UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingeniero de Sistemas

TEMA:

PROPUESTA DE REDISEÑO DE RED DE DATOS DE LA EMPRESA COBRAFACIL FABRASILISA S.A BAJO METODOLOGÍA PPDIOO Y DISEÑO TOP-DOWN.

AUTOR:

CRISTHIAN PAÚL LAGLA GALLARDO

TUTOR:

MANUEL RAFAEL JAYA DUCHE

Quito, enero del 2019

CESIÓN DE DERECHOS DE AUTOR

Yo, Cristhian Paúl Lagla Gallardo con documento de identidad N° 1720409471, manifestó mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de titulación con el tema: "PROPUESTA DE REDISEÑO DE RED DE DATOS DE LA EMPRESA COBRAFACIL FABRASILISA S.A BAJO METODOLOGÍA PPDIOO Y DISEÑO TOP-DOWN ", mismo que ha sido desarrollado para optar por el título de INGENIERO DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la ley de propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

……..

CRISTHIAN PAÚL

LAGLA GALLARDO

CI: 1720409471

Quito, enero del 2019

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema PROPUESTA DE REDISEÑO DE RED DE DATOS DE LA EMPRESA COBRAFACIL FABRASILISA S.A BAJO METODOLOGÍA PPDIOO Y DISEÑO TOP-DOWN realizado por Cristhian Paúl Lagla Gallardo, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, enero del 2019

MANUEL RAFAEL JAYA DUCHE

CI: 1710631035

DEDICATORIA

Dedico este trabajo en primer lugar a Dios por haberme guiado durante toda esta etapa de mi vida y darme toda la fuerza para continuar en los momentos más difíciles que se presentaron.

A mis Padres por toda la dedicación, amor, comprensión y apoyo incondicional en cada momento de mi vida y por ayudarme con todos los recursos para poder estudiar. Han sembrado en mí todos mis valores, mis principios, mi perseverancia y mi coraje para llegar a todas las metas que me proponga.

A mi esposa por su compañía que es una fuente de motivación, inspiración y felicidad.

Cristhian Paúl Lagla Gallardo

AGRADECIMIENTO

Agradezco a la Universidad Politécnica Salesiana que ha contribuido en mi formación profesional y personal, a mi tutor de proyecto de titulación el Ingeniero Manuel Rafael Jaya Duche por haberme orientado y motivado para realizar el trabajo, y sin duda alguna a mi familia y esposa que tuvieron paciencia y siempre confiaron en mí.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

El proyecto de titulación con el tema: "**PROPUESTA DE REDISEÑO DE RED DE DATOS DE LA EMPRESA COBRAFACIL FABRASILISA S.A BAJO METODOLOGÍA PPDIOO Y DISEÑO TOP-DOWN** ", busca rediseñar un red de datos haciendo uso de una metodología que permite conocer el modelo de negocio de la empresa para en base a eso y a las metas que la empresa tiene planteadas generar una propuesta que satisfaga y cumpla las mismas con un diseño que parte de la parte de la capa más eterna a la más interna, garantizando así un rediseño a detalle sin pasar por alto ningún requerimiento y función que se pretenda brindar a la red.

La metodología utilizada permitirá evidenciar las falencias actuales de la empresa al igual que sus virtudes tanto en el aspecto técnico como el aspecto administrativo ya que solo se puede pasar de fase cumpliendo a cabalidad cada una de las fases.

Se verifica en el capítulo 3 por medio de herramientas de monitoreo y simulación datos de mejora tales como: disminución del consumo de ancho de banda como resultante del QoS planteado en el rediseño para tráfico de voz y base d datos, mejora en un 90% en cuanto a throughput gracias a los enlaces entrantes y salientes de 10Gb planteados en el rediseño para la capa de acceso stack, la seguridad mejora en un 80% tomando en cuenta que se plantea un mayor porcentaje haciendo uso de la herramienta planteada en el rediseño basando su configuración e políticas de seguridad de TI.

Abstract

The titling project with the theme: "PROPOSAL OF REDESIGNING THE DATA NETWORK OF THE COMPANY COBRAFACIL FABRASILISA S.A UNDER METHODOLOGY PPDIOO AND DESIGN TOP-DOWN", seeks to redesign a data network using a methodology that allows knowing the business model of the company based on that and the goals that the company has proposed generate a proposal that satisfies and meets them with a design that starts from the part of the most eternal layer to the most internal, thus ensuring a detailed redesign without overlooking any requirement and function that is intended to provide the network..

The methodology used will make it possible to demonstrate the current shortcomings of the company as well as its virtues both in the technical aspect as well as the administrative aspect since only one phase can be passed, fully complying with each of the phases.

It is verified in chapter 3 by means of monitoring and simulation tools improvement data such as: decrease in bandwidth consumption as a result of the QoS raised in the redesign for voice traffic and data base, improvement by 90% in regarding throughput thanks to the incoming and outgoing links of 10Gb raised in the redesign for the stack access layer, security improves by 80% taking into account that a greater percentage is raised using the tool proposed in the redesign, basing its configuration and IT security policies.

INTRODUCCIÓN

Antecedentes

Cobra Facil S.A nace el Mes de Marzo del año 2014 como Contact-Center con el nombre comercial de "RECOVER", con el objetivo principal de darle una fuerte gestión al área de terreno (Motorizados).

Recover en sus 4 años ha logrado hacerse de varias carteras muy importantes como, por ejemplo: CNT, YANBAL, COOP. ALIANZA DEL VALLE, MOVISTAR, BANCO INTERNACIONAL, ICESA, entre otras.

El crecimiento de Recover ha sido de manera potencial debido a su innovadora manera de gestión tanto por parte del área de CALL-CENTER como del área de campo con su personal motorizado.

Problema

La Empresa Cobra Facil S.A. situada en la ciudad de Quito al contar con información financiera, administrativa y crediticia, no garantiza el buen funcionamiento tanto organizacional como tecnológico de los servicios y aplicaciones siendo esto un problema en la disponibilidad de la red provocando vulnerabilidades de seguridad, los problemas organizacionales se presentan a causa de no manejar un modelo de red bajo los estándares adecuados para su funcionamiento, por otro lado no se definen políticas de seguridad al personal técnico y administrativo que limiten el mal uso de los recursos informáticos.

El diseño de red de datos no tuvo planificación que avale el funcionamiento de la misma, el cual incumple con las normas y los estándares internacionales, otro punto importante es la ausencia de políticas ya que no se han establecido ni levantado procesos que establezcan el uso de los servicios informáticos en la empresa, la

capacidad de ancho de banda, implementación de alta disponibilidad en el centro de datos e implementación de un protocolo, mantenimiento de equipos, implementación de servidores, QoS y una mejor velocidad de transmisión de la información.

No tiene definida una Zona Desmilitarizada (DMZ) para colocar los servicios públicos de la entidad.

Justificación

Plantear el rediseño la red de datos de la Empresa Cobra Facil S.A para mejorar prestaciones de administración, monitoreo, seguridad, escalabilidad, manejo de sistemas en tiempo real, sistemas de redundancia y la optimización de recursos para la transmisión de datos permite reducir la probabilidad de caídas de aplicaciones de alta prioridad y a su vez disminuir los posibles ataques asegurando la confidencialidad de la documentación

Objetivo General

Rediseñar la red de datos de la Empresa Cobra Facil S.A, mediante el método PPDIOO bajo el diseño TOP-DOWN

Objetivos Específicos

Analizar el estado inicial de la red de datos de la Empresa Cobra Facil S.A, los servicios e infraestructura tecnológica en busca de fallos y vulnerabilidades de seguridad.

Generar la propuesta de rediseño en base a las metodologías PPDIOO para mejorar el desempeño de procesos y manejo de la información.

Simular la red propuesta y analizar los resultados obtenidos para solventar los problemas actuales y presentar una solución sostenible.

Realizar el análisis de factibilidad técnica y económica para justificar el rediseño de la red de datos propuesta.

CAPÍTULO 1

Resumen del Arte

1.1. Inicios de las Redes de Datos

Las redes de Datos se desarrollaron como solución para la necesidad de compartir recursos entre dispositivos que funcionan de forma independiente, el crecimiento de las redes fue de la mano con las nuevas tecnologías. Esto fue de gran ayuda para empresas quienes necesitaban satisfacer necesidades de control y administración de red (Cisco Networking Academy, 2010).

Inicios de las Redes de Datos

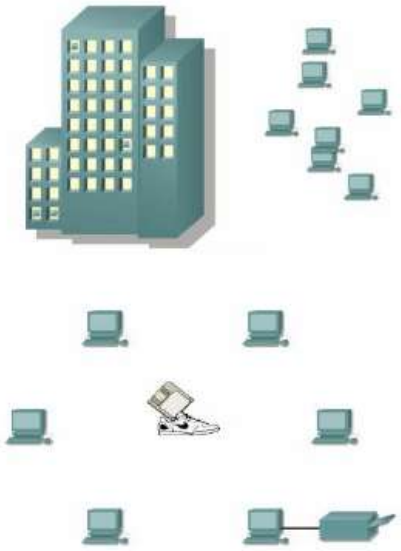

Figura 1. Inicios de Redes de Datos Dispositivos Separados.
Elaborado: (Cisco Networking Academy, 2010)

Las primeras redes aparecieron con diferente hardware y software, ya que cada empresa tenía sus propios estándares, esto ocasionaba incompatibilidad con las tecnologías. Como resultado se eliminaron los equipos obsoletos y adquirir nuevos

equipos de red dio como resultado las Redes de Área Local (LAN) (Cisco Networking Academy, 2010).

1.1.1. Redes de Área Local

Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo (Comunicaciones y Redes de Computadores).

LAN

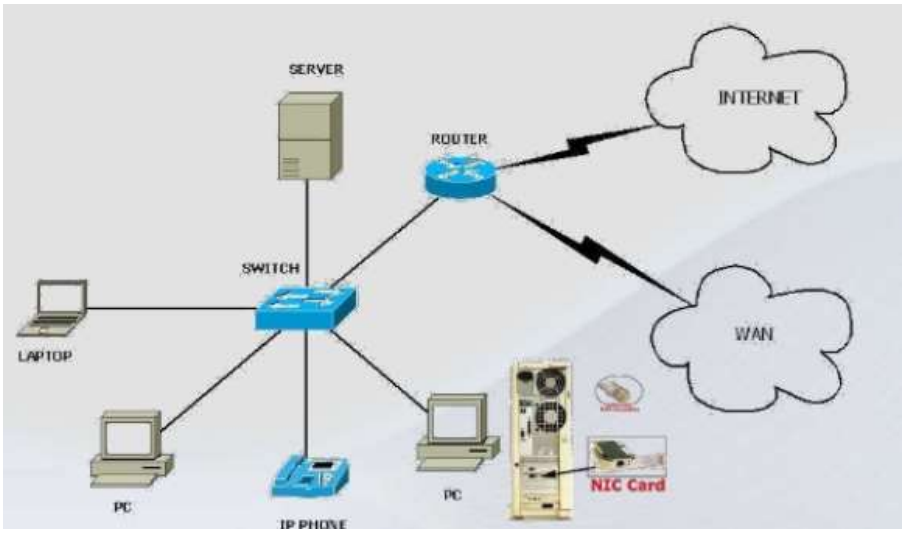

Figura 2. LAN (Red de Área Local)
Elaborado por: (Capacity Academy, 2014)

1.1.2. Características de las Redes LAN

Resistencia

Consiste en la disponibilidad que una red debe brindar ante posibles fallos lógicos o físicos de la red. La redundancia permite tener resistencia en una red. (Cisco Networking Academy , 2015)

Redundancia: El diseño de una red redundante reduce el riego de cortes o caídas de los servicios, garantizando funcionalidad de la red. (Cisco Networking Academy , 2015)

Flexibilidad

Esta característica brida la facilidad de agregar o quitar servicios o dispositivos según las necesidades de la empresa sin afectar el núcleo o base de la infraestructura de red. (Cisco Networking Academy , 2015)

Escalabilidad

Esta característica brinda la facilidad de agregar o quitar servicios o dispositivos según las necesidades de la empresa sin afectar el núcleo o base de la infraestructura de red. Escalabilidad: es un requisito importante en una red ya que brinda la capacidad de reaccionar y adaptarse a cambios en la topología de la red sin perder la calidad en él envió de datos. (Cisco Networking Academy , 2015)

Seguridad

La red debe tener un alto nivel de confiabilidad tanto físico como lógico para evitar ataque y pérdida de información; para esto se hace uso de las listas de control de acceso (ACL), redes virtuales (VLAN), etc. (Cisco Networking Academy, 2010)

Disponibilidad

Es la capacidad que debe tener la red para que los clientes puedan tener acceso a los servicios de manera permanente, es decir, la red debe permitir continuidad en las operaciones de la empresa. (Cisco Networking Academy, 2010)

1.2. Modelos Jerárquico y Modular

MODELO JERÁRQUICO DE CISCO

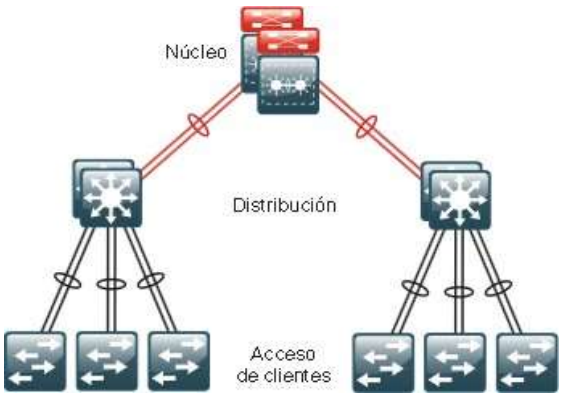

Figura 3. Modelo Jerárquico de Cisco
Elaborado por: (Padilla, 2016)

El Modelo tradicional de diseño jerárquico está conformado por las capas de núcleo, de distribución y de acceso, permite que cada parte de la red sea optimizada para una determinada funcionalidad. (Cisco Networking Academy , 2015).

