: archivos Cámara de Comercio Otavalo.

Aplicando la fórmula:

$$tasa\ de\ crecimiento = \frac{presente - pasado}{pasado} x\ 100\% \quad (1)$$

$$tasa\ de\ crecimiento\_5años = \frac{31 - 29}{29} x\ 100\%$$

$$tasa\ de\ crecimiento\_5años = 6{,}89\%$$

Se obtiene que, hubo un crecimiento del 6,89% de usuarios durante un periodo de 5 años, por lo que se debe dividir la respuesta obtenida para 5 con el fin de calcular un valor anual, quedando como resultado una tasa de crecimiento de 1,37% al año.

4.2. Requerimientos para el Sistema de Cableado Estructurado

4.2.1. Elección del medio de transmisión

- En primer lugar se descartan categorías inferiores, como UTP CAT-5 puesto que la velocidad de operación 10/100 de estos desaprovecharía las capacidades que tienen los equipos actuales de redes que generalmente son gigabit.
- Inicialmente la red no contará con ningún servidor o DMZ, sin embargo, no se descarta la posibilidad de que en un futuro se levanten servicios como: http, voz ip, ftp u otros. Es así que en la tabla 12 y tabla 13 se realiza una estimación de la capacidad que requieren las aplicaciones de mayor uso actualmente y en el futuro; con el fin de conocer el ancho de banda máximo que se podría alcanzar próximamente en caso de implementarse estos servicios.

Tabla 12

Requerimientos de ancho de banda pico actual

Requerimientos de ancho de banda actual	**Capacidad requerida (Mbps)**
Navegación	0,20
Actualizaciones en línea de sistemas	0,20

operativos	
Actualizaciones en línea de sistemas de seguridad	0,20
Acceso a servidores externos de correo	1,00
Transferencia de archivos entre usuarios	25,00
Descargas de videos	5,00
Otros	2,00
TOTAL	33,60

Microsoft support & (Gonzáles, 2014)

Se tiene un total de 33,60 Mbps de ancho de banda pico por usuario, en el estado de red sin servicios y con uso promedio normal de aplicaciones de internet. A continuación la tabla de requerimientos futuros:

Tabla 13

Requerimientos de ancho de banda pico futuro

Requerimientos de ancho de banda futuro	**Capacidad requerida (Mbps)**
Navegación	0,20
Actualizaciones en línea de sistemas operativos	0,20
Actualizaciones en línea de sistemas de seguridad	0,20
Acceso a servidores externos de correo	1,00
Transferencia de archivos entre usuarios	25,00
Descargas de videos	5,00
Servidor de correo electrónico	1,00
Servidor de voz ip	0,06
Servidor HTTP	0,05

Aplicaciones futuras de administración	20,00
Otros	15,00
TOTAL	67,71

Microsoft support & (Gonzáles, 2014)

Del análisis se obtiene que con una proyección a futuro se requerirá un ancho de banda de 67,71 Mbps, pero con el fin de evitar encolamientos o colisiones se necesitarán equipos y el medio de transmisión del doble de la capacidad calculada, es decir 135,42Mbps. De esta manera, el cable a escoger deberá soportar este valor así como también la velocidad del puerto de los equipos.

De acuerdo a las cifras numéricas de ancho de banda que presentan los pares trenzados 5, 5e, 6 y 6A, que serían los posibles a utilizarse; se recomienda utilizar cable utp categoría 6A, por lo menos en el enlace de backbone, puesto que, los enlaces de cada host convergen en uno solo hacia el firewall y hacia el router; si son en total 75 puntos de red, de los cuales se descartan los puntos de voz (estos solo tendrían acceso a puertos de voz SIP e IAX) y su tráfico ya está tomado en cuenta en las tablas 12 y 13 quedan en total 40 usuarios, siendo que cada uno genera 135,42 Mbps se obtiene entonces 5416,8 Mbps o 5Gbps de tráfico en dichos enlaces, en donde el cableado UTP CAT 5e no abastecería el enlace puesto que en condiciones óptimas llegaría a 1Gbps. Por tal motivo se recomienda utilizar el cable CAT-6ª que puede alcanzar hasta 10Gbps.

Sin embargo, para los requerimientos actuales, el cable UTP categoría 5e resulta suficiente ya que certifica 100Mbps, pudiendo alcanzar una tasa de transferencia superior, con los conectores adecuados llegando hasta el GigabithEthernet como máximo.

Si la red diseñada no debiera expandirse la implementación con una categoría superior sería subutilizar el cable dado que, el tráfico en megabits por segundo (Mbps) calculado, resultaría ínfimo en comparación al gigabit que ofrece un cable categoría 6, desperdiciando casi 900 Mbps.

4.2.2. Áreas de trabajo

En las áreas de trabajo se deberá tomar en cuenta:

- Mínimo dos tomas de telecomunicaciones para voz y datos, por cada área.
- El espacio considerado por área de trabajo es de 10 metros cuadrados.
- Las rutas de acceso del cableado puedan pasar por techos, columnas, paredes o pisos.
- Los patch cords que conecten el cableado horizontal con los equipos de telecomunicaciones deben tener la misma categoría que este.
- Los conectores del par trenzado debe respetar la norma T568A o T568B.

4.2.3. Cableado Horizontal

El cableado horizontal incluye:

- Las salidas de telecomunicaciones en las áreas de trabajo, que para el caso son conectores hembra del tipo RJ-45
- Patch panels y patch cords para las conexiones del cableado horizontal.
- Cables y demás conectores entre las salidas de telecomunicaciones y el cuarto de telecomunicaciones.

4.3. Topología de la red

La red tendrá una topología física y lógica tipo estrella. Es decir, que desde las salidas de telecomunicaciones de cada estación de trabajo saldrá un cable hasta el nodo central en el rack de la oficina presidencial.

4.3.1. Topología física

El router de la red actual actúa como punto de acceso inalámbrico lo que provoca una ralentización de la parte cableada además de que no existen restricciones para el acceso a páginas web inapropiadas, es así que se plantea como solución la implementación de un dispositivo intermedio entre los equipos de los usuarios y el router, con el fin de controlar el acceso a sitios web a través de la creación de usuarios con ciertos privilegios o no, dando lugar a una red más segura.

La figura 34 muestra la topología física propuesta para la red, que se encuentra distribuida en tres plantas como se puede observar.

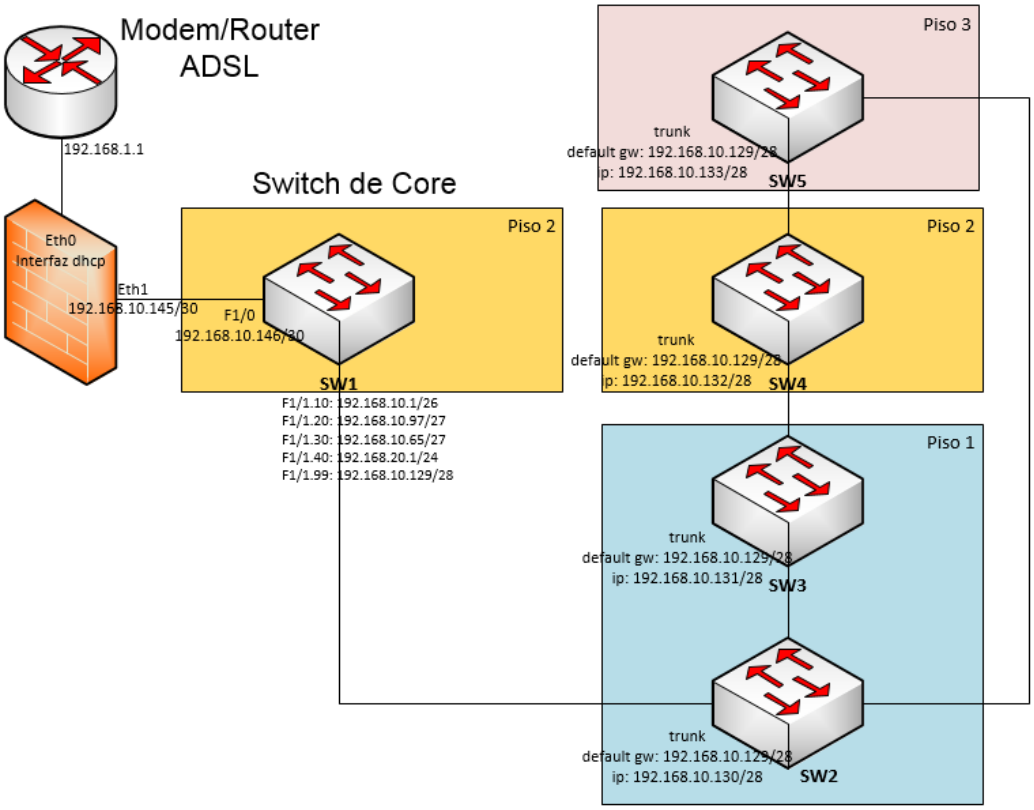


Figura 34. Topología física de red propuesta para la Cámara de Comercio. Microsoft Office Visio 2013. Fuente: El autor.

Lo que se pretende con esta arquitectura es proporcionar acceso a la red en todo el edificio a través de la interconexión de todos los switches hacia un nodo central y este a su vez deberá atravesar el firewall que será representado por un PC servidor con el fin de reducir costes.

4.3.2. Topología lógica

La conexión lógica de los equipos se realizará a través de redes lan virtuales creadas en cada uno de los switches de acceso, con el fin de reducir el dominio de broadcast y optimizar la administración de la red. La figura 35 muestra el esquema planteado:

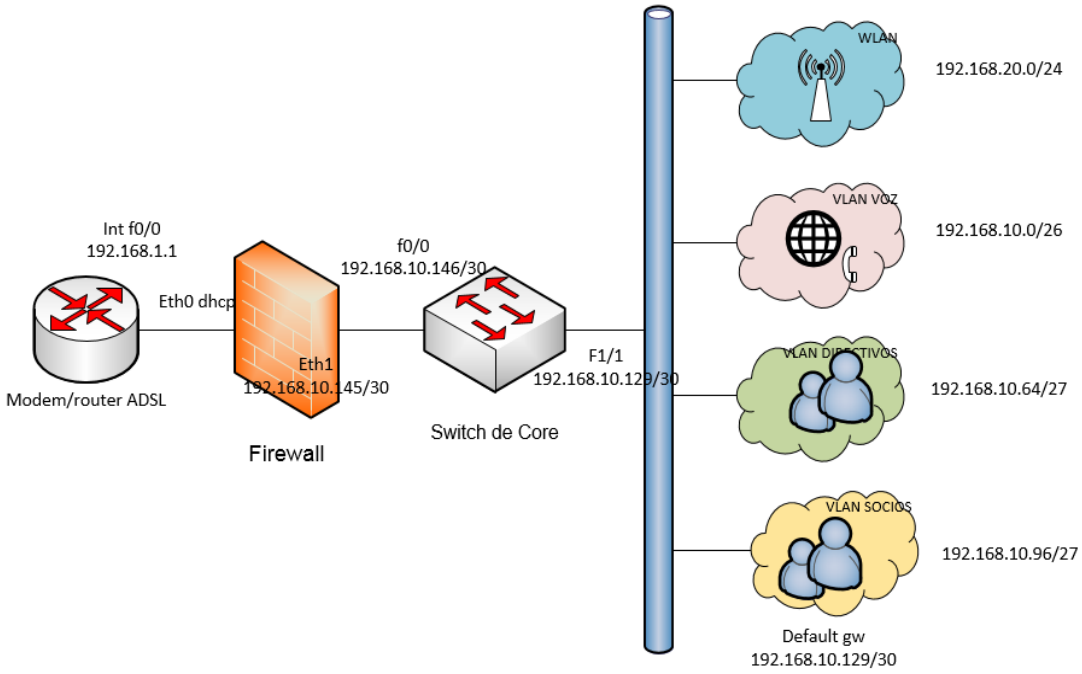


Figura 35. Topología lógica de red propuesta para la Cámara de Comercio. Microsoft Office Visio 2013. Fuente: el autor.

Se propone la creación de cuatro vlans:

- Vlans para datos: vlan directivos y vlan socios.
- Vlan para voz: una misma vlan en todo el edificio.
- Vlan para usuarios inalámbricos (WLAN)

De esta manera se logra segmentar la red LAN sin alterar el cableado físico, agrupando los usuarios según su condición y añadiendo seguridad en la red debido a que los datos ahora son encapsulados en un nivel más.

En la tabla 14 se muestra la propuesta de asignación de los hosts para cada vlan, dependiendo de su localización en la infraestructura del edificio.

Tabla 14

Propuesta de asignación de redes lan virtuales en las dependencias de la Cámara de Comercio.

Vlan	Dependencia	ID Vlan
Directivos	Oficina presidencial Secretaría Complemento Oficina Sala de reuniones Oficina 1 Oficina 2 Sala 1 Sala 2 Sala 3	30
Socios	Departamento general Departamento 1 Departamento 2 Departamento 3 Departamento 4 Salón de alquiler	20

	Salón máximo	
Voz	Todas las dependencias del edificio	10
WLAN	Hall	40

Fuente: El autor.

Las vlans estarán configuradas de manera estática ya que los cambios en la infraestructura son mínimos por lo que no será necesaria la configuración dinámica por MAC u otro parámetro. Los enlaces de los switches serán configurados en modo troncal para que sean capaces de transferir las tramas sin importar la vlan a la que los puertos pertenezcan.

4.3.3. Direccionamiento IP

Si se toma en cuenta que un sistema de cableado estructurado debe ser escalable al menos hasta 10 años se calcula que al término de este deberá tener capacidad para alojar a 36 usuarios según la tasa de crecimiento del 1,37% calculada anteriormente, además de que cada uno tendrá su salida de telecomunicaciones para voz y datos, siendo en total 80 puntos de red solamente para áreas de trabajo.

Es por esto que, se ha tomado la dirección 192.168.10.0 con una máscara de 255.255.255.0 perteneciente a una dirección IP privada de clase C, a la cual se procederá a dividir en subredes mediante el proceso de VLSM para dar cobertura a las vlans de voz y datos, según el número de hosts requeridos que se evidencian en la tabla 12, dado que un /24 permitirá asignar subredes en rangos válidos para los enlaces troncales y dejar espacio disponible para la creación de subredes en caso de ampliar la red con servidores; mientras que, la vlan para usuarios inalámbricos se creará con la dirección de red 192.168.20.0/24 de tal modo que resulte más fácil identificar cuando los usuarios se encuentren con conexión al a wlan, además de que se tendrá una dirección full class con capacidad para 254 hosts.

La tabla 15 detalla cuantitativamente los hosts que se requieren para cada vlan de acuerdo al piso en que se ubican las áreas de trabajo.

Tabla 15

Hosts requeridos en cada vlan

	Vlans de datos			
Piso	Vlan directivos	Vlan socios	Vlan de voz	WLAN
Planta baja	-	15	15	3
Primer piso	16	-	16	1
Segundo piso	-	4	4	1
TOTAL HOSTS REQUERIDOS	16	19	35	5

Fuente: El autor.

No se ha establecido el número de hosts específicos para la red inalámbrica dado que depende de la cantidad de dispositivos wireless que requieran acceder a esta. Cabe recalcar que el presente trabajo de grado no abarca la implantación de puntos de acceso inalámbrico, sin embargo sí se contempla la colocación de los puntos de red respectivos para su conexión.

A continuación se aplica el procedimiento de VLSM (véase tabla 16) que consiste en asignar máscaras variables a cada subred con el fin de optimizar el direccionamiento, evitando el desperdicio de direcciones, por lo que, en primer lugar se llenará la tabla de requerimientos y luego se procederá a asignar las direcciones IP.

Tabla 16

Tabla de requerimientos

Subred	#hosts	Bits Hosts	Bits prestados	Rango	/n	Total Direcciones 2^n-2
Vlan voz	36	6	2	64 (4°)	/26	62
Vlan socios	20	5	3	32 (4°)	/27	30
Vlan directivos	17	5	3	32 (4°)	/27	30
				TOTAL = 122 direcciones asignables		

Fuente: el autor.

En base a la tabla anterior se deduce que, para la vlan voz se utilizarán 36 direcciones IP de un total de 62, para la vlan de datos socios se utilizarán 20 direcciones ip de un total de 30 y para la vlan de datos directivos se utilizarán 17 direcciones ip de un total de 30. De esta manera se optimiza el recurso 192.168.10.0/24 ya que cada subred tiene su propia máscara.

En la tabla 17 se describe las direcciones ip que se asignarán para cada vlan, de acuerdo al rango calculado con el procedimiento VLSM.

Tabla 17

Tabla de direccionamiento

Subred	Dirección de subred	Primera dirección utilizable	Última dirección utilizable	Dirección de broadcast	Máscara de subred
Vlan voz	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63	255.255.255.192
Vlan socios	192.168.10.64	192.168.10.65	192.168.10.94	192.168.10.95	255.255.255.224
Vlan directivos	192.168.10.96	192.168.10.97	192.168.10.126	192.168.10.127	255.255.255.224
Vlan WLAN	192.168.20.0	192.168.20.1	192.168.20.254	192.168.20.255	255.255.255.0

Fuente: el autor.

4.4. Simulación de la red en GNS_3

GNS3 es un software de distribución libre que permite emular el comportamiento de los dispositivos de red específicamente Cisco, en diferentes topologías, ya que, es capaz de ejecutar los sistemas operativos reales de estos, lo que resulta de gran ayuda al momento de probar y diseñar una red antes de implementarla; los equipos y marcas a utilizarse en este proyecto serán analizados en un apartado posterior pero para efectos simulación resulta conveniente el uso de GNS_3.

De esta manera se procede a simular el diagrama de topología (véase figura 36) según el diseño realizado anteriormente:

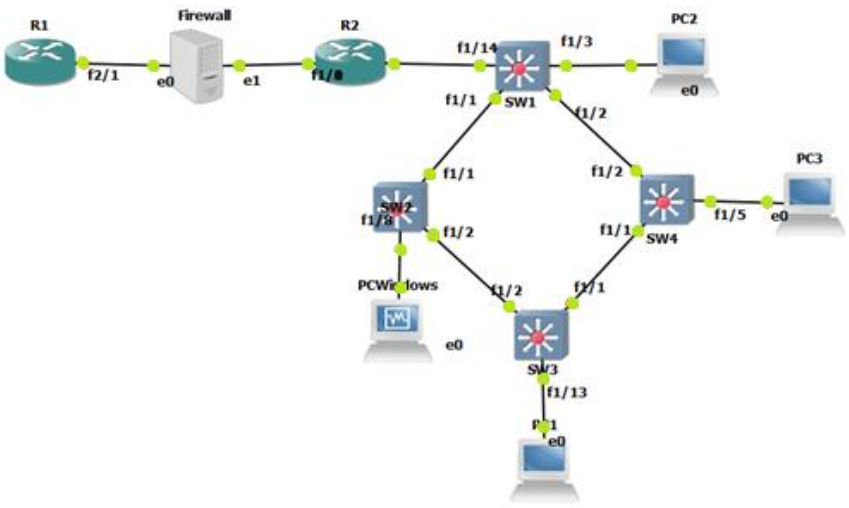


Figura 36. Topología simulada. Software Emulador GNS_3.
Fuente: el autor.

- La red está formada por 1 switch de core al cual están conectados 4 switches de acceso.
- Existirá segmentación en la red a través de 4 vlans creadas en todos los switches.
- El firewall será un PC-servidor localizado como dispositivo intermedio entre el modem router ADSL y el switch de core.
- Los enlaces para la propagación de vlans deberán ser configurados en modo troncal.

4.4.1. Procedimiento de configuración

- Creación de vlans en cada switch: al tratarse de equipos CISCO se utilizará el protocolo de vlan trunking o VTP para la propagación de vlans, de tal manera que, estas solo se crearán en el switch de core que estará configurado en modo servidor, mientras que los demás ya recibirán esa configuración al ser clientes. La figura 37 indica los comandos utilizados para la creación de vlans en modo server.

  vlan database
  vtp domain CamComercio password cisco
  vtp server
  vlan 10 name Voz

vlan 20 name Socios
vlan 30 name Directivos
vlan 40 name WLAN
exit

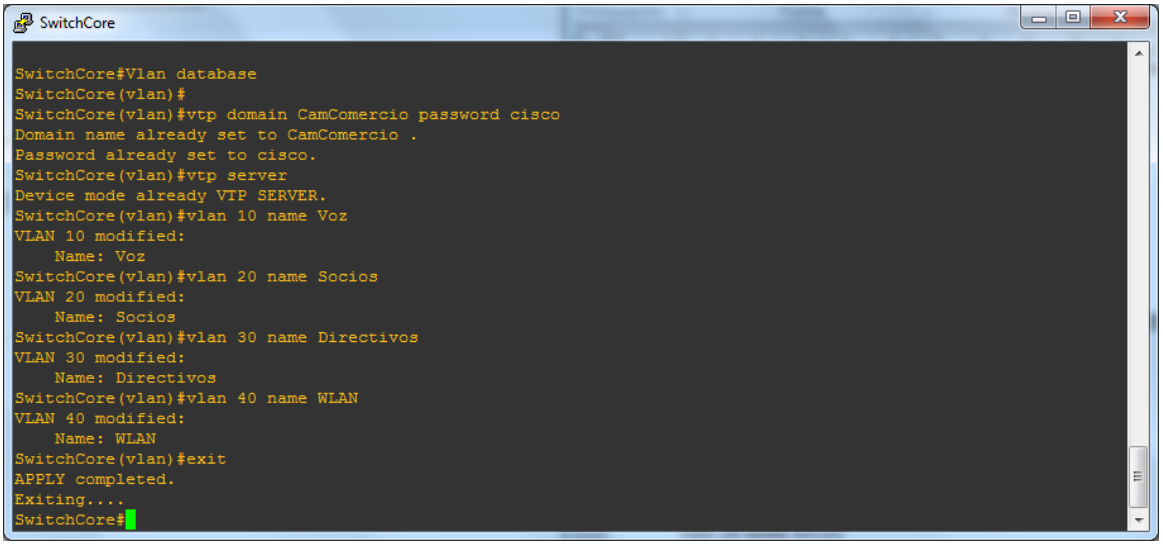


Figura 37. Creación de vlans y vtp en el switch principal. Software Emulador GNS_3. Fuente: el autor.

Ahora se configurarán los demás switches en modo cliente como se observa en la figura 38, para que reciban la configuración de vlans. No obstante, hay que recalcar que los enlaces entre los switches de acceso y el switch central deben configurarse en modo troncal.

vlan database
vtp domain CamComercio password cisco
vtp client

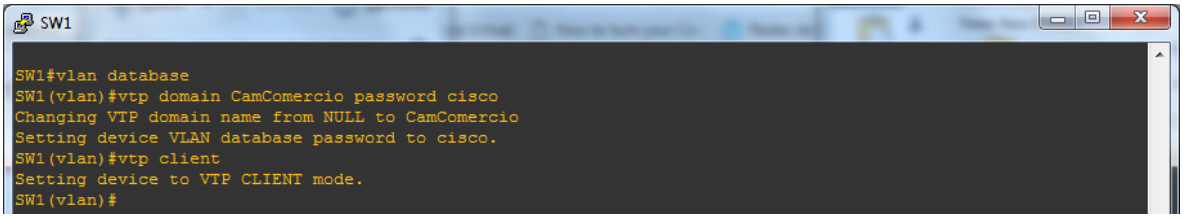


Figura 38. Configuración modo cliente de los switches de acceso. Software Emulador GNS3.
Fuente: El autor.

Es así que, mediante el comando que se muestra en la figura 39, será posible visualizar las vlans creadas en todos los switches

show vlan-switch

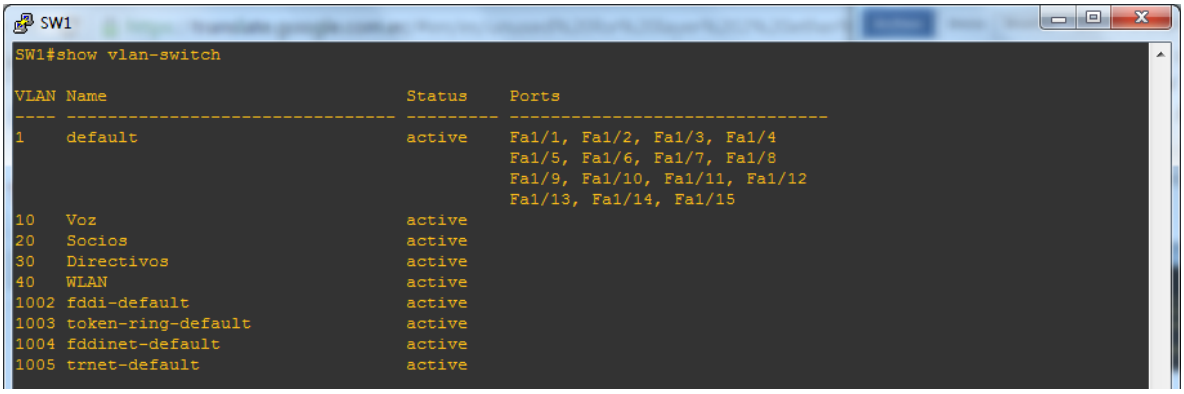


Figura 39. Vlans creadas en todos los switches. Software Emulador GNS3.
Fuente: el autor.

- Asignación de puertos en los switches: de acuerdo la localización de los puntos de red y a los usuarios que harán uso de esta, se realizará la asignación de puertos, tomando en cuenta también el piso en el que se ubicarán los switches basándose en la tabla 12 en donde se especifican los hosts requeridos en cada vlan. La tabla 18 expone los puertos asignados para cada switch.

Tabla 18

Asignación de puertos en los switches.

Piso	Switch	Vlan voz	Vlan socios	Vlan directivos	Vlan WLAN
Panta baja	SW1	fa0/2-fa0/9	fa0/10-fa0/17	-	fa0/18-fa0/19
Panta baja	SW2	fa0/2-fa0/9	fa0/10-fa0/17	-	fa0/18-fa0/19
Primer piso	Switch de	fa0/6-fa0/14	-	fa0/15-fa0/23	-

	core				
Primer piso	SW3	fa0/6-fa0/14	-	fa0/15-fa0/23	fa0/2-fa0/3
Segundo piso	SW4	fa0/2-fa0/6	fa0/7-fa0/11	-	fa0/12-fa0/13

Fuente: el autor.

Cada switch tiene un total de 24 puertos, en todos los switches se crearán las vlans, sin embargo la asignación de puertos para cada vlan será según se requiera, por ejemplo, en la planta baja no se necesita la vlan directivos, por lo que esta solo estará creada sin asignación de puertos. En la tabla 16 se enuncian los puertos a utilizarse y los puertos libres para cada switch, aclarando que cada switch utilizará su primer puerto para los enlaces troncales, a excepción del switch de core en el cual se interconectan 5 enlaces. La tabla 19 evidencia los puertos que se van a ocupar así como también los puertos que quedarán libres en cada switch.

Tabla 19

Puertos asignados y libres en cada switch

Dispositivo	Puertos asignados	Total puertos asignados	Puertos libres	Total puertos libres
SW1	fa0/1-fa0/19	19	fa0/20-fa0/24	5
SW2	fa0/1-fa0/19	19	fa0/20-fa0/24	5
Switch de core	fa0/1-fa0/23	23	fa0/24	1
SW3	fa0/1-fa0/3 y fa0/6-fa0/23	21	fa0/4-fa0/5 y fa0/24	3
SW4	fa0/1-fa0/13	13	fa0/14-fa0/24	11

Fuente: el autor.

Es así, que se procede a configurar los switches emulados en GNS3. Para efectos de simulación se realizó la misma configuración de puertos en cada switch, pero en el momento de la implementación se debe respetar los puertos designados según las tablas anteriores. La figura 40 muestra los comandos utilizados para la asignación de puertos.

interface range fa1/5 - 7
switchport mode access
switchport access vlan 10
exit
interface range fa1/8 - 10
switchport mode access
switchport access vlan 20
exit
interface range fa1/11 - 13
switchport mode access
switchport access vlan 30
exit
interface range fa1/14 - 15
switchport mode access
switchport access vlan 40
exit

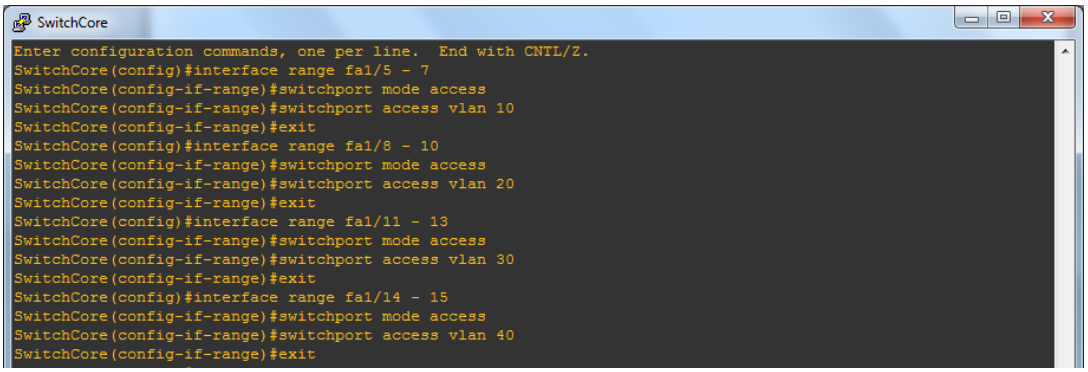


Figura 40. Asignación de puertos al switch. Software Emulador GNS3.
Fuente: El autor.

Ahora se ejecuta el comando de la figura 41, para visualizar las vlans y se verifica que los puertos ya han sido asignados.

show vlan-switch brief

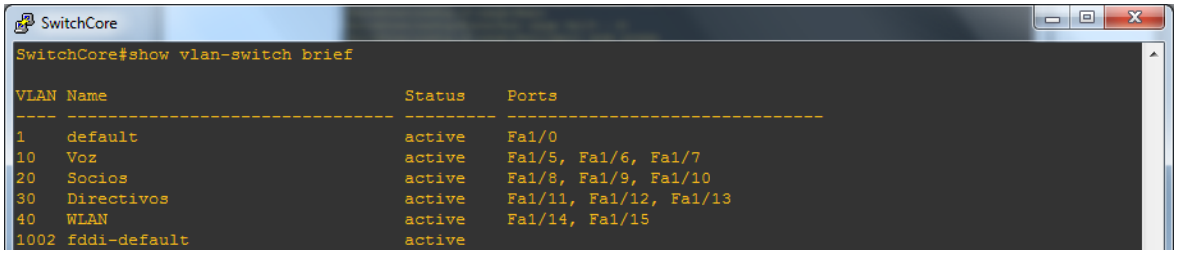


Figura 41. Verificación de puertos asignados. Software Emulador GNS3.
Fuente: El autor.

- Enrutamiento: este proceso será realizado por el switch principal que constituye el backbone de la red, siendo este un dispositivo de capa 3 con capacidad de enrutamiento intervlan.

  El primer paso será configurar la vlan administrativa en los switches de acceso, asignando una dirección IP a la vlan 99 de cada enlace troncal. La vlan tendrá la dirección 192.168.10.128/28 correspondiente a un rango de direcciones ip posterior al calculado y dentro de la ip 192.168.10.0/24 principal. Esta vlan, deberá crearse en todos los switches ya que a través de ella se realizará el enrutamiento. La figura 42 muestra este procedimiento.

Interface fa1/0
Switchport mode trunk
Switchport trunk native vlan 99
Exit
Ip default-gateway 192.168.10.129
Int vlan 99
Ip address 192.168.10.130 255.255.255.240

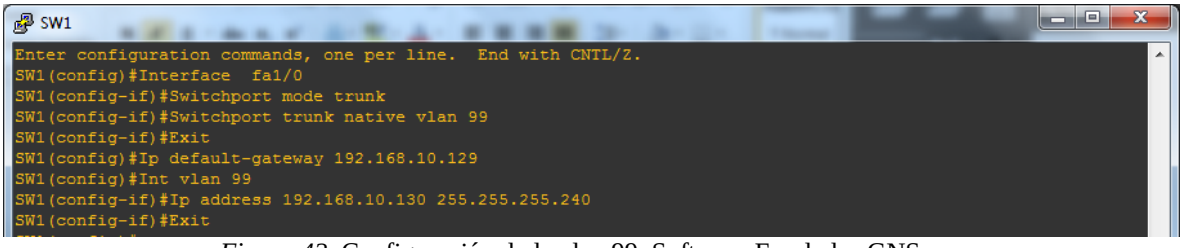


Figura 42. Configuración de la vlan 99. Software Emulador GNS3.
Fuente: El autor.

La configuración para los demás switches será la misma, modificando únicamente la dirección ip de la vlan 99 asignando su consecutiva, por ejemplo, el SW2 tendrá una dirección ip 192.168.10.131 con su máscara 255.255.255.240. A continuación se configurará el switch de core, en el cual se asignarán las direcciones ip para cada vlan y luego se configurará el enrutamiento mediante una ruta predeterminada.

```
interface  vlan 10
ip address 192.168.10.1 255.255.255.192
no shutdown
exit
interface  vlan 20
ip address 192.168.10.97 255.255.255.224
no shutdown
exit
interface  vlan 30
ip address 192.168.10.65 255.255.255.224
no shutdown
exit
interface  vlan 40
ip address 192.168.20.1 255.255.255.0
no shutdown
exit
interface  vlan 99
ip address 192.168.10.129 255.255.255.240
no shutdown
exit
```

La asignación de direcciones ip para cada vlan se muestra en la figura 43.