1.2.1.1. Capa de Núcleo

Funciona como centro de comunicación de la red y así mismo es la que da la velocidad a la misma. Su principal propósito es evitar las fallas de comunicación y garantizar la velocidad de la Red. (Padilla, 2016)

1.2.1.2. Capa de Distribución

La capa de distribución interactúa entre la capa de acceso y la capa de núcleo para proporcionar muchas funciones importantes, entre ellas:

- Funciones inteligentes de switching, de routing.
- Alta disponibilidad al usuario final mediante switch de capa de distribución redundantes, y rutas de igual costo al núcleo.

1.2.1.3. Capa de Acceso

La capa de acceso es la última capa del modelo jerárquico y es por la cual ingresa y sale el tráfico de la red. Se encuentra conformada con equipos de capa 2 para dar acceso. Los switch que conforman la capa de acceso se conectan a la capa de distribución donde está configurado el ruteo y seguridad de la red. (Cisco Networking Academy , 2015).

1.2.2. Modelo Modular

El modelo Modular se divide en unidades lógicas que brindan un servicio específico dentro de una red. (Padilla, 2016)

El diseño modular presenta los siguientes bloques:

- Conmutación: Esta función permite evitar el desborde de trafico broadcast y definir redes virtuales (VLAN) para limitar los dominios de difusión. (Padilla, 2016)
- Núcleo: La función principal es darle velocidad a la red. (Padilla, 2016)
- Granja de Servidores: La función es permitir la comunicación son los servidores desde cualquier capa de red, tomando en cuenta que los servidores deben estar conectados directamente a la red. (Padilla, 2016)
- Gestión: La función permite gestionar la red y es la capa en la cual se instalan las aplicaciones de administración.. (Padilla, 2016)
- Frontera: La función principal es permitir la interconexión de la red interna con la red externa (LAN-Internet). (Padilla, 2016)

DISEÑO MODULAR

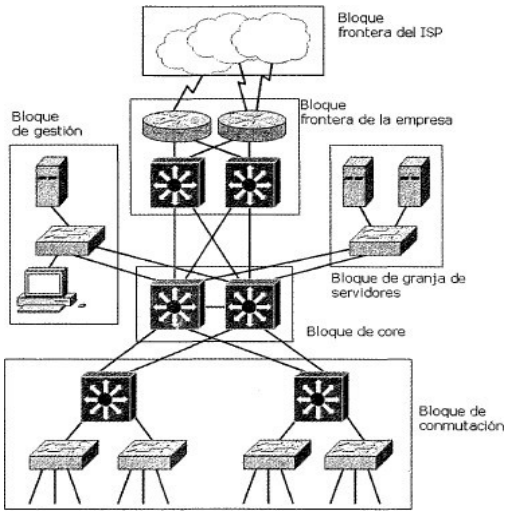

Figura 4. Diseño Modular
Tomado de: (Padilla, 2016)

1.3. Redes de Datos Convergentes

Una red convergente consiste en una arquitectura que soporte servicios de voz, video, video conferencia, lo cual, es muy beneficioso e importante para una empresa, permitiendo tener una red capaz de soportar tecnologías como datos, voz y video sobre una misma infraestructura IP, garantizando de esta manera el envío y recepción de datos. (D.Terán, 2011)

1.3.1. Protocolos de Voz en Redes Convergentes

Una red multiservicio que soporte diferentes tipos de trafico debe estar soportada por una infraestructura que le permita garantiza características fundamentales como la flexibilidad y habilidad de adaptarse a los cambios del tráfico, de esta manera poder prestar servicios en tiempo real y de esta manera garantizar el adecuado consumo de ancho de banda y calidad de comunicación evitando retardos y perdida de paquetes, entre otros. (Fajardo, 2004)

1.3.1.1. Protocolos de Transporte

Permiten digitalizar, codificar y decodificar, empaquetar, enviar, recibir y reordenar las muestras de voz: RTP, RTCP, SCTP. (Bleda, 2004)

RTP (Protocolo de Transferencia en Tiempo Real): Funciona bajo protocolo de Datagrama de Usuario (UDP) y permite él envió de voz y video en tiempo real. (Padilla, 2016)

RTCP (Protocolo de Control de Transferencia en Tiempo Real): Permite establecer un mecanismo de control en una sesión entre dos o más participantes con el envío constante de paquetes de control. (Padilla, 2016)

1.3.2. Ancho de Banda para Voz

El tráfico de voz IP tiene un consumo de ancho de banda que genera sobrecarga y esto se produce debido al empaquetado y encapsulado IP. (Joskowicz, 2013)

La Tabla 1, detalla los valores necesarios de ancho de banda de algunos códec. (Joskowicz, 2013)

Tabla 1. Detalle de Códec

Tipo de Códec	Duración de Trama(ms)	Bytes de voz/Trama	Bytes de Paquete IP	Bytes de trama Ethernet	Ancho de Banda en LAN (kbps)
G.711(64kb/s)	10	80	120	146	116.8
	20	160	200	226	90.4
	30	240	280	306	81.6
G.729 (8kb/s)	10	10	50	76	60.8
	20	20	60	86	34.4
	30	30	70	96	25.6
G.723.1 (6.3 kb/s)	30	24	64	90	23.9
G.723.1 (5.3 kb/s)	30	20	60	86	22.9

Tomado de: (Joskowicz, 2013)

1.3.3. Factores que Deterioran la Calidad de Audio

Compresión y codificación

El proceso de digitalización y codificación es necesario realizarlo para la transmisión de voz internamente por la red, sin embargo este proceso puede degradar la señal de voz original. (Joskowicz, 2013)

Demora por algoritmos de codificación

Afecta directamente a la calidad de voz ya que los códec requieren más tiempo para codificar cada muestra. (Joskowicz, 2013)

Tabla 2. Tabla de Demoras por Códec

Algoritmo	Demora típica introducida
G711 (64kb/s)	125 us
G.728 (16kb/s)	2.5 ms
G.729 (8kb/s)	10 ms
G.723 (5.3 o 6.4 kb/s)	37.5 ms
RT Audio (8kb/s)	40 ms

Tomado de: (Joskowicz, 2013)

Demoras propias de la red (latencia)

Son el resultante de la velocidad de transmisión de la red, así como su congestión y demoras producidas por sus equipos de ruteo y conmutación. (Joskowicz, 2013)

Efectos de Demoras en una Conversación

Figura 5. Efectos de Demoras en una Conversación
Tomado de: (Joskowicz, 2013)

1.4. Calidad de Servicio en Redes IP (QoS)

Calidad de Servicio, por sus siglas en inglés QoS, es una de las características que deben tener las redes convergentes modernas bien diseñada (junto con seguridad, escalabilidad y tolerancia a fallas) debido a que las aplicaciones y servicios que requieren los usuarios finales necesitan de la transmisión de voz y video en vivo con un buen nivel de QoE (Quality of Experience). Pero con el uso de estas aplicaciones, es posible que ocurra congestión en la red, justamente por la demanda excesiva de ancho de banda que generan dichas aplicaciones para que funcionen correctamente al ejecutarse simultáneamente es necesario mecanismos de control de tráfico y no degradar la experiencia del usuario. (Salazar, 2016)

Para aplicar QoS es requerido realizar los siguientes pasos:

Identificación de tipos de tráfico: consiste en determinar en base a una auditoria el tráfico que genera saturación en la red de datos. (Padilla, 2016)

Tabla 3. Políticas de QoS a Definir

Aplicación	**Clasificación Capa 3**			**Capa 2**	
	IPP	PHB	DSCP	**CoS/MPLS EXP**	
Ruteo IP	6	CS6	48	6	
Voz	5	EF	46	5	
Video	4	AF41	34	4	
Datos Críticos	3	____	25	3	
Data Transaccional	2	AF21	18	2	
Administración de red	2	CS2	16	2	
Datos Masivos	1	AF11	10	1	

Tomado de: (Padilla, 2016)

1.4.1. Modelos de Calidad de Servicios (QoS)

1.4.1.1. Modelo Best-Effort

Este modelo trata de igual manera a todos los paquetes que pasan por la red de datos, su ventaja es la implementación que no requiere mayor configuración, pero tomando

en cuenta este detalle la desventaja es que no existe ningún algoritmo que valide el QoS. (Padilla, 2016)

1.4.1.2. Modelo de Servicios Integrados

Este modelo de QoS está basado en la señalización y reserva de recursos (RSVP), bajo la implementación del modelo los router realizan una reserva de ancho de banda cuando una aplicación lo requiere, sin embargo, hace uso de muchos recursos lo que genera que el modelo no sea escalable. (Padilla, 2016)

1.4.1.3. Modelo de Servicios Diferenciados

La implementación de este modelo escalable es muy compleja por la clasificación de tráfico que maneja, tomando en cuenta esto el funcionamiento del modelo hace que en cada salto el equipo capa 3 proporcione niveles específicos para la clase de tráfico. (Joskowicz, 2013)

Los servicios diferenciados a considerar son los siguientes:

- Tráfico a ser clasificado.
- Aplicar QoS por clase.
- Dependiendo de las necesidades asignar un nivel de servicio. (Padilla, 2016)

Clasificación del tráfico: Las variaciones de tráfico dependen de la empresa y su giro de negocio (datos, voz, etc.). (Padilla, 2016).

1.5.2. Políticas de Encolamiento

1.5.2.1. Primero en Entrar Primero en Salir (FIFO)

Consiste en que el tráfico es organizado de manera en la cual los paquetes son procesados en el mismo orden en el que ingresan sin distinción. (Cadena, 2010)

Encolamiento FIFO

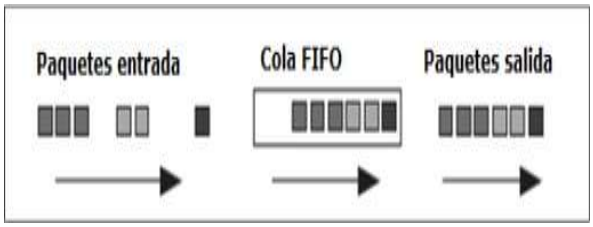

Figura 6. Primero en Entrar Primero en Salir
Tomado de: (Padilla, 2016)

1.5.2.2. Prioridad (PQ)

Se prioriza el tráfico en base a criterios como protocolos, interfaces, tamaño de paquete, etc. Se maneja con prioridades (Alta, Media, Normal y Baja).

A cada paquete se le asigna un nivel de prioridad, el paquete llevará prioridad normal, en caso de no ser asignado al mismo una prioridad. (Padilla, 2016)

Encolamiento PQ

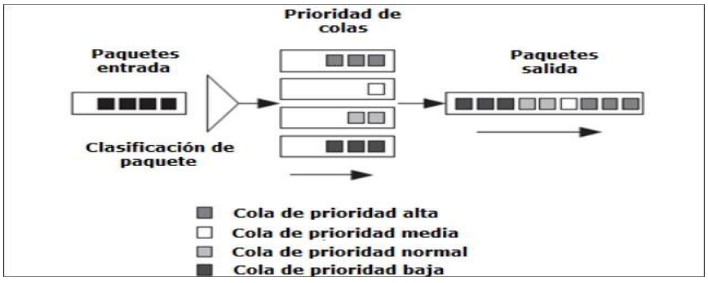

Figura 7. Encolamiento PQ
Tomado de: (Padilla, 2016)

1.5.2.3. Personalizado (CQ)

Crear colas de usuarios, colas que son atendidas secuencialmente a través de un proceso. Asegurando por medio de este mecanismo que todas las colas sean atendidas. (Padilla, 2016)

Encolamiento CQ

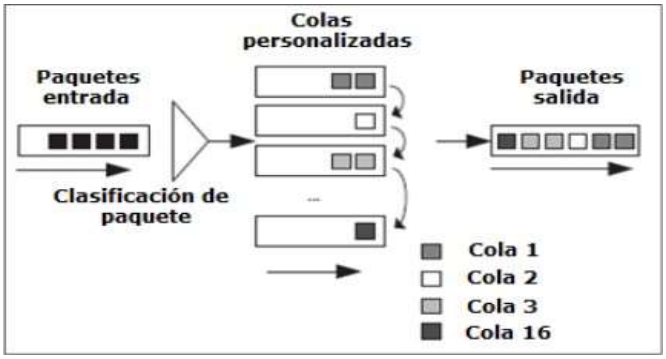

Figura 8. Encolamiento CQ
Tomado de: (Padilla, 2016)

1.5.2.4. Equitativo Ponderado (WFQ)

Asegura que la conversación por medio de un encolamiento dinámico en el cual la red comparte de manera parcial el total de ancho de banda. El encolamiento se adapta dinámicamente la topología, protocolos y aplicaciones. (Padilla, 2016)

1.5.2.5. Prioridad IP RTP

El tráfico de voz maneja un encolamiento estricto proporcionado por RTP. IP RTP debe asegurarse que la prioridad asignada no sobrepase el ancho de nada asignado para evitar congestión ya que de no ser así RTP descarta los paquetes. (Padilla, 2016)

1.5. Redes Inalámbricas

Una red inalámbrica al igual que la red cableada permite conectar equipos como computadores, impresoras, etc. Las características de las redes cableadas son las mismas que las redes inalámbricas, con la diferencia que la red inalámbrica usa el espectro radioeléctrico como medio de comunicación. Las principales ventajas de una red inalámbrica son: flexibilidad, planificación, diseño y robustez. (Dominguez, 2002)

1.6. Seguridad en Redes TCP/IP

Con el paso del tiempo los ataques a las redes de datos son más sofisticados, presentando vulnerabilidades tanto en el diseño de redes TCP/IP como en los sistemas

operativos y dispositivos conectados al Internet. TCP/IP al ser un modelo por capas un atacante puede explotar de manera independiente cada una de ellas. (Padilla, 2016)

A continuación, se describen las vulnerabilidades más comunes en cada una de las capas del modelo:

Vulnerabilidades de la Capa de Red

Estas vulnerabilidades hacen referencia al medio por el cual se realiza la conexión, por lo tanto, el problema de control de acceso y confidencialidad de la información es una de las principales desventajas de esta capa. Un ejemplo de vulnerabilidad de capa de red son los ataques punto a punto, por ejemplo desviar cables a otros sistemas, interceptación de comunicaciones, etc. (Padilla, 2016)

Vulnerabilidades de la Capa de Internet

Son ataques que afectan al datagrama IP. Los ataques más conocidos son: técnicas de sniffing, modificación de datos, entre otros. En esta capa los paquetes son autenticados mediante una dirección IP. (Padilla, 2016)

Vulnerabilidades de la Capa de Transporte

La vulnerabilidad más conocida en esta capa es la denegación de servicios. Además, se encuentran problemas como autenticación, integridad y confidencialidad. Lo más grave en esta capa es la interceptación de sesiones TCP que se encuentran ya establecidas, esto debido a las debilidades que presenta el protocolo TCP. (Padilla, 2016)

Vulnerabilidades de la Capa de Aplicación

Las vulnerabilidades dependen de la cantidad de protocolos presentes en esta capa, los protocolos más conocidos que presentan deficiencia de seguridad son: Servicio de Nombres de Dominio (DNS), Telnet, Protocolo de Transferencia de Archivos (FTP), Protocolo de Transferencia de Hyper Texto (HTTP). (Padilla, 2016)

1.6.1. Mecanismos de Prevención

Dentro de una red de computadoras con conexión a Internet, cualquier dispositivo de red puede ser un potencial riesgo de seguridad, al existir servicios que constantemente están abiertos y expuestos al exterior (Internet) como por ejemplo los servicios Web y DNS, cualquier equipo podría ser el origen de algún potencial ataque a la intranet. La prevención de ataques informáticos consiste en colocar mecanismos de seguridad que proporcionen de alguna manera un nivel de defensa que eviten el acceso no autorizado a la red interna. (García Alfaro, 2004), a continuación, se describen los mecanismos más conocidos:

1.6.1.1. Cortafuegos (Firewalls)

Un cortafuego ayuda a no comprometer la red interna del internet, es decir es una pared que permite evitar ataques provenientes del Internet, además refuerza la seguridad de los servicios que se ejecutan tanto en la red interna como en la red externa (Internet). (Padilla, 2016). Algunas de las características de un sistema cortafuegos son las siguientes:

- Filtrado de contenidos.
- Red privada virtual. (VPN por sus siglas en inglés)
- Traducción de direcciones de red. (NAT por sus siglas en inglés)
- Balanceo de carga.
- Tolerancia a fallos.
- Detección de ataques e intrusos.
- Autenticación de usuarios. (Padilla, 2016).

1.7.1.2. Zonas Desmilitarizadas (DMZ)

Una DMZ permite aislar ciertas aplicaciones o servicios separando la red empresarial del Internet. Los servicios Web y DNS al ser públicos es necesario ubicarlos en una DMZ para evitar que los atacantes logren acceder a la red interna a través de estos servidores. (García Alfaro, 2004).

Zona Desmilitarizada

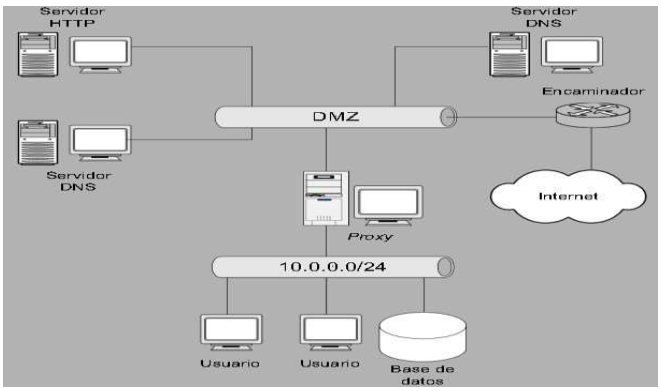

Figura 9. Zona Desmilitarizada (DMZ)

Ciclo de Vida del Desarrollo de Sistemas

En redes de datos los diseños lógicos y físicos de la red se desarrollan y continúan existiendo durante un periodo de tiempo determinado. (Padilla, 2016)

La gran mayoría de sistemas incluyendo las redes de datos siguen pasos o fases, que indican la creación, planeación, optimización y pruebas, incluso la retroalimentación

Ciclo de Vida de Desarrollo de Sistemas

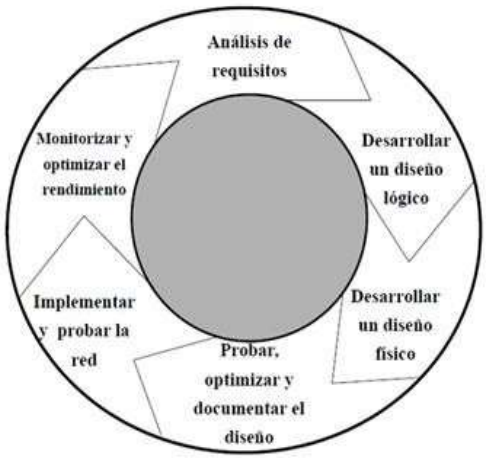

Figura 10. Ciclo de Vida de Desarrollo de Sistemas
Tomado de: (Padilla, 2016)

por parte de los usuarios hace que estas fases sean ejecutadas nuevamente para lograr un mejor diseño. (Padilla, 2016)

1.6.2. Metodología de Redes

El administrador de red hace uso de las metodologías de red para hacer un diseño óptimo y adaptable a las necesidades informáticas de la empresa alineado a su presupuesto. (Padilla, 2016).

A continuación, se describen algunas de las metodologías de redes:

1.6.2.1. Metodología de Diseño Top-Down

Permite diseñar una red capaz de atender las necesidades del cliente comenzando desde las capas superiores del modelo OSI hasta llegar a las capas inferiores, con el propósito de cumplir con los objetivos, metas del negocio. (Padilla, 2016)

Ventajas

- Optimización en gestión de proyectos.
- Flexible a cambios.
- Reduce los errores en el diseño.
- Aumenta la productividad.
- Retroalimentación de errores para su corrección. (Padilla, 2016)

1.8.1.2. Metodología PPDIOO

La metodología PPDIOO posee su origen bajo los lineamientos propuestos en el ciclo de vida PPDIOO que usa Cisco para administración de red. El seguimiento de este ciclo de vida propuesto ayuda a cumplir objetivos trazados como son la disminución del costo total de administración de la red y aumento de disponibilidad de la red a su vez mejora en agilidad para implementación de cambios en la estructura de la red. El

ciclo de vida así puede ser útil para implementación de nuevas redes, así como para actualizaciones en redes existentes. Los elementos que conforman el ciclo de vida forman un círculo sin fin puesto que por ejemplo el paso de optimización conlleva a realizar actividades como identificar cambios, validar en la infraestructura existente; misma que conllevarían a iniciar desde el paso de preparación. (Guerra, 2016).

Metodología PPDIOO

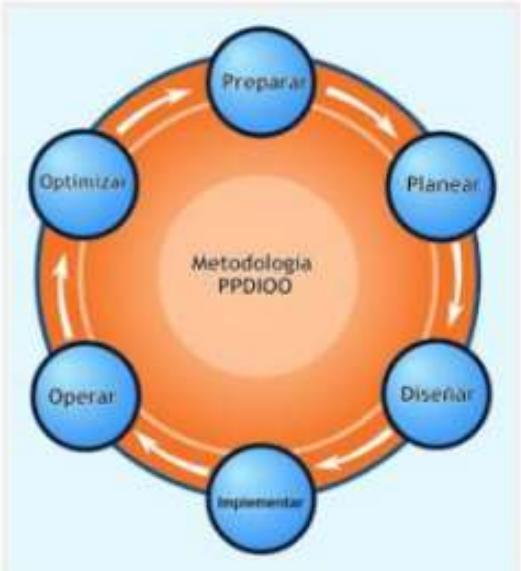

Figura 11. Fases de Metodología PPDIOO
Tomado de: (Guerra, 2016)

Beneficios de PPDIOO

Disminución de costo de propiedad al realizarse validaciones de: requerimientos de tecnología, planeación de cambios en la infraestructura y determinación de requerimientos de recursos. Además, al contemplar y alinearse con los requisitos técnicos y objetivos de negocio. Y finalmente al mejorar la eficiencia de red y del personal de apoyo y disminución en costos operativos (Guerra, 2016)

Aumento de disponibilidad de la red al proporcionar un diseño solido de la red que posee altas consideraciones de seguridad que soportan el diseño propuesto. Además

de ejecutar pruebas piloto o prototipos previo a la implementación en producción (Guerra, 2016)

Agilidad de los negocios estableciendo requisitos de negocio, integrando requisitos técnicos y objetivos de negocio en un diseño detallado y mediante un alto dominio de experiencia en la configuración, instalación e integración de los componentes del sistema además de existencia de mejora continúa (Guerra, 2016)

Mayor velocidad de acceso a aplicaciones y servicios mediante análisis profundo de objetivos técnicos y análisis de equipos y tecnologías a ser implementados que soportan los servicios de red actuales y previstos. Aumento de disponibilidad de la red y de las aplicaciones que se ejecutan sobre ella (Guerra, 2016)

Fases del ciclo de vida PPDIOO

PPDIOO conforma su acrónimo con cada primera letra (tomado del inglés) de la fase que la compone, siendo:

- P (Prepare) Fase de Preparación involucra temas de presupuesto, estrategia de red.
- P (Plan) Fase de Planeación involucra evaluación de la red, análisis de deficiencias.
- D (Design) Fase de Diseño involucra el diseño de la solución (productos, servicios).
- I (Implement) Fase de Implementación involucra la puesta en marcha dela solución.
- O (Operate) Fase Operativa involucra el mantenimiento de la red.
- O (Optimize) Fase de Optimización involucra la administración proactiva de la red.

Recopilación de requisitos de red

El proceso de recopilación de requisitos se puede dividir en cinco pasos. Durante estos pasos (en lenguaje de proyectos denominado hitos), el diseñador analiza el proyecto con el personal del cliente para determinar y reunir los datos necesarios, incluyendo la documentación apropiada, siendo los pasos:

1. Identificar las aplicaciones de red y servicios de red planificados.
2. Determinar los objetivos de la organización.
3. Determinar las posibles limitaciones de la organización.
4. Determinar los objetivos técnicos.
5. Determinar las limitaciones técnicas que deben ser tomados en cuenta.

Caracterizar la red existente

En términos generales se analiza el estado de salud de los componentes de la red con fines de determinar requerimientos de hardware o software. Su fin es modernizar y re estructurar la red. Para la ejecución de esta actividad se sirve de herramientas de recolección de datos que permiten evaluar y analizar la red (Guerra, 2016).

Diseño de la topología de red y solución

Una vez que la red ha sido examinada y se han definido los componentes de la misma: es necesario crear un diseño de red. En primer lugar es indispensable el poder definir un diseño lógico para lo cual se recomienda el subdividir la red en módulos, mucho más si se trata de redes medianas o grandes (Guerra, 2016).

Si bien esta tercera fase es la última de esta metodología dentro de la misma incluye la realización de un piloto o prototipo, así como la puesta en producción. Es decir, esta fase incorpora las fases restantes del ciclo de vida (Guerra, 2016).

CAPÍTULO 2

ANÁLISIS DE REQUERIMIENTOS Y DE LA SITUACIÓN ACTUAL DE RECOVER

2. Introducción

El siguiente capítulo contiene el levantamiento de información y requerimientos de Recover tanto de la situación actual de la empresa como las metas del negocio y la infraestructura con la cual se cuenta al momento.

Analizando servicios tanto internos como externos que pasan por la red, yendo de lo general hasta lo más específico que son las aplicaciones y comunidad de usuarios, sustentado cada dato con el respectivo monitoreo del servicio.

2.1. Aspectos Fundamentales de la Infraestructura de Recover

Para realizar un correcto rediseño de red que cumpla con los requerimientos de Recover es necesario levantar el estado actual de los equipos, personal y servicios de los cuales disponen y así poder determinar el impacto que va a tener en los mismos el rediseño.

2.2. Estado Actual

Recover cuenta con su matriz en Quito, lugar en el cual se encuentra concentrado la mayor cantidad de personal Administrativo, Operativo y Ejecutivo de la empresa, mientras que en su otra sucursal ubicada en la ciudad de Guayaquil cuenta con una cantidad menor de personal.

La red de Recover conecta amabas sucursales por medio de un enlace WAN, el mismo por el cual para tráfico de datos, voz y video.

2.3. Ubicación

Recover dispone de su matriz en la ciudad de Quito ubicada en la Av.6 de diciembre y Santa Lucía.

Ubicación de Recover Matriz

Figura 12. Ubicación Recover Matriz
Tomado de: (Recover, 2018)

2.4. Análisis de Requerimientos

2.4.1. Análisis de las Metas del Negocio

Misión

"Somos una empresa de servicios y soluciones de Contact Center, que busca liderar el mercado, generando fuentes de trabajo; para satisfacción de nuestros clientes y trabajadores brindando un servicio de calidad y excelencia en la gestión" (Recover, Mision,Vision, 2015).

Visión

"En el 2018 seremos reconocidos por una gestión efectiva en servicios de Contact Center para instituciones financieras, puntos comerciales y el mercado a nivel nacional, promoviendo una cultura de responsabilidad, disciplina y compromiso" (Recover, Mision,Vision, 2015).

Objetivos

- Liderar el mercado de Cobranza y Contact-Center.
- Brindar un servicio de calidad y excelencia en la gestión innovando siempre frecuentemente a la par de tecnología.
- Generar fuentes de trabajo para la satisfacción de nuestros clientes y trabajadores.
- Mantener el personal operativo y administrativo altamente capacitado para tener una garantía técnica y profesional con los clientes.

2.4.2. Análisis de las Metas Técnicas

Recover cuenta con una red que no se encuentra debidamente estructurada ya que aún se encuentra muy lejos de ser una red convergente que permita el soportar el tráfico de datos, voz y video sin presentar problemas de retardo o pérdida de datos.

Al presentar el rediseño se busca dar mejor Calidad de Servicio y hacer una buena experiencia para el usuario, entre las principales metas de rediseño se detallan las siguientes:

- Brindar un correcto tratamiento a la información.
- Reducir gastos de operación.
- Tener una administración centralizada.
- Implementar una red inalámbrica con seguridad y monitoreo.
- Implementar seguridad interna en la red.
- Tener una homogeneidad de los equipos de red.
- Buscar futuras certificaciones que permitan a la empresa una mayor competitividad en el mercado.