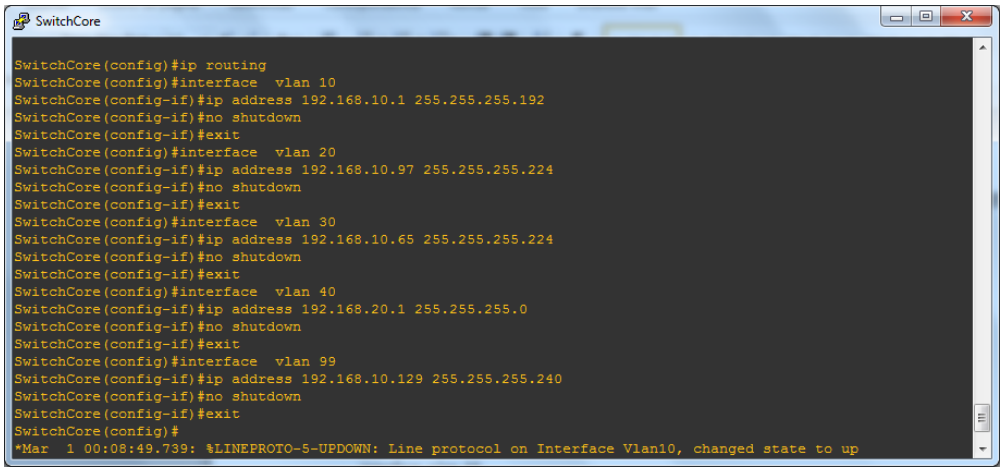


Figura 43. Asignación de direcciones IP para cada vlan. Configuración de la vlan 99. Software Emulador GNS_3.
Fuente: el autor.

Hasta el momento ya se cuenta con conectividad entre las vlans, para lograr la salida hacia el firewall es posible configurar una ruta estática predeterminada.

4.5. Diseño del Cableado Horizontal

La localización de los puntos de red está sujeta a las características de infraestructura del edificio, que cuenta con el espacio adecuado para oficinas respetando la distancia de acuerdo al área de trabajo ($10m^2$)

4.5.1. Cableado horizontal de la Planta Baja

Para el cableado estructurado de la planta baja se consideró la utilización de un rack de pared por la poca cantidad de puntos de red, a partir del cual se distribuirán los cables para las estaciones de trabajo, siguiendo una topología tipo estrella como se muestra en la imagen de la figura 44. La tabla 20 indica la distribución de puntos de red en esta zona.

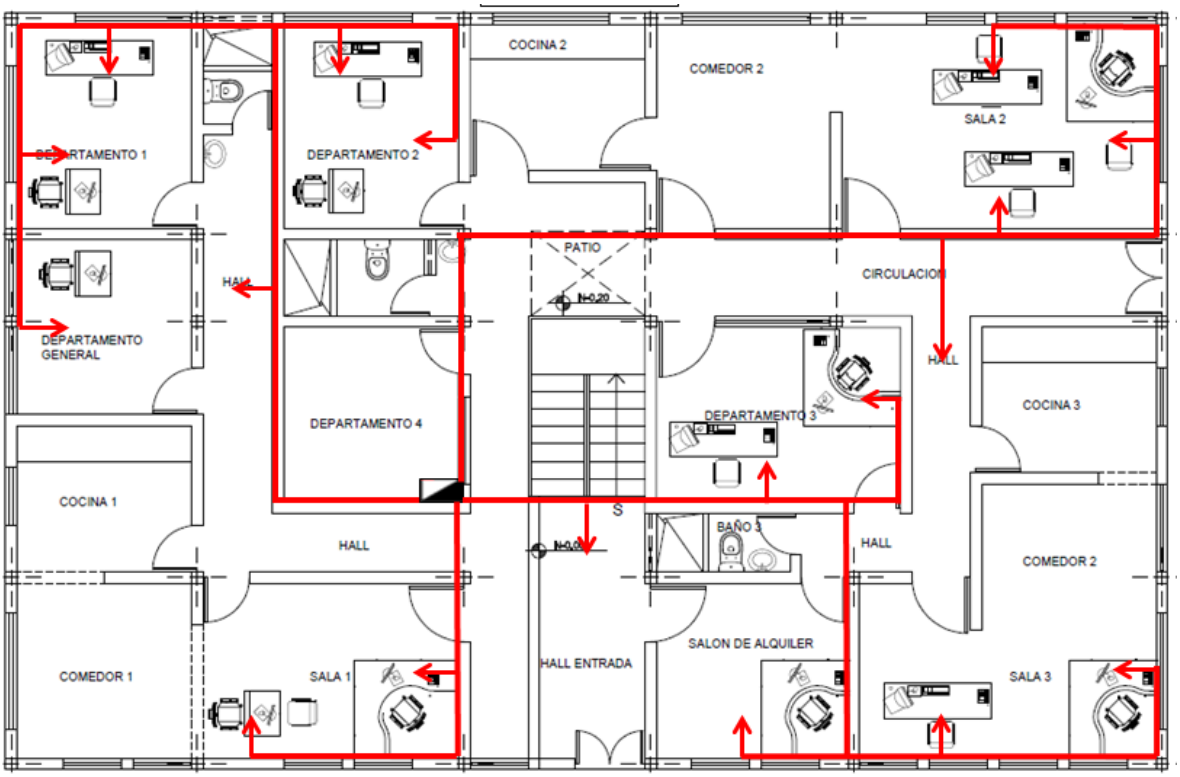


Figura 44. Esquema del cableado horizontal planta baja.
Fuente: El autor.

Tabla 20

Distribución de puntos de red de la Planta Baja

Item	Dependencia	Puntos de red para datos	Puntos de red para voz	Puntos adicionales de red para datos
1	Sala 1	2	2	-
2	Sala 2	3	3	-
3	Sala 3	2	2	-
4	Departamento general	1	1	-
5	Departamento 1	2	2	-
6	Departamento 2	2	2	-

7	Departamento 3	2	2	-
8	Departamento 4	-	-	-
9	Salón de alquiler	1	1	-
10	Hall	-	-	3
				TOTAL DE PUNTOS DE RED = 33

Fuente: el autor.

En este piso se tienen 15 puestos de trabajo principalmente para socios, por lo que se instalará una salida de telecomunicaciones doble para voz y datos por cada uno, siendo en total 15 puntos dobles para voy y datos destinados a los puestos de trabajo, y a más de esto, se considerarán tres puntos de red adicionales para la futura instalación de Access Point en los pasillos.

Cada punto de red, sea de voz o datos necesita su conector hembra RJ-45 cuyo número se detalla en la tabla 21:

Tabla 21

Jacks y face plates para la Planta Baja

Item	Dependencia	Jack RJ-45	Número de faceplates dobles	Número de faceplates simples
1	Sala 1	4	2	-
2	Sala 2	6	3	-
3	Sala 3	4	2	-
4	Departamento general	2	1	-
5	Departamento 1	4	2	-

6	Departamento 2	4	2	-
7	Departamento 3	4	2	-
8	Departamento 4	-	-	-
9	Salón de alquiler	2	1	-
10	Hall	3	-	3
	TOTAL	33	15	3

Fuente: el autor.

Observar el diagrama completo en el ANEXO C.

4.5.2. Cableado horizontal del Primer Piso

En el cableado horizontal del primer piso se siguió la misma topología tipo estrella, considerando que el rack principal se ubicará dentro de la oficina presidencial, al cual se conectará el cableado de backbone como se indica en la figura 45. La distribución y número de puntos de red se detallan en la tabla 22.

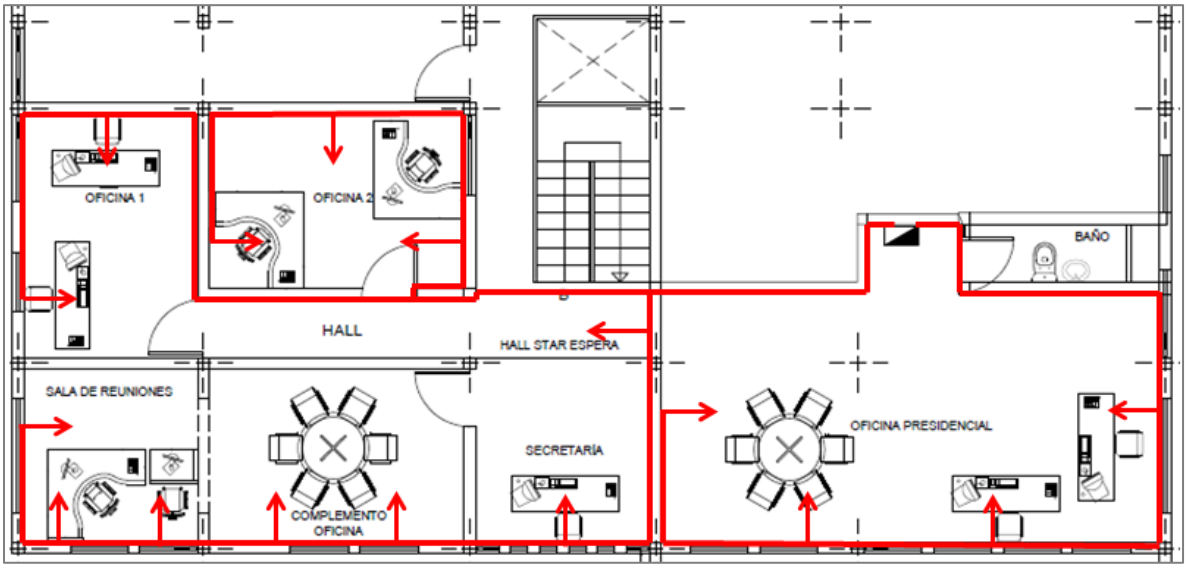


Figura 45. Esquema del cableado horizontal primer piso.
Fuente: El autor.

Tabla 22

Distribución de puntos de red del Primer Piso

Item	Dependencia	Puntos de red para datos	Puntos de red para voz	Puntos de red adicionales para datos	Puntos de red adicionales para voz
1	Oficina presidencial	3	3	1	1
2	Secretaría	1	1	-	-
3	Complemento Oficina	2	2	-	-
4	Sala de reuniones	2	2	1	1
5	Oficina 1	2	2	1	1
6	Oficina 2	2	2	1	1
7	Hall	-	-	1	-
				TOTAL PUNTOS DE RED = 33	

Fuente: El autor.

Tomando en cuenta la norma ANSI/EIA/TIA-568B que dice que un área de trabajo no debe estar por debajo de los 10 metros cuadrados, se colocarán cuatro puntos dobles adicionales en la oficina presidencial, las oficinas 1 y 2 y la sala de reuniones de esta planta, dado que en las demás dependencias los puntos de red ya cubren toda la extensión en metros cuadrados de las áreas de trabajo y se dejará un punto de red adicional en el pasillo para la futura implantación de un Access Point.

Debido a que se necesita enrutar 33 cables de par trenzado, se los ha divido para el soporte de tres canaletas como se muestra en la tabla 23:

Tabla 23

Distribución de puntos de red para las canaletas del primer piso

Canaleta	Dependencias a cubrir	Número de puntos de red
Canaleta 1	Oficina Presidencial Secretaria	8
Canaleta 2	Complemento Oficina Sala de reuniones Oficina 1	12
Canaleta 3	Oficina 2 Hall	13

Fuente: el autor.

De esta manera será posible calcular el área mínima que debe tener cada una, para lograr la canalización entre las salidas de telecomunicaciones y el rack. Para esto, se calculará el área del par trenzado 5e en base a su diámetro como se expone en la ecuación (1).

$$Diámetro\ del\ par\ trenzado\ UTP\ cat5e = 4.9mm$$

$$Área\ del\ par\ trenzado\ UTP\ cat5e = \pi x(\frac{4.9mm}{2})^2 = 18.86\ mm^2 \qquad (1)$$

$$Área\ del\ par\ trenzado\ UTP\ cat6A = \pi x(\frac{6.1mm}{2})^2 = 29.22\ mm^2$$

$$Área\ requerida\ del\ medio = \#Par\ trenzado\ xArea\ par\ trenzado(mm)^2 \quad (2)$$

Para categoría 5e:

$$Área\ requerida\ del\ medio - canaleta\ 1 = 8x18.86\ mm^2 = 150.86\ mm^2$$

$$Área\ requerida\ del\ medio - canaleta\ 2 = 12\ x18.86\ mm^2 = 226.32\ mm^2$$

$$Área\ requerida\ del\ medio - canaleta\ 3 = 13\ x18.86\ mm^2 = 245.18\ mm^2$$

Para categoría 6A:

$$Área\ requerida\ del\ medio - canaleta\ 1 = 8x29.22mm^2 = 233.76\ mm^2$$

$$Área\ requerida\ del\ medio - canaleta\ 2 = 12\ x29.22\ mm^2 = 350.64\ mm^2$$

$$Área\ requerida\ del\ medio - canaleta\ 3 = 13\ x29.22\ mm^2 = 379.86mm^2$$

De acuerdo al estándar solamente debe utilizarse el 40% del área del medio para futuros puntos de red y para evitar interferencias electromagnéticas. Entonces:

$$40\%xÁrea\ total\ mínima\ del\ medio\ = Area\ requerida\ del\ medio$$

$$Área\ total\ mínima\ del\ medio = \frac{A.requerida\ del\ medio}{40\%}$$

$$Área\ total\ mínima\ del\ medio = A.requerida\ del\ medio\ x\frac{1}{0{,}4}$$

$$Área\ total\ mínima\ del\ medio\ = Area\ requerida\ x\ 2.5 \quad (3)$$

Para categoría 5e:

$$Área\ total\ mínima\ del\ medio\ - canaleta\ 1 = 150.86mm^2x\ 2.5 = 377.15mm^2$$

$$Área\ total\ mínima\ del\ medio\ -canaleta\ 2 = 226.32mm^2 x\ 2.5 = 565.8mm^2$$

$$Área\ total\ mínima\ del\ medio\ -canaleta\ 3 = 245.18mm^2 x\ 2.5 = 612.95mm^2$$

Para categoría 6A:

$$Área\ total\ mínima\ del\ medio\ -canaleta\ 1 = 233.76\ mm^2 x\ 2.5 = 584.4\ mm^2$$

$$Área\ total\ mínima\ del\ medio\ -canaleta\ 2 = 350.64\ mm^2 x\ 2.5 = 876.6mm^2$$

$$Área\ total\ mínima\ del\ medio\ -canaleta\ 3 = 379.86mm^2 x\ 2.5 = 949.65mm^2$$

Es así que la canaletas 1, 2 y 3 deben tener un área de 377.15, 565.8 y 612.95 milímetros cuadrados o superior respectivamente; todas las dependencias tendrán puntos para voz y datos, por lo que las salidas de comunicaciones serán con cajetines dobles a excepción del pasillo o hall que tendrá un único punto de red.

La tabla 24 muestra la cantidad de conectores machos y hembra se utilizarán en el primer piso.

Tabla 24

Jacks y faceplates requeridos en el primer piso

Item	Dependencia	Jack RJ-45	Número de faceplates dobles	Número de faceplates simples
1	Oficina presidencial	8	4	-
2	Secretaría	2	1	-
3	Complemento Oficina	4	2	-
4	Sala de reuniones	6	3	-
5	Oficina 1	6	3	-

6	Oficina 2	6	3	-
7	Hall	1	-	1
	TOTAL	33	16	1

Fuente: el autor.

Observar el diagrama completo del diseño en el ANEXO D.

4.5.3. Cableado horizontal del Segundo Piso

Para el cableado horizontal del segundo piso se considerará la instalación de 9 puntos de red, dado que solamente existe un salón y el pasillo que se pueden observar en la figura 46, por lo que con un rack de pared ubicado en el salón máximo será suficiente.

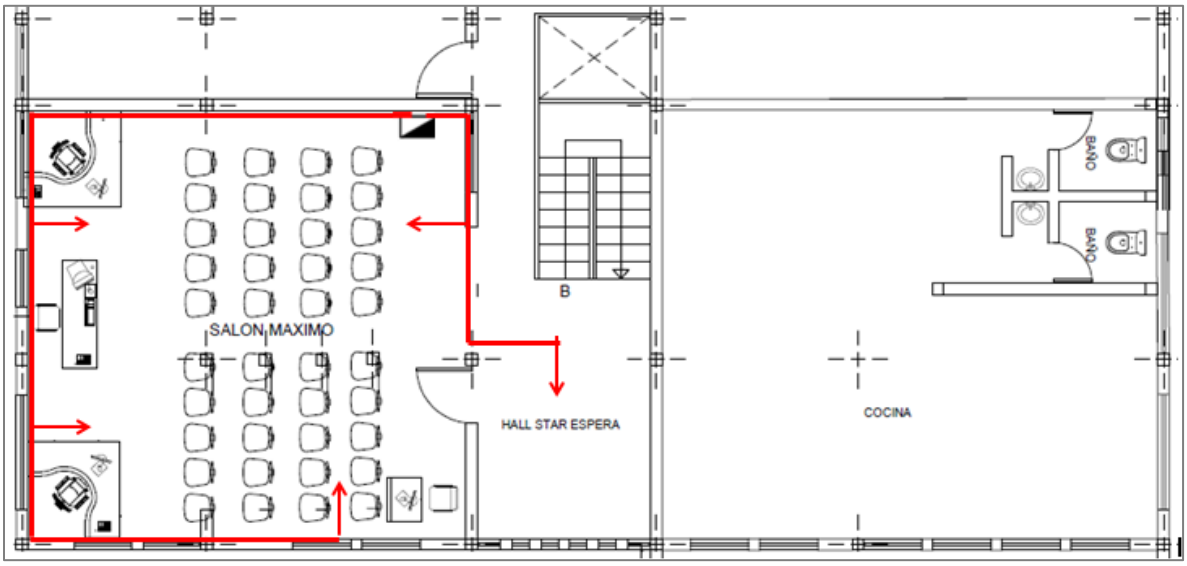


Figura 46. Esquema del cableado horizontal segundo piso.
Fuente: El autor.

La tabla 25 muestra la cantidad de puntos distribuidos acorde a las dependencias de esta planta.

Tabla 25

Distribución de puntos de red del Segundo Piso

Item	Dependencia	Puntos de red para voz	Puntos de red para datos	Puntos de red adicionales para datos
1	Salón máximo	4	4	-
2	Hall	-	-	1
			TOTAL DE PUNTOS DE RED = 9	

Fuente: el autor.

La ruta que abarca desde el rack de pared hasta las áreas de trabajo será por canaleta cuya capacidad se da mediante el siguiente cálculo:

$$Área\ requerida\ del\ medio\ 5e = 9x18.86\ mm^2 = 169.74\ mm^2$$

$$Área\ requerida\ del\ medio\ 6A = 9x29.22\ mm^2 = 262.98\ mm^2$$

De acuerdo al estándar solamente debe utilizarse el 40% del área del medio para futuros puntos de red y para evitar interferencias electromagnéticas. Entonces:

$$Área\ total\ mínima\ del\ medio\ 5e = 169.74m^2x\ 2.5 = 424.35mm^2$$

$$Área\ total\ mínima\ del\ medio\ 6A = 262.98m^2x\ 2.5 = 657.45mm^2$$

Es así que la canaleta debe tener un área de 424 mm^2 o superior para categoría 5e o 657.45 mm^2 para CAT-6A; todas las dependencias tendrán puntos para voz y datos, por lo que las salidas de comunicaciones serán con faceplates dobles y punto de red adicional para un Access point.

En la tabla 26 se detalla la cantidad de jacks y face plates a utilizarse.

Tabla 26

Jacks y faceplates requeridos en el segundo piso

Item	Dependencia	Jack RJ-45	Número de faceplates dobles	Número de faceplates simples
1	Salón máximo	8	4	-
2	Hall	2	-	1
	TOTAL	10	4	1

Fuente: el autor.

Observar el diagrama completo del diseño en el ANEXO E.

4.5.4. Resumen de la capacidad de canaletas a utilizarse

Se utilizarán canaletas plásticas de tres áreas diferentes, de 20x12mm^2 para enrutar hacia las áreas de trabajo, de 32x12mm^2 y 40x25mm^2 de área.

Entonces se procede a calcular el número de cables que caben en éstas, despejando la ecuación de capacidad utilizada anteriormente, que da lugar a la ecuación 4:

$$\#de\ Pares\ Trenzados = \frac{área\ de\ canaleta}{área\ del\ cable\ x\ 40\%} \quad (4)$$

$$\#de\ Pares\ Trenzados\ CAT-5e = \frac{área\ de\ canaleta}{18.86mm^2\ x\ 2.5}$$

$$\#de\ Pares\ Trenzados\ CAT-6A = \frac{área\ de\ canaleta}{29.22mm^2\ x\ 2.5}$$

La tabla 27 muestra cuántos pares trenzados categoría 5e son capaces de albergar estos tres tipos de canaletas.

Tabla 27

Cálculo del número de pares trenzados por canaleta

CANALETA (mm)	ÁREA(mm^2)	NÚMERO DE PARES TRENZADOS CAT-5e (#)	NÚMERO DE PARES TRENZADOS CAT-6A (#)
20x12	240	5	3
32x12	384	8	5
40x25	1000	21	14

Fuente: el autor.

Es así que a continuación se grafica el rack con la cantidad de cables que deben llegar a él así como también la ruta que estos deben seguir para determinar cuántas canaletas saldrán de dicho gabinete.

La nomenclatura utilizada es la siguiente:

PLANTA BAJA

En la figura 47 se observa como llegan los grupos de cables hacia el rack. En base al número de cada grupo se determinó la canaleta a utilizarse.

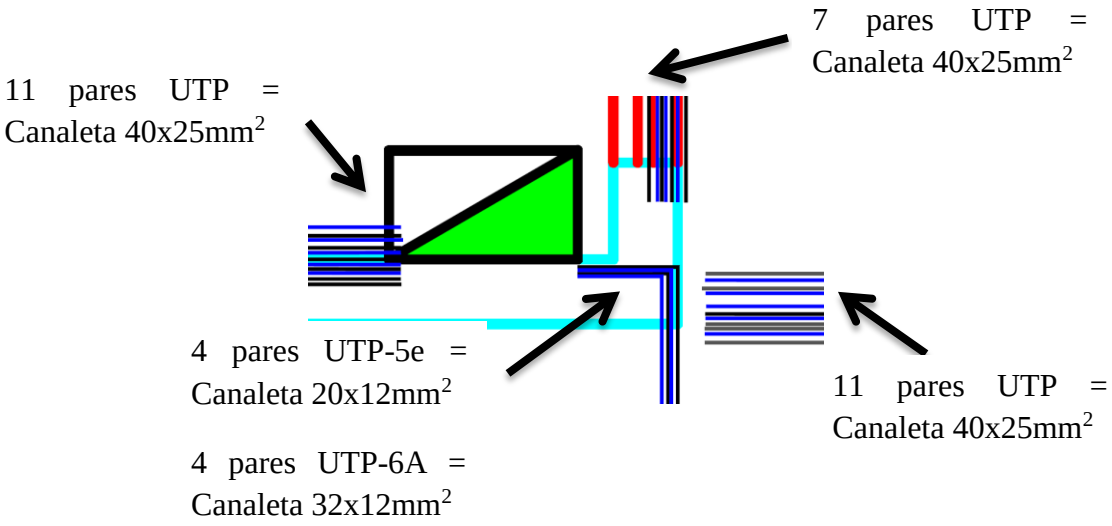


Figura 47. Canaletas planta baja.
Fuente: El autor.

PRIMER PISO

En el rack ubicado en el primer piso llegarán tres grupos de cables por lo que la elección de canaleta se realizó como lo indica la figura 48.

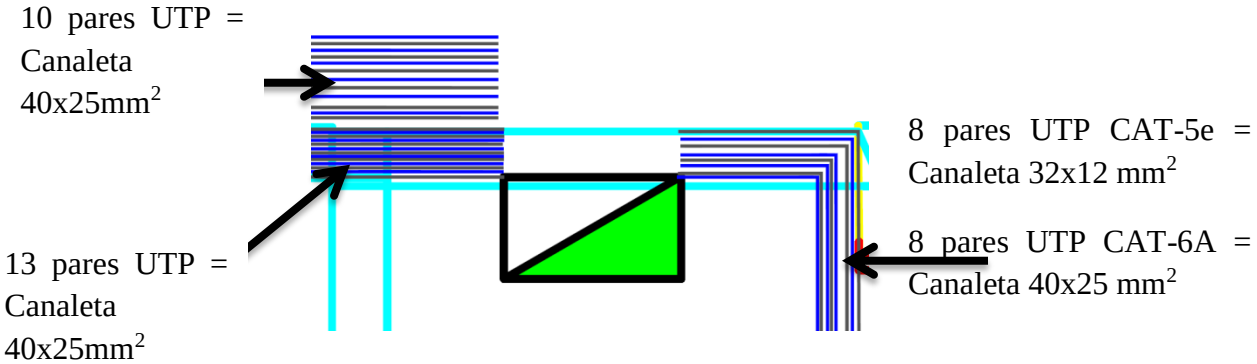


Figura 48. Canaletas primer piso.
Fuente: El autor.

SEGUNDO PISO

La figura 49 indica la capacidad de canaleta a utilizarse en el segundo piso donde únicamente se tienen nueve puntos de red enrutados en dos grupos de cables.

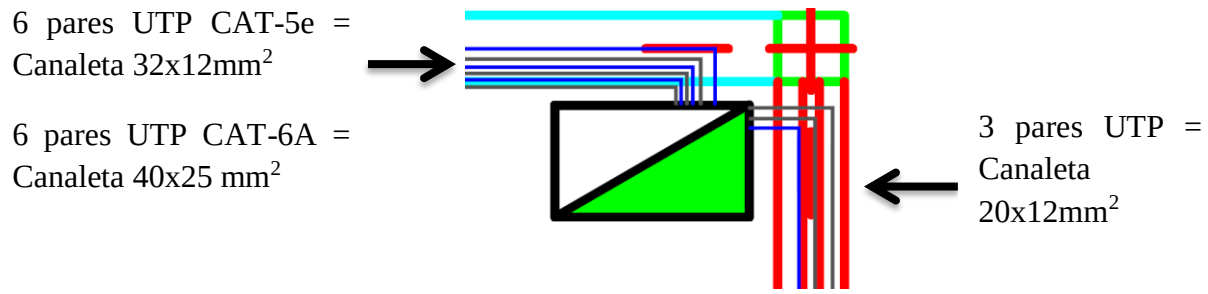


Figura 49. Canaletas segundo piso.
Fuente: El autor.

4.6. Cantidad de Cable UTP para el cableado horizontal

El cálculo aproximado del par trenzado a utilizarse en el enrutamiento horizontal será en base al punto promedio, que consiste en medir las longitudes de los puntos de red más largo y más corto respectivamente, y así obtener la longitud media, añadiendo el 10% de holgura con el fin de cubrir la distancia hacia los faceplates, como se enuncia en la ecuación (5):

$$Punto\ promedio = \frac{Pto.\ largo + Pto.corto}{2} x(1 + 10\%) \qquad (5)$$

4.6.1. Cable UTP requerido para la Planta Baja

Las mediciones en metros del punto más corto y el más largo se detallan en la tabla 28.

Tabla 28

Cálculo del punto promedio Planta Baja

Item	Dependencia	Punto más largo (metros)	Punto más corto (metros)	Punto promedio (metros)
1	Sala 1	7,6	4,2	6,49
2	Sala 2	21,2	16,5	20,74
3	Sala 3	6,7	3,5	5,61
4	Departamento general	14	11,5	14,03
5	Departamento 1	15,5	14,7	16,61
6	Departamento 2	17,5	12,7	16,61
7	Departamento 3	12,7	4,6	9,52
8	Departamento 4			0
9	Salón de alquiler	6	3,2	5,06
10	Hall	3	3	3,3

Fuente: El autor.

4.6.2. Cable UTP requerido para el Primer Piso

Las distancias obtenidas acorde a la ecuación del punto promedio se describen en la tabla 29.

Tabla 29

Cálculo del punto promedio Primer Piso

Item	Dependencia	Punto más largo (metros)	Punto más corto (metros)	Punto promedio (metros)
1	Oficina presidencial	22.75	8.55	17.22
2	Secretaría	11.88	11.88	13.07

3	Complemento Oficina	17.6	15.28	18.08
4	Sala de reuniones	22.85	18	22.47
5	Oficina 1	20.56	14.76	19.43
6	Oficina 2	23	15.49	21.17
7	Hall	7.54	7.54	8.3

Fuente: El autor.

4.6.3. Cable UTP requerido para el Segundo Piso

La tabla 30 muestra el cálculo del punto más corto y el más largo de las dependencias localizadas en la última planta.

Tabla 30

Cálculo del punto promedio Segundo Piso

Item	Dependencia	Punto más largo (metros)	Punto más corto (metros)	Punto promedio (metros)
1	Salón máximo	8	3	6,05
2	Hall	3	3	3,3

Fuente: El autor.

Mediante este cálculo ya es posible determinar el número de corridas por rollo (véase ecuación 6) y a su vez la cantidad de rollos a utilizarse (véase ecuación 7). La primera es una cantidad que debe aproximarse por debajo, mientras que la segunda a su inmediato superior. Se sabe que la longitud del par trenzado es una constante de 305 metros

$$\#\ de\ corridas\ por\ rollo = \frac{305}{Punto\ promedio} \quad (6)$$

$$\#\ de\ rollos = \frac{\#\ puntos\ de\ red}{\#\ corridas\ por\ rollo} \quad (7)$$

La tabla 31 muestra el detalle de la cantidad de cable UTP a utilizarse en el cableado horizontal de la planta baja.

Tabla 31
Cálculo del número de rollos Planta Baja

Item	Dependencia	Puntos de red	Punto promedio (metros)	Número de corridas por rollo	Número de rollos
1	Sala 1	2	6,49	47	0,043
2	Sala 2	3	20,735	15	0,204
3	Sala 3	2	5,61	54	0,037
4	Departamento general	1	14,025	22	0,046
5	Departamento 1	2	16,61	18	0,109
6	Departamento 2	2	16,61	18	0,109
7	Departamento 3	2	9,515	32	0,062
8	Departamento 4	2	0	0	-
9	Salón de alquiler	1	5,06	60	0,017
10	Hall	3	3,3	92	0,032

TOTAL= 0,66 rollos

Fuente: El autor.

La cantidad de par trenzado necesario para levantar el cableado horizontal del primer piso se evidencia en la tabla 32.

Tabla 32

Cálculo del número de rollos Primer Piso

Item	Dependencia	Puntos de red	Punto promedio (metros)	Número de corridas por rollo	Número de rollos
1	Oficina presidencial	8	17.22	17	0.47
2	Secretaría	2	13.07	23	0.09
3	Complemento Oficina	4	18.08	16	0.25
4	Sala de reuniones	6	22.47	13	0.46
5	Oficina 1	6	19.43	15	0.4
6	Oficina 2	6	21.17	14	0.43
7	Hall	1	8.3	36	0.0.3
					TOTAL =2.13 rollos

Fuente: El autor.

La tabla 33 muestra el par trenzado requerido para el segundo piso.

Tabla 33

Cálculo del número de rollos Segundo Piso

Item	Dependencia	Puntos de red	Punto promedio (metros)	Número de corridas por rollo	Número de rollos
1	Salón máximo	8	6,05	50,41	0,16
2	Hall	1	3,3	92,42	0,01
	TOTAL				0,17 rollos

Fuente: El autor.

Cantidad total de cable UTP

La ecuación 8 consiste en la integración de todo el cable requerido para en enrutamiento horizontal.

$$Cantidad\ de\ cable\ UTP = Cable\ UTP\ PB + Cable\ UTP\ PP + Cable\ UTP\ SP \quad (8)$$

$$Cantidad\ de\ cable\ UTP = 0{,}66 + 2{,}13 + 0{,}17 = 2{,}96\ rollos$$

Esta sería la cantidad de cable UTP a utilizarse en el cableado horizontal, a la cual debe agregarse el cable UTP a implementarse en el backbone.

4.7.Diseño del Backbone o Cableado Vertical

El cuarto de equipos se ubicará en la oficina presidencial localizada en el primer piso, de momento únicamente contará con un rack que se conectará mediante una topología en estrella, con los demás racks de pared de los pisos superior e inferior respectivamente con el fin de interconectar toda la infraestructura y los proporcionar los servicios requeridos. (véase figura 51).

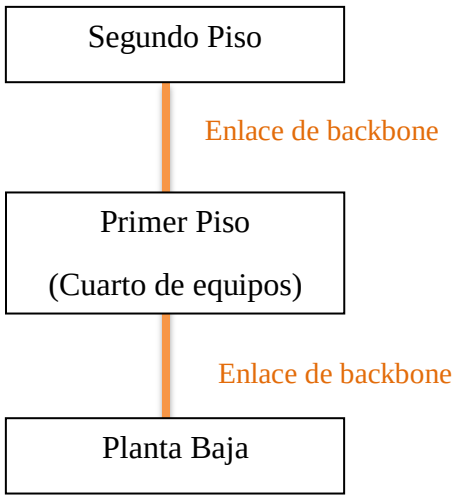


Figura 50. Interconexión del backbone.
Fuente: El autor.

Se recomienda que el medio de transmisión para el backbone sea de igual o superior categoría que el cableado horizontal, en este caso será de la misma categoría UTP 5e.

Las distancias se calcularán en base a los planos realizados, determinando así la cantidad de cable a utilizarse.

$$Enlace\ backbone\ \ primer\ piso - planta\ baja = 27\ metros$$

$$Enlace\ backbone\ \ primer\ piso - segundo\ piso = 18\ \text{metros}$$

$$Enlace\ backbone\ \ Total = 45\ \text{metros}$$

A esta cantidad se le debe añadir 5 metros más por reserva en caso de movilidad de los equipos.

Cantidad total de cable UTP

La ecuación 9 representa el total de par trenzado en metros a utilizarse para el sistema de cableado estructurado.

$$Cantidad\ total\ UTP = Cableado\ horizontal + Enlace\ de\ backbone \quad (9)$$

$$Cantidad\ total\ UTP = 915\ metros + 45\ metros + 5 = 965\ metros \approx 4\ rollos\ de\ cable$$

4.8. Rutas y Etiquetado

La etiquetación de puntos se especifica detalladamente en la norma ANSI/TIA/EIA 606A que corresponde a la administración de infraestructura de telecomunicaciones en donde se establece que las etiquetas deben ser adhesivas y de preferencia auto-laminadas. Se plantea el siguiente formato:

Piso en donde se ubica el punto – Número de patch panel – Especificación Voz/Datos- Número de punto de red.

La tabla 34 muestra el etiquetado según la ruta que sigue cada punto:

Tabla 34

Etiquetado de cada punto.

Item	**Dependencia**	**N° Punto de red (#)**	**N° Patch panel (D#)**	**Etiquetado Final**
Planta Baja (PB)	Sala 1	1	D1	PBD1V-01
		2	D1	PBD1D-02
		3	D1	PBD1V-03
		4	D1	PBD1D-04
	Sala 2	5	D1	PBD1V-05
		6	D1	PBD1D-06

		7	D1	PBD1V-07
		8	D1	PBD1D-08
		9	D1	PBD1V-09
		10	D1	PBD1D-10
	Sala 3	11	D2	PBD2V-11
		12	D2	PBD2D-12
		13	D2	PBD2V-13
		14	D2	PBD2D-14
	Departamento general	15	D2	PBD2V-15
		16	D2	PBD2D-16
	Departamento 1	17	D2	PBD2V-17
		18	D2	PBD2D-18
		19	D2	PBD2V-19
		20	D2	PBD2D-20
	Departamento 2	21	D2	PBD2V-21
		22	D2	PBD2D-22
		23	D2	PBD2V-23
		24	D2	PBD2D-24
	Departamento 3	25	D2	PBD2V-25
		26	D2	PBD2D-26
		27	D2	PBD2V-27
		28	D2	PBD2D-28
	Salón de alquiler	29	D2	PBD2V-29

		30	D2	PBD2D-30
	Hall	31	D2	PBD2D-31
		32	D2	PBD2D-32
		33	D2	PBD2D-33
Primer Piso (PP)	Oficina presidencial	34	D3	PPD3V-34
		35	D3	PPD3D-35
		36	D3	PPD3V-36
		37	D3	PPD3D-37
		38	D3	PPD3V-38
		39	D3	PPD3D-39
		40	D3	PPD3V-40
		41	D3	PPD3D-41
	Secretaría	42	D3	PPD3V-42
		43	D3	PPD3D-43
	Complemento Oficina	44	D3	PPD3V-44
		45	D3	PPD3D-45
		46	D3	PPD3V-46
		47	D3	PPD3D-47
	Sala de reuniones	48	D3	PPD3V-48
		49	D3	PPD3D-49
		50	D4	PPD4V-50
		51	D4	PPD4D-51
		52	D4	PPD4V-52

		53	D4	PPD4D-53
	Oficina 1	54	D4	PPD4V-54
		55	D4	PPD4D-55
		56	D4	PPD4V-56
		57	D4	PPD4D-57
		58	D4	PPD4V-58
		59	D4	PPD4D-59
	Oficina 2	60	D4	PPD4V-60
		61	D4	PPD4D-61
		62	D4	PPD4V-62
		63	D4	PPD4D-63
		64	D4	PPD4V-64
		65	D4	PPD4D-65
	Hall	66	D4	PPD4D-66
Segundo Piso (SP)	Salón máximo	67	D5	PSD5V-67
		68	D5	PSD5D-68
		69	D5	PSD5V-69
		70	D5	PSD5D-70
		71	D5	PSD5V-71
		72	D5	PSD5D-72
		73	D5	PSD5V-73
		74	D5	PSD5D-74

	Hall	75	D5	PSD5V-75

Fuente: el autor

4.9. Montaje de equipos en los racks

Para el alojamiento de los equipos se ha considerado la utilización de racks de pared, uno por piso, como manifiesta la norma ANSI/EIA/TIA 568-B, de tal modo que para la planta baja y primer piso se necesitará un rack con capacidad de almacenamiento para 2 patch panel/24puertos, 2 switches/24 puertos y sus organizadoras horizontales, cada uno de estos dispositivos ocupa una unidad de rack, lo que sugiere que cada gabinete deberá ser de mínimo 6UR y 19 pulgadas como se indica en la figura 51.

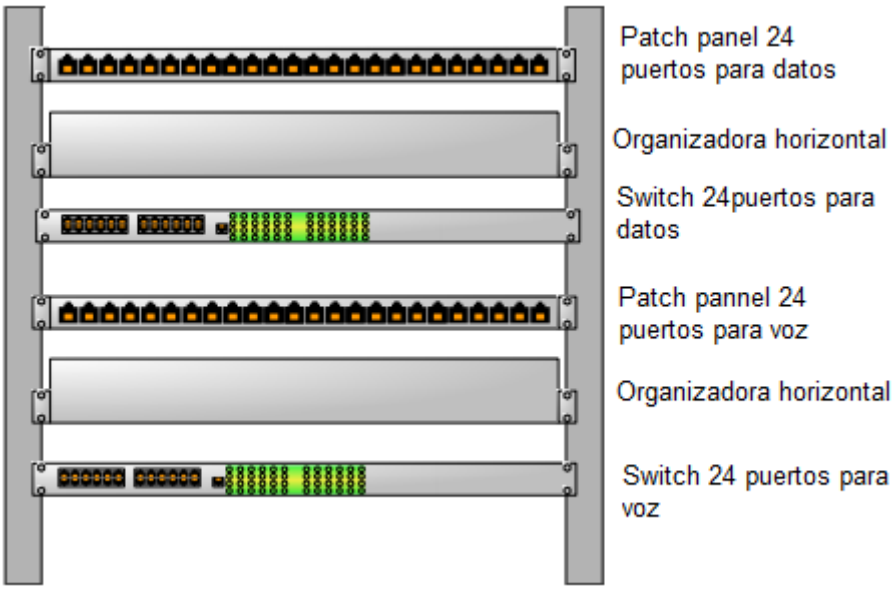


Figura 51. Montaje de equipos en el rack planta baja y primer piso.
Fuente: El autor.

Para el segundo piso, debido a la cantidad de puntos de red solamente se necesita albergar un switch de 24 puertos y un pacth panel sumando 2UR. Sin embargo, se debe considerar los racks disponibles en el mercado, siendo el de 6 unidades el más cercano a la capacidad

requerida dejando a la elección del cliente la compra de éste, que se detallará en el capítulo de implementación. No obstante se sugiere montar los equipos de acuerdo a la figura 52.

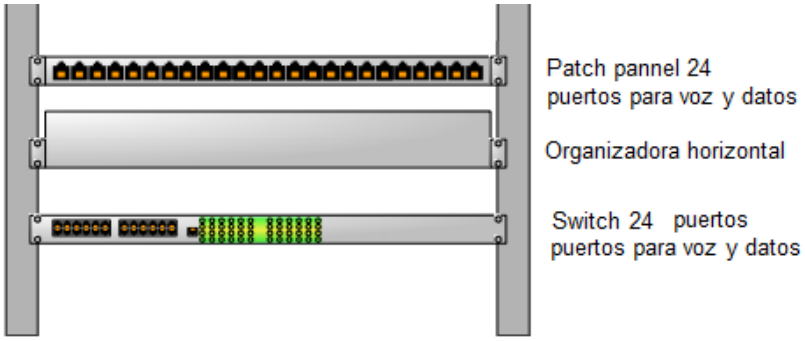


Figura 52. Montaje de equipos en el rack segundo piso.
Fuente: El autor.

4.10. Seguridad en la red

Para el diseño de un esquema de seguridad se propone en primer lugar, la creación de un instructivo que detalle las políticas de seguridad que todos los usuarios relacionados con la red de datos de la Cámara de Comercio de la Ciudad de Otavalo deban seguir. Luego, establecer los lugares clave en donde se implantarán los controles de acceso con su respectivo diagrama de conexión y, finalmente crear las políticas de acceso en los dispositivos de red

4.10.1. Políticas de seguridad

La creación de políticas de seguridad en una empresa es vital para el resguardo de la información, de tal manera que, basado en las buenas prácticas proporcionadas por la norma ISO-27002 para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, (ISO27000, 2016) y acorde a lo que la Cámara de Comercio requiere se plantea un manual con los dominios correspondientes a la

Cámara de Comercio. La norma ISO-27002 cuenta con catorce dominios, que abarcan desde la seguridad del personal hasta la seguridad ambiental, sin embargo estos parámetros se han descartado puesto que el manual engloba únicamente políticas de acceso.

	CÁMARA DE COMERCIO "OTAVALO" **Manual de políticas de seguridad de acceso**
Introducción	El presente manual contiene el consolidado de todas las políticas de acceso tanto físico como lógico que regularán la gestión de sistemas de la Cámara de Comercio "Otavalo" en la ciudad del mismo nombre. Es responsabilidad de la Dirección Ejecutiva, Directores, Jefes y todos los empleados el cumplimiento de los lineamientos aquí establecidos en lo que fuere pertinente.
Objetivo General	El Manual de Políticas de Seguridad tiene como propósito consolidar los lineamientos que regulen el acceso de los usuarios de la Cámara de Comercio, proporcionando información acerca del procedimiento a seguir en caso de suscitarse alguna anomalía.
Objetivos Específicos	• Brindar los lineamientos necesarios para ejercer un correcto uso de la infraestructura y dispositivos de la Cámara de Comercio estableciendo derechos y obligaciones para sus usuarios.

	• Definir procedimientos a seguir en caso de presentarse algún evento. • Elevar la productividad del personal a través de los procesos de gestión que se detallan aquí, mejorando la eficacia de las actividades.
Versión	Primera versión. Versión 1.0
Elaborado por:	Srta. Marcela López

4.10.1.1. Políticas de acceso físico

Incluye los dominios de políticas de seguridad y control de acceso en donde los involucrados son todas aquellas personas que por alguna situación desean ingresar al edificio, entonces se convierten en "usuarios" y las personas encargadas o designadas para controlar el ingreso de los mismos.

CAMARA DE COMERCIO "OTAVALO"	CÁMARA DE COMERCIO "OTAVALO"
	Manual de políticas de seguridad de acceso
DOMINIO	POLÍTICAS DE SEGURIDAD
DESTINATARIO	Todos los usuarios de la Cámara de Comercio.
OBJETIVO	Notificar la existencia de políticas de seguridad hacia todos

	los usuarios de la Cámara de Comercio de Otavalo.
LINEAMIENTOS	a) Todas las personas que hagan uso de los departamentos, otras áreas o equipos activos serán considerados usuarios internos del establecimiento. b) El presidente de la Cámara de Comercio u otra persona designada por el mismo, será responsable de dar a conocer las políticas de seguridad que se manejarán en el lugar. c) Para cualquier modificación de las políticas de seguridad, será necesario convocar a una reunión con la presencia de los directivos para su respectiva aprobación.
ACCIÓN	Creación y difusión de un manual de políticas.

CAMARA DE COMERCIO "OTAVALO"	CÁMARA DE COMERCIO "OTAVALO"
	Manual de políticas de seguridad de acceso
DOMINIO	CONTROL DE ACCESO
DESTINATARIO	Usuarios de la Cámara de Comercio.
OBJETIVO	Limitar el ingreso de personas hacia los departamentos que

	albergan los equipos principales.
LINEAMIENTOS	a) El/los encargados de la red de datos deberán llevar una bitácora o registros de acceso de los usuarios y/o cualquier otra persona que visite esas áreas. b) Los visitantes que se les permita el ingreso a áreas restringidas estarán acompañados de un funcionario del lugar. c) Los directivos que tengan acceso al monitoreo del control físico deben vigilar periódicamente que se cumpla tal cual para lo que fue implantado. d) Los directivos podrán autorizar el ingreso temporal de cualquier persona si así lo desean siempre y cuando sea bajo su responsabilidad.
ACCIÓN	Registro de ingreso en una bitácora.

4.10.1.2. Políticas de acceso lógico

Existirán privilegios de acceso para cada usuario o grupo de usuarios de la red de datos, optimizando su uso.

CAMARA DE COMERCIO "OTAVALO"	CÁMARA DE COMERCIO "OTAVALO"
	Manual de políticas de seguridad de acceso
DOMINIO	CIFRADO
DESTINATARIO	Personal de la Cámara de Comercio.
OBJETIVO	Gestionar las claves y cuentas de usuario.
LINEAMIENTOS	a) Las contraseñas de los dispositivos que conforman la red de datos deberán cumplir con los lineamientos mínimos de seguridad como: mínimo ocho caracteres, mayúsculas, minúsculas, números y símbolos, y no utilizar secuencias lógicas de letras o números como por ejemplo: 1234, abcd, entre otras. b) Los directivos, socios o invitados que quieran hacer uso de la red, antes de acceder a esta, deben contar con su respectiva cuenta de usuario previamente autorizada. c) El/los encargados de la red de datos previa autorización de los jefes a cargo podrán bloquear, crear, modificar o eliminar cuentas de usuario de acceso en la red.

	d) Los directivos estarán en la capacidad de solicitar perfiles o cuentas de usuario para el personal que trabaje en sus áreas. e) Si algún funcionario de la entidad se desvincula de esta, el/los encargados de la red de datos deben establecer mecanismos que garanticen la eliminación de las cuentas de usuario pertenecientes a dicho funcionario. f) El personal no debe revelar su cuenta de usuario o contraseña a terceros.
ACCIÓN	Actualización periódica de contraseñas que cumplan los parámetros establecidos.

CAMARA DE COMERCIO "OTAVALO"	CÁMARA DE COMERCIO "OTAVALO"
	Manual de políticas de seguridad de acceso
DOMINIO	SEGURIDAD DE LAS OPERACIONES
DESTINATARIO	Usuarios de la Cámara de Comercio.
OBJETIVO	Gestionar la seguridad de la red limitando el acceso a determinados sitios web.
LINEAMIENTOS	a) Los equipos de usuario final que son parte del

	inventario de la Cámara de Comercio de la ciudad de Otavalo, tendrán que cumplir solamente las tareas para las que han sido designadas. b) Los socios y usuarios invitados no deben modificar la configuración de las computadoras que son propiedad de la Cámara de Comercio. c) Todos los usuarios de la red de datos son responsables de las acciones ejecutadas en los equipos que se encuentren utilizando.
ACCIÓN	Revisión eventual por parte del jefe encargado, de las actividades que están desarrollando los usuarios en los equipos.

CAMARA DE COMERCIO "OTAVALO"	CÁMARA DE COMERCIO "OTAVALO"
	Manual de políticas de seguridad de acceso
DOMINIO	SEGURIDAD DE LAS COMUNICACIONES
DESTINATARIO	Usuarios de la Cámara de Comercio.

OBJETIVO	Optimizar el uso del ancho de banda de la red.
LINEAMIENTOS	a) Los usuarios y personal en general deben hacer uso del Internet cuando sea necesario y en relación a las actividades que realizan. b) El acceso a páginas pornográficas, drogas, alcohol y/o cualquier otra página de este tipo se encuentra terminantemente prohibido para cualquier usuario de la red. c) Los socios e invitados tienen limitado el acceso a facebook, twitter, youtube u otro servicio que pueda ser utilizado con fines diferentes a las actividades destinadas.
ACCIÓN	Utilización de servidor PROXY SQUID que restringirá los accesos indebidos o se controlará el ancho de banda.

4.10.2. Control de acceso físico

Se instalarán controles de acceso biométricos mediante huella digital, con el objetivo de controlar el ingreso del personal a las instalaciones del edificio. El sistema se encargará de almacenar los datos registrados de las personas con parámetros de fecha y hora principalmente.

Las características mínimas de estos dispositivos son:

- Funcionamiento en modo red o independiente: inicialmente se colocará un biométrico en la entrada por lo que este funcionará en modo independiente, pero con el pasar del

tiempo se prevé localizar más de estos dispositivos por lo que el dispositivos por lo que este deberá soportar conexión en red.

- Transferencia de registros en tiempo real: los reportes deberán generarse al día por lo que la transferencia debe ser en tiempo real
- Batería integrada en caso de cortes de energía. (Revisar ANEXO)
- Interfaz de comunicación Ethernet: para conexión en red.
- Capacidad de usuarios: 100 mínimo entre huellas dactilares y contraseñas numéricas ya que esta es la cantidad máxima de personas que han llegado al lugar en un determinado día.
- Entrada USB, TCP/IP: para guardar los reportes generados.

Las lectoras biométricas se ubicarán, una en la entrada del edificio y otra en el ingreso a los departamentos de directivos puesto que allí se aloja el rack principal de la red. Las lectoras biométricas expuestas en el documento cuentan con dos tipos de configuración, que dependiendo del harware que se disponga se hará uso del diagrama individual de la figura 53 o el diagrama en red de la figura 54.

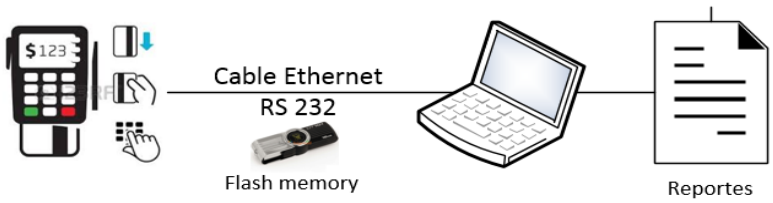


Figura 53. Diagrama de conexión individual. Microsoft Office Visio 2013.
Fuente: El autor.

El diagrama de conexión individual o standalone se utiliza cuando no existe gran cantidad de lectoras biométricas o en su defecto no es necesario el monitoreo conjunto de todos estos

dispositivos; si por el contrario se desea un seguimiento más profundo se debe realizar una configuración en red, de la siguiente manera:

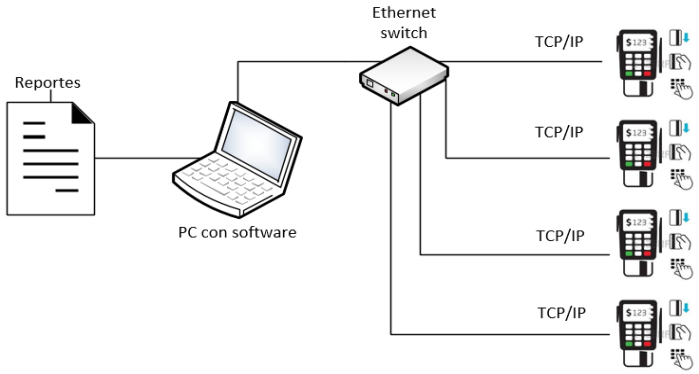


Figura 54. Diagrama de conexión en red. Microsoft Office Visio 2013.
Fuente: El autor.

El control de acceso biométrico estará sujeto a la pared como indica la figura 55, ubicado del lado derecho; este tendrá conexión directa con el pivote electromagnético que se localizará en la parte superior de la puerta de acuerdo al diagrama siguiente:

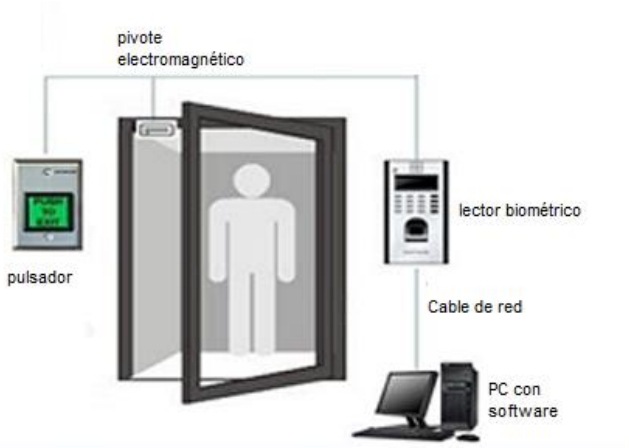


Figura 55. Diagrama de conexión hacia la puerta. TechnologiesINH, 2016.
Recuperado de http://www.inh.com.co/index.php?page=./HTML/controldeacceso

4.10.3. Elección del software o hardware para el Firewall

Para determinar los requerimientos del sistema se utilizó la norma ISO/IEC/IEEE 29148:2011 que especifica los Requerimientos de Software, a través de una serie de parámetros que se deben tomar en cuenta al momento de seleccionar determinado sistema; corresponde a una actualización de la norma IEEE Std 830, para lo cual supone llenar un esquema con la información requerida, como se muestra a continuación:

Introducción	Se requiere la implementación de un servidor firewall/proxy para la Red de Datos del Edificio de la Cámara de Comercio del Cantón Otavalo	
Propósito	Obtener los requerimientos para seleccionar el firewall/proxy más ideal para la Red de Datos del Edificio de la Cámara de Comercio del Cantón Otavalo.	
Ámbito del sistema	El servidor firewall/proxy debe re direccionar todo el tráfico hacia una conexión segura, para que los paquetes de la red interna atraviesen las políticas que se vayan a configurar.	
Descripción general	Un servidor firewall/proxy actúa como intermediario entre una red privada y una pública.	
Funciones del producto	• Soporte de redes lan virtuales (vlan). • Creación de políticas. • Filtrado de paquetes. • Filtrado de contenido. • Memoria caché . • Generación de reportes	
Características de los usuarios	Los usuarios tendrán acceso al contenido web dependiendo de varios factores: tipo de usuario, horarios y contenido.	
Requisitos futuros	Soportar la implementación de protocolos más avanzados como agregación de enlace.	
Requisitos específicos	**Interfaces**	2 interfaces (Pública y privada)

	Funciones	Restricciones por horarios, control de ancho de banda, Restricción de contenido web no deseado
	Requisitos de rendimiento	Soportar el tráfico de todos los usuarios
	Restricciones de diseño	NO
	Atributos el sistema	Compatible con los equipos que conforman el resto de la topología.
	Otros requisitos	-

Para determinar que solución resulta más factible se realizó una comparativa entre los Firewalls de software y un equipo físico diseñado para firewall exclusivamente. En la tabla a continuación se especifican los detalles:

Tabla 35

Selección del firewall

FIREWALL	Cisco ASA 5505	Proxy Squid CentOS 6.6	Checkpoint
Características principales			
Capacidad máxima de procesamiento (Mbps)	150		
Cantidad máxima de sesiones de acceso remoto	10	Ilimitado	Ilimitado
Memoria (MB)	256	asignable	asignable

Número de puertos	8	2	2
Soporte VLAN(802.1q)	SI	SI	SI
Cantidad máxima de interfaces virtuales (VLAN)	50/100	256	255
Prevención de intrusiones	No disponible	SI	SI
Seguridad en la capa de aplicaciones	SI	SI	SI
Funciones de firewall transparente	SI	SI	NO
Autenticación RADIUS	SI	SI	SI
Interfaz web	SI	SI	SI
Autenticación Portal Cautivo	NO	SI	SI
Calidad de servicio	NO	SI	SI
Enrutamiento ospf, rutas estáticas, rip	SI	SI	NO
NAT y PAT	SI	SI	SI
Multizona servidor DNS	NO	SI	NO
PoE	SI	NO	NO

Recopilado de https://www.linux.com/ - http://www.zeroshell.net/es/ - http://www.cisco.com/c/dam/global/es_es/assets/publicaciones/07-08-cisco-dispositivos-serie-ASA5500.pdf

Se selecciona así el firewall en software libre puesto que cumple con las mismas funciones de acuerdo al diseño de red propuesto que un equipo físico, en este caso Cisco Asa, a un menor costo.

Es así que, el PC servidor que actúe como firewall, contará con el kernel de Linux en su versión CentOS 6.7; en donde se deberán configurar dos interfaces de red tal y como se ilustra en la figura 56.

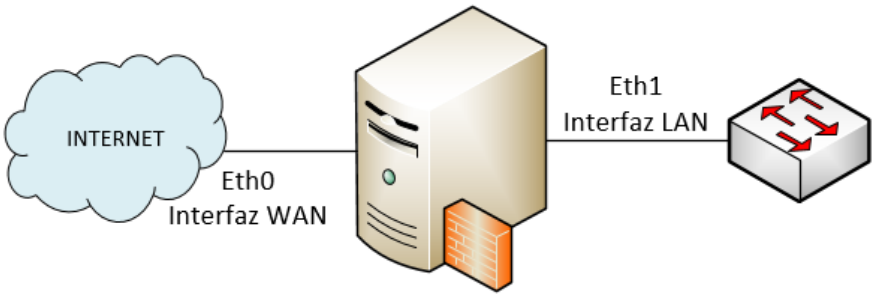


Figura 56. Interfaces del firewall. Microsoft Office Visio 2013.
Fuente: El autor.

4.10.3.1. Configuración de las tarjetas de red

La interfaz eth0 será la que tenga la dirección ip pública desde el ISP, para configurar esta interfaz de red se ejecuta el comando expuesto en la figura 57.

sudo gedit /etc/sysconfig/network-scripts/ifcfg-eth0

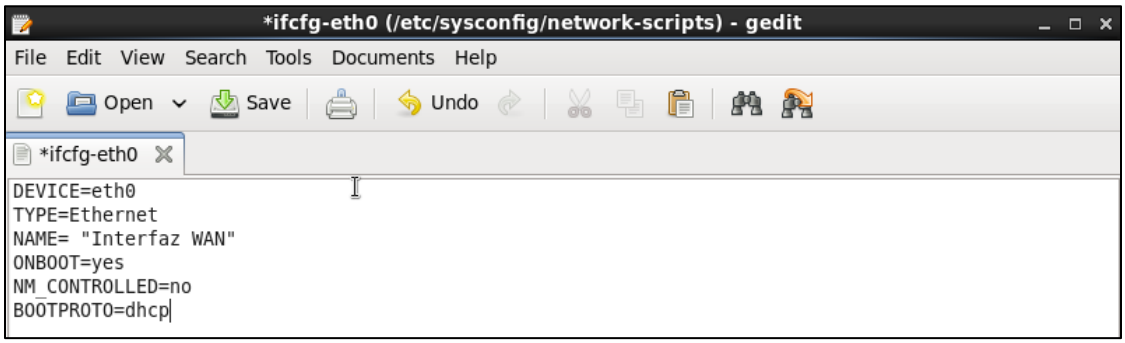


Figura 57. Configuración de la interfaz de red eth0. VirtualBox/Centos 6.7.
Fuente: El autor.

El firewall podrá comunicarse con la red lan a través de la interfaz eth1 que tendrá asignada una dirección ip estática como se indica en la figura 58.

sudo gedit /etc/sysconfig/network-scripts/ifcfg-eth1

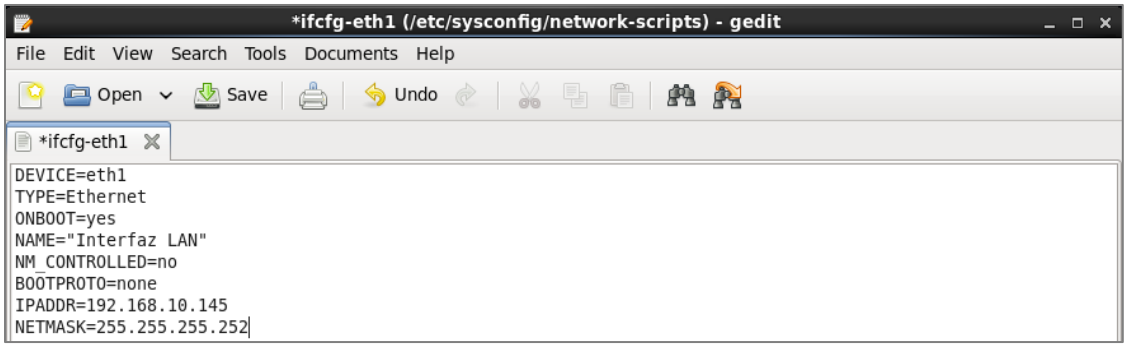


Figura 58. Configuración de la interfaz de red eth1. VirtualBox/Centos 6.7.
Fuente: El autor.

4.10.3.2. Proxy SQUID

Squid es un proxy caché web que además de proporcionar mayor seguridad al redireccionar el puerto 80 por el 3128 , permite la creación de controles de acceso, mediante la creación de políticas y simplificando la administración de la red. (CentOS, 2016). Para su instalación y configuración básica revisar el ANEXO G.

Una vez instalado el squid se procede a configurar según las condiciones requeridas, creando en primer lugar la lista de control de acceso y luego su correspondiente regla. Para determinar que tipo de políticas configurar se realizó una entrevista hacia el presidente de la Cámara de Comercio y encuestas a sus usuarios que se puede visualizar mediante el ANEXO B.2. En donde se determinó que:

- El 40% de los usuarios acceden a internet todos los días laborables, todo el tiempo, el 33% lo hace mínimo dos horas diarias, el 17% menos de una hora y únicamente el 10% no utiliza internet.
- Los empleados de la Cámara de Comercio son los que manipulan las peticiones de marketing electrónico mediante redes sociales, especialmente Facebook, por lo que deberán tener acceso a esto sin restricciones. Los empleados ocupan la vlan directivos.

- Los socios de la Cámara de Comercio no cumplen funciones específicas de e-commerce o alguna otra que beneficie directamente a la institución sino más bien ocupan las instalaciones de la Cámara como un servicio por el cual están pagando; por lo que estos seguirán teniendo acceso, pero se deberá controlar su ancho de banda.
- Las redes sociales de mayor uso por parte de estos usuarios son Facebook, youtube y twitter.
- El 46% de los usuarios piensan que resultaría útil controlar el acceso web, como sugerencia algunos de los empleados manifestaron estar de acuerdo con la implementación de un dispositivo para esta finalidad, ya que en muchas ocasiones los socios utilizan la red para otros fines y provocan la ralentización de los hosts de empleados.
- Todos los usuarios podrán acceder a comunicaciones por voz.

Además de esto se debe tomar en cuenta que el acceso a páginas indebidas de tipo pornográfico está terminantemente prohibido.

Cabe recalcar que el acceso a internet es considerado un derecho humano, así lo establece la Organización de las Naciones Unidas en el artículo 19 de la Declaración Universal de los Derechos por lo que es importante proteger el acceso a Internet ya que "facilita enormes oportunidades para la educación asequible e inclusiva a nivel mundial" (ONU, 2016). Es así que resulta inadmisible la suspensión total de este servicio sea para cual fuere su fin. Entonces se plantean las políticas acorde a la tabla 36:

Tabla 36

Políticas a configurar en el servidor proxy SQUID

POLÍTICA	DIRIGIDA A	DENEGAR/ PERMITIR
	Directivos	PERMITIR sin restricciones
Acceso a facebook, twitter y youtube	Socios	PERMITIR con control de ancho de banda
Descargas	Directivos	Permitidas
	Socios	Permitidas en determinado horario
Acceso al servidor FIREWALL	Encargado de la red	PERMITIR
	Resto de usuarios	DENEGAR
Acceso a páginas pornográficas, drogas o alcohol	Todos los usuarios	DENEGAR

Fuente: El autor.

4.10.3.3. Reglas de acceso

Antes de configurar los accesos, se deben establecer ciertas políticas por defecto, que permitan el enrutamiento de los paquetes. Para ello se ingresa al fichero /etc/sysconfig/iptables y se digita lo siguiente:

#Vaciar las reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
#Políticas por deafutl
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
 # Enmascaramiento de las direcciones IP
iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
#Habilita el Forwarding entre tarjetas de red
sysctl -p /etc/sysctl.conf
 # Cierre de los accesos indeseados del exterior:
 # Nota: 0.0.0.0/0 significa: cualquier red

- Regla para configurar el reenvío de paquetes entre las dos tarjetas de red eth0 y eth1.

  iptables -A INPUT -i lo -j ACCEPT

  iptables -A FORWARD -i eth1 -j ACCEPT

  iptables -A FORWARD -o eth1 -j ACCEPT

- Regla para que en la vlan de voz únicamente se pueda acceder a los puertos de voz ip de SIP e IAX.

iptables -A FORWARD –s 192.168.10.0/24 –i eth1 –p udp –dport 5060 –j ACCEPT

iptables -A FORWARD –s 192.168.10.0/24 –i eth1 –p udp –dport 4569 –j ACCEPT

4.10.3.4. Configuración de políticas

De acuerdo a la tabla 31 obtenida en base a los requerimientos de usuario se procede configurar las siguientes reglas en el archivo /etc/squid/squid.conf:

- Listas de acceso y reglas de control:
  acl redlocal src 192.168.10.0/24
  acl directivos src 192.168.10.64/27
  acl socios src 192.168.10.96/27
  http_access allow redlocal
  http_access allow directivos
  http_access allow socios

- Permitir todo el tráfico a la red local:

  delay_pools 5

  delay_class 1 1

  delay_parameters 1 -1/-1 -1/-1

  delay_access 1 allow redlocal.

- Asignar 2Mbps para descargas en la vlan socios durante el horario laboral.
  Se crea a acl detallando el horario laboral:

  acl horario_laboral time MTWHF 07:00-13:00

  En este caso se debe crear un archivo con las extensiones de las posibles descargas, en este caso denominado formatos:

\.avi$	\.mp3$	\.mpg$	\.mov$
\.mp4$	\.swf$	\.mpeg$	\.wma$

\.wmv$	\.mp$	\.cab$	\.gz$
\.wav$	\.flv$	\.tar$	\.kdc$
\.exe$	\.asf$	\.bz2$	\.vob$
\.iso$	\.rm$	\.upd$	\.js$
\.zip$	\.ra$	\.gsg$	
\.rar$	\.ogg$	\.dll$	
\.3gp$	\.bin$	\.msi$	

Ahora se detalla el delay_pool correspondiente, expresando los 2Mbps en bytes que serían 250000 bytes una vez que los archivos superen los 6kb:

delay_class 2 1

delay_parameters 2 250000/6000

acl formatos_videos urlpath_regex -i "/etc/squid/formatos"

delay_access 2 allow redlocal formatos horario_laboral

- Asignar 3Mbps para los usuarios de la vlan socios para el acceso a redes sociales, durante el horario laboral.