- Mejorar la Calidad de Servicio tanto para los usuarios internos como para usuarios externos y clientes.

En base a las metas anteriormente detalladas el departamento de sistemas busca que su red de datos e infraestructura en general cumpla con los requerimientos técnicos con la finalidad de acceder a una certificación.

2.4.3. Análisis de la Red Existente

Para realizar un correcto rediseño es necesario analizar correctamente la infraestructura tomando en cuenta todos los dispositivos instalados junto con la segmentación actual y así plantear los cambios a realizar para cumplir los requerimientos de Recover.

En la Figura 17, se muestra la topología que actualmente dispone Recover en la ciudad de Quito, se debe tomar en cuenta que el cableado vertical y horizontal de la empresa

Topología Física Recover Matriz

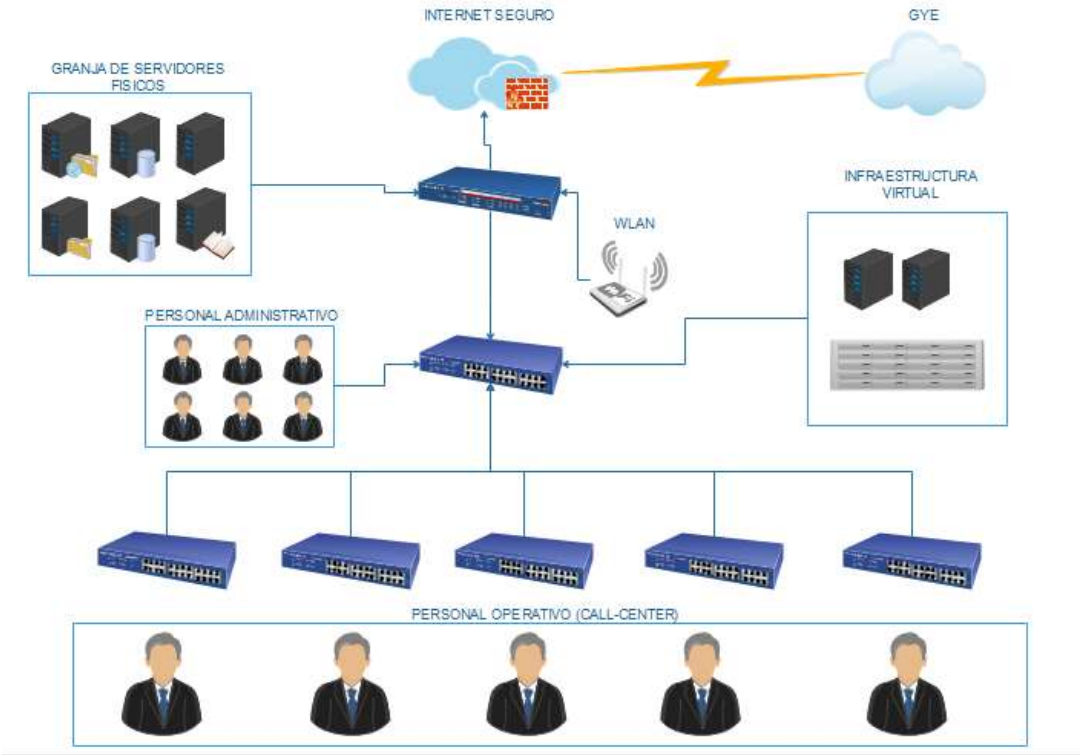

Figura 13. Topología Física Recover Matriz
Tomado de: (Recover, 2018)

La sucursal de GYE tiene una red básica que permite la comunicación del personal por medio de cableado estructurado, tal cual la Figura 18.

Topología de Red Sucursal GYE

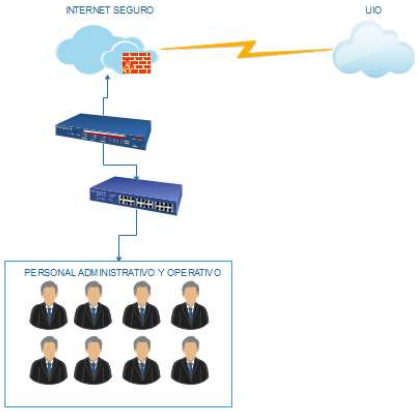

Figura 14. Topología de Red GYE
Tomado de: (Recover, 2018)

2.4.3.1. Análisis de la Infraestructura Física

Recover es una empresa que ha crecido de manera exponencial en los últimos años por lo tanto la red al igual que sus componentes se han tenido que ir adecuando conforme a las necesidades que surgen como resultado de un crecimiento.

La granja de Servidores, equipos de Conmutación y Ruteo se encuentran ubicados en el primer piso de la Matriz en un cuarto de racks en los cuales no se dispone de un enfriamiento total del cuarto, sino que hay dos Racks que tiene enfriamiento interno, la seguridad de ingreso al Cuarto de Data Center es obsoleta ya que es cuestión de chapas de puertas normales para su acceso.

Los racks internos cuentan con una fuente de alimentación eléctrica ininterrumpida (UPS), a su vez dentro de ellos se encuentra en funcionamiento un ATS que permite realizar un mantenimiento periódico al UPS de Data Center de manera regular.

Data Center Recover Matriz

Figura 15. Data Center Recover Matriz
Tomado de: (Recover, 2018)

2.4.3.2. Distribución Física de Dependencias

Recover dispone de una instalación física en su matriz de dos pisos los cuales se encuentra distribuidos de la siguiente manera:

Planta Baja:

- Call-Center1.
- Departamento de Cobranza Domiciliaria.
- Inteligencia de Operaciones.
- Cuarto de UPS y Rack Eléctrico.
- Servicio al Cliente.

Planta Baja Recover Matriz

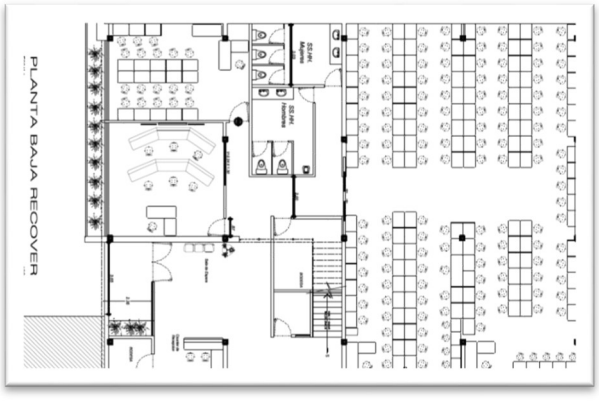

Figura 16. Planta Baja Recover Matriz
Tomado de: (Recover, 2018)

Primer Piso:

- Gerencia General
- Departamento Financiero
- Departamento de RRHH
- Departamento de Sistemas
- Data-Center (Cuarto de Racks)

Primer Piso Recover Matriz

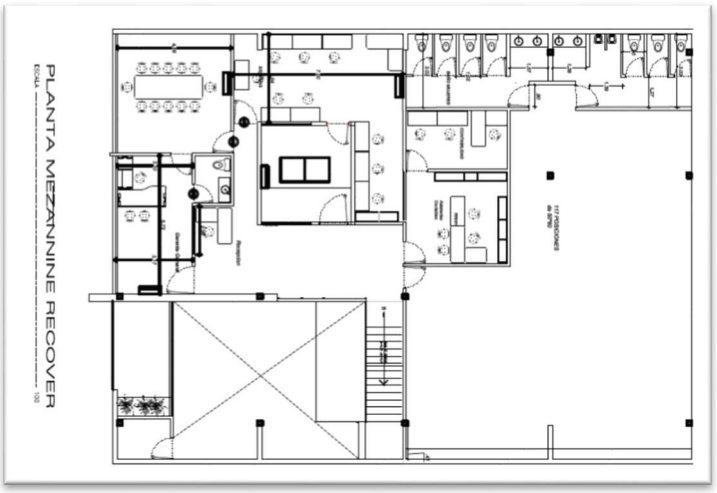

Figura 17. Primer Piso Recover Matriz
Tomado de: (Recover, 2018)

En el Data Center se encuentran ubicados servidores y equipos de red de manera en la cual solo el router que al momento hace de core junto con el Switch de distribución están juntos en un rack con todos los servidores físicos, Storage y NAS, mientras en el otro Rack se encuentra todos los switch de acceso y los enlaces de fibra y router de proveedores con los cuales se tiene un servicio.

Fotografía Frontal de Racks.

Figura 18. Vista Frontal de Racks
Tomado de: (Recover, 2018)

La Figura 18, muestra la parte frontal de los Racks con los equipos de red y servidores.

Fotografía Posterior de Racks

Figura 19. Vista Posterior Racks
Tomado de: (Recover, 2018)

La Figura 19, muestra el cableado que permite la comunicación entre dispositivos de red y servidores con los diferentes usuarios que acceden a la LAN de Recover.

2.4.3.3. Infraestructura de Datos y Voz

Como resultante del análisis del levantamiento inicial se podrá observar que el cableado de datos se encuentra perfectamente etiquetado y certificado sin embargo es cierto que no está correctamente ordenado el cableado interno en los racks ya que existen muchos cables tanto de datos como eléctricos que se encuentran mezclados internamente. Además, es importante mencionar que se encuentran funcionando switches de diferentes marcas los cuales no permiten que la administración sea centralizada y pudiendo dar a notar que uno de ellos ya se encontraba presentados puertos sin funcionamiento.

2.4.3.4. Dispositivos de Red

Para verificar el estado de cada dispositivo de red es necesario tomar en cuenta el número de usuarios concurrentes que acceden a la red.

Tabla 4. Equipos de Red Detallados

Cantidad	Detalle	Total de Puertos / Puertos Disponibles	Función
1	Switch HP V1910-48g	52/15	Acceso
1	Switch HP V1910-48g	52/24	Acceso
1	Switch HP V1920-48g	52/32	Acceso
1	Switch HP V1910-48g	52/11	Acceso
1	Switch Cisco SG300-52p	52/4	Acceso
1	Switch Cisco 2960-48p	50/12	Distribución
1	Router Cisco C891-24x	24/6	Núcleo
1	Router RV110W	4/4	WIFI

Nota: Número de puertos ocupados y disponibles por equipo.

2.4.3.5. Estado Actual del Switch de Distribución/Núcleo

Recover maneja como núcleo un Router Cisco de la Serie C891, el mismo que dispone de 24 puertos este presenta el siguiente detalle de CPU.

Procesos de Switch de Core

```
recover_uio_001#show processes cpu sorted | e 0.00
CPU utilization for five seconds: 13%/5%; one minute: 13%; five minutes: 12%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  99   108392476   132602241        817  5.51%  5.57%  5.59%   0 c891_24x_dx_mrvl
   6     7998284      988248       8093  1.19%  0.21%  0.13%   0 Check heaps
  97    36366676     8998223       4041  0.79%  0.74%  0.72%   0 ILPM
 407      316028     5484706         57  0.23%  0.19%  0.18%   0 Per-Second Jobs
 161      479460     9084120         52  0.07%  0.07%  0.07%   0 Spanning Tree
 321       16684    84952514          0  0.07%  0.04%  0.05%   0 MMA DP TIMER
  35     3607808    29610906        121  0.07%  0.07%  0.07%   0 ARP Input

recover_uio_001#show processes memory sorted | e 0.00
Processor Pool Total:  800747736 Used:   67616304 Free:  733131432
      I/O Pool Total:   61787840 Used:   17285568 Free:   44502272
```

Figura 20. Resultado Comando show processes
Tomado de: (Recover, 2018)

Se puede observar en la Figura 20, que el uso del CPU está siendo moderado sin embargo esto se mejoraría haciendo uso de un Switch capa 3 con mayor capacidad de CPU y memoria, con esto se evitaría la saturación en la red y por ende una cantidad de errores inferiores a los que actualmente se generan con un router, evitando resultados como el de la Figura 21.

Errores en Interfaces del Switch de Core

```
recover_uio_001#show interfaces counters errors

Port        Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize
Gi1/1               0          0          0          0         0
Gi1/2               0          0          0          0         0
Gi1/3               0          0          0          0         0
Gi1/4               0          0          0          0         0
Gi1/5               0          0          0          0         0
Gi1/6               0          0          0          0         0
Gi1/7               0          0          0          0         0
Gi1/8               0          0          0          2         0
Gi1/9               0          0          0     176974         0
Gi1/10              0          0          0          0         0
Gi1/11              0          0          0   13589614         0
Gi1/12              0          0          0          0         0
Gi1/13              0          0          0    8996735         0
Gi1/14              0          0          0         54         0
Gi1/15              0          0          0          0         0
Gi1/16              0          0          0          0         0
Gi1/17              0          0          0          0         0
Gi1/18              0          0          0     143962         0
Gi1/19              0          0          0      45819         0
Gi1/20              0          0          0     175469         0
Gi1/21              0          0          0          0         0
Gi1/22              0          0          0          0         0
Gi1/23              0          0          0          0         0
Gi1/24              0          0          0          0         0
```

Figura 21. Resultado Comando show interfaces counters errors
Tomado de: (Recover, 2018)

2.4.3.6. Análisis de Infraestructura Lógica

Para entender el funcionamiento lógico actual de la red es necesario saber la velocidad de transmisión y a la cual trabajan los dispositivos de red tomando en cuenta si manejan una plataforma administrable que permita dar un seguimiento y control a cada dispositivo conectado. A continuación, un detalle de cada dispositivo en la Tabla 6.

Tabla 5. Detalle de Equipos de Red (Administración)

Tipo	Modelo	Administrable
Switch	v1910-48g	Si (Web)
Switch	v1910-48g	Si (Web)
Switch	v1910-48g	Si (Web)
Switch	v1920-48g	Si (Web)
Switch	2960x	Si (CLI)
Router	C891	Si (CLI)
Router	RV1100W	Si (Web)
Switch	SG-300	Si (CLI)

Nota: Descripción de equipos de red, modelo y administración.