  Se crea un archivo con los dominios a controlar, en este caso denominado "redes_sociales".

  #Redes Sociales
  facebook.com
  www.facebook.com
  https://www.facebook.com
  twitter.com
  www.twitter.com
  youtube.com
  www.youtube.com

Y su delay pool quedaría de la siguiente manera:

delay_class 3 1

delay_parameters 3 375000/2000

acl redes_sociales url_regex -i “/etc/squid/redes_sociales”

delay_access 3 allow redlocal redes_sociales laboral

- Permitir el acceso sin restricciones por parte de cualquier usuario durante el horario no laboral.
  Se crea la acl especificando el horario en que no se labora:
  acl horario_no_laboral time MTWHF 14:00-06:59

  Y la regla queda así:

  delay_class 4 1

  delay_parameters 4 -1/-1 -1/-1

  delay_access 4 allow redlocal horario_no_laboral

- Permitir el acceso total los fines de semana (sábado y domingo):

  Lista de acceso:

  acl findes time AS 00:00-23:59

  Regla delay pool:

  delay_class 5 1

  delay_parameters 5 -1/-1 -1/-1

  delay_access 5 allow redlocal findes.

4.11. Presupuesto estimado para la implementación de la red

Para la estimación de costos se consideraron n los precios que se exponen en las páginas de los fabricantes, además de mercado libre Ecuador como precio referencial; es así que, se presenta un presupuesto detallando los precios unitarios de los materiales que serán necesarios en este

diseño. Para obtener el costo total de la red pasiva se tomará en cuenta: canaletas, cables, conectores, patch cord, racks y demás accesorios.

4.11.1. Cables y accesorios

Para el cableado horizontal y las área de trabajo se usarán: cable UTP, jacks, patch cord, face plates dobles y simples, todos los materiales deben ser de la misma categoría que el cable. La tabla 37 muestra una comparativa entre las marcas Conalep y Furukawa.

Tabla 37

Precios de cables y accesorios

		Precios			
Descripción	Cantidad	Conalep Unitario	Furukawa Unitario	Conalep Total	Furukawa total
Rollo de cable UTP Cat. 5e	5	58.00	99.00	290.00	495.00
Patch Cord Cat. 5e (7 pies) Azul	50	2.50	9.50	125.00	475.00
Face Plate Doble.	40	1.00	2.75	40.00	110.00
Face Plate Simple	20	1.00	2.50	20.00	50.00
Jack RJ45 Cat.5e	100	2.70	7.00	270.00	700.00
			Total:	745.00	1830.00

Fuente: Recopilación por el autor. Tomado de páginas MercadoLibre, Amazon, Furukawa.

4.11.2. Racks y patch pannels

La tabla 38 detalla los precios de dos marcas: Next y Panduit.

Tabla 38

Precios de gabinetes rack y sus accesorios

Descripción	Cantidad	Next Unitario	Next Total	Panduit Unitario	Panduit Total
Patch Panels Cat. 5e de 24 Puertos	5	50.00	250.00	225.00	1125.00
Organizadores de Cables Horizontal	5	20.00	100.00	100.00	500.00
Gabinete Cerrado de Pared 6UR	3	115.00	345.00	299.00	897.00
			Total	624	2522

Fuente: Recopilación por el autor. Tomado de páginas MercadoLibre, Amazon, Furukawa.

4.11.3. Canaletas y accesorios

Se propone trabajar con la marca Dexson debido a que su costo resulta más económico, en la tabla 34 se describe el número aproximado de canaletas, valores unitarios, el total del costo y sus respectivos accesorios

Tabla 39

Precios de canaletas

DESCRIPCIÓN	CANTIDAD	DEXSON Unitario ($)	DEXSON Total ($)
Canaleta 60x40	15	8.75	131.24
Canaleta 40x25	20	6.25	125.00
Angulo Interno 60x40	20	2.25	45.00
Angulo Interno 40x25	20	0.85	17.00
Angulo Externo 60x40	10	2.25	22.50

Angulo Externo 40x25	20	0.85	17.00
Adaptador T 60x40	11	2.00	22.00
Adaptador T 40x25	25	0.85	21.25
		Total:	400.99

Fuente: Recopilación por el autor. Tomado de páginas MercadoLibre, Amazon, Furukawa.

4.11.4. Selección de equipos activos

En la tabla 40 se muestran los requerimientos que se necesitan de acuerdo al equipo.

Tabla 40

Requerimientos para la selección de equipos

Dispositivo	Requerimientos
Switch principal	- Administrable: Sí -24 puertos -Soporte Vlan -Enrutamiento intervlan
Switches de acceso	- Administrable: Sí -24 puertos - Soporte de vlan
Biométricos	-Funcionamiento en modo red o independiente. -Transferencia de registros en tiempo real. -Batería integrada en caso de cortes

	de energía de al menos 6 horas de duración pudiéndose cubrir el registro con una bitácora de ser necesario .(Ver ANEXO H) -Interfaz de comunicación Ethernet. -Teclado numérico. -Pantalla LCD.
CPU Firewall	- Mínimo 64MB de memoria RAM - Mínimo 1024 MB de espacio en disco duro. - Procesador INTEL o AMD

Fuente: El autor.

4.11.4.1. Comparación de switches de red según la marca

La comparación de switches se muestra en la tabla 36 tomando en cuenta sus principales características.

Switch Central

Corresponde al equipo principal de acuerdo a la topología planteada, el cual se encargará del enrutamiento de paquetes hacia la red pública. En la tabla 41 se presenta las características de los equipos.

Tabla 41

Selección del switch principal

MARCA	**CISCO**	**HP/3COM**	**D-LINK**
MODELO	**SMB 110-24**	**3226**	**DES-1024D**
IMAGEN			
CARACTERÍSTICAS PRINCIPALES			
Switch Layer 3	SI	SI	SI
Puertos 10/100/1000	24	24	24
Puertos 100 BASE T-SFP	2	2	4
Soporte Ipv4	SI	SI	SI
Soporte Ipv6	SI	SI	SI
Capacidad de conmutación agregada	SI	SI	NO
Capacidad de conmutación individual	10 Gbps	10Gbps	24 Gbps
Capacidad de envío de paquetes	13.2Mbps	No especifica	17.86 Mbps
Monitoreo IGMP (v1/v2/v3)	SI	SI	SI
Monitoreo MLD (v1/v2/v3)	No especifica	No especifica	SI
Spanning Tree (802.1d)	SI	SI	SI
Múltiple Spanning Tree (802.1w)	SI	SI	SI
Link aggregation	SI	SI	SI
Manejo de tramas jumbo	SI	SI	No especifica
Soporte VLAN (802.1q)	SI	SI	SI
N° de vlans que puede manejar	255	255	255
Soporte GVRP	SI	No especifica	SI
Autenticación RADIUS	SI	SI	SI
Autenticación TACACS+	SI	SI	No especifica

Acceso SSH	SI	SI	SI
Seguridad de puerto	SI	SI	SI
Control de aceso por MAC	SI	SI	SI
Vlan invitada	SI	No especifica	SI
Autenticación 802.1x	SI	SI	SI
Control de tormenta de broadcast	SI	SI	No especifica
Control de banda ancha	SI	No especifica	No especifica
Listas de acceso	SI	SI	SI
Acceso web	SI	SI	SI
Acceso vía línea de comandos	SI	SI	SI
Acceso Telnet	SI	SI	SI
Servidor TFTP	SI	SI	SI
SNMP	SI	SI	SI
Monitoreo remoto RMON v1	SI	SI	SI
DHCP Relay	SI	No especifica	SI
Syslog	SI	SI	SI
MDI-X	SI	SI	SI

Mercado Libre Ecuador, 2016. Recuperado de http://computacion.mercadolibre.com.ec

Se recomienda el switch HP/3COM 3226 Superstack, ya que cumple con las características de diseño de la red. El switch 3226 es un conmutador de capa 3 ideal para redes LAN o entornos sucursales. Sus puertos 10/100/1000 permiten la utilizacion de aplicaciones como video y telefonía ip, cctv, administración remota, entre otras.

Se escogió un switch de 24 puertos ya que resulta más económico adquirir dos de estos independientemente de la marca, que uno de 48 puertos.

En conlusión el switch HP/3COM 3226 cumple con las mismas funciones que los switches de la comparativa de acuerdo al diseño de red, pero, a un menor costo.

Switches de acceso

Se compararán las mismas marcas anteriores Cisco, hp/3com y D-Link. Véase la tabla XX.

Tabla 42

Selección de los switches de acceso

MARCA	**CISCO**	**HP/3COM**	**D-LINK**
MODELO	**SG 2960**	**2530**	**DES-1024D**
IMAGEN			
CARACTERÍSTICAS PRINCIPALES			
Switch Layer 2	SI	SI	SI
Puertos 10/100	24	24 (10/100/1000)	24 (10/100/1000)
Puertos 100 BASE T-SFP	2	2	2
Soporte Ipv4	SI	SI	SI
Soporte Ipv6	SI	SI	SI
Capacidad de conmutación agregada	SI	SI	NO
Capacidad de envío de paquetes	6.5Mbps	7 Mbps	No especifica
Monitoreo IGMP (v1/v2/v3)	SI	SI	SI
Monitoreo MLD (v1/v2/v3)	No especifica	No especifica	SI
Spanning Tree (802.1d)	SI	SI	SI
Múltiple Spanning Tree (802.1w)	SI	SI	SI
Link aggregation	SI	SI	SI
Manejo de tramas jumbo	SI	SI	No especifica
Soporte VLAN (802.1q)	SI	SI	SI
N° de vlans que puede manejar	255	255	255
Soporte GVRP	SI	No especifica	SI

Autenticación RADIUS	SI	SI	SI
Autenticación TACACS+	SI	SI	No especifica
Acceso SSH	SI	SI	SI
Seguridad de puerto	SI	SI	SI
Control de aceso por MAC	SI	SI	SI
Vlan invitada	SI	No especifica	SI
Autenticación 802.1x	SI	SI	SI
Control de tormenta de broadcast	SI	SI	No especifica
Control de banda ancha	NO	No especifica	No especifica
Listas de acceso	SI	SI	SI
Acceso web	SI	SI	SI
Acceso vía línea de comandos	SI	SI	SI
Acceso Telnet	SI	SI	SI
Servidor TFTP	SI	SI	SI
SNMP	SI	SI	SI
Monitoreo remoto RMON v1	SI	SI	SI
DHCP Relay	SI	No especifica	SI
Syslog	SI	SI	SI
MDI-X	SI	SI	SI

Mercado Libre Ecuador, 2016. Recuperado de http://computacion.mercadolibre.com.ec

Se recomienda el L2 hp/3com 2530 ya que cumple con los requerimientos de diseño de la red: administrable, soporte de vlan, ssh, telnet, MDI-X. Este switch constituye un equipo de capa 2 apto para redes locales de pequeñas y medianas empresas; ya que representa también una alternativa en costos respecto a cisco y d-link cumpliendo las mismas funciones.

4.11.4.2. Comparación de lectoras biométricas según la marca

Las características mínimas requeridas se enuncian en el apartado de la sección anterior, y los equipos que se muestran en la tabla 43 son los que cumplen con estos parámetros.

Tabla 43

Comparación de lectoras biométricas según la marca

Características Lectoras Biométricas	ONE AF-261	ANVIZ	ZK-teco 628
Imagen			
CPU 32bits		x	x
Capacidad superior a 500 huellas	x	x	x
Identificación por huella	x	x	x
Identificación por contraseña	x	no	x
Tiempo real	x	x	x
Modo red	x	x	no
Costo	120.00	225.00	189.00

Fuente: El autor.

Los equipos adecuados a utilizarse no necesariamente deben ser los más avanzados en tecnología sino aquellos que respondan mejor a los requerimientos de usuario, con el fin de que le permita a la red implementada su expansión posteriormente; en la tabla 44 se muestran los equipos activos a utilizarse, en donde el factor económico jugó un papel importante puesto que se seleccionó los más económicos sin dejar de satisfacer los requerimientos solicitados:

Tabla 44

Precios de los equipos activos

DESCRIPCIÓN	CANTIDAD	Precio Unitario ($)	Precio Total ($)
Switch Hp/3com 3226	1	300.00	300.00
Switch Hp/3com 2530	4	120.00	480.00
Lectoras biométricas ONE	2	120.00	240.00
		Total:	1020

Fuente: El autor.

4.11.5. Resumen total de costos

En este apartado se expone una tabla resumen (véase tabla 45) de los costos que se necesitan para la implementación del proyecto, tomando en cuenta que se han escogido los más económicos debido al presupuesto limitado.

Tabla 45

Resumen total de costos

Descripción	Costo ($)
Cables y Accesorios	745.00
Canaletas y Accesorios	400.99
Racks	624.00
Equipos activos	1020.00
Mano de obra	750.00
Total	3289.99

Fuente: El autor.

Al realizar la suma correspondiente de todos los costos necesarios se concluye que se requieren 3290 dólares para la implementación del proyecto.

CAPÍTULO V

IMPLEMENTACIÓN DE LA RED DE DATOS Y CONTROL DE ACCESO EN LA CÁMARA DE COMERCIO DE LA CIUDAD DE OTAVALO.

En este capítulo se mostrará cómo se ejecutó la implantación del proyecto, considerando que para ello se tuvieron que realizar pequeñas modificaciones en el diseño estipulado debido al presupuesto limitado de la Cámara de Comercio.

El objetivo del proyecto continúa siendo el de tener una red en la cual se conecten todos los equipos de usuarios teniendo un acceso rápido y seguro, además de proveer internet hacia cualquier punto de la red optimizando el procesos de los trabajadores del lugar, restringiendo también el acceso físico de intrusos o personal no autorizado a través de los controles biométricos.

En primer lugar se detallará el proceso de instalación del sistema de cableado estructurado, para el cual se utilizó como medio de transmisión par trenzado UTP categoría 5e en todo el edificio incluyendo el cableado horizontal, de backbone y el requerido para los controles biométricos; para lograr el enrutamiento de todos los cables se empleó canaletas plásticas de diferentes dimensiones de acuerdo al número de cables que deben portar, los cuales se detallan en el capítulo de diseño.

A continuación se procedió a realizar el montaje de los dispositivos en los racks, que para el caso son gabinetes de pared de 6 y 8 unidades de rack para finalmente configurar todos los equipos y realizar las pruebas pertinentes.

5.1. Ponchado del par trenzado

Para el ponchado del cable se consideró la norma T568B y T568A para cada extremo respectivamente, logrando cables cruzados cuya configuración se muestra en la tabla 40. Se debe considerar que para las canalizaciones del cableado horizontal, uno de los extremos es RJ-45 macho que se conectará hacia el pacth panel mientras que el otro extremo es el Jack RJ-45 o conector hembra que se ubicará en el faceplate que conecta a las áreas de trabajo.

El cable que se utilizó es categoría 5e aunque se dejó la recomendación de realizarse con categoría 6A; pero dado que el costo fue uno de los requerimientos se ajustó el proyecto al par trenzado UTP Cat-5e.

Tabla 46

Conexión de pines para cable cruzado

568ª	**568B**
Blanco naranja	Blanco verde
Naranja	Verde
Blanco verde	Blanco naranja
Azul	Azul
Blanco azul	Blanco azul
Verde	Naranja
Blanco café	Blanco café
Café	Café

Ecotec, 2012. Recuperado de ww.ecotec.edu.ec/y/5922_TRECALDE_DOC_00032.pdf

5.1.1. Conector RJ-45

Para comenzar se debe quitar la cobertura del par trenzado y ordenar los hilos de acuerdo a la norma, se igualan los cables y se coloca el conector, se debe asegurar que estos lleguen hasta el fondo del plug para finalmente ajustar con herramienta cripeadora o ponchadora como se muestra en la figura 59.

Figura 59. Ponchado de cable UTP con conector RJ-45. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

5.1.2. Jack RJ-45

El Jack RJ-45 es el correspondiente conector hembra del RJ-45, que al igual que el anterior debe seguir la norma. Los jacks que se utilizaron son de la marca LANPRO; en primer lugar se retira la cobertura del cable UTP y se colocan los diferentes hilos en las ranuras del jack y por último se lo ajusta con unas pinzas de alto impacto o impactool y se coloca el seguro del conector.

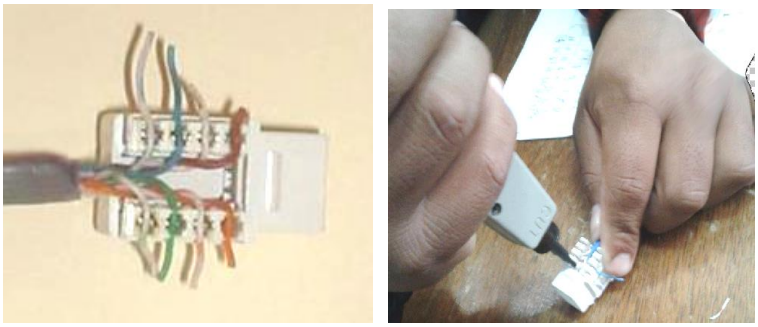


Figura 60. Ponchado de cable UTP con jack RJ-45. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: el autor.

5.2. Instalación de faceplates

Se instalaron faceplates dobles y simples de la marca DEXSON sobre la pared, que comprenden un cajetín blanco de 10x6 centímetros de color blanco, en los cuales se colocaron los jacks RJ-45 propuestos inicialmente con colores azul y rojo pero finalmente todos son blancos que contarán con su etiquetado.

Lo primero que se realizó fue perforar el cajetín dejando el espacio pertinente para que pase el cable UTP y luego atornillarlo hacia la pared como se ilustra en la figura 61.

Figura 61. Instalación de faceplates. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

Los puntos de voz de esta red, no se encuentran inicialmente destinados a telefonía IP, por lo que, a ellos se conectarán teléfonos analógicos pudiendo cambiarse esto a futuro, sin embargo se

presentó un inconveniente dado que los conectores de estos son RJ-11, que si bien, se adaptan al jack RJ-45, no es recomendable forzarlo debido a que es posible que se obstruyan los pines 1 y 8 de este último, por lo que se optó por modificar el conector de los enlaces telefónicos de RJ-11 a RJ-45 (véase figura 62); no obstante en el mercado existen conversores pero por facilidad de costos esta opción no resulta viable.

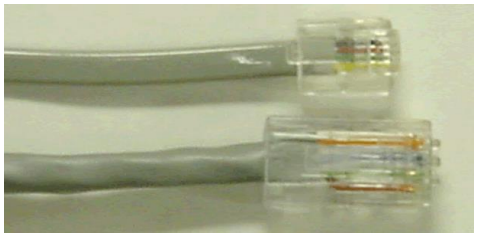


Figura 62. Reemplazo de conector RJ-11 por RJ-45. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

5.3. Canalizaciones

El tipo de par trenzado que se utilizó es UTP 5e 24AGW sólido para los puntos de voz y datos de la marca CONELSA como se puede observar en la figura 63.

Figura 63. Bobina de cable UTP 5e. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: el autor.

Para el enrutamiento de estos, se utilizó canaletas plásticas decorativas DEXSON que se encuentran de forma visible ya que no existe cielorraso. La figura 64 muestra los tres tipos de canaleta.

Figura 64. Canaletas plásticas varias dimensiones. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

El procedimiento consistió en ajustar cada canaleta en la pared con la ayuda de algunas herramientas y la guía del diseño para después empezar a cruzar el par trenzado a través de estas como se puede observar a continuación.

Figura 65. Enrutamiento con canaleta plástica. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

5.4. Racks de Cableado Estructurado

Se instalaron dos rack de pared de 6 y 10 UR y uno de piso de 48 UR de la marca BEAUCOUP de color negro, en éstos se colocaron los patch panels para la recepción del cableado horizontal y demás dispositivos que conforman la red de datos.

Los rack se localizan de acuerdo a la tabla 47:

Tabla 47

Distribución de racks en el edificio

Planta	Nombre del Rack	Dependencia	Medida
Planta Baja	R-PB	Departamento 4	10 UR
Primer Piso	R-PP	Oficina Presidencial	48 UR
Segundo Piso	R-SP	Salón Máximo	6 UR

Fuente: El autor.

5.4.1. Rack planta baja

El rack de la planta baja (véase figura 66) está ubicado en el departamento N°4 que actualmente está totalmente vacío. Este gabinete contiene dos switches de acceso de la marca 3COM.

Figura 66. Rack de pared planta baja. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

5.4.2. Rack primer piso

Se localiza en la oficina presidencial y es el rack es el más importante de la red puesto que aquí se encuentra el switch central en donde se concentran las conexiones de los switches de acceso. (véase figura 67).

En el diseño realizado se propuso conectar los puntos de voz hacia una vlan voz en el switch, sin embargo con el fin de aprovechar las centrales telefónicas que ya tenía la Cámara de Comercio, no se realizó este procedimiento, puesto que estos dispositivos son analógicos, por lo tanto, los enlaces provenientes de los puntos de voz implementados se conectaron directamente desde el patch panel a esta central que fue alojada en el rack.

Figura 67. Rack central del primer piso. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

5.4.3. Rack segundo piso

En el segundo piso se localizan la menor cantidad de puntos de red, siendo 10 en total, puesto que aquí solo se necesita acceso a la red para una dependencia que es el salón máximo. El rack colocado se evidencia en la figura 68.

Figura 68. Rack segundo piso. Red de datos de la Cámara de Comercio de Otavalo.
Fuente: El autor.

5.5. Dispositivos de red

Para la implementación de la red de datos en el edificio de la Cámara de Comercio se utilizaron cinco switches, que antes de enlazarlos al SCE fueron probados con comunicación hacia PCs conectadas en ese momento, probando así el enlace, que resultó exitoso.

5.5.1. Configuración de los dispositivos

A continuación se detalla la configuración de los switches 3com que son los que se utilizaron para la implementación del proyecto.

5.5.1.1. Switch 3COM 3226 L3

Los parámetros a configurar se exponen en la tabla 48:

Tabla 48

Parámetros configurados en el switch 3COM

Parámetro	Configuración
Hostname	CComercio
Usuario administrador	Admin
Password	CCom123
Vlans	10, 20, 30, 40

Fuente: El autor

Para revisar la configuración completa diríjase al ANEXO I.

5.5.1.2. Tarjetas de red de usuarios

La configuración de las tarjetas de red mediante el protocolo TCP/IP se realizó a través de un direccionamiento estático que incluye la dirección IP, máscara, Gateway y DNS.

Esta configuración se debe repetir en cada computadora acorde al direccionamiento establecido, aclarando que para agregar un nuevo dispositivo a la red se debe revisar la tabla de direccionamiento propuesta con el fin evitar inconvenientes y problemas de conexión.

5.6. Control de acceso

Se instalaron controles de acceso biométricos, con el fin de registrar el ingreso del personal autorizado a la Cámara de Comercio de la ciudad de Otavalo, limitado a: presidente, vicepresidente, secretaria, directores financieros y administrativos. La tabla 49 indica los usuarios registrados en el biométrico.

Tabla 49

Usuarios de los controles biométricos

USUARIO	DESCRIPCIÓN
Socios	Miembros pertenecientes a la Cámara de Comercio que al ingresar al establecimiento también son registrados.
Directivos	Presidente, vicepresidente, secretaria y directivos en general. Incluido el administrador que será el encargado de proveer las cuentas de usuario.

Fuente: El autor.

Este control se valida por lectura biométrica basado en la huella dactilar del usuario así como también a través de una contraseña alfanumérica. Las lectoras biométricas poseen una base de datos autónoma en donde se almacena la información del personal autorizado para lograr un control de acceso de forma permanente.

El proceso de enrolamiento del sistema es el siguiente:

- Configuración de la cuenta de administrador.
- Se registran los datos de los usuarios en la base de datos.
- Se enlaza la huella dactilar de los usuarios registrados previamente a la base de datos.
- Se guardan los cambios.

El proceso de utilización por parte de los usuarios se describe a continuación:

- El usuario coloca su dedo en el lector biométrico.
- El lector se encarga de capturar la huella digital y enviar la información de autenticación a la base de datos.
- El sistema verifica la huella
- El usuario accede al lugar y el sistema guarda la información para la generación de reportes.

En el diagrama de la figura 69 se puede observar claramente el funcionamiento:

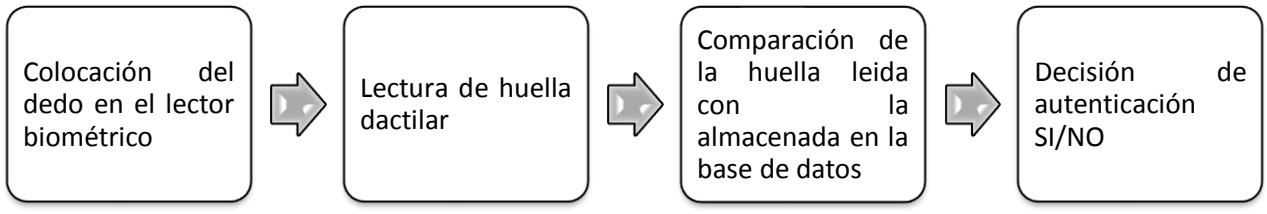


Figura 69. Proceso de funcionamiento del lector biométrico.

Fuente: El autor.

La figura 70 indica el pivote electromagnético instalado en la puerta del edificio.

Figura 70. Pivote electromagnético instalado en la puerta de entrada del edificio. Control biométrico de la Cámara de Comercio de Otavalo.
Fuente: El autor

5.7. Pruebas de funcionamiento

Es importante realizar pruebas de funcionamiento en un ambiente real, para determinar su buen desempeño puesto que asegura su correcta instalación, ya que no basta que la información se transmita de un extremo a otro, sino que lo haga óptimamente.

Es así que, se verificó el acceso a internet desde cada uno de los equipos, a través de diferentes navegadores así como también utilizando el comando ping que constituye el método más fácil para probar la conectividad TCP/IP

5.7.1. Pines exitosos desde un host a su Gateway

La figura 71 muestra la dirección IP configurada en la tarjeta de red de un usuario de la vlan directivos.

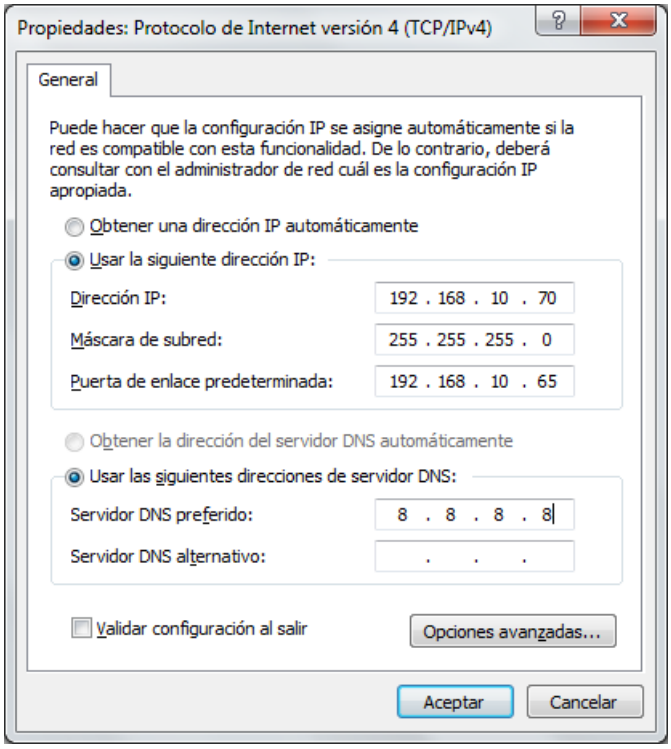


Figura 71. Configuración de tarjeta de red de host vlan directivos (vlan 30). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

La figura 72 muestra un ping exitoso a su Gateway.

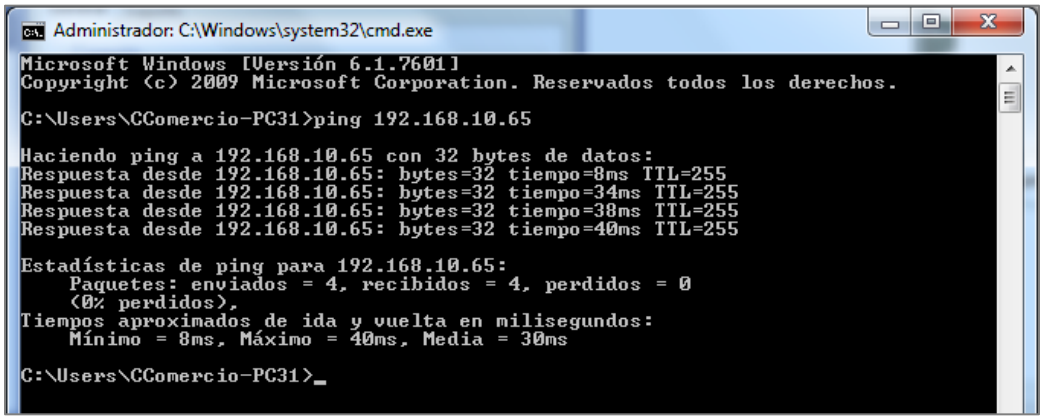


Figura 72. Ping hacia Gateway de host vlan directivos (vlan 30). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

La figura 73 muestra la dirección IP configurada en la tarjeta de red de un usuario de la vlan socios y en la figura 82 se observa el ping realizado con éxito hacia su Gateway.

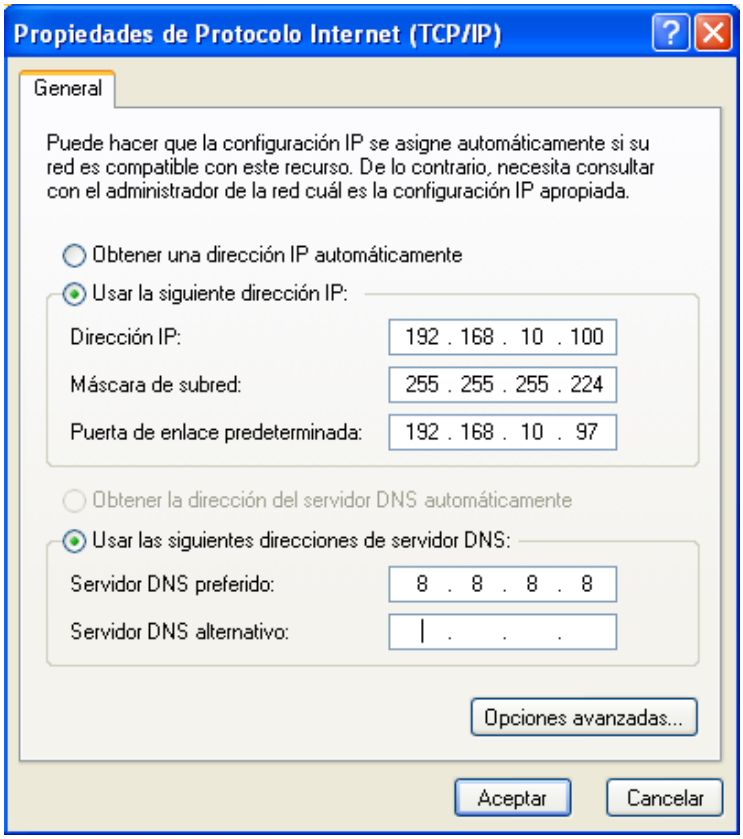


Figura 73. Configuración de tarjeta de red de host vlan socios (vlan20). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

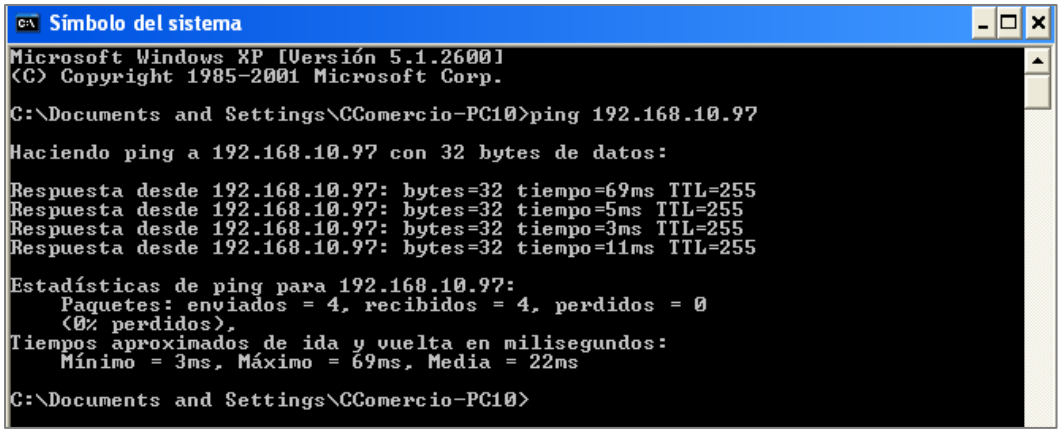


Figura 74. Ping hacia Gateway de host vlan socios (vlan 20). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

5.7.2. Pines exitosos entre hosts de diferentes vlans

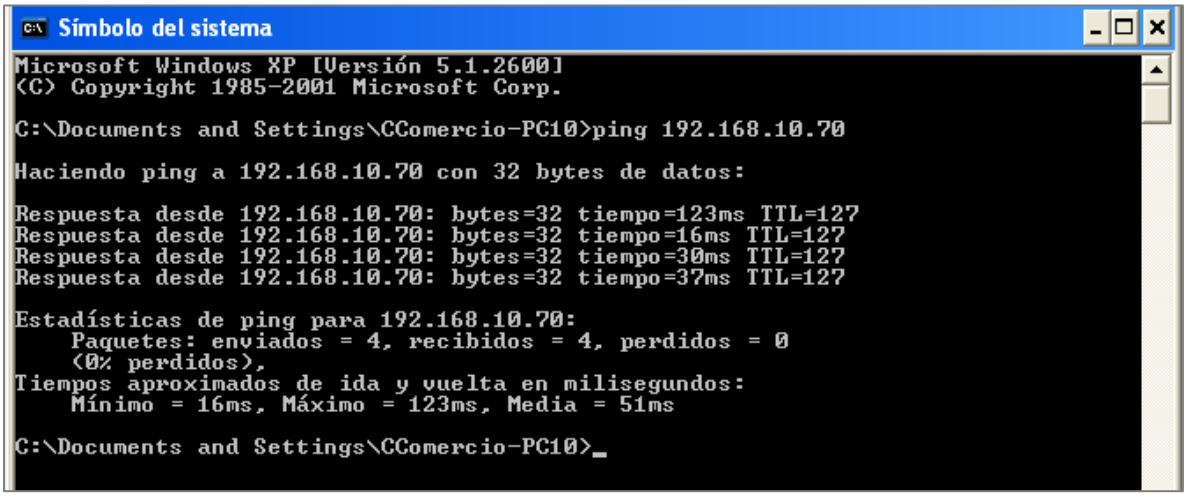


Figura 75. Ping desde host de la vlan socios (vlan 20) hacia host de la vlan directivos (vlan 30). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

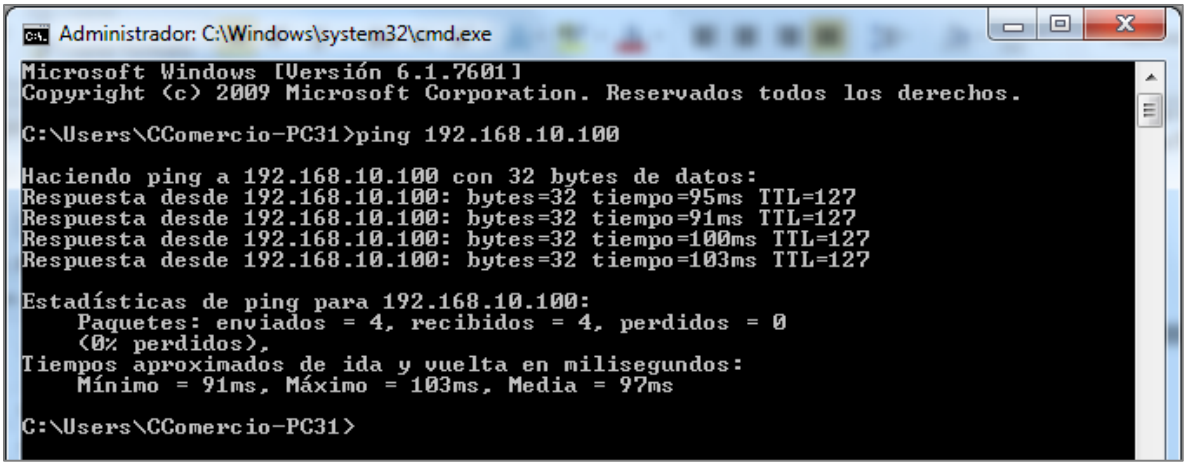


Figura 76. Ping desde host de la vlan directivos (vlan 30) hacia host de la vlan socios (vlan 20). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

5.7.3. Traza entre hosts de diferentes vlans

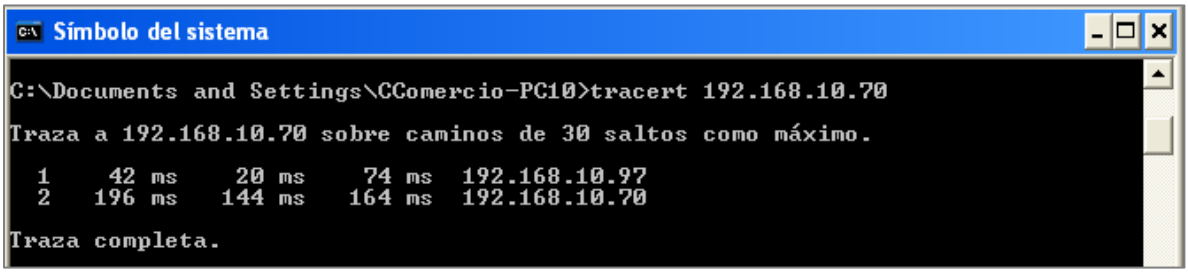


Figura 77. Traza desde host de la vlan socios (vlan 20) hacia host de la vlan directivos (vlan 30). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

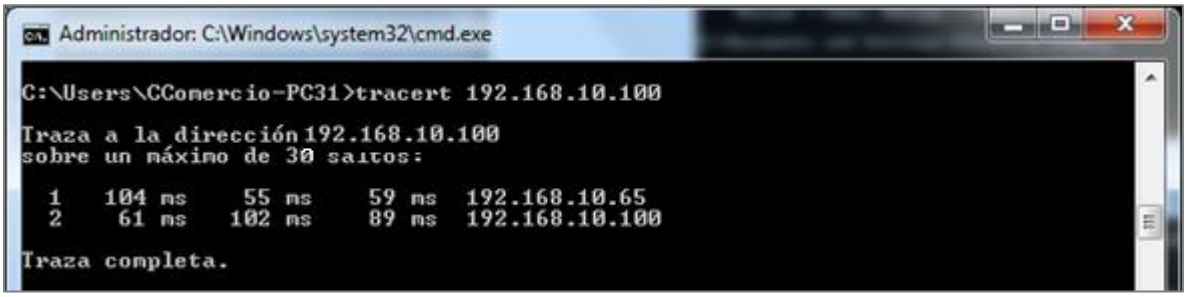


Figura 78. Traza desde host de la vlan directivos (vlan 30) hacia host de la vlan socios (vlan 20). Red de Datos de la Cámara de Comercio de Otavalo.
Fuente: El autor

5.7.4. Ingreso al servidor firewall únicamente desde la PC del presidente y del encargado de red.

Ingreso por SSH a Firewall

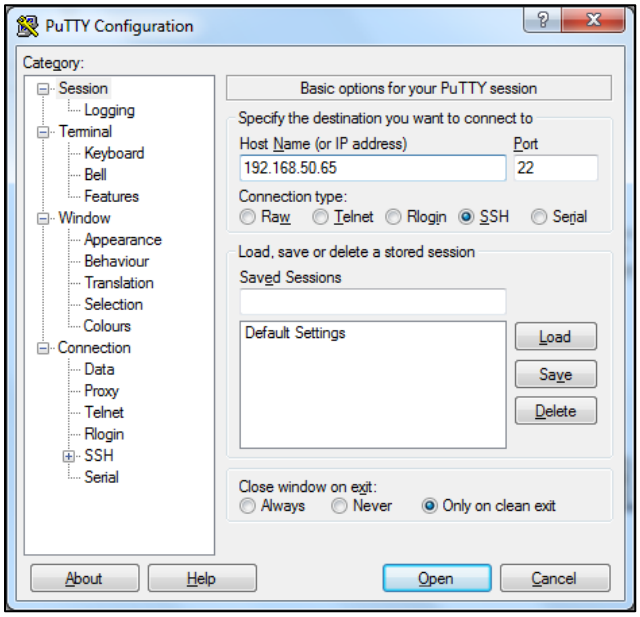


Figura 79. Pruebas de funcionamiento. Configuración de putty.
Fuente: El autor.

Login servidor Firewall

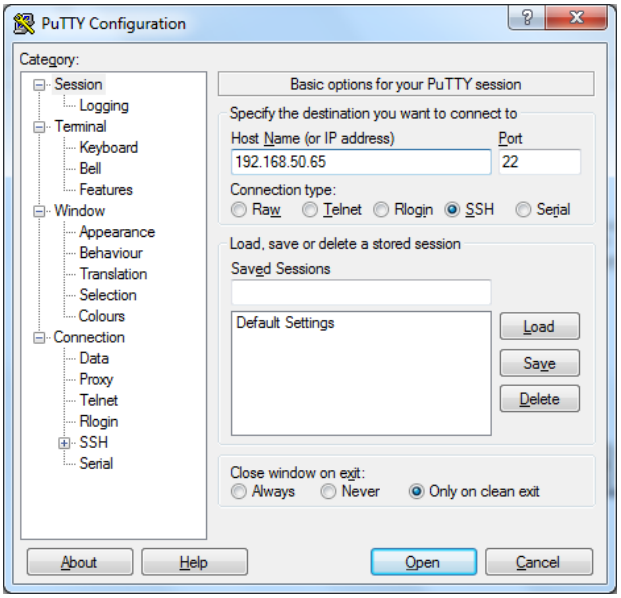


Figura 80. Pruebas de funcionamiento. Configuración de putty.
Fuente: El autor.

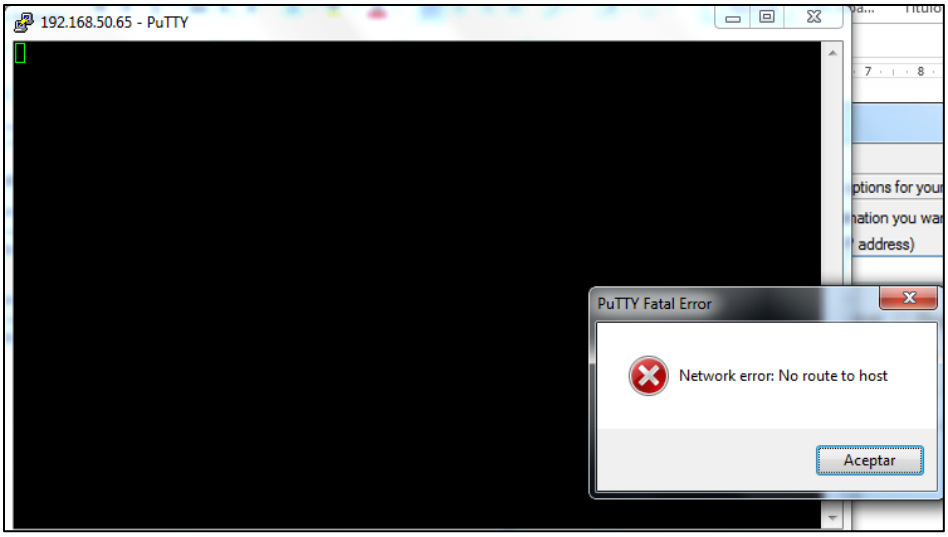


Figura 81. Pruebas de funcionamiento. No hay acceso por ssh desde los hosts de la vlan socios.
Fuente: El autor.

Es importante redireccionar el puerto para poder acceder al firewall desde la PC administrador

Ahora ya es possible acceder desde putty a traves del Puerto 1025

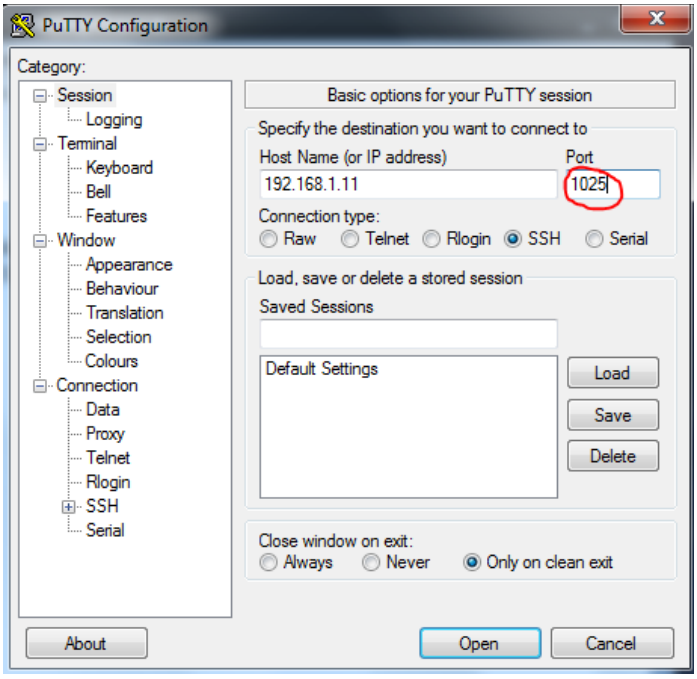


Figura 82. Pruebas de funcionamiento. Configuración de putty con otro puerto.
Fuente: El autor.

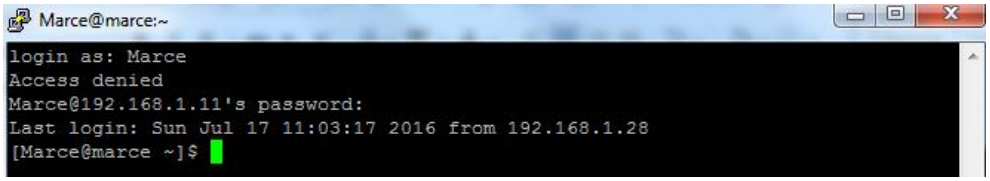


Figura 83. Pruebas de funcionamiento. Ingreso exitoso desde la PC administrador.
Fuente: el autor.

23.1.1. Configuración del servidor proxy en los navegadores.

Para que los hosts de toda la red atraviesen el proxy y las reglas funcionen de acuerdo a lo configurado, es necesario indicar el puerto por el cual está escuchando el servidor, por lo que se procede a configurar el navegador de cada PC.

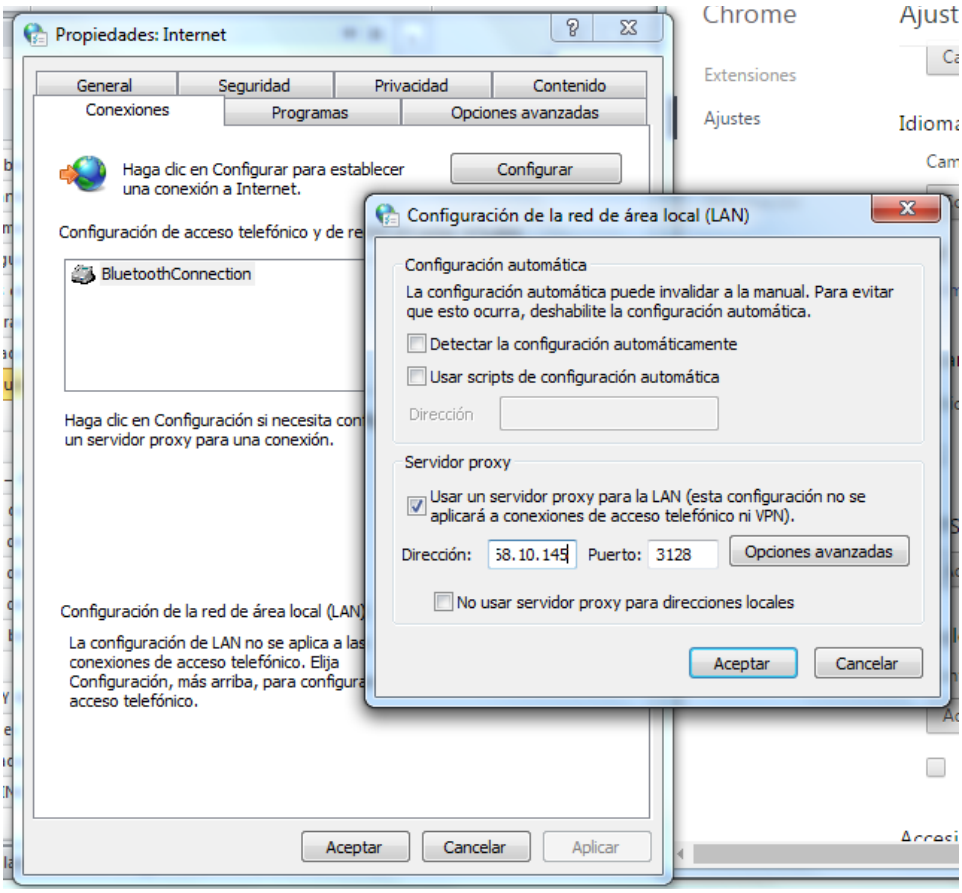


Figura 84. Configuración de servidor proxy en los hosts.
Fuente: El autor.

En propiedades de internet se busca la configuración LAN y se marca la casilla que dice servidor proxy; la dirección IP corresponde la dirección configurada en el servidor Linux y el puerto por default es el 3128.

23.1.2. Políticas de acceso en proxy SQUID

Para saber si los hosts están atravesando el servidor proxy es posible visualizarlo mediante la página: http://www.webtoolhub.com/tn561399-proxy-detector.aspx

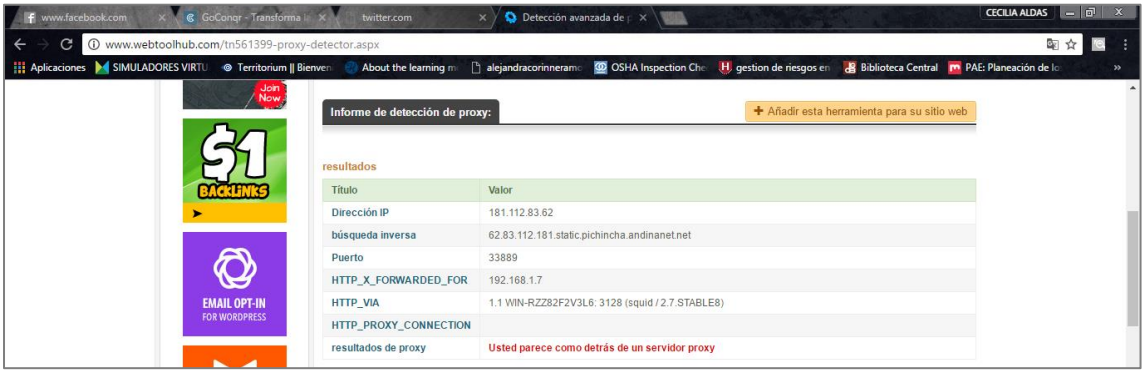


Figura 85. Web page para detectar el proxy.

Fuente: El autor.

ACCESO A SITIOS NO DESEADOS

Política: el acceso a páginas web de contenido inapropiado estará restringido totalmente hacia todos los usuarios.

Mediante un host escogido al azar se intentó ingresar a una página no deseada y se puede observar claramente como el proxy rechaza la conexión.

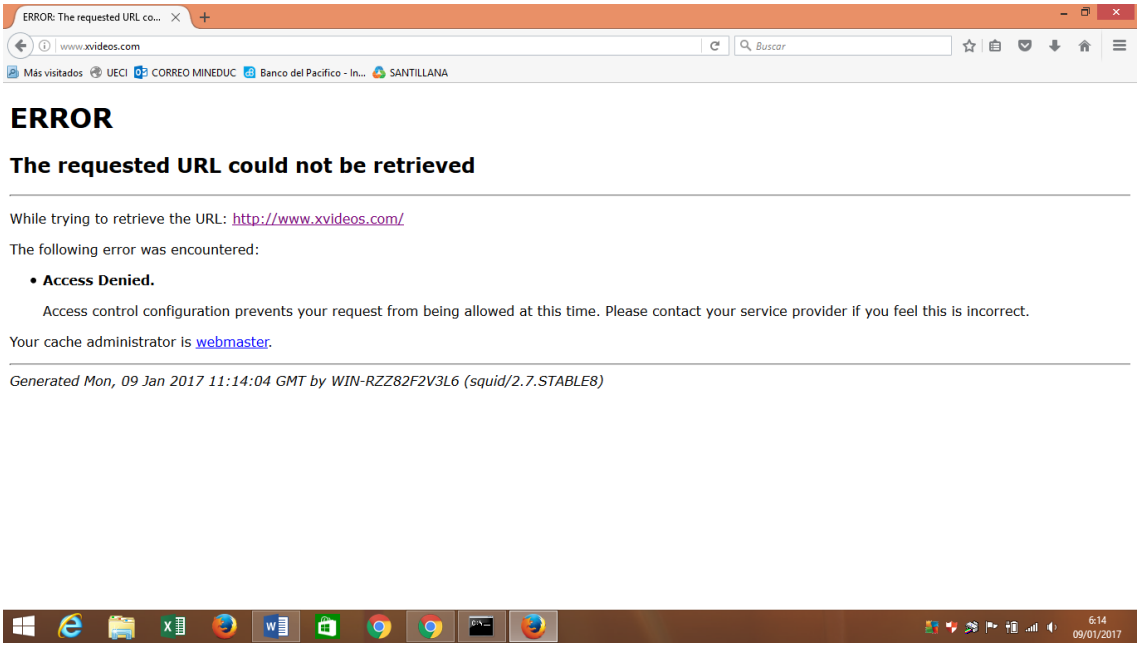


Figura 86. Acceso restringido a sitios no deseados por parte de todos los usuarios.
Fuente: El autor.

CAPÍTULO VI

ANÁLISIS COSTO – BENEFICIO DEL PROYECTO

Los costos y beneficios que trae consigo la realización un proyecto se pueden interpretar de forma tangible o intangible. Siendo los tangibles aquellos medibles en dólares que se acreditan o se adeudan a la organización o empresa; mientras que los intangibles corresponden a todos los procesos que implican una mejora en la toma de decisiones, aumentar la competitividad de la empresa o mejorar la imagen, es decir, son parámetros difíciles de medir pero importantes en el análisis de un proyecto. (Kendall & Kendall, 2011).

6.1. Presupuesto en una organización sin fines de lucro o de tercer sector.

La Cámara de Comercio del cantón Otavalo es una Organización No Gubernamental, es decir carece de un fin lucrativo, sin embargo sí necesita fondos monetarios para su subsistencia; a continuación se detallan algunos términos importantes:

Ganancias: el dinero y ganancias recaudados se devuelven o se retienen en la organización para el cumplimiento de su misión. No se reparte entre sus dueños a diferencia de las organizaciones con fines de lucro.

Bienes: pertenecen exclusivamente a la organización.

Donaciones: corresponde al aporte de cada socio, así como también la ayuda económica de otras organizaciones o sindicatos.

Presupuesto: práctica organizacional cuyo fin es informar en términos económicos y financieros las decisiones contenidas en los planes y proyectos que en su mayoría se basan en estimaciones.

Con estos parámetros se procede a realizar el análisis de costo-beneficio tomando en cuenta que, dado el tipo de organización que representa la Cámara de Comercio (Tercer Sector), no se espera un lucro económico sino más bien social, pero como evidencia de los fondos invertidos se deja en constancia el detalle de costos que está basado en estimaciones, ya que en su mayoría los ingresos dependen de donaciones, por lo que podría variar en la realidad.

6.2. Análisis de costos

El análisis de costos a presentar está basado en el presupuesto invertido que se detalla en el ANEXO I, correspondiente a la factura de compra de estos, por lo que se tomaron en cuenta costos de dispositivos, configuración y mantenimiento.

6.2.1. Costos de dispositivos y materiales del SCE.

En la tabla 50 se detallan los costos realizados para la infraestructura de red así como también para los equipos activos.

Tabla 50

Costos de dispositivos y materiales

Item	Descripción	Cantidad	Precio Unitario	Precio Total
1	Rollo de cable UTP Cat. 5e	5	58.00	290.00
3	Face Plates Doble.	40	1.00	40.00
4	Face Plate Simple	20	1.00	20.00

5	Jack RJ45 Cat.5e	100	2.70	270.00
6	Patch Panels Cat. 5e de 24 Puertos	5	50.00	250.00
7	Organizadores de Cables Horizontal	5	20.00	100.00
8	Gabinete Cerrado de Pared 6UR	3	115.00	345.00
9	Canaleta 60x40	15	8.75	131.24
10	Canaleta 40x25	20	6.25	125.00
11	Angulo Interno 60x40	20	2.25	45.00
12	Angulo Interno 40x25	20	0.85	17.00
13	Angulo Externo 60x40	10	2.25	22.50
14	Angulo Externo 40x25	20	0.85	17.00
15	Adaptador T 60x40	11	2.00	22.00
16	Adaptador T 40x25	25	0.85	21.25
17	Switch 3com 3226	1	300.00	300.00
16	Switch 3com 3c1700	4	120.00	480.00
18	Lectoras biométricas ONE Af-261	2	120.00	240.00
	TOTAL			2735.99

Fuente: El autor. Recopilación de proforma SEDYM S.A. Ver proforma en ANEXO J

6.2.2. Costos de instalación y configuración.

La tabla 51 muestra los costos que implica la mano de obra considerando las horas empleadas para el tendido de cable y luego la configuración de los equipos.

Tabla 51

Costos de instalación y configuración

Item	Descripción	Cantidad	Precio Unitario	Precio Total
1	Instalación del SCE	1	750	750
3	Configuración de equipos	1	200	100
4	Pruebas de funcionamiento	1	100	100
5	Varios	1	50	50
	TOTAL			450

Fuente: El autor. Recopilación de proforma SEDYM S.A. Ver proforma en ANEXO I

No obstante es importante recalcar que los costos de instalación y configuración no se tomarán en cuenta puesto que forman parte del trato realizado con la organización y el presente trabajo de grado.

6.2.3. Costos de mantenimiento

Estos costos están relacionados con el cuidado y mantenimiento de la infraestructura de red, los equipos activos, actualizaciones de software o nuevas configuraciones. Los costos de mantenimiento se muestran en la tabla 52.

Tabla 52

Costos de mantenimiento

Item	Descripción	Cantidad	Precio Unitario	Precio Total
1	Mantenimiento de hardware y software	1	500	500
	TOTAL			500

Fuente: el autor.

6.2.4. Inversión inicial

Corresponde al dinero invertido en el proyecto cuyo valor se indica en la tabla 47.

Tabla 53

Inversión inicial

Item	Descripción	Cantidad	Precio Unitario	Precio Total
1	Equipos de red y materiales de cableado estructurado	1	2735.99	2735.99
	TOTAL			2735.99

Fuente: El autor.

Redondeando, se obtiene un total de 2736 dólares invertidos.

6.2.5. Rentabilidad del proyecto

Para determinar qué tan rentable ha resultado el proyecto se procede a calcular el flujo de caja que no es más que el cálculo que evidencia la recuperación de la inversión a través del valor actual neto (VAN), tasa interna de retorno (TIR), relación costo/beneficio (B/C).

6.2.5.1. Flujo de Caja

El flujo de caja registra el dinero que entra y sale de un negocio durante un tiempo específico de modo que se sea posible conocer la liquidez de una organización (Kendall & Kendall, 2011) según la tasa de inflación del 1.31% obtenida de la página del Banco Central del Ecuador se realizó el flujo de caja proyectado en la tabla 48.

.

6.2.5.2.Valor actual neto

Consiste en la actualización de cobros y pagos de un proyecto o inversión y así calcular su diferencia. Para ello trae todos los flujos de caja al momento presente descontándolos a un tipo de interés determinado. (Kendall & Kendall, 2011)

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{(1+k)^t} = -I_0 + \frac{F_1}{(1+k)} + \frac{F_2}{(1+k)^2} + \cdots + \frac{F_n}{(1+k)^n} \qquad (10)$$

Ft: son los flujos de dinero en cada periodo t

Io: es la inversión realiza en el momento inicial (t = 0)

n: es el número de periodos de tiempo

k: es el tipo de descuento o tipo de interés exigido a la inversión

6.2.5.3.Tasa interna de retorno

Es la tasa efectiva anual compuesto de retorno o tasa de descuento que hace que el valor actual neto de todos los flujos de efectivo (tanto positivos como negativos) de una determinada inversión igual a cero. (Kendall & Kendall, 2011)

$$-\mathrm{Io} + \sum_{n=1}^{m} \frac{Fn}{(1+r)^n} = 0 \qquad (11)$$

t: el tiempo del flujo de caja

i: la tasa de descuento (la tasa de rendimiento que se podría ganar en una inversión en los mercados financieros con un riesgo similar) .

Fn: el flujo neto de efectivo (la cantidad de dinero en efectivo, entradas menos salidas) en el tiempo n.

6.2.5.4. Relación costo/beneficio

La relación costo beneficio toma los ingresos y egresos presentes netos del estado de resultado, para determinar cuáles son los beneficios por cada dólar que se sacrifica en el proyecto.

$$\frac{B}{C} = \frac{\sum_1^n VANn}{Io}$$

El registro de ingresos y egresos se evidencian en el flujo de caja, sabiendo que, está basado en estimaciones puesto que sus fondos monetarios dependen también de otros factores y organizaciones como por ejemplo: inflación del país, variaciones y tendencias de la moneda e relación a otros países, relaciones con otros sindicatos u organizaciones, entre otras; por lo que se lo ha realizado con el fin de llevar el control y examinar el desarrollo del presente trabajo de grado.

Tabla 54
Flujo de caja

RUBRO	0	PROYECCIÓN ANUAL 1	2	3	4	5
Inversión inicial	-2735,99					
Aportes socios		2592,00	2625,96	2660,36	2695,21	2730,51
Donaciones de Organizaciones		300,00	303,93	307,91	311,95	316,03
Deudas por cobrar a 2 años incl. Impuestos		800,00	800,00	0,00	0,00	0,00
Ahorro de mano de obra por implementación		750,00	0,00	0,00	0,00	0,00
Ahorro de contratación personal de seguridad		768,00	778,06	788,25	798,58	809,04
Ahorro instalaciones provisionales de equipos		300,00	303,93	307,91	311,95	316,03
Consumo de energía eléctrica		-1124,32	-1139,05	-1153,97	-1169,09	-1184,41
Mantenimiento de hardware y software		-1920,00	-1945,15	-1970,63	-1996,45	-2022,60
FLUJO NETO	-2735,99	2465,68	1727,67	939,82	952,14	964,61
VA Ingresos		4919,64	3836,00	2892,98	2616,86	2367,09
Va Egresos		-2718,15	-2458,71	-2224,03	-2011,76	-1819,74
Valor actual		2201,50	1377,29	668,95	605,10	547,35

Fuente: El autor.

Con la información de la tabla 49, el valor de inversión inicial de 2735,99, la tasa de inflación del 1,31% una tasa de interés del 12% se obtienen los siguientes resultados:

VALOR ACTUAL NETO	2664,19
TIR	58%
B/C	1,4

INTERPRETACIÓN

- El Valor Actual Neto (VAN) de 2664,19 dólares representa el dinero que generará la inversión del proyecto en un período de 5 años más allá del retorno del capital invertido, transformado a un valor actual, puesto que no es lo mismo 1000 dólares actualmente, que 1000 dólares dentro de 10 años. Para que un proyecto resulte viable su VAN debe ser superior a cero; no obstante entre mayor sea el VAN, las ganancias también serán mayores
- La tasa interna de retorno (TIR) del 65% expresa que si se sube el interés hasta un valor inferior cercano al 65% el proyecto seguirá resultando viable; sin embargo entre mayor sea la TIR más ganancias representa el proyecto.
- La relación beneficio/costo expresa que la organización tendrá una rentabilidad positiva dentro de un período de 5 años, siendo que, por cada dólar invertido se ha recuperado su valor y además se obtendrá una ganancia de 0,4. Un valor superior a 1 demuestra la viabilidad del proyecto.

6.3. Análisis de beneficios

Los beneficios del diseño e implementación de la red de datos y control de acceso biométrico para el edificio de la Cámara de Comercio en Otavalo se presentan en mayor parte de forma intangible o denominados también beneficios sociales; y se describen en los siguientes puntos:

- Mayor satisfacción por parte del personal que labora en el lugar, puesto que sus actividades se optimizaron ahorrando tiempo, los minutos que se podría tardar una persona en transferir información del primero al segundo piso manualmente, ahora se lo realiza instantáneamente.
- Mejora de la seguridad en los niveles físico y lógico, minimizando la posibilidad de intrusión por parte de extraños que puedan hurtar información o hardware valioso.
- Mediante los biométricos se logra una mayor seguridad ya que se tiene más control de los usuarios que ingresan al establecimiento.
- Mayor disponibilidad de la información que aloja la Cámara de Comercio, la cual sirve entre otras cosas, para proporcionar información variada a los residentes y visitantes en general que incluye folletos, mapas, revistas, información de transporte y otros.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se implementó la Red de Datos y Control de Acceso biométrico en base a los requerimientos obtenidos y basado en las normas ANSI/TIA/EIA 568-B y 569-A mejorando así la infraestructura tecnológica del edificio de la Cámara de Comercio.
- Se realizó el estudio de la situación actual para determinar los requerimientos de usuario y así plantear el diseño óptimo.
- Las características de infraestructura del edificio y las exigencias de los usuarios fueron los parámetros que definieron la implementación final del proyecto, no obstante, para el diseño del presente trabajo de grado se cumplió con los puntos descritos en las normas de cableado estructurado ANSI/TIA/EIA 568-B y 569-A; sin embargo sí existieron variaciones mínimas al momento de la implementación debido a características físicas propias de la infraestructura.
- En el edificio de la Cámara de Comercio se necesitaban 33 puntos de red para las áreas de trabajo que se están ocupando, sin embargo tomando en cuenta la expansión futura y como resultado del estudio de la situación actual se pudo determinar que el número de puntos de red requeridos son 75, distribuidos en todo el edificio, incluyendo puntos de red requeridos para los puestos de trabajo, puntos de red adicionales en base a la dependencia en metros cuadrados y al porcentaje de crecimiento de usuarios en un período de 10 años; y puntos de red en los pasillos para una posible implantación de puntos de acceso inalámbricos.
- La segmentación de la red en pequeñas redes lan virtuales (vlans) que se realizó en la red de la Cámara de Comercio implicó un procedimiento efectivo para prevenir la

congestión de tráfico, haciendo un uso eficiente del ancho de banda además de que proporciona seguridad en la red, por lo que, en el diseño realizado se planteó este mecanismo como solución para reducir el dominio de broadcast hasta en un 60% dependiendo del envío de paquetes.