Si bien es cierto que cada dispositivo es administrable también es cierto que al no ser de una misma marca su administración central es compleja e inestable, en cuanto a seguridad existen serios problemas ya que hay equipos que se encuentran funcionando con sus configuraciones de fábrica lo que genera mucho tráfico broadcast y da como resultado un bajo rendimientos de los equipos.

2.4.3.6.1. Direccionamiento en Privado

Recover mantiene una segmentación de red por departamentos para lo cual maneja dos segmentos de red una para servidores y otra para los distintos departamentos que tiene.

Tabla 6. Segmentación y Direccionamiento de Recover

Departamento	Rango de Direcciones	Vlan (ID)
Equipos de Red	172.17.5.0/24	5
Servidores	192.168.10.0/24	6
SAN	172.17.7.0/24	7
Call-Center	172.17.10.0/24	10
Call-Center 1	172.17.8.0/24	8
Call-Center 2	172.17.9.0/24	9
Gerencia	172.17.11.0/24	11

Sistemas	172.17.12.0/24	12
Operaciones	172.17.13.0/24	13
Financiero	172.17.14.0/24	14
Telefonos_Impresoras	172.17.15.0/24	15
Telefonia_Dragon	172.17.16.0/24	16
Wifi	172.17.20.0/24	20
Enlace_Icesa	172.17.21.0/24	21
Cnt_1		31
Cnt_2		32
Dragon_Cnt_1	7.7.7.0/24	34
Enlace_Level_3	10.141.141.101/30	64
SIP_Telefonica		65

Nota: Rango de direccionamientos y vlan correspondiente.

El equipo que realiza el ruteo entre las Vlan es el router que hace de Núcleo y baja las mismas por medio de un puerto troncal hacia el Switch de Distribución.

Se tiene una red independiente de Servidores los cuales tienen el direccionamiento fijo a continuación detallado en la Tabla 8.

Tabla 7. Detalle de Servidores y Direccionamiento

Equipo	Dirección IP
VMWARE Esxi1	192.168.10.60
VMWARE Esxi2	192.168.10.61
VMWARE VCenter	192.168.10.62
Storage	192.168.10.66
Telefonía Dragón	192.168.10.159
Aplicaciones Dragón	192.168.10.158
Base de Datos Dragón	192.168.10.160
Telefonía Dragón	192.168.10.64
Aplicaciones Dragón	192.168.10.63
Base de Datos Dragón	192.168.10.65
Base de Datos SYSSGECO	192.168.10.74
Base de Datos SYSSGECO	192.168.10.75
Active Directory / DNS	192.168.10.100
Sistema Financiero (SAFI)	192.168.10.50
NAS	192.168.10.148
FTP/SFTP	192.168.10.115
SBC	192.168.10.90
Servidor de Antivirus	172.17.12.125

Nota: Direcciones Ip de servicios ofrecidos.

2.4.3.6.2. Servicios Internos

Recover cuenta con servidores que prestan un determinado servicio al interno de la LAN, a continuación, se detallarán en la Tabla 9.

Servidor de Antivirus: El servidor es un medio de protección para cada usuario que se encuentra conectado a la red y tiene debidamente instalado el antivirus, este permite la creación de reglas y políticas conforme a la institución que lo requiera.

Servidor Active Directory: Facilita la creación, localización y administración de cuentas y usuarios, además de brindar un servicio de directorio que puede tener políticas y reglas conforme a los requerimientos de la Empresa.

Servidor FTP/SFTP: Permite compartir información con los clientes y usuarios de acuerdo a su necesidad.

Servidores de Bases de Datos: Estos servidores de Datos contienen información importante la misma que es utilizada por cada uno de los departamentos por medio de cubos de información y reportes diarios.

2.4.3.6.3. Direccionamiento Público

Recover tiene asignada como direccionamiento publico la subred 181.188.211.114 con mascara 255.255.255.248, esto quiere decir que se dispone de 6 direcciones públicas las cuales serán detalladas en la Tabla 9.

Tabla 8. Direccionamiento Público

Dirección IP Pública	Equipo/ Servicio
181.188.211.115	Servidor Web
181.188.211.116	Servidor Ftp
181.188.211.117	Disponible

181.188.211.118	Firewall
181.188.211.119	Disponible
181.188.211.120	Disponible

Nota: Direcciones Ip públicas.

Adicional a esto, posee 2 troncales con CNT las mismas que se son pasadas por vlans por medio del switch de distribución, estas se encuentran configuradas para las llamadas inbound y están detalladas en la Tabla 10.

Tabla 9. Troncales Telefónicas

Troncal	Direccionamiento	Número Telefónico
Cnt_1	10.208.43.8/30	23932400
Cnt_2	10.208.43.12/30	23932420

Nota: Direcciones de troncales telefónicas.

2.4.3.6.4. Servicios Externos

El Servicio de Internet es por medio de un punto de red que va conectado punto a punto a un router de Telefónica ubicado en las instalaciones de Recover y el mismo por el cual se tiene acceso al servicio de Internet con una velocidad de 10 Mbps, Seguridad perimetral con Firewall FortiGate y Troncal SIP por diferente Interface.

Se cuenta con un enlace de datos de 2 Mbps para la ciudad de Guayaquil y otro con ICESA con las mismas características.

Todo lo anteriormente detallado en la Figura 25.

WAN de Recover

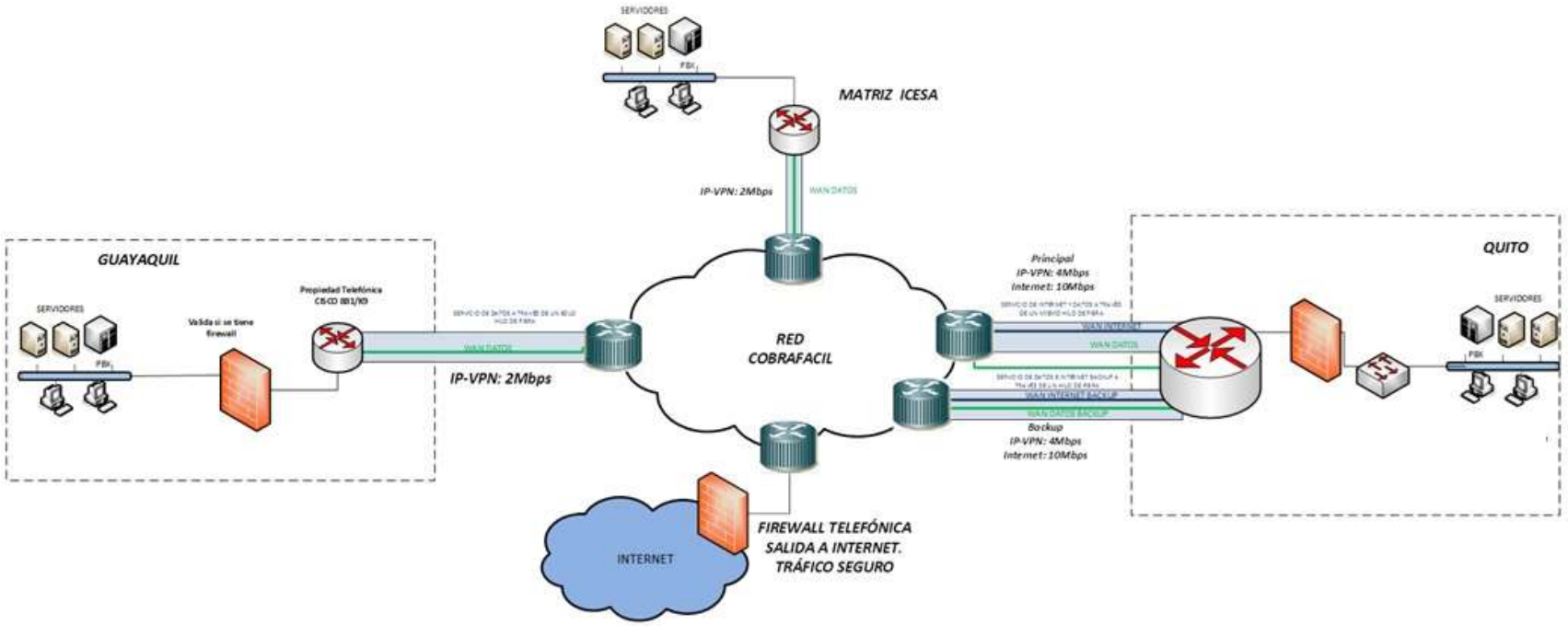

Figura 22. Topología WAN de Recover
Tomado de: (Recover, 2018)

2.4.3.6.5. Análisis de Aplicaciones y Comunidades de Usuarios

Si bien es cierto Recover maneja una segmentación por Vlan que le permite tener un control de permisos a nivel de accesos a Internet mas no en cuanto a permisos internos por la falta de ACL de control, ese es el motivo por el cual se detalla la siguiente tabla con los permisos actuales de cada departamento hacia los aplicativos internos y externos.

Tabla 10. Detalle de Accesos y Permisos para Aplicativos.

Departamento	Piso	Aplicación							
		DragonTech (PBX)	Enriquecedor	Correo Electrónico	Sis. Crédito	Sis. Financiero	Ftp/Sftp	Carpetas Compartidas	SAFI
Gerencias	1	X	X	X	X		X	X	X
Financiero	1	X	X	X	X	X		X	X
Sistemas	1	X	X	X	X	X	X	X	X
Operaciones	Pb	X	X	X	X		X	X	X
Call-Center	Pb	X	X					X	X

Nota: Detalles de aplicaciones y permisos.

Si bien es cierto hay departamentos que no tienen acceso a determinados servicios, pero en estos casos es por simple compartición especifica o porque no está creado el acceso directo en determinado departamento.

2.4.4. Análisis del Tráfico de la Red

Luego de verificar los servidores que prestan un servicio interno dentro de la LAN, es necesario analizar el tráfico que ellos generan tanto de entrada como de salida para lo cual será necesario realizar el respectivo monitoreo del equipo de comunicación al que se encuentran conectados.

Para capturar el tráfico de cada servidor utilizaremos la herramienta de monitoreo PRTG, la misma que permite medir el tráfico y el uso de los componentes de red.

El monitoreo de cada uno de los Servidores en mención a continuación detallado fue realizado por un periodo de una semana.

2.4.4.1. Análisis del Tráfico de Datos

Servidor DNS

El Servidor DNS tiene problemas con actualizaciones, pero el servicio como tal se encuentra funcionando correctamente como se puede ver en la Figura 23 a continuación detallada:

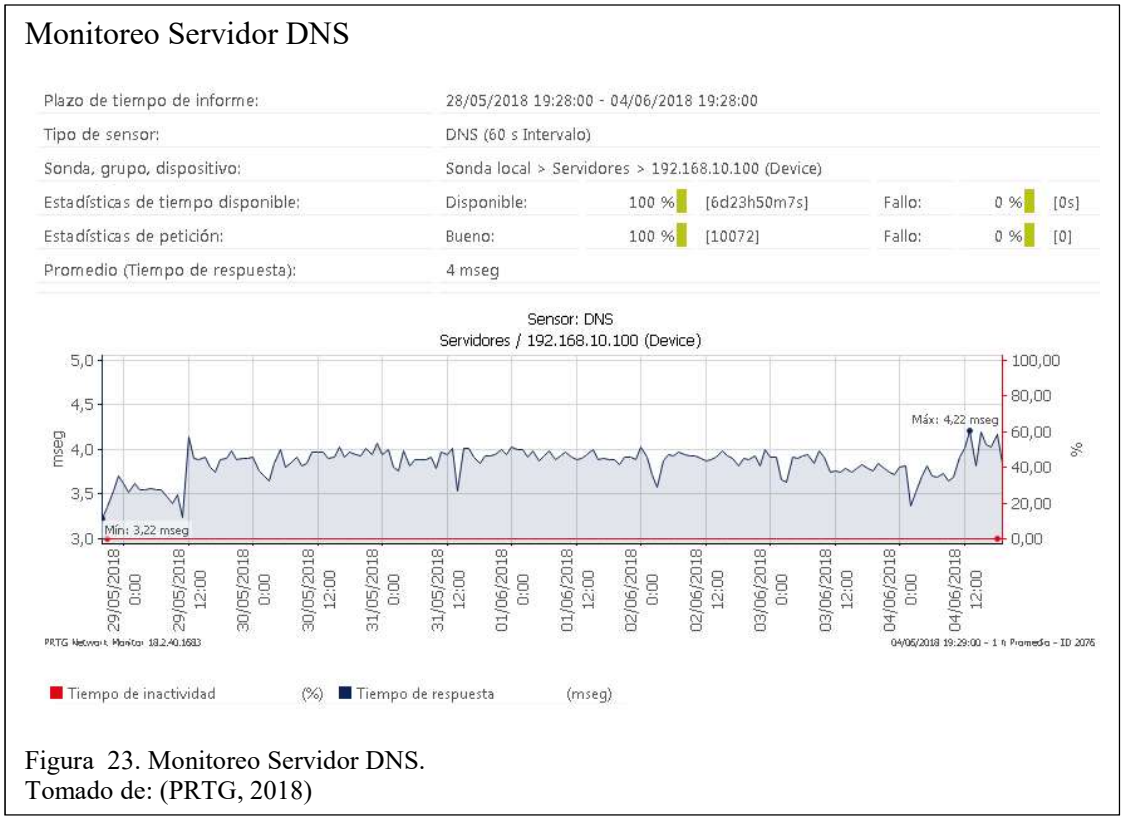

Figura 23. Monitoreo Servidor DNS.
Tomado de: (PRTG, 2018)

Servidor de Base Datos

El servidor de Base de Datos es muy importante en cuanto a la producción de Recover debido al constante ingreso de gestiones y consumo de Web Services, sin contar con que la reportera y los cubos de información se encuentran pegados directamente a la Base y al momento de actualizarse generan una gran lentitud e incluso una pérdida de conexión entre la Base y la Aplicación Web ver Figura 24.