- En la implementación de la red, se creó la vlan voz, sin embargo los puntos de voz se conectaron a una central telefónica analógica, debido a que la empresa carece de equipos o servidores que soporten el protocolo IP, separándolos físicamente de los puntos de red, dejando los switches únicamente para estos últimos, sin descartar la posibilidad que a posteriori sea posible brindar el servicio de telefonía IP adquiriendo nuevos dispositivos de red y realizando un mínimo cambio en el direccionamiento.
- Los dispositivos biométricos actuales presentan características que pueden utilizarse acorde a los requerimientos, como por ejemplo, permitir configuraciones dependiendo del rol como vacaciones o permisos, satisfaciendo todas las necesidades solicitadas en la Cámara de Comercio concluyendo que no siempre el dispositivo más costoso resulta ser el mejor.
- Mediante los cálculos del VAN, TIR y relación B/C se determinó que el proyecto sí es viable recuperando la inversión en un periodo de dos años y obteniendo una ganancia de 1,4 anual por cada dólar invertido.

Recomendaciones

- Para lograr un diseño óptimo de cableado estructurado se recomienda tomar en cuenta la estructura física del edificio, los requerimientos de usuario y el presupuesto a invertir, para posteriormente realizar el diseño y ajustarlo a las normas y recomendaciones propuestas por los organismos que rigen los sistemas de cableado estructurado.

- En caso de que se requiera la instalación de nuevos puntos de red o dispositivos de telecomunicaciones se sugiere tomar en cuenta los planos y diseños ya elaborados que se encuentran en los anexos para que sirvan como guía en la solución requerida, así como también la revisión y/o modificación de las políticas de seguridad actuales.
- En el momento de almacenar las huellas dactilares de los usuarios se recomienda realizarlo varias veces con la mayor calidad posible, regulando el brillo del dispositivo biométrico y al repetir el proceso verificar que el lector biométrico muestre la menor tasa de error al comparar la imagen actual con la anterior.
- Es importante orientar a los trabajadores y personal en general de cualquier empresa que maneje sistemas de control de acceso tecnológico acerca de cómo utilizarlos correctamente, a través de recomendaciones, a fin de ahorrar el tiempo de registro al validar exitosamente su ingreso a partir del primer intento.
- Es muy necesario mantener limpia la zona de lectura de los biométricos , caso contrario proporcionarán lecturas erróneas e ilegibles para el sistema que almacena la base de datos.
- Realizar las pruebas de funcionamiento de la red mediante ténsters midiendo los parámetros de desempeño del par trenzado para garantizar el buen desempeño de la infraestructura de red.
- A medida que se vaya expandiendo la red o la cantidad de usuarios se recomienda reemplazar los switches actuales por dispositivos que permitan el soporte de las nuevas tecnologías y exigencias proporcionando una mayor capacidad de conexión.

- En caso de que se ejecute algún cambio en la red de datos de la Cámara de Comercio es vital actualizar la documentación concerniente para que quede un registro claro de lo que se modificó y sea posible su utilización como guía a futuro.
- Es recomendable llevar una bitácora de las modificaciones realizadas en el manual de políticas con el propósito de registrar y controlar los sucesos que llevaron a dicho cambio. La falta de estos registros puede ocasionar pérdida de tiempo.

GLOSARIO DE TÉRMINOS

ANSI

American National Standard Institute (Instituto Nacional Americano De Estándares). Se trata de una organización americana que se encarga de la formulación de normas en diversos sectores técnicos.

Antivirus

Programa que busca y en algunos casos elimina los virus informáticos que pueden haber infectado un dispositivo de almacenamiento

Aplicación

Software diseñado para solucionar un problema o realizar un tipo de trabajo en específico. Generalmente se encarga de la automatización de tareas de un usuario.

Archivo

Conjunto de datos (bits) que se almacenan en un dispositivo.

Backup

Respaldo o copia de seguridad que se realiza para evitar la pérdida de información.

Bps

Bits por segundo. Medida utilizada para calificar a la velocidad de transmisión.

Conexión

Circuito que permite la comunicación entre dos o más dispositivos.

Enlace

Camino o conexión que puede ser física o lógica desde un dispositivo a otro.

Fichero

Unidad mínima de almacenamiento de información. Un archivo suele considerarse un fichero

Firewall

Sistema que permite o restringe la comunicación entre una red y el internet a través de la configuración de políticas de seguridad.

Host

Dispositivo que permite la comunicación hacia la red.

Implementación

Es la ejecución o puesta en marcha de un plan, es decir llevar a la práctica un trabajo diseñado con anterioridad.

Internet

Internet es un conjunto de redes que se conectan entre sí, a nivel global con el objetivo de compartir información a través de diferentes dispositivos.

IP

Protocolo de Internet de bajo nivel, que pertenece a la capa Internet de TCP/IP

ISO

Organización Internacional de Estándares (International Standard Organization) formada por varios organismos a nivel mundial que se encargan de la creación de estos.

ISP

Proveedor de Servicios de Internet (Internet Service Provider)

LAN

Local Area Network. Red de Area Local diseñada para la comunicación en un edificio u organización.

OSI

Interconexión de Sistemas Abiertos (Open Systems Interconnection). Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO.

Proxy

Servidor encargado de redireccionar el puerto por default para lograr la conexión a internet; actuando como dispositivo intermedio entre los usuarios de la LAN y el internet.

RAM

Memoria de Acceso Aleatorio (Random Access Memory) en donde la información que se almacena es provisional, pudiendo grabarse una y otra vez.

RJ-45

Conector o plug de cable Ethernet con 8 pines.

Router

Enrutador que se encarga de dirigir los paquetes hacia diferentes redes.

Switch

Dispositivo conmutador que conecta diferentes segmentos de red pudiendo incluso realizar funciones de un enrutador al operar en capa 3.

Topología

Disposición física o lógica de los dispositivos que conforman una red.

URL

Universal Resource Locator. Nombre genérico de la dirección en Internet, Indica al usuario dónde localizar un archivo HTML determinado, en la Web.

UTP

Par trenzado sin blindaje utilizado como medio de transmisión en redes.

VLAN

Red Lan Virtual en donde los nodos lógicamente pertenecen a un mismo segmento de red pero físicamente se encuentran en diferentes segmentos.

BIBLIOGRAFÍA

1244, R. (s.f.). *Site security Handbook.*

Andrade Sánchez, P. (2014). *Manual de Funciones por procesos para la Cámara de Comercio del cantón Otavalo, Provincia de Imbabura.* Ibarra.

ANIXTER. (2008). Obtenido de Subsystems of structured cabling: https://www.anixter.com/en_mx/resources/literature/techbriefs/the-six-subsystems-of-a-structured-cabling-system.html

Anixter. (2015). *Wire & Cable*. Obtenido de https://www.anixter.com/en_us/services-and-solutions/solutions/building-technologies/enterprise.html

ANSI. (2016). *ANSI: Standards activities.* Obtenido de https://www.ansi.org/standards_activities/overview/overview?menuid=3

Ardita, J. C. (2012). *Security System & Ex-Hacker.* Obtenido de Entrevista para Cybsec S.A: http://www.cybsec.com

Black, U. (1997). *Redes de computadores: protocolos, normas e interfaces.*

CentOS. (2016). *Project Centos*. Obtenido de https://www.centos.org/

CISCO. (2005). Obtenido de http://www.cisco.com/web/ES/solutions/es/vpn/index.html

CISCO. (2014). *Internet of everything*. Obtenido de http://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus_wp_cte_es-xl_42333.pdf

Cisco Networking Academy Program. (2003). Obtenido de https://www.academia.edu/10355935/CCNA_Discovery_Networking_para_el_hogar_y_peque%C3%B1as_empresas

CISCO Web Support. (2012). Obtenido de http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

Coopersmith, J. (2015). *Faxed.* Obtenido de The Rise and Fall of the Fax Machine: http://www.garretwilson.com/essays/computers/group3fax.html

EC&M. (2016). *Electrical Construction and Maintenance.* Obtenido de http://ecmweb.com/ntc-yellow-book-cctv-systems-design-and-installation

Ecotec. (2012). *Cableado de redes*. Obtenido de www.ecotec.edu.ec/y/5922_TRECALDE_DOC_00032.pdf

EIA. (2016). *Electronic Industry Association.*

Escrivá Gascó, G., & Romero Serrano, R. M. (2013). *Seguridad informática.* London: MacMillan.

Frazer, C. (2002). Structured cabling comes of age. *IEEE Review*.

Gigabit Ethernet and structured cabling. (Agosto de 2008). Obtenido de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=866884&isnumber=18760

Hayes, J., & Rosenberg, P. (2009). *Cableado de redes para voz, video y datos: Planificación, diseño y construcción.* Cengage Learning.

Hidrobo Moya, J. M. (2015). *Telecomunicaciones: tecnologías, redes y servicios.*

HUAWEI. (2013). *Huawei User Guide*. Obtenido de http://www.manualslib.com/manual/73171/Huawei-Echolife-Hg520c.html?page=2#manual

IEEE. (2016). *IEEE: Institute of Electrical and Electronics Engineers.* Obtenido de https://www.ieee.org/index.html

INEC. (diciembre de 2016). Obtenido de http://www.ecuadorencifras.gob.ec/el-171-de-las-empresas-realizan-comercio-electronico-en-ecuador/

INFORMATICAHOY. (2016). Obtenido de http://www.informatica-hoy.com.ar/redes/contenidos-redes.php

ISO. (2016). *ISO: Internacional Organization for Standardization.* Obtenido de https://www.iso.org/iso-9001-quality-management.html

ISO27000. (2016). *Estándar ISO27000 en español*. Obtenido de www.iso27000.es

Katz, M. (2013). *Redes y seguridad, apoyo en la web.* Alfaomega.

Kendall, K. E., & Kendall, J. E. (2011). *Análisis y diseño de sistemas* (Sexta edición ed.). México: Pearson Educación.

Lamus, F. (2014). *Global News Room Cisco*. Obtenido de http://globalnewsroom.cisco.com/es/la/press-releases/cisco-ocupa-el-primer-lugar-en-el-mercado-de-segur-1156779

Líderes, R. (2016). Obtenido de http://www.revistalideres.ec/lideres/negocios-activan-inseguridad.html

Manual de Cableado Estructurado. (2015). Obtenido de http://dgtic.tabasco.gob.mx/sites/all/files/vol/dgtic.tabasco.gob.mx/fi/Cableado%20Estructurado.pdf

Martínez Ferreira, M. (2014). Análisis de Sistemas. En Intranet, *Intranet o Internet.* Caracas.

ONU. (2016). *Declaración Universal de los Derechos Humanos.*

PC Magazine. (2016). Obtenido de http://www.pcmag.com/article2/0,2817,2372364,00.asp

Plaza, M., & Janés, P. (2013). *La galaxia Internet – Reflexiones sobre Internet, empresa y sociedad.*

Plevyak, T. (2015). *Telecommunications Management Network.* Wiley-IEEE Press.

Reid, A., & Lorenz, J. (2016). *Networking para el hogar y pequeñas empresas.* Madrid: CISCO Systems.

Rivera, J. D. (2016). *Fundamentos de Redes Informáticas.* México: IT Campus Academy.

Shane, D. (2010). *HP Media Notices*. Obtenido de http://phx.corporate-ir.net/phoenix.zhtml?c=61382&p=irol-newsArticle&ID=1354403&highlight=

Soto Gil, J. L. (22 de Enero de 2015). *Manual para el curso de Diseño de Redes.* Obtenido de http://www.portatiles-pcs.net/files/documents/MANUAL-PARA-EL-CURSO-DE-DISE%C3%91O-DE-REDES-2015.pdf

Stallings, W. (2014). *Data and computer communications* (Vol. 10). Madrid: PearsoN Education.

Structured cabling and EMC. (2014). Obtenido de EMC- It's Nearly All About the cabling: : http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1300117&isnumber=28884

Tanenbaum, A. S. (2012). *Redes de computadoras.* México: Pearson Educación.

Technologies, I. (2016). Obtenido de http://www.inh.com.co/index.php?page=./HTML/seguridadelectronica&subpage=./HTML/controldeacceso

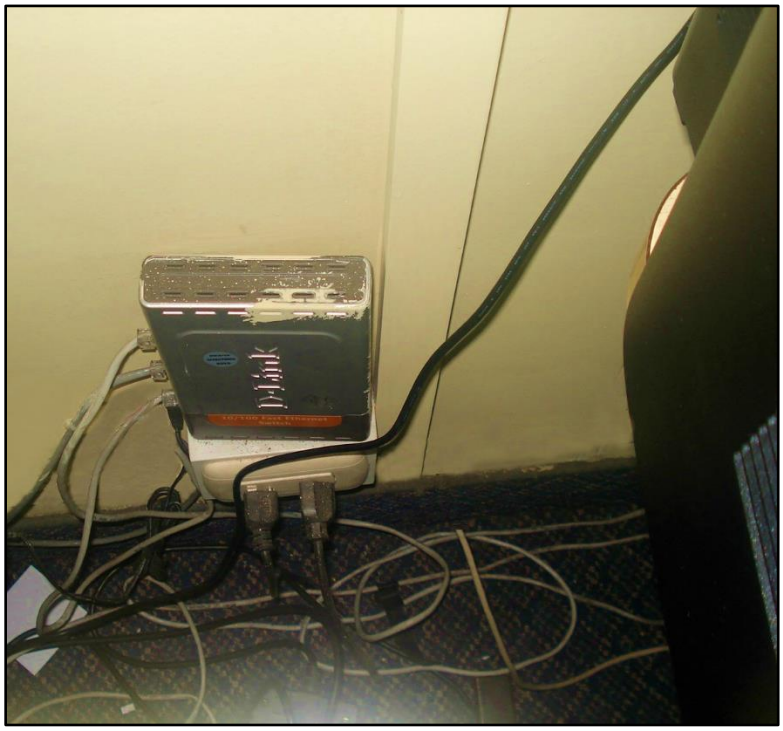
TIA. (2016). *Advancing Global Communications.* Obtenido de http://www.tiaonline.org/standards/tia-digital-training-library

Windows, M. (2012). Obtenido de http://windows.microsoft.com/es-419/windows/what-is-bluetooth-personal-area-network#1TC=windows-7

ANEXO A. Situación actual de la red y del sistema de cableado estructurado.

Router/módem ADSL HUAWEI en un lugar inestable. Único dispositivo de red.

Switch D-Link que se coloca eventualmente.



Par trenzado enredado que da lugar a desconexiones.

ANEXO B. Entrevistas y encuestas realizadas.

Las encuestas realizadas se efectuaron en una sola ocasión a través de un mismo documento; pero para efectos de análisis se separaron las preguntas en dos bloques, siendo el primero correspondiente a los requerimientos de usuario y el segundo al levantamiento de políticas.

ANEXO B.1. Requerimientos de usuario para el levantamiento de la red.

FORMATO DE ENCUESTAS REALIZADAS A SOCIOS Y EMPLEADOS

Muy buenos días, esta encuesta tiene como finalidad conocer su percepción acerca de la infraestructura y tecnología del edificio de la Cámara de Comercio del cantón Otavalo, para determinar los parámetros que requieren los usuarios del lugar y levantar una red de datos eficiente.

Nombre: …….

Cargo: ……..

E-mail: …….....

Indicaciones

El cuestionario siguiente contiene dos bloques, en el primero encontrará interrogantes que usted deberá valorar de acuerdo a la tabla que se muestra a continuación. Siendo el nivel 1 correspondiente a la calificación mínima y el nivel 5 a la máxima.

Nivel	Estado	Descripción
1	No o no existe	Carencia total
2	Impreciso o negligente	Se realiza de forma descuidada.
3	Medianamente o definido	Es aceptable
4	Ideal o administrable	Permite modificaciones de acuerdo a las exigencias.
5	Sí u óptimo	Se ejecuta de manera satisfactoria.

Mientras que el segundo bloque deberá seleccionar alguna de las opciones planteadas y si le resulta necesario puede añadir observaciones.

Bloque I.

Item	Pregunta	Nivel (1-5)
1	Actualmente todos los usuarios comparten información entre sí a través de sus computadoras locales dentro de la empresa mediante una conexión física o inalámbrica. (red)	
2	Le gustaría compartir información mientras se moviliza dentro de la empresa además de hacerlo a través de su computadora personal.	
3	La infraestructura actual abastece a todos los usuarios de la Cámara de Comercio. (En cuanto a espacio en metros cuadrados).	
4	Su equipo de trabajo (computadora) cuenta con un sistema de prevención de malware o antivirus.	
5	El edificio tiene algún tipo de seguridad o restricción para su acceso.	

ANEXO B.2. Requerimientos para el levantamiento de políticas de acceso.

Bloque II.

1. **¿Con qué frecuencia accede a internet dentro de la empresa? (Seleccione una opción)**
    a. Todos los días, todo el tiempo.
    b. Todos los días, más de dos horas diarias.
    c. Menos de una hora.
    d. No utilizo redes sociales.

2. **¿Cuáles son los sitios web que más visita? (Seleccione hasta dos opciones)**
    a. Redes sociales.
    b. Sitios de marketing.
    c. Noticias.
    d. Otros……

Si entre sus opciones marcó el literal a) continué con el cuestionario; caso contrario se le agradece por su participación. Si desea puede comentar sus sugerencias relacionadas con el tema.

3. **¿Para qué utiliza principalmente las redes sociales dentro de la empresa? (Puede seleccionar hasta 2 opciones)**
    a. Gestionar servicios o productos.
    b. Visualizar a la competencia.
    c. Contactar posibles clientes
    d. Comunicarse con otros trabajadores del lugar.
    e. Chatear con amigos.

4. **¿En qué redes sociales posee una cuenta? (Seleccione las que sean necesarias)**
    a. Facebook.
    b. Twitter.
    c. Youtube.
    d. Instagram.
    e. Otras……..

5. **¿Le parecería útil que el acceso a sitios web sea controlado a través de un dispositivo de software o hardware con el fin de optimizar el acceso a internet?**
    a. Por supuesto, resultaría de gran ayuda.
    b. No, el control podría ser manual.
    c. Me resulta indiferente.
    d. Otros……

TABULACIÓN DE DATOS

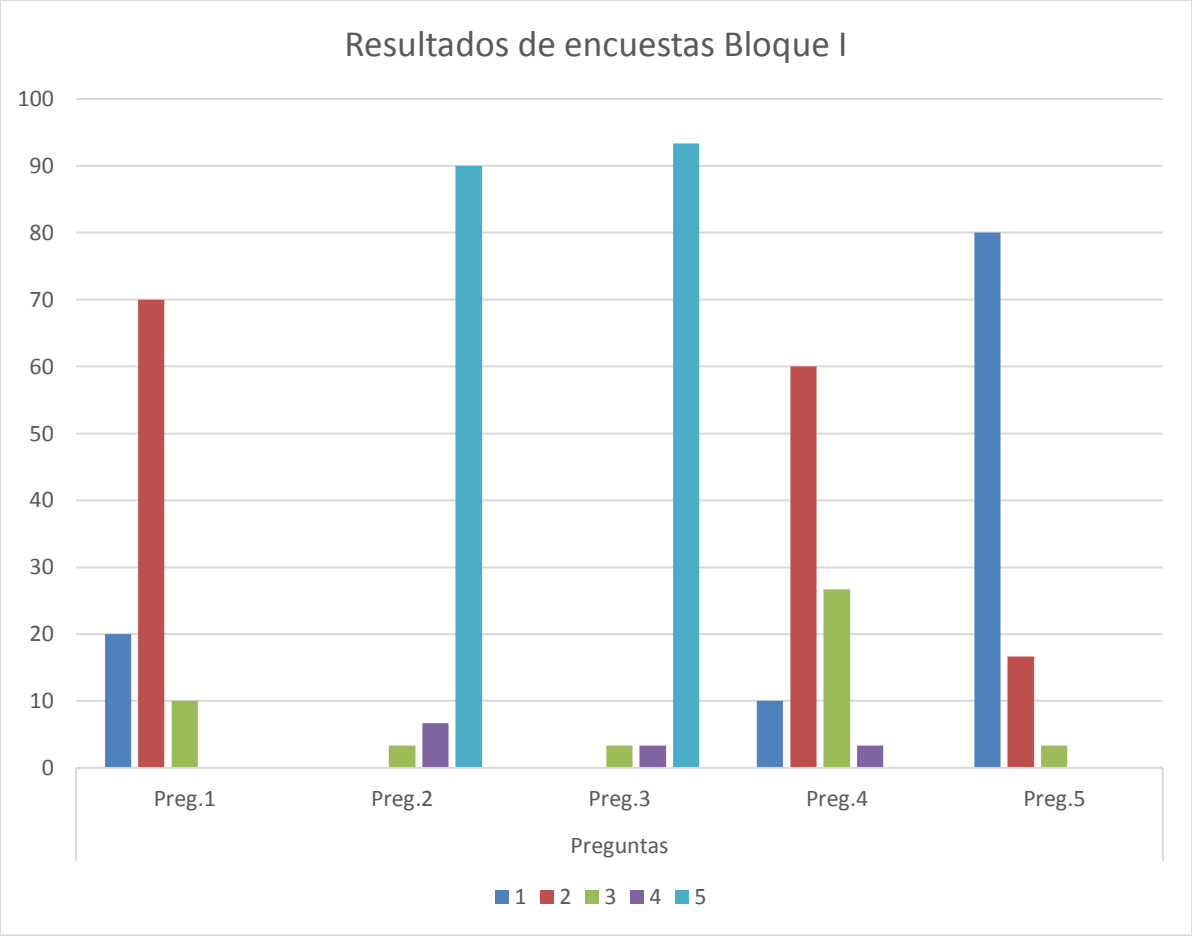
Bloque I

La tabla a continuación muestra los resultados a las interrogantes correspondientes al bloque I, siendo las preguntas planteadas de forma horizontal y su calificación respectiva en la columna denominada “nivel”.

	Preguntas				
Nivel	1	2	3	4	5
1	6	0	0	3	24
2	21	0	0	18	5
3	3	1	1	8	1
4	0	2	1	1	0
5	0	27	28	0	0
Total usuarios	**30**	**30**	**30**	**30**	**30**

Es posible evidenciar los resultados en porcentajes, como se muestra en la siguiente tabla y su correspondiente gráfica de barras.

	Preguntas				
Nivel	1	2	3	4	5
1	20%	0	0	10%	80%
2	70%	0	0	60%	16,7%
3	10%	3,3%	3,3%	26,7%	3,3%
4	0	6,7%	3,3%	3,3%	0
5	0	90%	93,3%	0	0
Total (%)	**100**	**100**	**100**	**100**	**100**

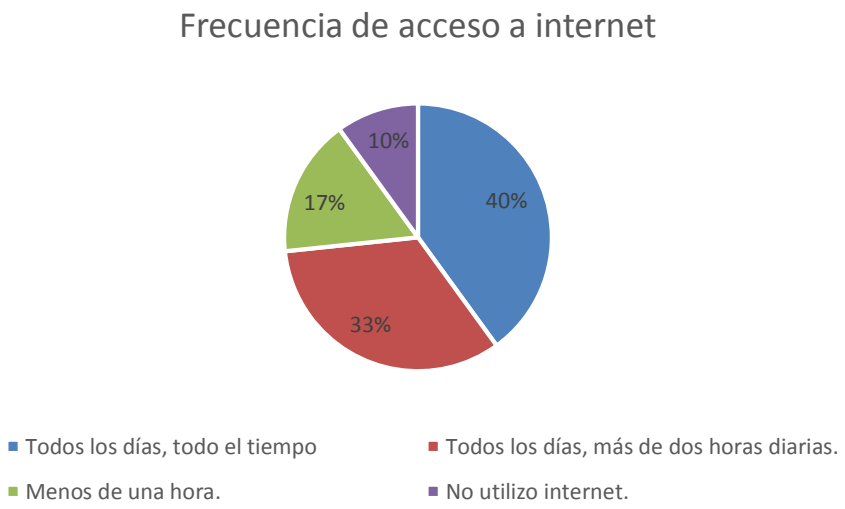


En la parte inferior se indican las cinco preguntas que componen este bloque, los colores muestran la puntuación (1-5) que han recibido estas interrogantes y las barras en cambio, se refieren al porcentaje de usuarios que puntuó estas interrogantes, que se detallan así:

1. Actualmente todos los usuarios comparten información entre sí a través de sus computadoras locales dentro de la empresa mediante una conexión física o inalámbrica. (red)
2. Le gustaría compartir información mientras se moviliza dentro de la empresa.
3. La infraestructura actual abastece a todos los usuarios de la Cámara de Comercio. (En cuanto a espacio en metros cuadrados).
4. Su equipo de trabajo (computadora) cuenta con un sistema de prevención de malware o antivirus.
5. El edificio tiene algún tipo de seguridad o restricción para su acceso.

Bloque II

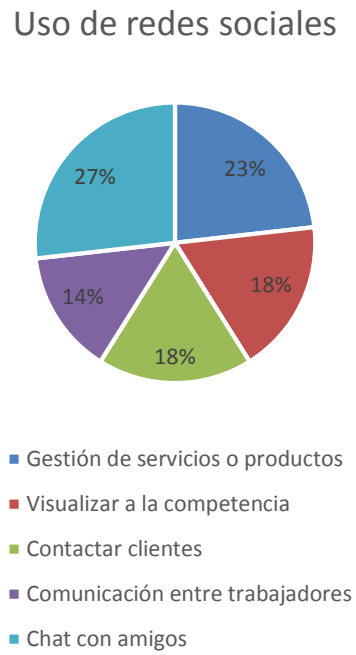
1. **¿Con qué frecuencia accede a internet dentro de la empresa? (Seleccione una opción)**



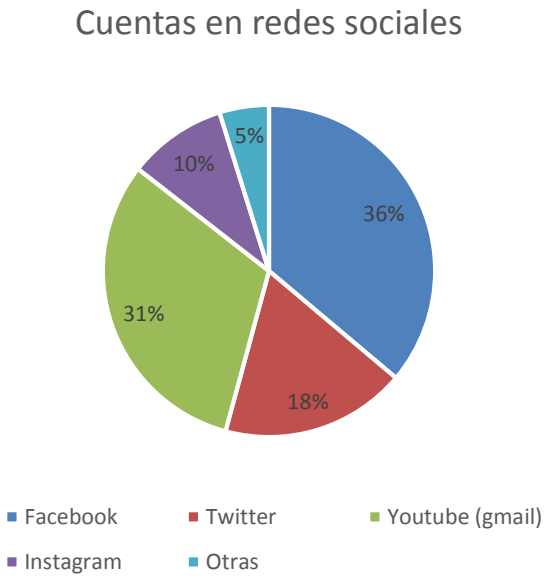
2. **¿Cuáles son los sitios web que más visita? (Seleccione hasta dos opciones)**

Si entre sus opciones marcó el literal a) continué con el cuestionario; caso contrario se le agradece por su participación. Si desea puede comentar sus sugerencias relacionadas con el tema.

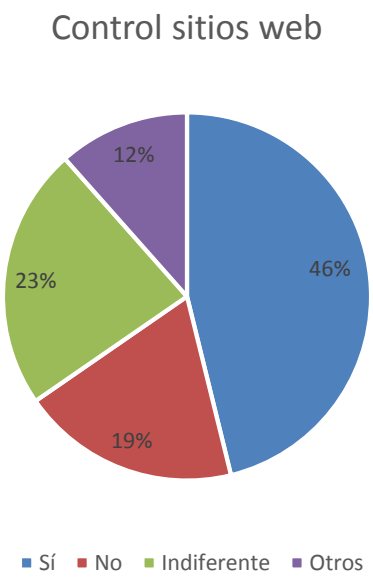
3. **¿Para qué utiliza principalmente las redes sociales dentro de la empresa? (Puede seleccionar hasta 2 opciones)**



4. **¿En qué redes sociales posee una cuenta? (Seleccione las que sean necesarias)**



5. **¿Le parecería útil que el acceso a sitios web sea controlado a través de un dispositivo de software o hardware con el fin de optimizar el acceso a internet?**



Entrevista realizada al Lic. Robert Cadena-Presidente de la Cámara de Comercio.

1. **¿El edificio de la Cámara de Comercio cuenta con una red local?**
   No precisamente, por el momento solo tenemos un router conectado directamente a las computadoras; en ciertas ocasiones se dispone de un switch; sin embargo a veces no abastece a todos los usuarios.

2. **Ustedes planean la implementación de una red LAN; ¿piensa que es importante separar ciertos servicios, como por ejemplo voz y datos?**
   Sería lo ideal, una por mantener el orden y otra por evitar interferencias de cierto modo.

3. **¿Considera importante controlar el acceso web a determinados sitios a través de un equipo configurado previamente?**
   Sí, para poder hacer un uso eficiente de la red.

4. **Actualmente, ¿existe un documento que contenga las actividades y procedimientos a seguir en caso de que se susciten determinadas circunstancias dentro de la organización?**

   Por el momento no, simplemente ideas que no han sido redactadas y han quedado ahí.

5. **¿Cómo se realiza el registro de ingreso de personas?**

   Cuando hay eventos masivos existe un guardia de seguridad que controla el acceso pidiendo la credencial a las personas y registrándolas en un cuadernillo. En días normales llevamos un registro de firmas pero nos gustaría optimizar este proceso.

6. **¿Cuál es el porcentaje estimado de usuarios que utiliza su computador en su rutina normal de trabajo?**

   Casi todos, digamos que un 85%.

7. **¿La empresa recibe órdenes de compra a través de internet?**

   Órdenes de compra no, pero sí existen peticiones que luego se pueden concretar en compras.

8. **¿Cuál es el objetivo principal del uso de las redes sociales dentro de la empresa?**

   Principalmente para promocionar servicios o productos de nuestros miembros.

9. **¿Para qué servicios o actividades la empresa utiliza internet?**

   - Comunicación
   - Transacciones
   - Servicio al cliente
   - Distribución de productos en línea.
   - Búsqueda de información
   - Actividades de investigación.

10. ¿Cuáles son las redes sociales que más se utilizan dentro de la organización?

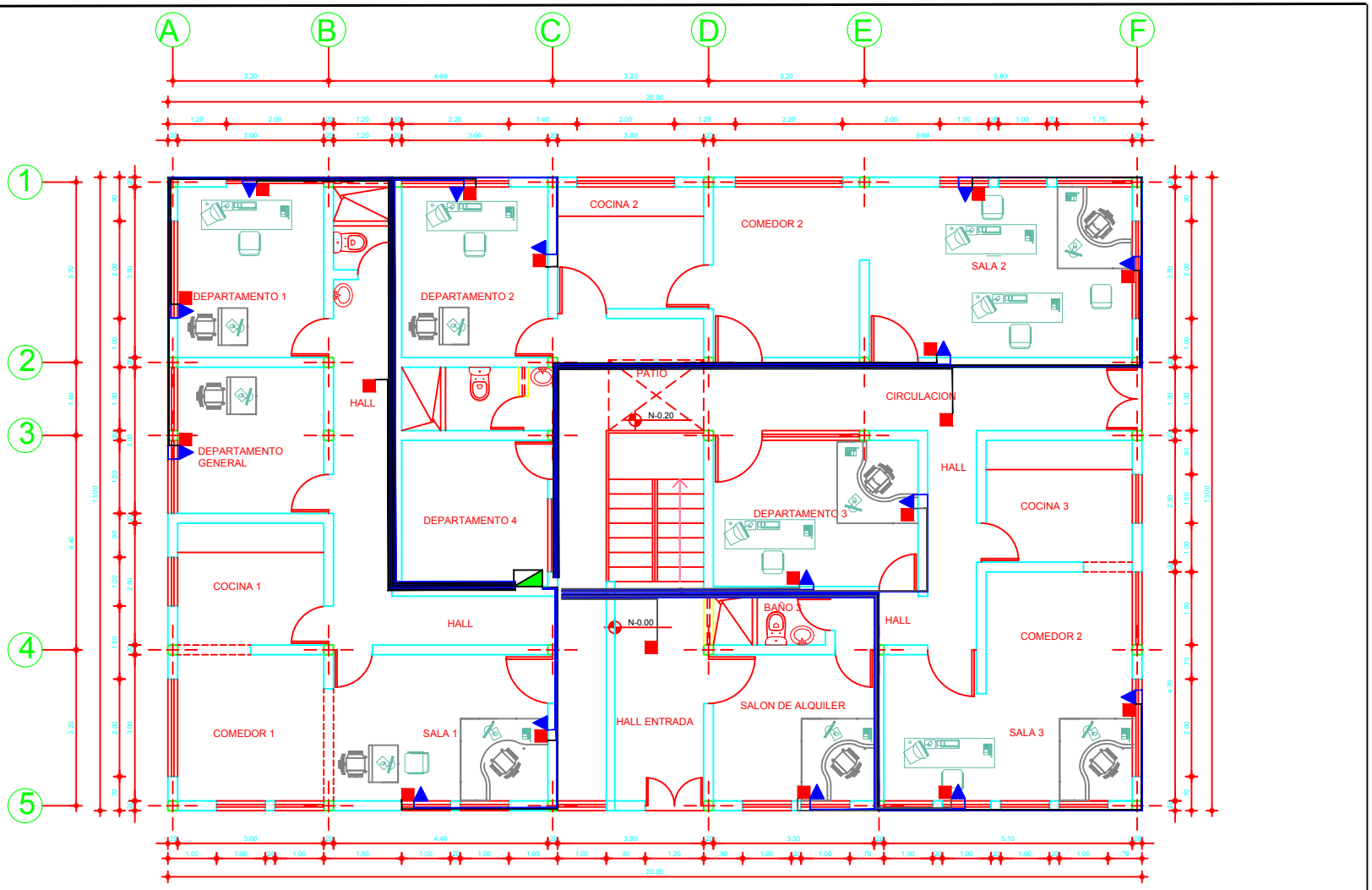
Bueno , las redes sociales en las que operamos son Facebook, twitter, youtube, google+ y eventualmente linkedin.

11. ¿La empresa tiene un sitio web?

No, pero la idea de crearlo está planteada.

12. ¿Cuál es su horario laborable y/o de almuerzo?

Normalmente trabajamos desde las 7 hasta la 1pm. Sin horario para almuerzo ya que este estaría fuera de horario laboral.



PLANTA BAJA

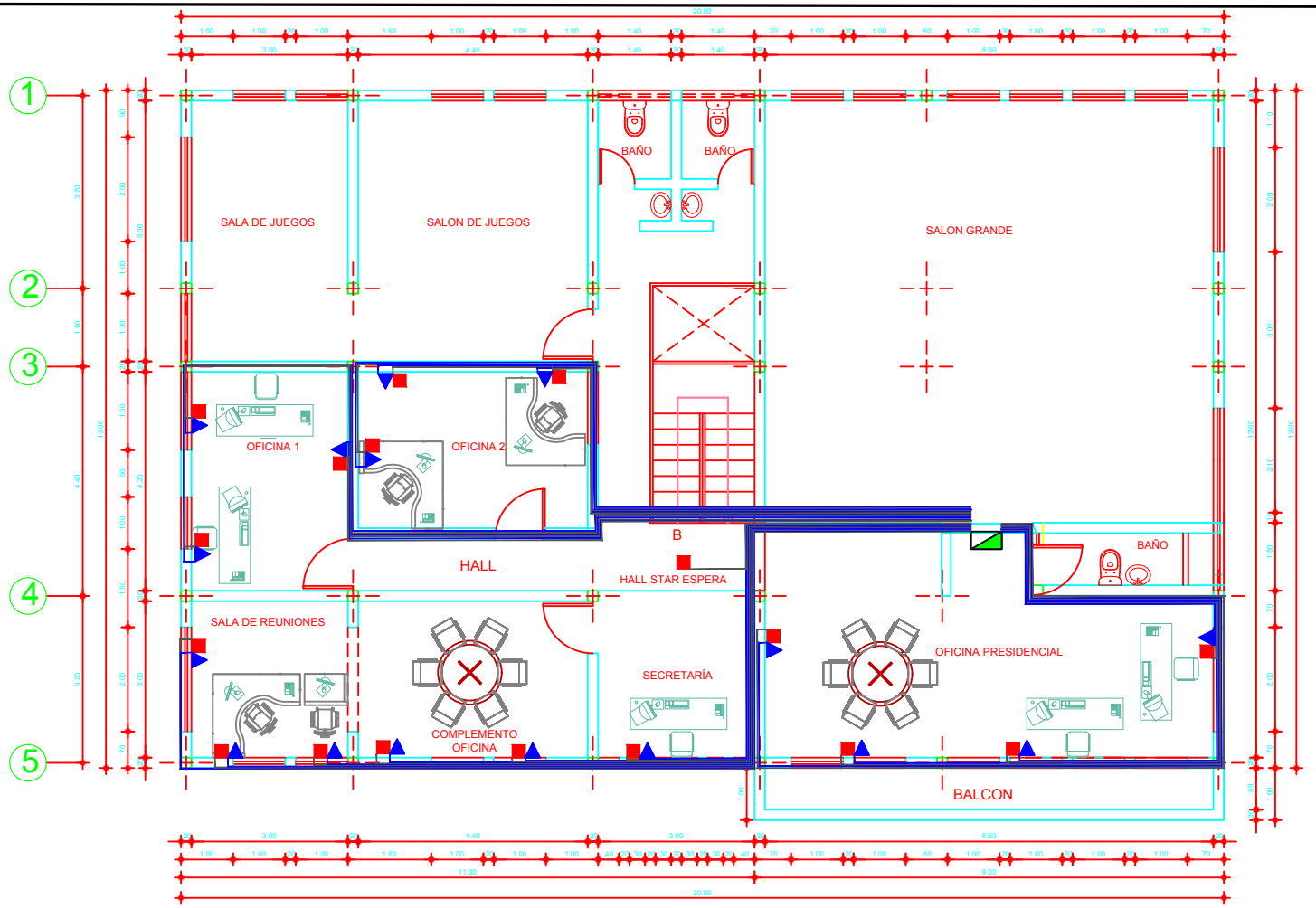
ESCALA: _____ 1:100

SIMBOLOGÍA	
	RACK (TC)
	SALIDA DE DATOS
	SALIDA DE VOZ
	CABLEADO VOZ
	CABLEADO DATOS
	MAMPOSTERÍA

Proyecto:	DISEÑO DE CABLEADO ESTRUCTURADO
Unidad:	Edificio Cámara de Comercio de Otavalo
Contiene :	UBICACIÓN DE SALIDAS DE VOZ Y DATOS

Escala :	1/100
Por :	Marcela López
UTN	FICA
CIERCOM	Lámina : 1/3
Fecha:	

ANEXO C. Diseño cableado estructurado planta baja.



PRIMER PISO

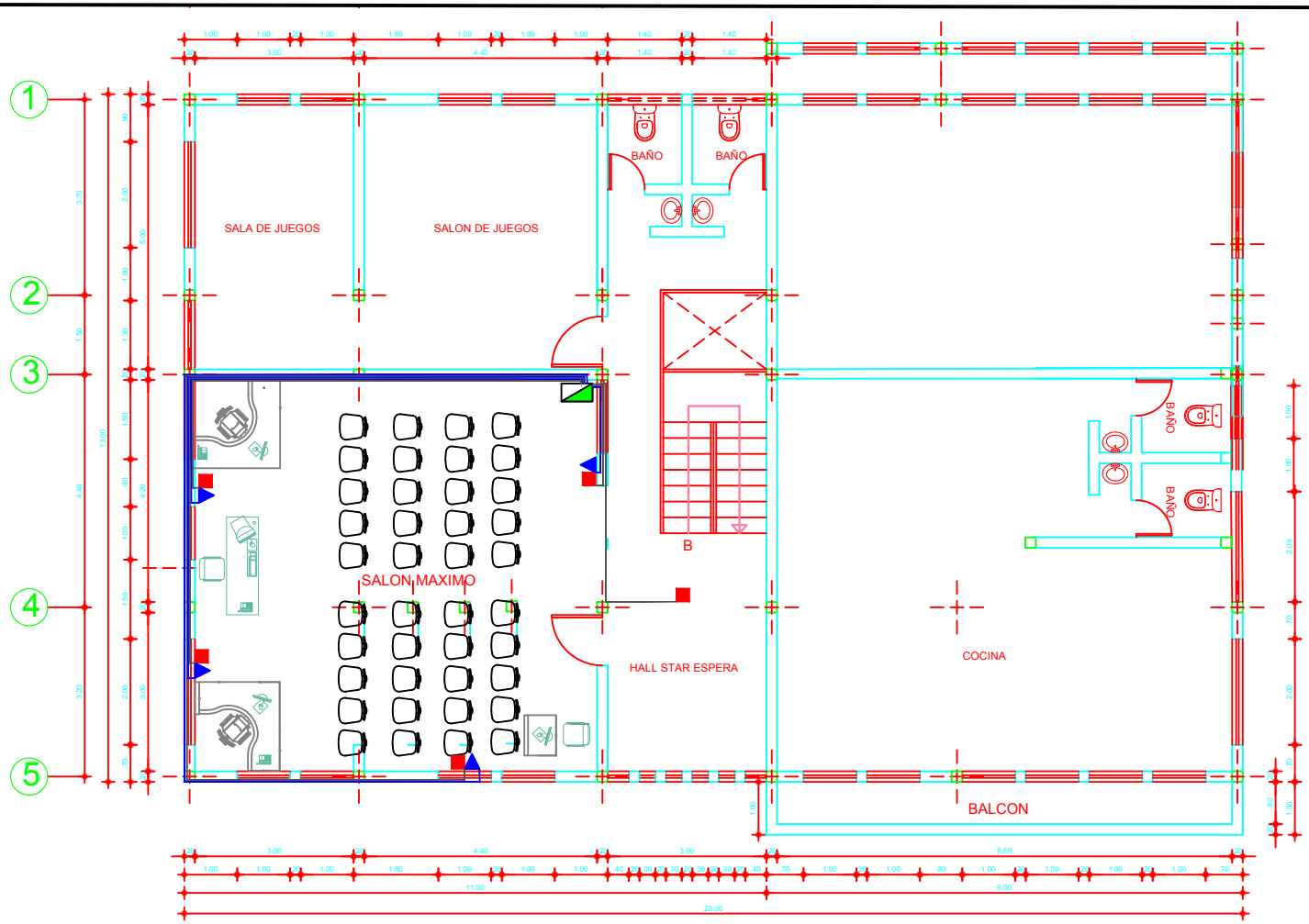
ESCALA: _____ 1:100

SIMBOLOGÍA	
	RACK (TC)
	SALIDA DE DATOS
	SALIDA DE VOZ
	CABLEADO VOZ
	CABLEADO DATOS
	MAMPOSTERÍA

Proyecto:	DISEÑO DE CABLEADO ESTRUCTURADO
Unidad:	Edificio Cámara de Comercio de Otavalo
Contiene :	UBICACIÓN DE SALIDAS DE VOZ Y DATOS

Escala :	1/100
Por :	Marcela López
UTN	FICA
CIERCOM	Lámina : 2/3
Fecha:	

ANEXO D. Diseño cableado estructurado Primer Piso



SEGUNDO PISO

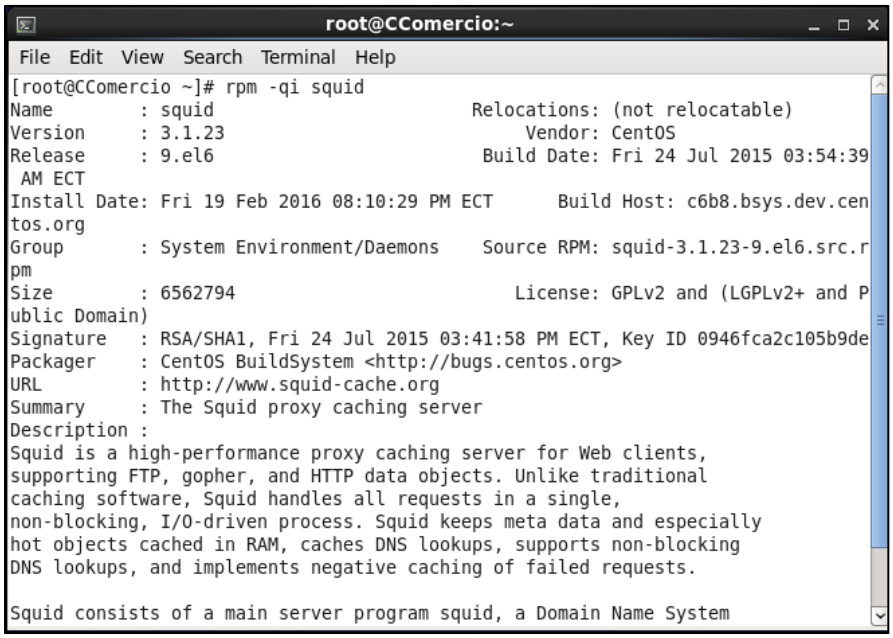
ESCALA: _____ 1:100

SIMBOLOGÍA		Proyecto: DISEÑO DE CABLEADO ESTRUCTURADO	Escala : 1/100
	RACK (TC)		Por : Marcela López
	SALIDA DE DATOS	Unidad: Edificio Cámara de Comercio de Otavalo	
	SALIDA DE VOZ		
	CABLEADO VOZ	Contiene : UBICACIÓN DE SALIDAS DE VOZ Y DATOS	UTN / FICA
	CABLEADO DATOS		CIERCOM / Lámina : 3/3
	MAMPOSTERÍA		Fecha:

ANEXO E. Diseño cableado estructurado Segundo Piso.

ANEXO F. Instalación y configuración de proxySQUID

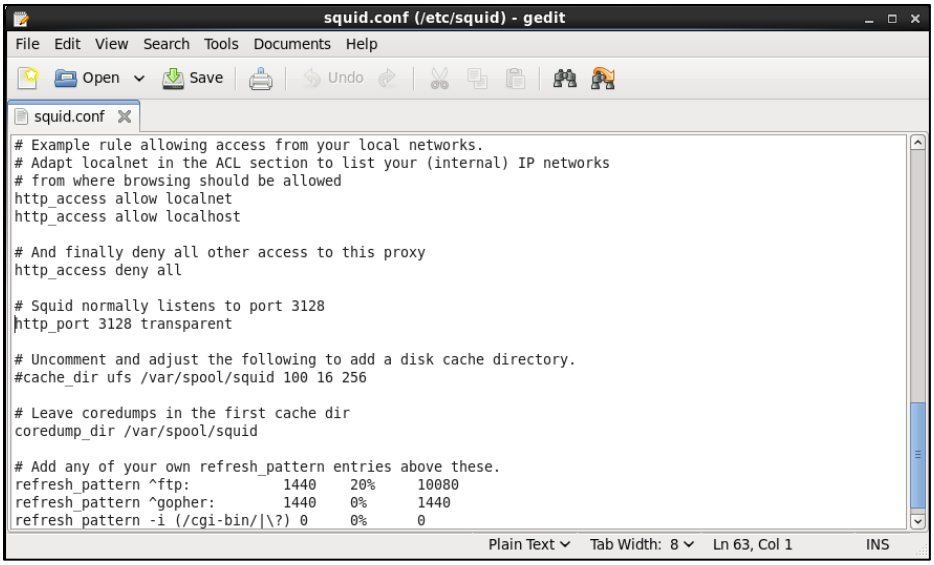
1. Antes de proceder a instalar es posible verificar si el paquete de SQUID ya se encuentra en los repositorios de centOS mediante el comando *rpm -qi squid*



   Si el comando no muestra salida, entonces se instalará mediante yum. En este caso no fue necesario.

   yum -y install squid

2. Ahora es posible realizar la configuración básica mediante el fichero */etc/squid/squid.conf,* para lo cual se ingresa a este mediante cualquier editor de texto.



3. A continuación se deben ejecutar las siguientes modificaciones:

http_port: indicar el puerto a través del cual escuchará el squid

cache_dir ufs: memoria utilizada por el squid para el almacenamiento de caché en el disco duro

cache_mem: tamaño de los objetos en el caché

cache_swap_low: porcentaje a partir del cual se limpiará el caché

cache_swap_high: porcentaje a partir del cual se limpiará el caché agresivamente

PARÁMETRO	ANTES DE MODIFICAR	DESPUES DE MODIFICAR

http_port	`# Squid normally listens to port 3128`
	`http_port 3128`
		`# Squid normally listens to port 3128`
		`http_port 3128`
		`http_port 8080`

cache_dir ufs	`#cache_dir ufs /var/spool/squid 100 16 256`	`cache_dir ufs /var/spool/squid 1000 16 256`
cache_mem	Añadir la línea	`cache_mem 128 MB`
cache_swap_low	Añadir línea	`cache_swap_low 90`
cache_swap_high	Añadir línea	`cache_swap_high 95`

4. Una vez terminada la configuración se debe ejecutar el siguiente comando para dar inicio al servicio:

service squid start

En caso de recargar la configuración sin parar el servicio se debe ejecutar lo siguiente:

service squid reload

Si necesita reiniciar para probar cambios realizados en la configuración, digitar el siguiente comando:

service squid restart

Para que Squid corra automáticamente cuando se inicie el sistema digitar el comando:

chkconfig squid on

ANEXO G. Registro de cortes de luz en el sector de la Cámara de Comercio.

El circuito de energía eléctrica que abarca la ubicación del edificio se denomina Otavalo 3 y de acuerdo a la información proporcionada por la Empresa Eléctrica Regional Norte (EMELNORTE) se analizaron los cortes de luz producidos durante el año 2016 que en total fueron 10 en donde el mínimo tuvo una duración de 12 segundos y el máximo de 8 horas con 45 minutos.

	Etapa funcional en la que se presentó la falla	Instalación / Equipo donde se presentó la falla	Tipo de protección que actuó	Descripción de Interrupción	Fecha Inicio de Interrupción (dd:mm:ay)	Hora Inicio de Interrupción (hh:mm)	Fecha Fin de Interrupción (dd:mm:ay)	Hora Fin de Interrupción (hh:mm)	Duración de Interrupción (Horas:minutos:segundos)	Duración de Interrupción (Horas)
105	Distribución	Red de Media	Fusible	Viento Fuerte	19/04/2016	19:00:00	19/04/2016	19:45:00	0:45:00	0,750000
106	Distribución	Red de Media	Fusible	Viento Fuerte	20/04/2016	12:46:00	20/04/2016	12:58:00	0:12:00	0,200000
107	Distribución	Red de Media	Fusible	Descargas Atmosfericas (Rayos)	21/04/2016	8:25:00	21/04/2016	10:35:00	2:10:00	2,166667
108	Distribución	Red de Media	Fusible	Viento Fuerte	22/04/2016	15:10:01	22/04/2016	15:45:01	0:35:00	0,583333
109	Distribución	Red de Media	Fusible	Poste Chocad	22/04/2016	20:00:00	22/04/2016	20:45:00	0:45:00	0,750000
110	Distribución	Red de Media	Fusible	Transformadc	26/04/2016	16:30:00	26/04/2016	18:45:00	2:15:00	2,250000
111	Distribución	Red de Media	Fusible	Transformadc	26/04/2016	19:20:00	26/04/2016	20:20:00	1:00:00	1,000000
112	Distribución	Red de Media	Fusible	Transformadc	27/04/2016	10:15:00	27/04/2016	19:00:00	8:45:00	8,750000
35	Distribución	Red de Media	Fusible	Linea Rota	12/09/2016	11:40:00	12/09/2016	12:25:00	0:45:00	0,750000
96	Distribución	Red de Media	Fusible	Cambio de el	12/10/2016	8:00:00	12/10/2016	9:15:00	1:15:00	1,250000

Formato de registro de usuarios.

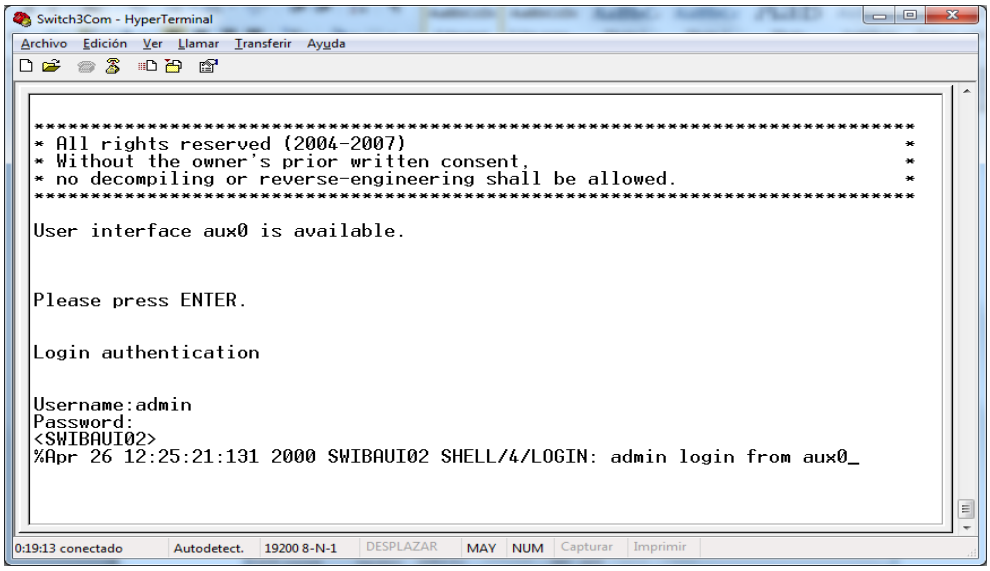
Fecha	Hora entrada	Hora salida	Firma	Observaciones

ANEXO H. Configuración switch 3COM

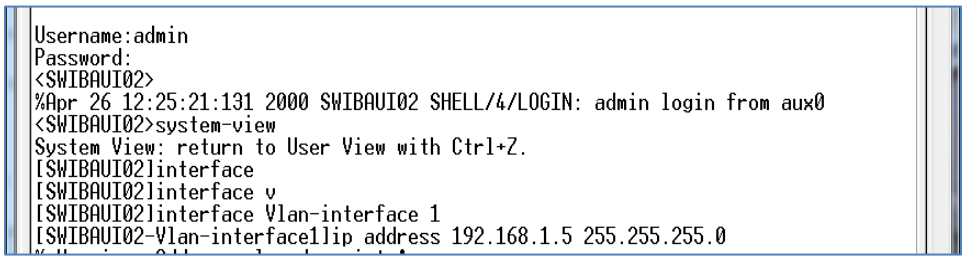
Configuración inicial

Para configurar el switch se debe establecer una conexión en modo consola a través del puerto serial DB-9 y la aplicación que nos permite visualizar, en este caso hyperterminal configurada a una velocidad de 19200 baudios.

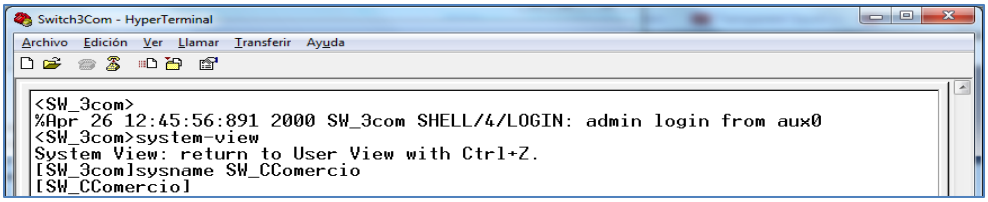
Una vez que se establece la conexión se mostrará la pantalla siguiente en donde el usuario por defecto es admin y la contraseña se deja en blanco.



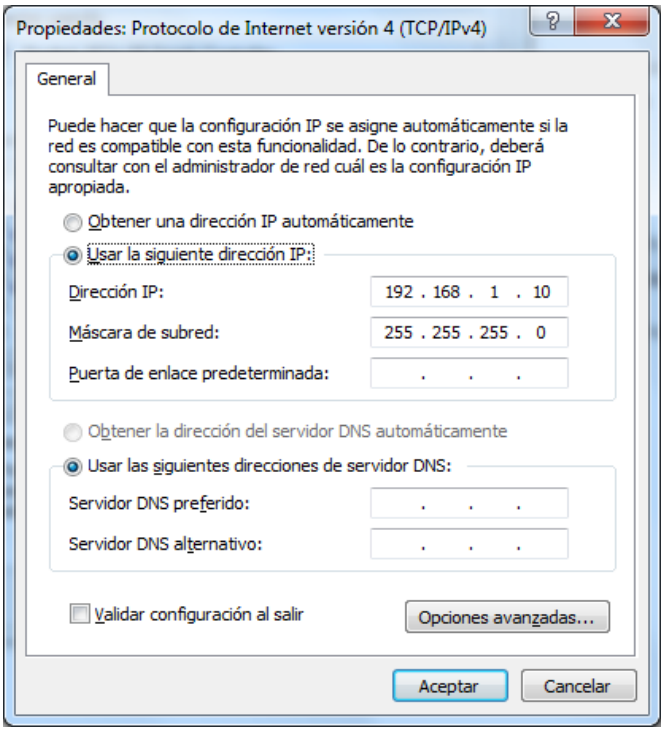
A continuación es necesario configurar una dirección Ip para así acceder a la configuración en modo web. Y mediante el comando señalado es posible modificar el nombre del dispositivo.



Se realiza el cambio de nombre y listo.



Ahora se configura la computadora con una dirección ip perteneciente a la misma red del switch y se abre el navegador internet explorer mediante la dirección ip asignada anteriormente y enseguida aparecerá la pantalla de configuración del dispositivo.

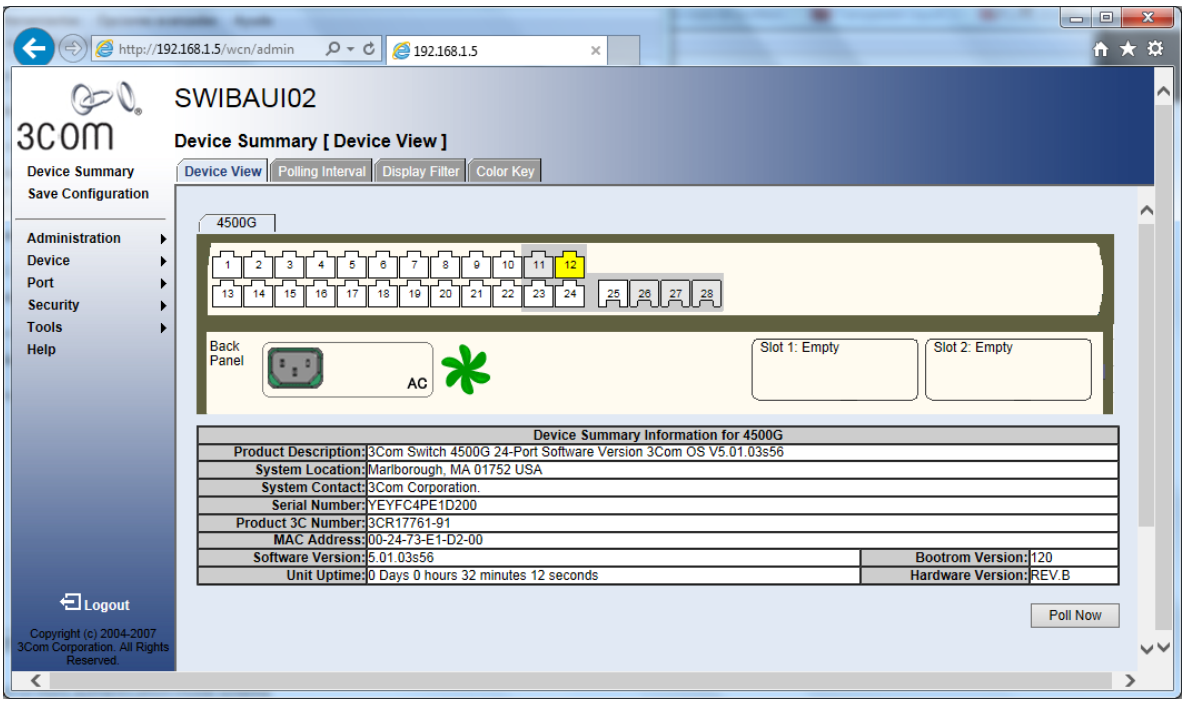


Y de esta manera se logra ingresar a la interfaz web del dispositivo mediante la ip asignada en la configuración por consola.

Ingreso a la interfaz Web

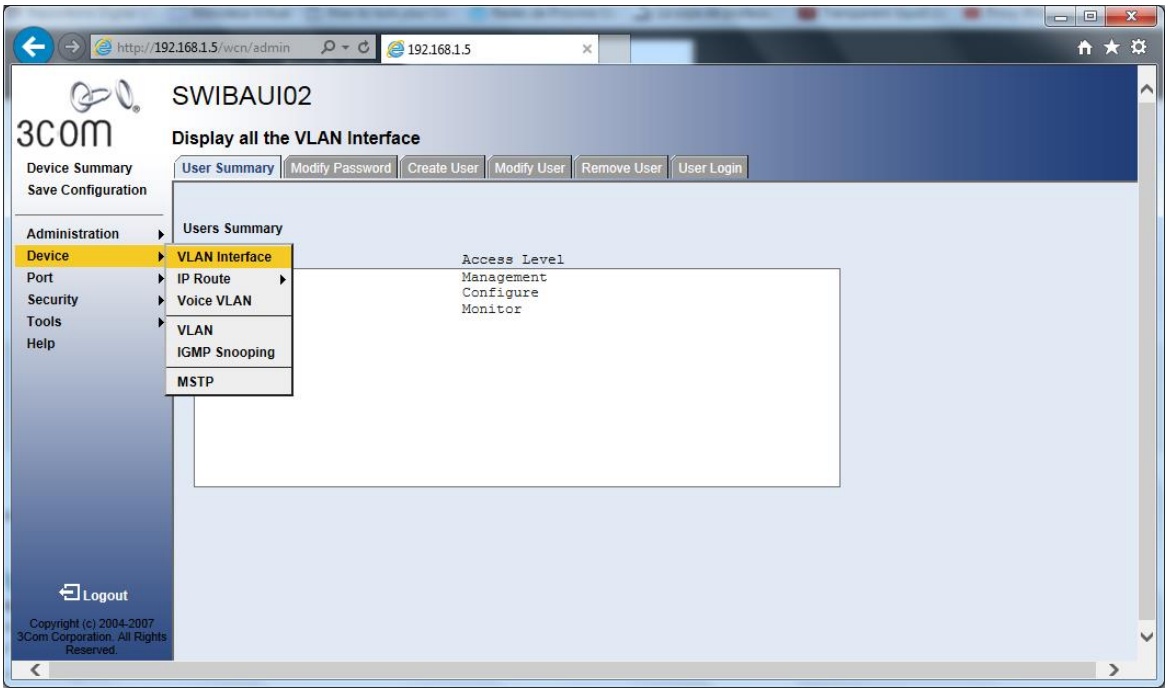
Una vez ingresada la dirección IP se ingresa a la configuración en modo Web en donde la primera pantalla solicita el usuario y contraseña de administrador.

Y finalmente se procede a realizar las configuraciones respectivas según muestra el menú.

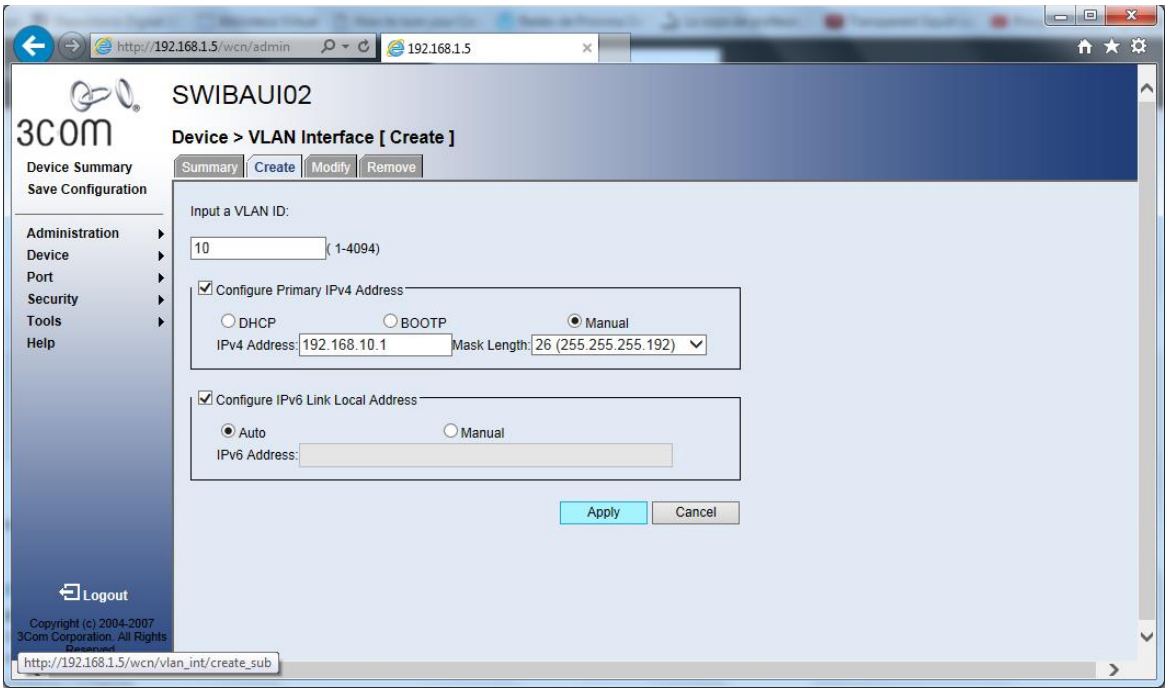


Configuración de vlans

En el menú de la izquierda se escoge la opción *device* y luego *vlan interface*, como se muestra en la imagen:

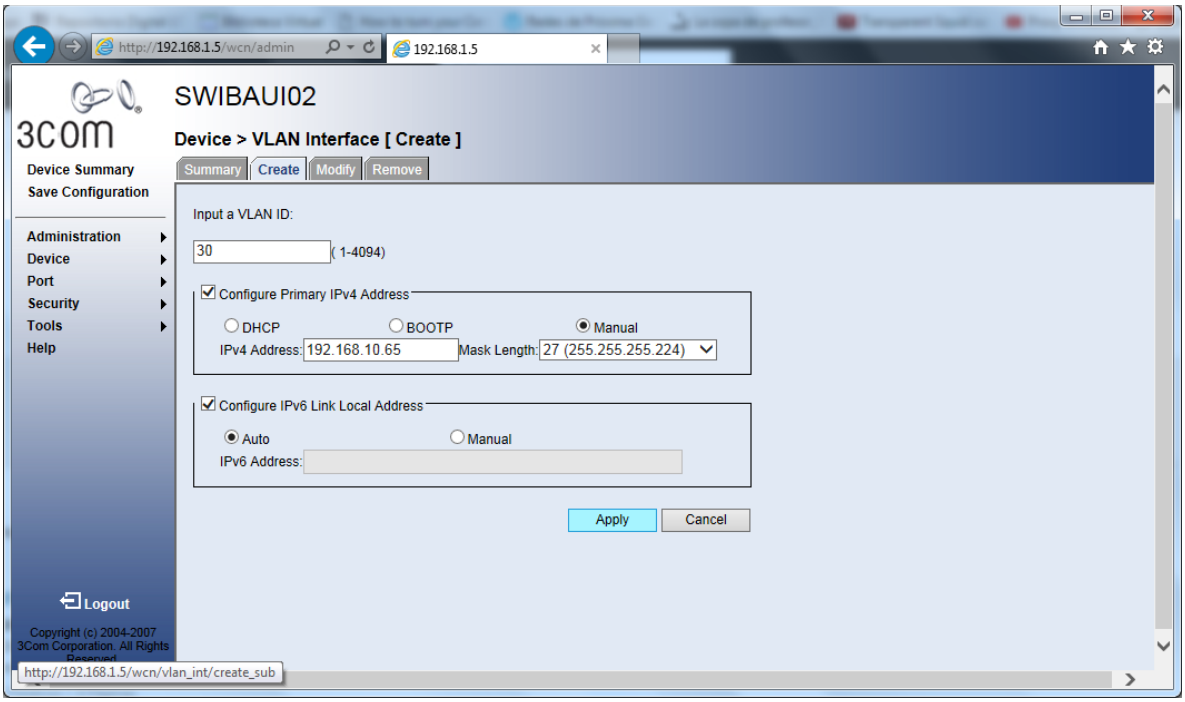


Se da click en la opción *create* y se procede a digitar los parámetros necesarios para la configuración de vlan: id de vlan y dirección IP.