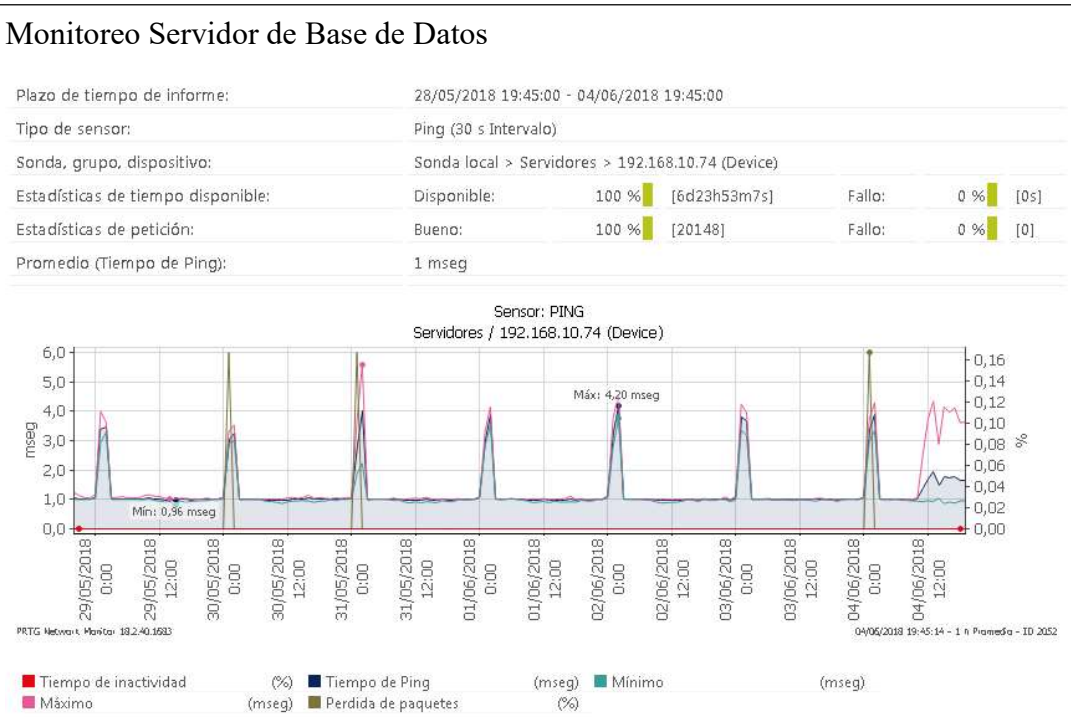

Figura 24. Monitoreo de Base de Datos
Tomado de: (PRTG, 2018)

Servidor de Aplicaciones Web

Es necesaria una revisión del consumo del aplicativo web a continuación en la Figura 25, se detalla el consumo de data del Servidor de Base de Datos:

Monitoreo Servidor de Aplicaiones Web

Figura 25. Monitoreo de Aplicativo Web.
Tomado de: (PRTG, 2018)

Servicio de Internet

El Servicio de Internet seguro que dispone Recover fue monitorizado por medio de la herramienta Orion para verificar el consumo tanto del Servicio de Internet como de los enlaces que se encuentran levantados con la sucursal de Guayaquil y la Compañía ICESA, las gráficas resultantes se encuentran detallados en las Figuras 26,27,28 y 29:

Monitoreo Servicio de Internet

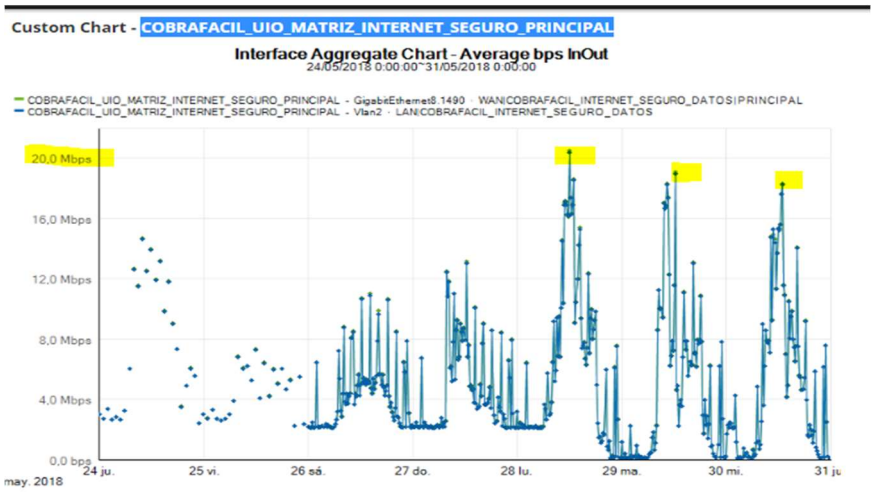

Figura 26. Monitoreo de Servicio de Internet Recover Matriz
Tomado de: (ORION, 2018)

En la Figura 26, la gráfica muestra una saturación total del canal en varios días y se pudo validar que esto sucedió los días que se actualizaron los servidores.

Monitoreo Enlace Backup Servicio de Internet

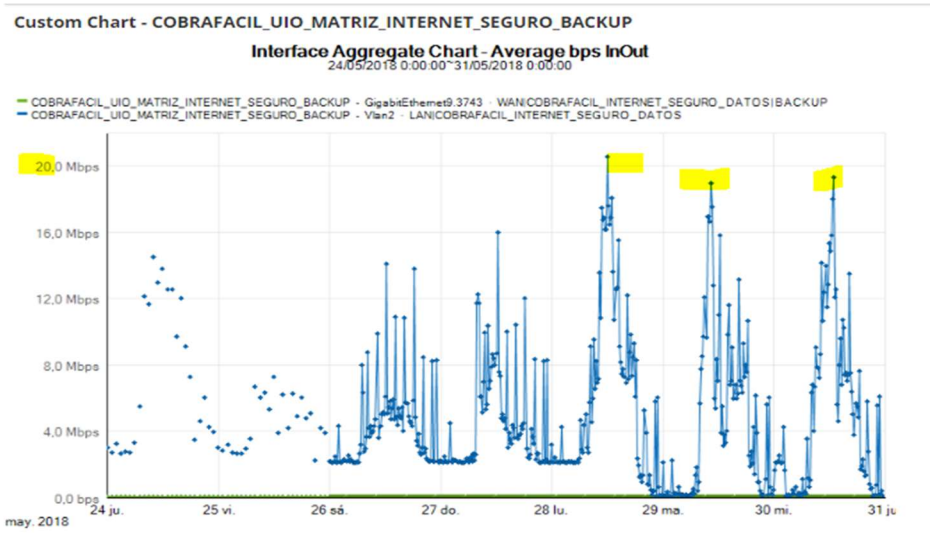

Figura 27. Monitoreo del enlace Backup de Servicio de Internet Matriz
Tomado de: (ORION, 2018)

La Figura 27, Muestra el tráfico que pasa por el enlace backup de Internet que se tiene con el mismo proveedor y que se puede notar tiene la misma saturación que el enlace normal.

Monitoreo Enlace Guayaquil Servicio de Internet

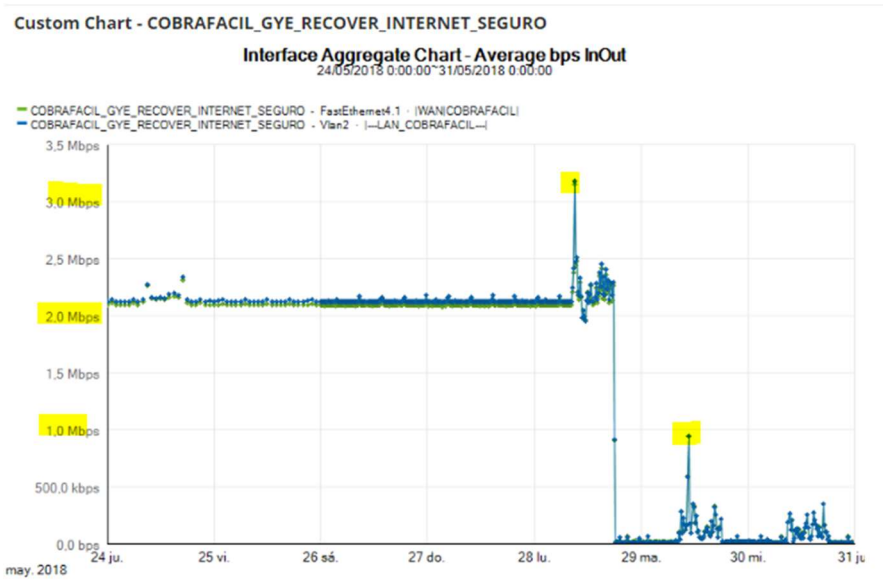

Figura 28. Monitoreo de Enlace Sucursal Guayaquil
Tomado de: (ORION, 2018)

La Figura 28, muestra la saturación del Enlace Quito-Guayaquil demostrando que al hacer uso del servicio de internet por medio del enlace el internet en Guayaquil presenta lentitud.

Monitoreo Enlace WAN ICESA.

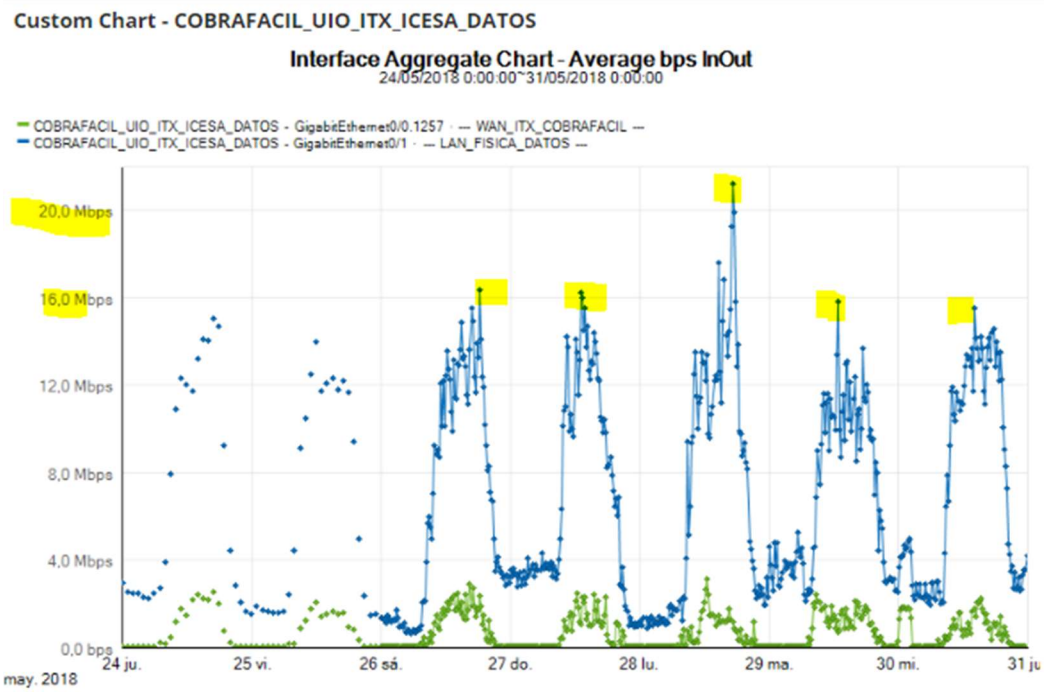

Figura 29. Monitoreo de Enlace con ICESA.
Tomado de: (ORION, 2018)

En la Figura 29, se puede notar que el uso del enlace tanto de Quito y Guayaquil produce una saturación que determinados días sobrepasan la capacidad del enlace.

CAPÍTULO 3

REDISEÑO DE RED DE DATOS CONVERGENTE

3. Introducción

El siguiente capítulo contiene el rediseño propuesto en base al Capítulo 2 en el cual se menciona la situación actual de la empresa, tomando en cuenta a detalle cada punto de la Red a Rediseñar desde la topología de Red hasta el cableado estructurado.

3.1. Desarrollo del Rediseño Lógico de la Red

El rediseño lógico de red busca brindar múltiples servicios a la red con la finalidad de mejorar el funcionamiento reduciendo costos y a su vez el mantenimiento haciendo de la red una red convergente.

3.1.1. Rediseño de la Topología de Red

Una topología de red permite ubicar un equipo dentro de la red, es necesario tomar en cuenta en el rediseño el crecimiento potencial de usuarios en los distintos departamentos al igual que el cableado vertical y horizontal que esto requiere.

3.1.1.1. Selección de Medio de Transmisión

Se puede tomar en cuenta varios medios de transmisión guiados, para lo cual es necesario tomar en cuenta la Tabla 12.

Tabla 11. Medios Guiados Detallados.

Categoría	Estándar	Ancho de Banda	Velocidad	Distancia que Soporta
Categoría 6	ANSI/TIA/EIA-568B-2.1	250 MHz	1 Gbps	90 Metros
Categoría 6a	ANSI/TIA/EIA-568B-2.10	550 MHz	10 Gbit/s	100 Metros
Fibra Óptica Monomodo	IEEE 802.3 1000Base BX	100 GHz	622 Mbps	100 Km
Fibra Óptica Multimodo	IEEE 802.3 1000Base SX	500 GHz	10-155 Mbps	2.4 Km

Nota: Medios guiados, ancho de banda y velocidad.

Actualmente el cableado vertical y horizontal usado es UTP Categoría 6 y 6a, este medio de transmisión puede tranquilamente ser reutilizado en el rediseño y también utilizado para las nuevas instalaciones como resultado del crecimiento que se tiene planificado.

3.1.1.2. Crecimiento de Usuarios

Recover tiene departamentos administrativos y operativos que crecer conforme a los requerimientos y crecimiento del negocio.

Los departamentos existentes actualmente son:

- Gerencias.
- Product Manager.
- Financiero.
- RRHH.
- Control de Calidad.
- Sistemas.
- Jefaturas.
- Call-Center.

De los departamentos anteriormente detallados el más susceptible a un crecimiento potencial es el de Call-Center, no se puede determinar un crecimiento porcentual a medida del tiempo, sino que el crecimiento es en base al crecimiento del negocio y es por eso que la empresa necesita manejar un margen de crecimiento en el rediseño de al menos un 50% de crecimiento en este departamento.