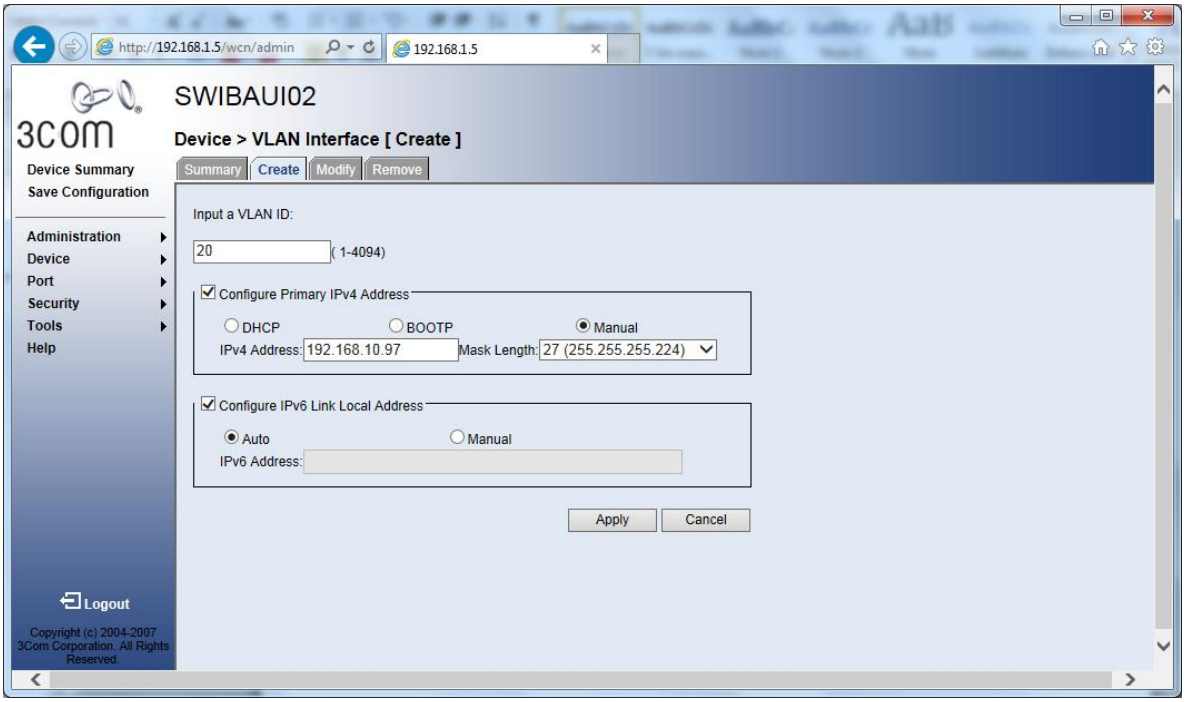


Y de la misma manera se crean el resto de redes lan virtuales.

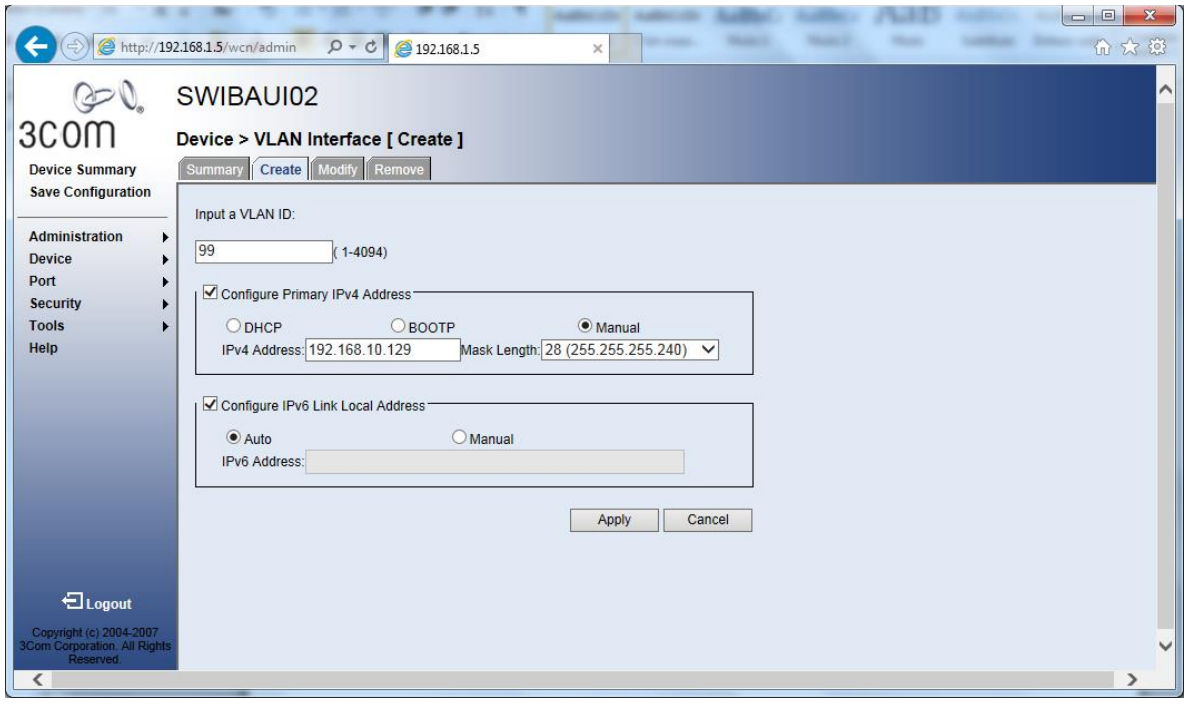
Vlan 30: vlan directivos



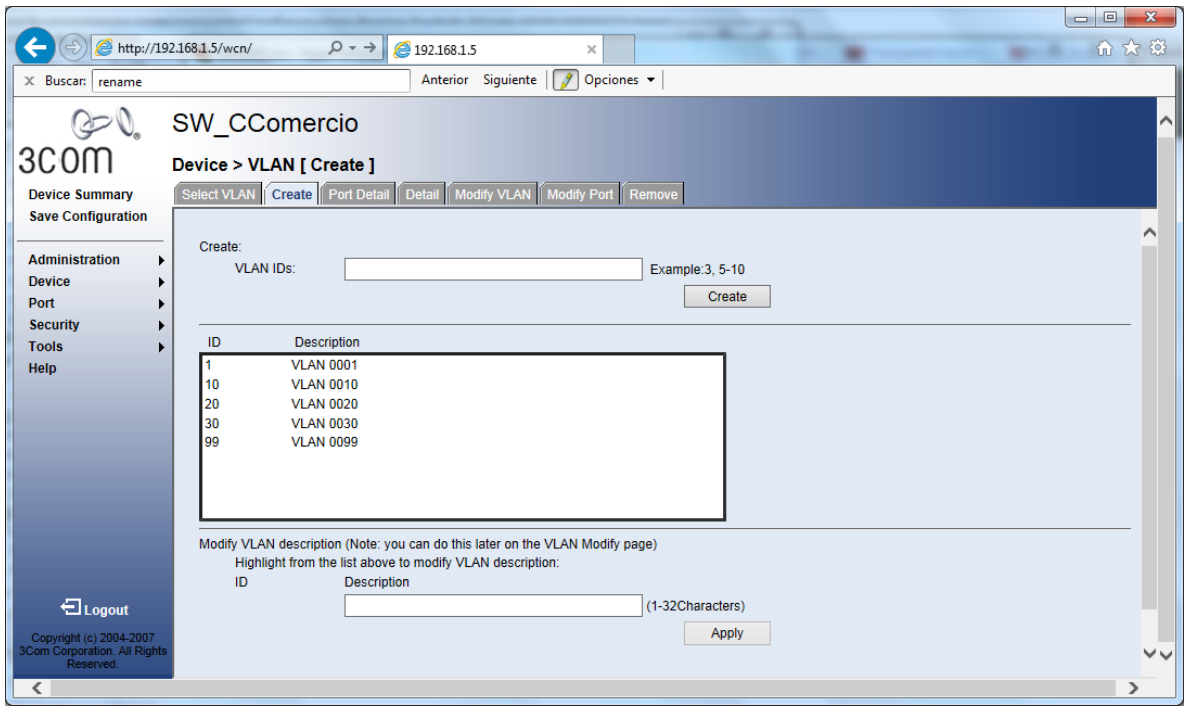
Vlan 20: vlan socios



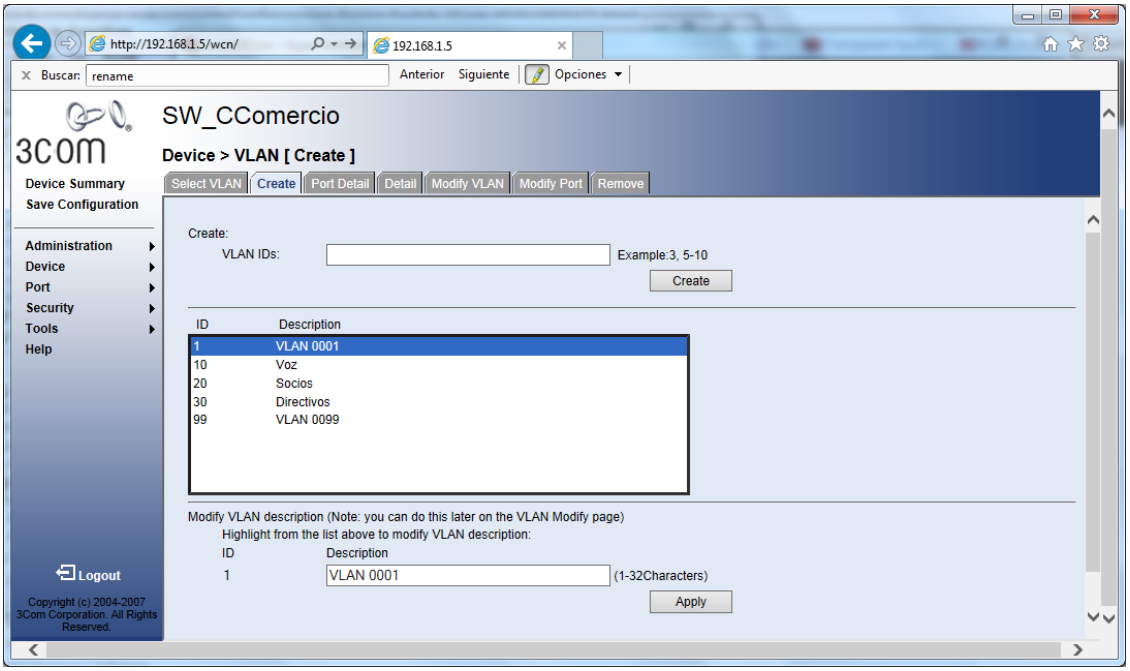
Vlan administrativa: vlan 99



Ahora se puede observar el resumen de las vlans creadas.

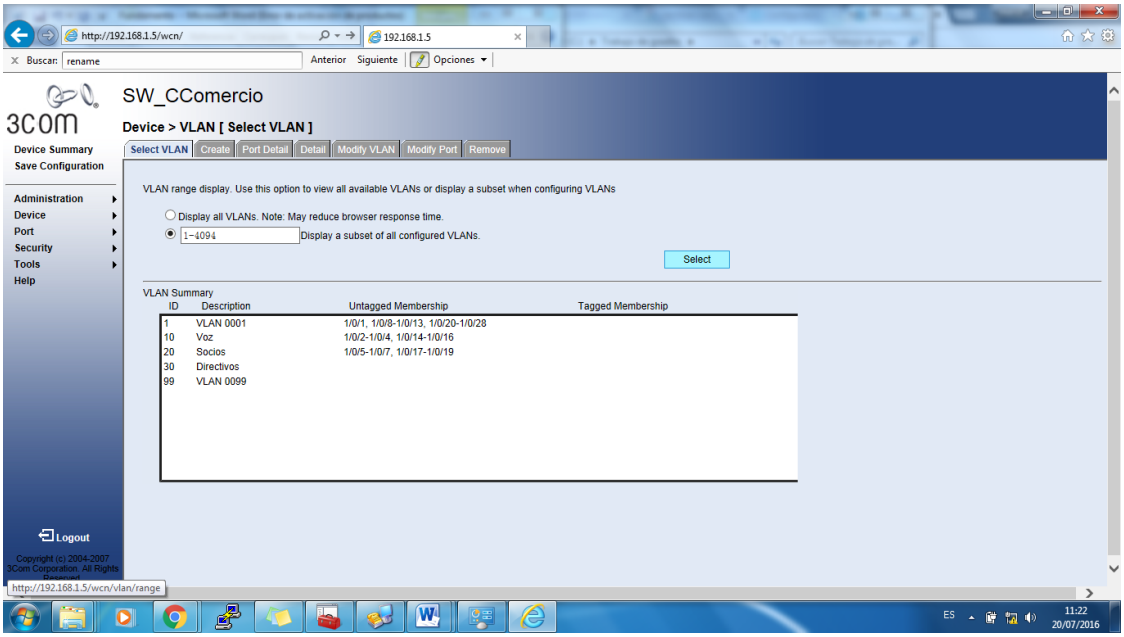


Como se puede observar se tienen las vlans creadas pero carecen de la descripción necesaria para identificarlas, no obstante es posible agregar una mediante la opción *description* de la parte inferior.



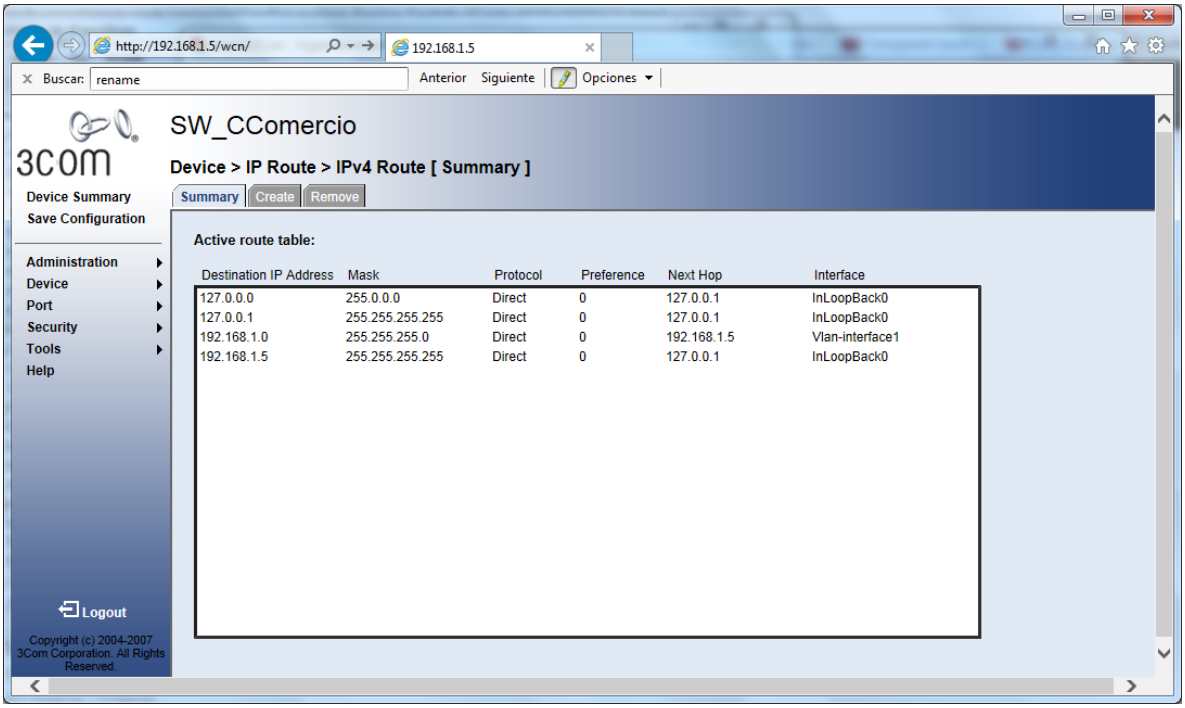
Agregar puertos a las vlans

Se selecciona la vlan en la misma opción *device* y se van escoguendo los puertos según lo requerido



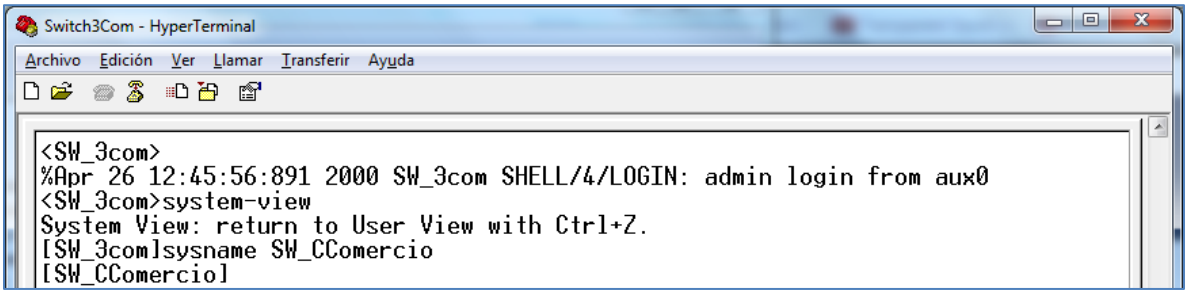
Enrutamiento inter vlan

Este switch cuenta la opción de enrutamiento; del menú que se muestra se deberá escoger la opción *device >> ip route >> ipv4 route* y allí se agregan las subredes según el direccionamiento realizado.

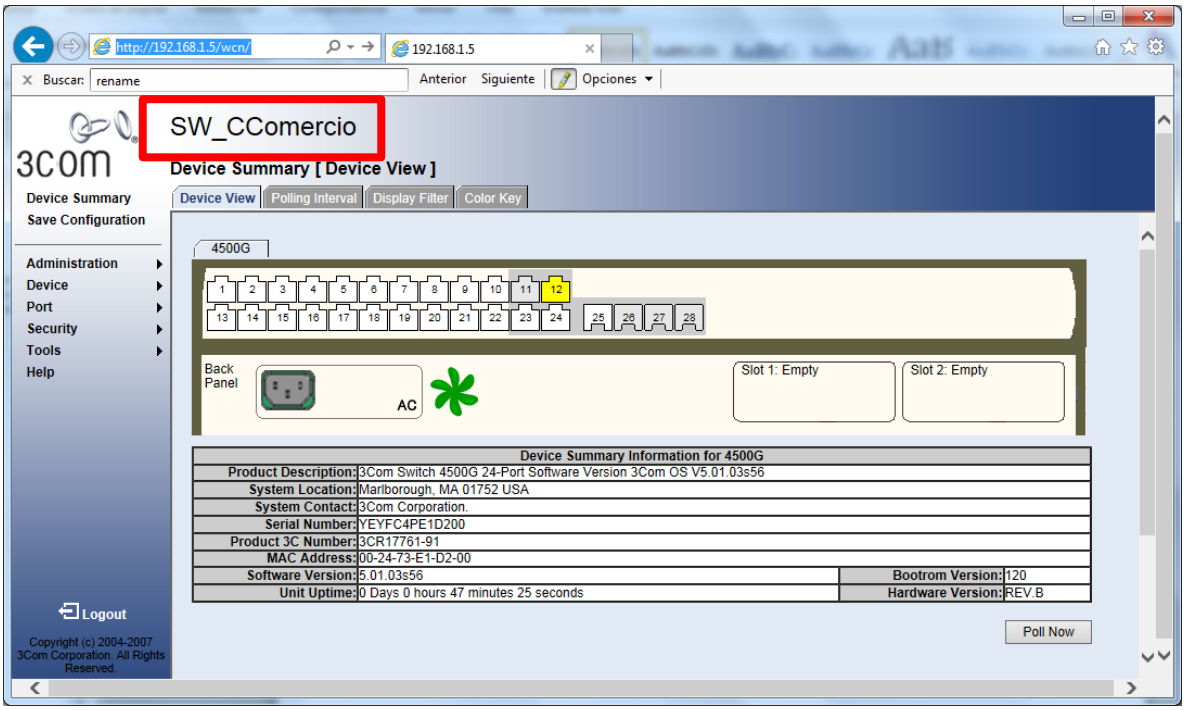


Configuración del hostname y password

En modo consola se digita el comando sysname seguido del nombre que se desee asignar al swicth.



Se refresca la página web y se observan inmediatamente los cambios.



ANEXO I. Proforma de precios acordados.

Sistemas Electrónicos Digitales y Monitoreo

PROFORMA

EMPRESA	SRS CAMARA DE COMERCIO
ATENCION	Srta. Marcela López
DIRECCION	Ibarra
TELÉFONO	(2) 558-392
FECHA	Lunes 06 de junio de 2016

ITEM	DESCRIPCION	CANTIDAD	PRECIO U	PRECIO T
1	Rollo de cable UTP Cat. 5e	5	58.00	290.00
3	Face Plates Doble.	40	1.00	40.00
4	Face Plate Simple	20	1.00	20.00
5	Jack RJ45 Cat.5e	100	2.70	270.00
6	Patch Panels Cat. 5e de 24 Puertos	5	50.00	250.00
7	Organizadores de Cables Horizontal	5	20.00	100.00
8	Gabinete Cerrado de Pared 6UR	3	115.00	345.00
9	Canaleta 60x40	15	8.75	131.24
10	Canaleta 40x25	20	6.25	125.00
11	Angulo Interno 60x40	20	2.25	45.00
12	Angulo Interno 40x25	20	0.85	17.00
13	Angulo Externo 60x40	10	2.25	22.50
14	Angulo Externo 40x25	20	0.85	17.00
15	Adaptador T 60x40	11	2.00	22.00
16	Adaptador T 40x25	25	0.85	21.25

17	Switch 3com 3226	1	300.00	300.00
16	Switch 3com 3c1700	4	120.00	480.00
18	Lectoras biométricas ONE Af-261	2	120.00	240.00
19	Mano de obra	1	750.00	100,000
CONDICIONES GENERALES			**SUBTOTAL**	2438.95
VALIDEZ DE LA OFERTA: 15 días laborables			**IVA 14%**	297.04
GARANTÍA: 1 año contra defectos por fabricación			**GRAN TOTAL**	2735.99
FORMA DE PAGO: contado				

Ing. Mery Villarreal

Dep./de Ventas

SEDYM CIA. LTDA

Otavalo: Ciudadela Ángel Escobar calle San Pedro Telft: 2904-288; 0984006623

Ibarra: Borrero 2-52 y Maldonado Telf: 2604-758 ; 0999921725

Mail: sedymalarmas@hotmail.com

…….

Aprobado por cliente

ANEXO J. Certificado de implementación del trabajo de grado y Certificado de aprobación del Manual de Políticas.

CAMARA
DE
COMERCIO "OTAVALO"

Otavalo, 22 de julio de 2016

CERTIFICO:

Yo Robert Fernando Cadena Carvajal en calidad de Presidente de la Cámara de Comercio de Otavalo con cédula de ciudadanía N°100203820-4; a petición verbal de la señorita Marcela Elizabeth López Huera con cédula de ciudadanía N°100359767-9 estudiante de la Universidad Técnica del Norte de la Facultad de Ingeniería en Ciencias Aplicadas de la carrera de Electrónica y Redes de Comunicación certifico que ha culminado satisfactoriamente el proyecto de tesis "Diseño e implementación de la red de datos y control de acceso biométrico de la Camara de Comercio de la ciudad de Otavalo.

Atentamente,

Cámara de Comercio de Otavalo
DEPARTAMENTO
ADMINISTRATIVO

Lic. Robert Fernando Cadena Carvajal

PRESIDENTE DE LA CAMARA DE COMERCIO DE OTAVALO

Dirección: calle García Moreno 7-43 y Modesto Jaramillo
Telf.: 062-920-626
e-mail: camcomotavalo@hotmail.com
Otavalo - Ecuador

CAMARA
DE
COMERCIO "OTAVALO"

Otavalo , 05 de mayo de 2017

CERTIFICO:

Que, el MANUAL DE POLÍTICAS DE ACCESO realizado por la señorita Marcela Elizabeth López Huera con CI: 100359767-9, estudiante de la Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas ha sido revisado y aprobado por los miembros directivos de la Cámara de Comercio de Otavalo. Por lo que Yo, Robert Fernando Cadena Carvajal firmo en calidad de Presidente de la Cámara de Comercio de Otavalo.

Atentamente,

Cámara de Comercio de Otavalo
DEPARTAMENTO
ADMINISTRATIVO

Lic. Robert Fernando Cadena Carvajal
PRESIDENTE DE LA CAMARA DE COMERCIO DE OTAVALO

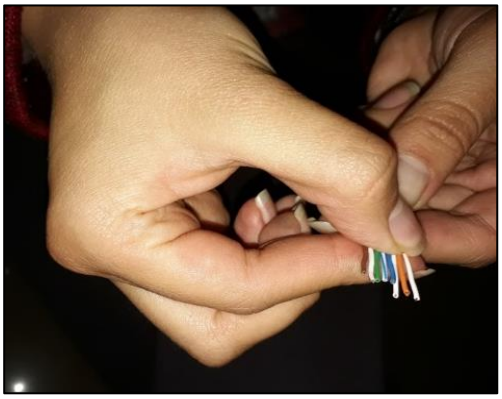
Dirección: calle García Moreno 7-43 y Modesto Jaramillo
Telf.: 062-920-626
e-mail: camcomotavalo@hotmail.com
Otavalo - Ecuador

ANEXO K. Fotografías Varias

Las siguientes fotografías representan la fachada del edificio de la Cámara de Comercio.

Metodología de procedimiento

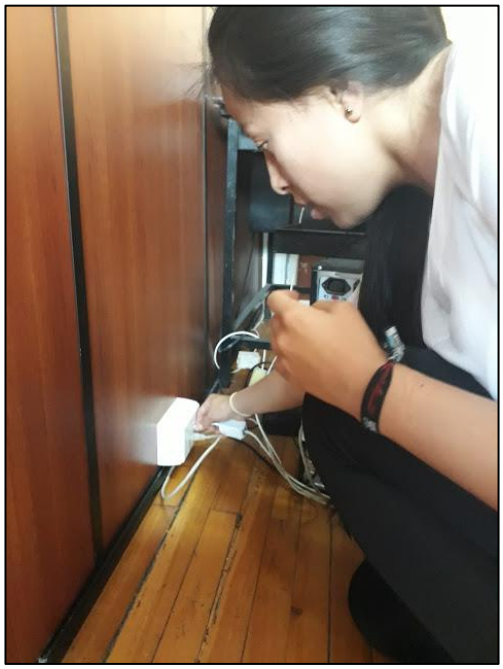
En primer lugar se realizó el ponchado de los pacth cords con la norma 568-B de acuerdo a las distancias ya calculadas



Lo siguiente fue realizar el corte (de ser necesario) de las canatelas plásticas dexon y su respectivo empotramiento en la pared para posteriormente pasar el cable a través de estas.

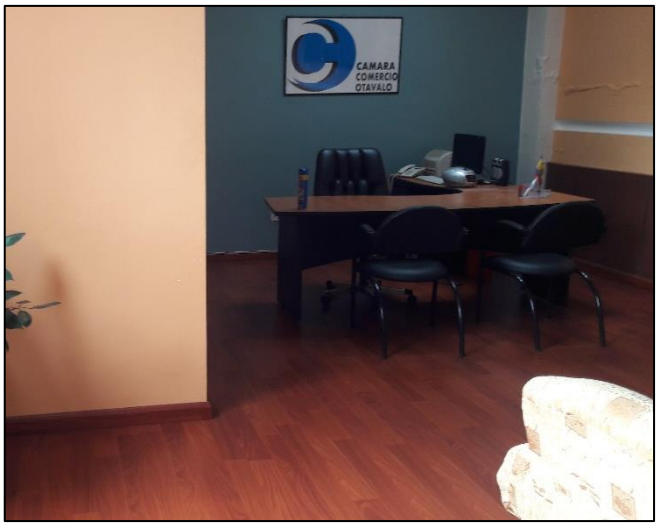
Una vez canalizados todos los pares trenzados se procedió a colocar la cubierta de las canaletas conjuntamente con los ángulos externos e internos.

Se cubrió con los cajetines cada punto doble y simple de red. Conectando adicionalmente el pacth cord de longitud 3 metros.

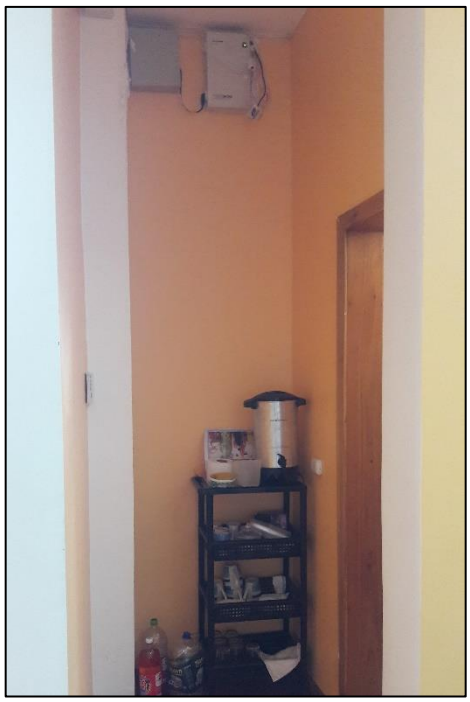


Aquí se presentan fotografías de la vista final de la infraestructura.

En esta foto, se observa la canaleta en la parte inferior correspondiente al antes y al después.

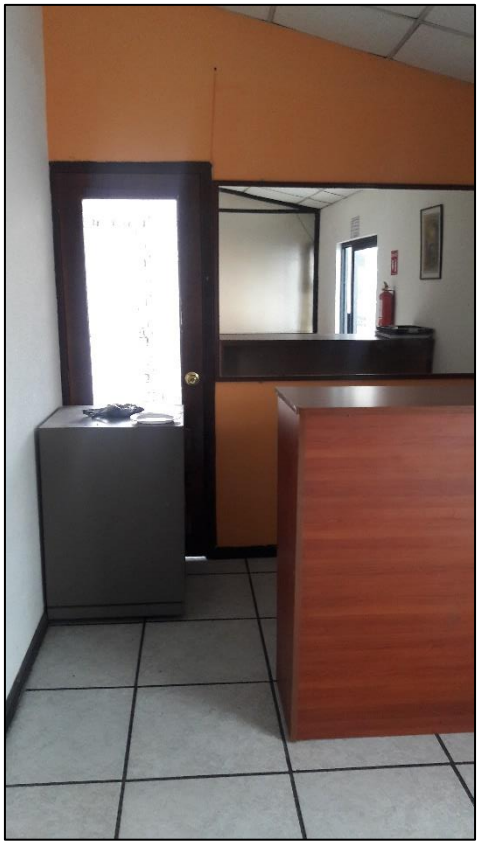


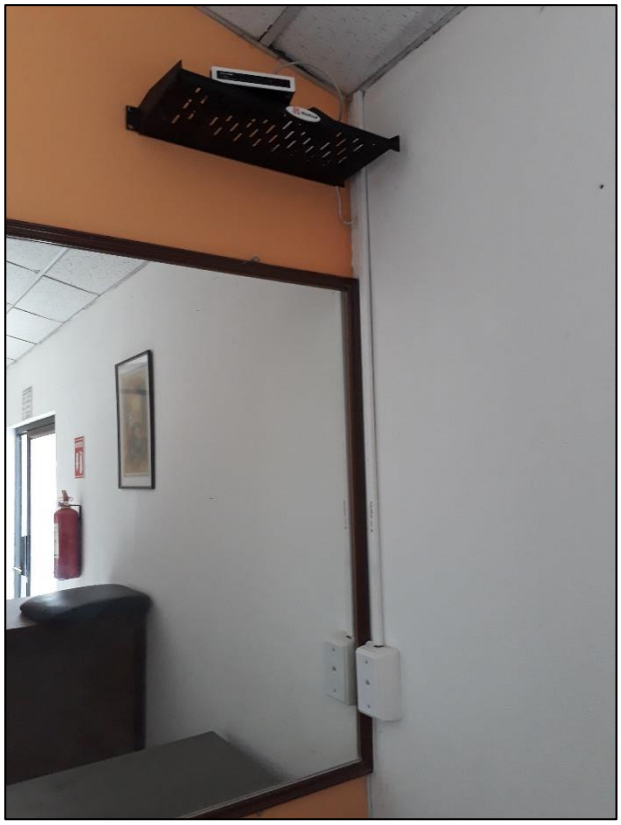
Antes y después de la colocación del rack.



Pivote electromagnético ubicado en la puerta principal que se activa con el control biométrico.

Antes y después de la colocación del rack de pared.





Finalmente se realizó el etiquetado de puntos para la identificación de estos.