3.1.1.3. Puntos de Red

Los puntos de red actualmente colocados se encuentran en buen estado y cada máquina posee uno con la excepción del departamento de Control de Calidad que se encuentra en un área no cableada por Recover, sino que se llega halla usando un cableado de una empresa que anteriormente funcionaba en las instalaciones.

Los teléfonos IP se encuentran asignados a personal definido por las Gerencias y Jefaturas por tal motivo se respetará su asignación.

3.1.1.4. Rediseño de Cuarto de Racks

El Cuarto de Racks básicamente tendrá una redistribución para separar Gateways, Servidores, NAS y Storage de Equipos de Red por lo tanto los racks ubicados en el Segundo Piso estarán distribuidos de la siguiente manera:

- Rack1: Servidores, Gateways, NAS y Storage.
- Rack2: Firewall (ASA), Switch de Núcleo, Switch de Distribución y Switch de Acceso.

Es necesario tomar en cuenta que el acceso al Data Center debe ser únicamente para el personal autorizado y bajo la responsabilidad del departamento de sistemas, para lo cual se recomienda un cambio de seguridad de acceso.

3.1.1.5. Etiquetado del Cableado

El etiquetado es una parte importante del rediseño ya que es necesario tener identificados cada punto de acceso para la correspondiente distribución por vlan y no presentar ningún problema de acceso con determinado usuario.

Actualmente Recover mantienen un etiquetado por Departamento, sin embargo, hay que tomar en cuenta la norma TIA/EIA 568-B de cableado estructurado.

Cableado Estructurado

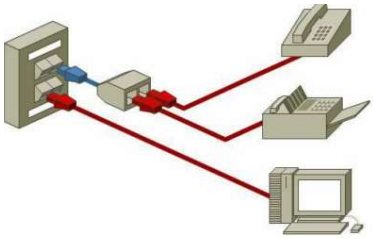

Figura 30. Conexión Multiusuario
Tomado de: (DGTIC, 2014)

El cableado debe tener etiquetas adhesivas que no dañen ni marquen el cable para su correspondiente localización.

Etiquetado de Cableado Estructurado

Figura 31. Etiquetas Adhesivas.
Tomado de: (Padilla, 2016)

Para identificar el punto de red el método de codificación será el siguiente:

Nomenclatura de Cableado Estructurado

1	-	A	SIS	01
PISO		RACK	DEP.	POSICION

Figura 32. Etiquetado de Cable UTP.
Tomado de: (DGTIC, 2014)

Nomenclatura Patch Panel

SIS 01

DEP. POSICION

Figura 33. Etiquetado de Patch Panel.
Tomado de:(DGTIC, 2014)

Nomenclatura Jack

1 - A SIS 01

PISO RACK DEP. POSICION

Figura 34. Etiquetado Jack RJ45
Tomado de: (DGTIC, 2014)

3.1.1.6. Esquema del Rediseño de la Red

El esquema de rediseño presenta la capa de núcleo, distribución y acceso a detalle además de la creación de una DMZ y el fortalecimiento de la WLAN que actualmente dispone la empresa, la Figura 35 detalla todo lo expuesto anteriormente.

Propuesta de Topologia Recover UIO

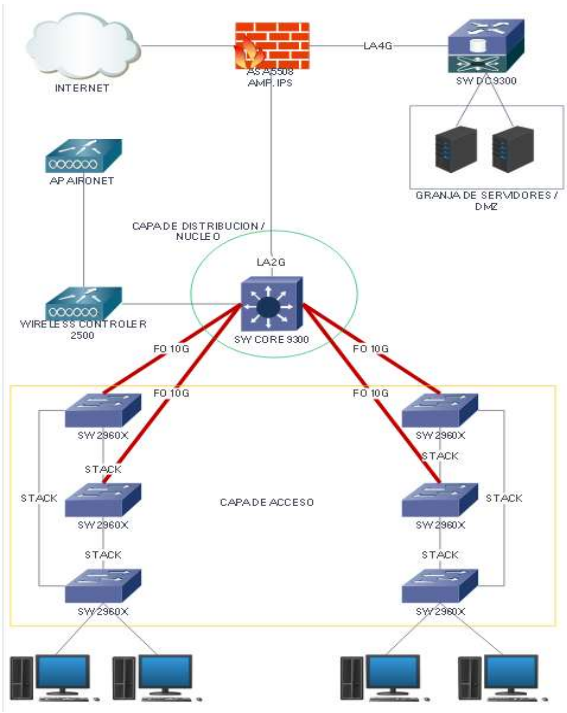

Figura 35. Rediseño de Red de Datos de Recover.
Tomado de: (Recover, 2018)

3.1.2. Diseño Jerárquico de la Red

El presente rediseño se basa teóricamente en el modelo jerárquico de tres capas mencionado en el Capítulo 1 sin embargo la red planteada cuenta con dos por los siguientes motivos:

- Falta de Presupuesto.
- Cantidad de Usuarios Concurrentes.

3.1.2.1. Capa de Acceso

En esta capa se encontrarán conectados cada uno de los dispositivos de red sean computadoras. Laptops, teléfonos IP, impresoras, etc.

Cada switch destinado para la capa de acceso cuenta con 48 puertos de los cuales 2 de cada uno se pondrá en modo troncal, dejando así un total de puertos de 276 disponibles con el rediseño todo esto tomando en cuenta que Recover actualmente tiene una totalidad de 212 usuarios concurrentes directamente conectados a la LAN, con el rediseño tendríamos 64 puertos disponibles para un futuro crecimiento es decir obtener más de un 20% de crecimiento asegurado.

En el caso de la WLAN se podrá mantener un mayor control mediante el Wireless Controler pudiendo así monitorizar el uso del servicio de WIFI, actualmente existe un promedio de 30 a 40 usuarios concurrentes por este medio que necesita ser controlado para un funcionamiento óptimo de la red.

3.1.2.2. Capa de Distribución / Núcleo

Las funciones correspondientes a la capa de Núcleo y Distribución las realizará un solo switch tomando en cuenta que este tiene la capacidad de funcionar en capa 2 y 3 esto debido al presupuesto y a la topología planteada ya que como se puede observar se está adquiriendo un switch que únicamente se encargará de la parte de servidores y la

DMZ esto garantizará que no generen cuellos de botella por los enlaces y la capacidad de procesador que este posee.

Este switch tendrá directamente conectado el servicio de Internet Seguro y la troncal SIP, Firewall ASA, Wireless Controler, será el encargado de proveer a la red la velocidad de transmisión y procesamiento que esta requiere.

3.1.3. Direccionamiento Lógico

Con el levantamiento de información realizado en el capítulo 2, se pudo notar el uso de vlan, sin embargo, las mismas no se encuentran bien segmentadas ya que cada una tiene un desperdicio de direcciones para lo cual tomamos en cuenta el número de usuarios por departamento con un máximo de crecimiento, también como medida de control de procederá a dividir la vlan de servidores en dos segmentos diferentes para separar Granja de Servidores de la DMZ. En la Tabla 13, se muestra la distribución por departamento con su determinada vlan a ser creada.

Tabla 12. Segmentación de VLAN

Departamento/Servicio	Vlan ID	Nombre
Gerencia	1	VGerencia
Sistemas	2	VSistemas
Financiero	3	VFinanciero
RRHH	4	VRRHH
Control de Calidad	5	VControl de Calidad
Servicio al Cliente	6	VServicio al Cliente
Telefonía	7	VTelefonía
Impresoras	8	VImpresoras
Wifi	9	VWifi
SAN	13	VSAN
Voz	14	VVoz
CALL-CENTER1	15	VCALL-CENTER1
CALL-CENTER2	16	VCALL-CENTER2

Nota: Segmentación Vlans, incluye ID y nombre.

Para proceder con el direccionamiento es necesario conocer el número máximo de crecimiento de cada departamento detallado a continuación en la Tabla 14.

Tabla 13. Cantidad de Direcciones IP

Departamento/Servicio	Vlan ID
Gerencia	20
Sistemas	30
Financiero	20
RRHH	20
Control de Calidad	20
Servicio al Cliente	12
Telefonía	100
Impresoras	20
Wifi	100
SAN	20
Domiciliarios	80
CALL-CENTER1	200
CALL-CENTER2	200
Total	842

Nota: Número de direcciones Ip por vlan.

Para direccionar los departamentos detallados anteriormente se propone el uso de la red 172.17.0.0 con máscara 255.255.0.0 y partiendo de la misma se procederá en base al cálculo del VLSM como se puede observar en la Tabla 15.

Tabla 14. Direccionamiento IP mediante VLSM

DEPARTAMENTO/SERVICIO	RED		MÁSCARA	DIRECIONES DISPONIBLES
CALL-CENTER1	172.17.0.0	/24	255.255.255.0	172.17.0.1 - 172.17.0.254
CALL-CENTER2	172.17.1.0	/24	255.255.255.0	172.17.1.1 - 172.17.1.254
TELEFONIA	172.17.2.0	/25	255.255.255.128	172.17.2.1 - 172.17.2.126
WIFI	172.17.2.128	/25	255.255.255.128	172.17.2.129 - 172.17.2.254
DOMICILIARIOS	172.17.3.0	/25	255.255.255.128	172.17.3.1 - 172.17.3.126
SISTEMAS	172.17.3.128	/27	255.255.255.224	172.17.3.129 - 172.17.3.158
CONTROL_CALIDAD	172.17.3.160	/27	255.255.255.224	172.17.3.161 - 172.17.3.190
FINANCIERO	172.17.3.192	/27	255.255.255.224	172.17.3.193 - 172.17.3.222
GERENCIA	172.17.3.224	/27	255.255.255.224	172.17.3.225 - 172.17.3.254
IMPRESORAS	172.17.4.0	/27	255.255.255.224	172.17.4.1 - 172.17.4.30
RRHH	172.17.4.32	/27	255.255.255.224	172.17.4.33 - 172.17.4.62
SAN	172.17.4.64	/27	255.255.255.224	172.17.4.65 - 172.17.4.94
SERVICIO_CLIENTE	172.17.4.96	/28	255.255.255.240	172.17.4.97 - 172.17.4.110

Nota: Direccionamiento.

El direccionamiento en el caso de servidores será con la subred 192.168.10.0/24 y la nueva subred a crear será la DMZ con la dirección 192.168.50.0/24.

3.1.4. Protocolos de Conmutación y Ruteo

PROTOCOLO STP

El objetivo del protocolo árbol de extensión (STP) es mantener una red libre de bucles, generando que la red bloquee puertos redundantes y determine caminos libres.

Explora la red de manera constante, de manera que detecta un fallo o adición en un enlace al instante.

Los switch intercambian información cada dos segundos al encontrar algún comportamiento extraño en algún puerto STP cambiará de estado automáticamente utilizando algún camino redundante sin que se pierda conectividad. (Martinez, 2016)

PROTOCOLO VTP

VTP es un protocolo que permite configurar Vlan de manera centralizada. Implementando VLAN en nuestra red y no activar el protocolo VTP, la escalabilidad de la red será compleja debido a que se deberá crear en cada uno de los Switch instalados y manualmente cada una de las Vlan. Esta forma administración de recursos es desorganizada y poco eficaz. (CAPACITY, 2014)

VTP es un protocolo que permite bajar las Vlan creadas en un determinado switch hacia otro sin la necesidad de volver a crearlas manteniendo así la consistencia sobre la creación, administración y eliminación de VLAN, evitando errores de configuración y facilitando y centralizando la administración de las mismas. En la actualidad existen tres versiones de VTP (versión 1, 2 y 3). (CAPACITY, 2014)

PROTOCOLOS DE RUTEO

El enrutamiento será realizado por el Switch de Core por su CPU y memoria que permite dar velocidad a la capa de núcleo y a su vez interactuar directamente con el ISP por lo cual cualquier ruteo será interno y de no serlos se utilizará una ruta estática.

Las rutas estáticas son administradas y configuradas por el administrador, sin embargo esto no es escalable ya que cualquier cambio en la topología es necesario agregar, eliminar rutas de la tabla de enrutamiento de forma manual. (Cisco Networking Academy, 2010)

3.1.5. Calidad de Servicio (QoS)

Con el QoS se dará un mejor trato a los usuarios y aplicaciones que funcionan internamente en la red, además de implementar mecanismos para dar prioridad a un determinado tráfico que genere una saturación en la red.

Para detallar las aplicaciones internas junto con la prioridad de QoS asignada en base a su importancia en el comportamiento de la red y la experiencia del usuario en base a las prioridades de la Tabla 16.

Tabla 15. Análisis de Prioridades (QoS)

Aplicaciones	Puerto	QoS	
		Prioridad	Clase
HTML	80	2	Transactional Data
Correo	25	3	Business Mission Critical
Datos	-	2	Transactional Data
Sql Server	1433	2	Transactional Data
Voz	16384 - 32767	5	Voice
FTP/SFTP	21-22	3	Business Mission Critical

Nota: Análisis de calidad de servicio

3.1.6. Estrategias de Seguridad de Red

Actualmente no se cuenta con un sistema de seguridad que proporcione la seguridad necesaria ante amenazas y ataques.

A continuación, se detallan estrategias a realizar para tener una seguridad tanto en servidores como en los equipos finales.

3.1.6.1. Zona Desmilitarizada (DMZ)

Con la información obtenida se puede decir que los servidores que están constantemente expuestos al exterior (Internet), sin ninguna protección interna de seguridad son el Servidor Ftp/Sftp y Servidor Web.

Motivos por los cuales es necesario tener las debidas políticas que aseguren la red interna de cualquier ataque, es por ese principal motivo que el uso de una DMZ permite tener una seguridad extra para la protección de los servidores internos.

Para que la DMZ tenga conectividad a internet se procederá a usar un NAT, esto consiste en traducir en direcciones privadas a las direcciones públicas, de acuerdo a este concepto se procederá a hacer el uso de las direcciones públicas disponibles en el rango adquirido.

3.1.7. Estrategias de Administración de la Red

Para administrar la red es necesario conocer los componentes de la misma e identificar los puntos a ser evaluados y monitoreados, de esta manera se puede plantear estrategias para dar un mantenimiento a los dispositivos de red, servidores e incluso UPS.

Servidores:

- CPU.
- Memoria RAM.

- Espacio Disco Duro.

Equipos de Comunicación:

- Tráfico.
- Ancho de Banda.
- Interfaces dañadas o con error.

UPS:

- Nivel de Temperatura.
- Banco de Baterías.

El mantenimiento de los equipos que hacen parte de la red debe ser realizado cada 6 meses en horarios establecidos en los cuales no se afecta a la producción de la empresa esto se definiría cada año.

Es necesario implementar el protocolo de simple de Administración de Red (SNMP), el mismo que permite intercambiar información de cada equipo.

Para una administración y gestión centralizada es muy necesario que este protocolo se encuentre correctamente levantado, esto permitirá un monitoreo constante y permitirá dar alarmas cuando un determinado dispositivo no se encuentra funcionando correctamente o llegue a apagarse.

Las alertas son un punto muy importante ya que cada una de ellas permitirá dar un buen rendimiento a red, las alertas a tomar en cuenta son:

- Tráfico de Red.
- Ancho de Banda.
- Errores en Interfaces.

- CPU.
- Memoria RAM.
- Disco Duro.
- Equipo fuera de Servicio.

3.2. Selección de Tecnologías y Dispositivos de Red

Recover busca tener un estándar en cuanto al fabricante de los dispositivos de red en cada una de las capas del modelo jerárquico.

Es importante detallar cada equipo a ser adquirido con los diferentes requerimientos que cada uno necesita.

Switch de Acceso

Tomando en cuenta el tráfico capturado en el capítulo 2 y las especificaciones tanto de cableado como de topología de red es requerida la compra de switch de capa 2 con velocidades 10/100Mbps y para los puertos troncales 1/10 Gbps, para que el rediseño sea notable, es necesario cumplir con las especificaciones técnicas detalladas en la Tabla 17.

Tabla 16. Switch de Capa de Acceso

Característica	Descripción
IEEE 802.3u	FastEtehrnet - Puertos de Acceso
IEEE 802.3ab	GigaEthernet - Puertos Troncales
IEEE 802.3x	Control de Flujo
IEEE 802.1q	VLAN Trunking
IEEE 802.1p	QoS
IEEE 802.1d	Spanning-Tree
IEEE 802.1w	Rapid Spanning-Tree
IEEE 802.3af	Power Over Ethernet (PoE)
Puertos Acceso	Velocidad 10/100 Mbps
Puertos Troncales	Velocidad 1000 Mbps
Capa	2

Conmutación	Store and Forward
Negociación	full - half Duplex
Seguridad en el Puerto	Port Security
IOS	Versión 12 o superior

Nota: Switch de capa de acceso.

Capa de Distribución / Núcleo

En el caso de Recover un solo equipo realizara el trabajo de la capa de distribución y núcleo motivo por el cual es necesario que tenga un procesador robusto que garantice la velocidad necesaria en la capa núcleo, adicional se debe tomar en cuenta los puertos a ser troncales como se muestra en la Tabla 18.

Tabla 17. Switch de Distribución / Núcleo

Característica	Descripción
IEEE 802.3ab	GigaEthernet - Puertos Troncales
IEEE 802.3x	Control de Flujo
IEEE 802.1q	VLAN Trunking
IEEE 802.1p	QoS
IEEE 802.1d	Spanning-Tree
IEEE 802.1w	Rapid Spanning-Tree
Puertos Troncales	Velocidad 1000 Mbps
Capa	3
Conmutación	Store and Forward
Negociación	full - half Duplex
IOS	versión 12 o superior

Nota: Protocolos de comunicación.

3.3. Análisis de Factibilidad

Luego de analizar las características de los equipos que se necesitan para el rediseño se debe tomar en cuenta que el deseo de Recover es manejar un solo estándar de equipos, es decir, una sola marca, en este caso es CISCO que fue elegida de manera

unánime luego del caso de éxito en la empresa ICESA perteneciente al mismo consorcio.

Es importante mencionar que CISCO es un líder en el cuadrante mágico de Gartner como se puede ver en la Figura 36.

Cuadrante de Gartner Marcas de Equipos de Red.

Figura 36. Cuadrante de Gartner Equipos de Red.
Tomado de: (GARTNER, 2016)

CAPÍTULO 4

ANÁLISIS Y RESULTADOS

4. Introducción

El capítulo a continuación se detalla la simulación del estado actual y la propuesta de red junto con las gráficas resultantes, dando la prioridad a cada uno de los servicios que son de mayor importancia en el comportamiento de la red, haciendo énfasis en las soluciones propuestas como QoS y equipos de seguridad.

4.1. Simulación de Estado Inicial y Rediseño Propuesto

La situación inicial es simulada tal cual se encuentra la actualmente la Red de Recover, sin ningún esquema de seguridad interno ni QoS de servicios en el simulador Opnet el mismo que fue diseñado bajo la siguiente topología detallada en la Figura 37.

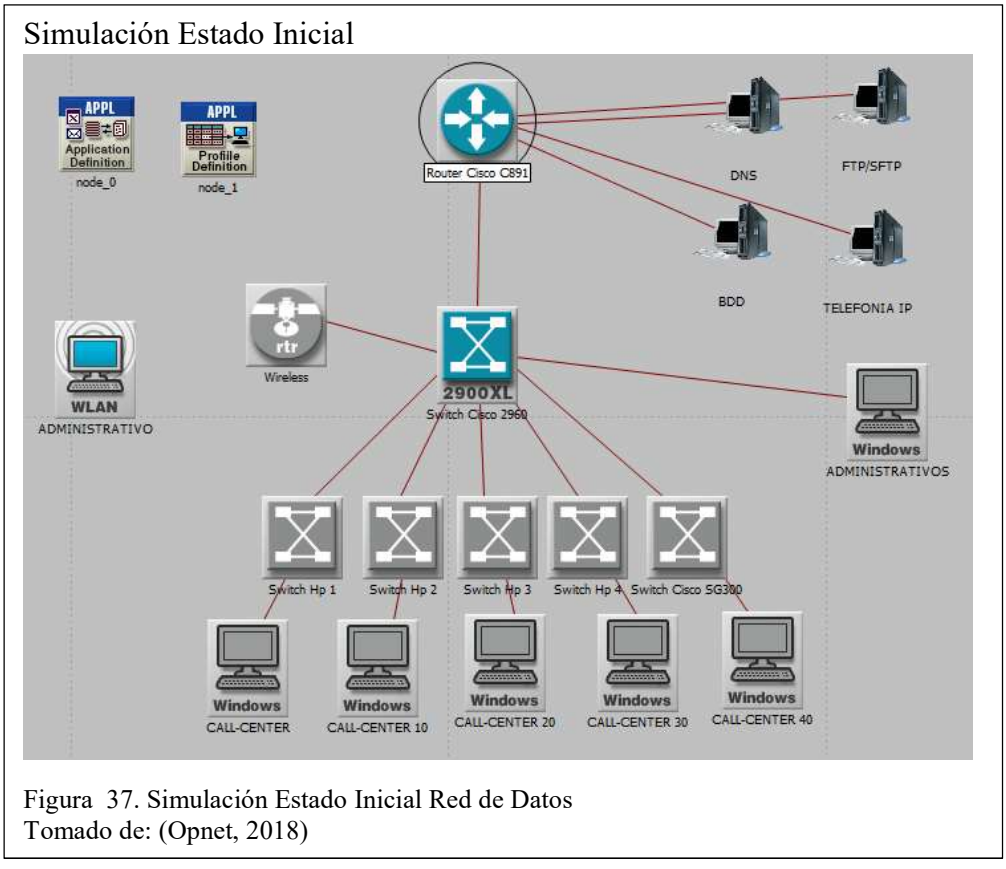

Figura 37. Simulación Estado Inicial Red de Datos
Tomado de: (Opnet, 2018)

La topología correspondiente a la situación inicial consta con todos los equipos que actualmente posee Recover de tal manera que permite generar graficas acorde a la realidad.

La simulación de la topología propuesta esta detallada en la Figura 38, que permite el desplegar los resultados para un análisis posterior.

Simulación de Propuesta de Red

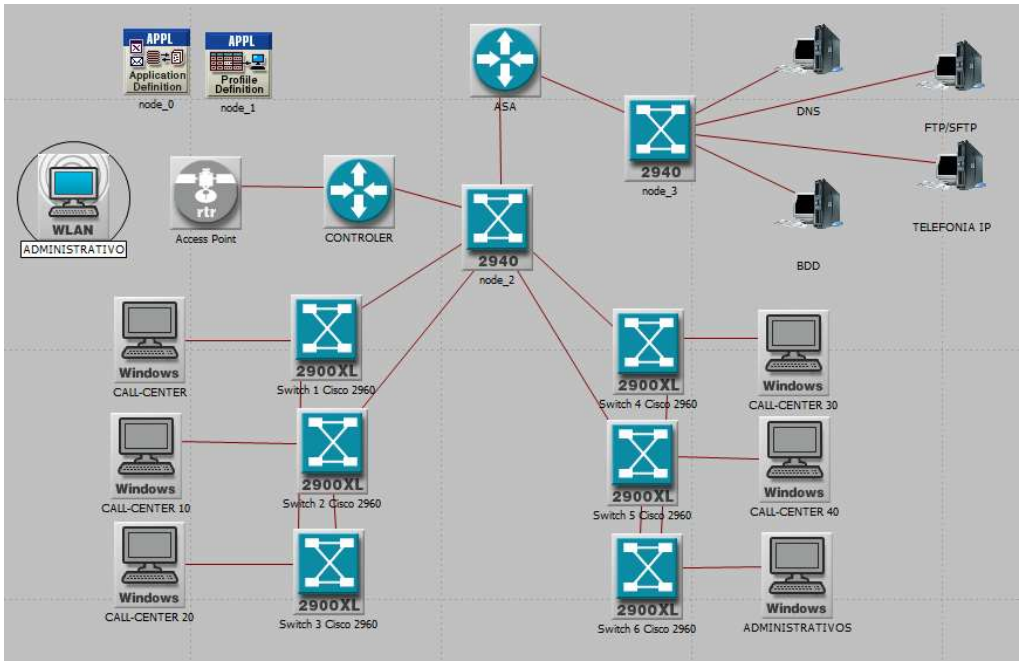

Figura 38. Simulación Propuesta de Rediseño de Red de Datos
Tomado de: (Opnet, 2018)

La topología se encuentra conectada con enlaces de 10Gb a los Switch de acceso que se encuentran en Stack y a su vez con un Wireless Controler para el control de la red inalámbrica de la empresa.

4.2. Gráficas Resultantes de la Situación Inicial y Rediseño Propuesto.

4.2.1. Situación Inicial

WLAN Cliente BDD

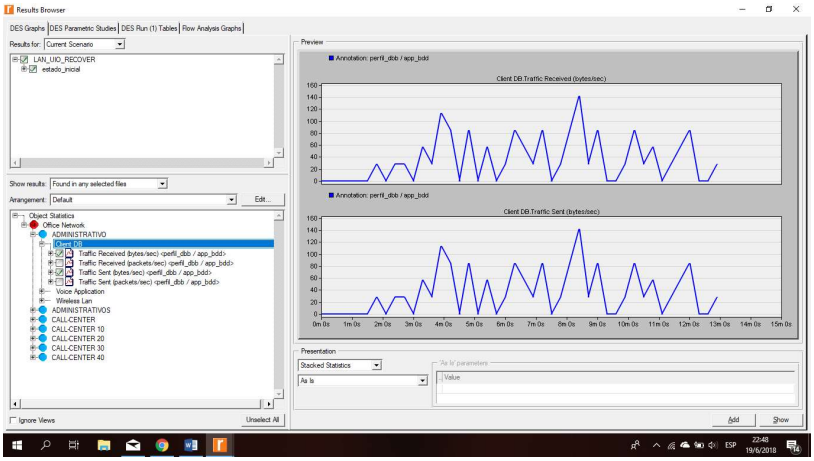

Figura 39. WLAN Tráfico Enviado y Recibido Cliente BDD
Tomado de: (Opnet, 2018)

En la Figura 39, se detalla y se verifica que el tráfico enviado y recibido de un cliente de base de datos con puntos de alto consumo que tienen como máximo el tope de 140 bytes/s y un promedio de 90 bytes/s, esto genera que las Aplicaciones Web se tornan lentas al momento de generar algún proceso interno en la base de datos.

WLAN Aplicación de Voz

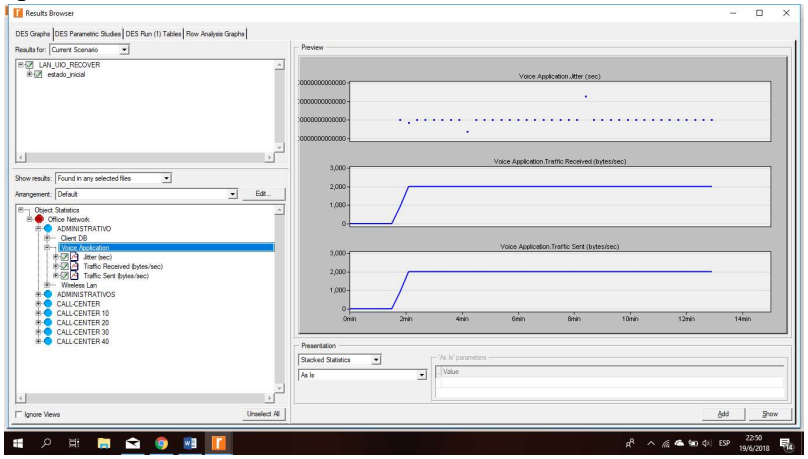

Figura 40. Aplicación de Voz sobre IP.
Tomado de: (Opnet, 2018)

En la Figura 40, se muestra el tráfico de voz IP detallado con un jitter de 1×10^{-16} s, un tráfico enviado y recibido de datos que llega a un punto de 2000 bytes/s en el cual se estabiliza y consume el canal de manera permanente generando un consumo de ancho de banda que genera cuellos de botella al hacer uso de Aplicaciones Web el momento de ingresar gestiones a la base de datos.

WLAN

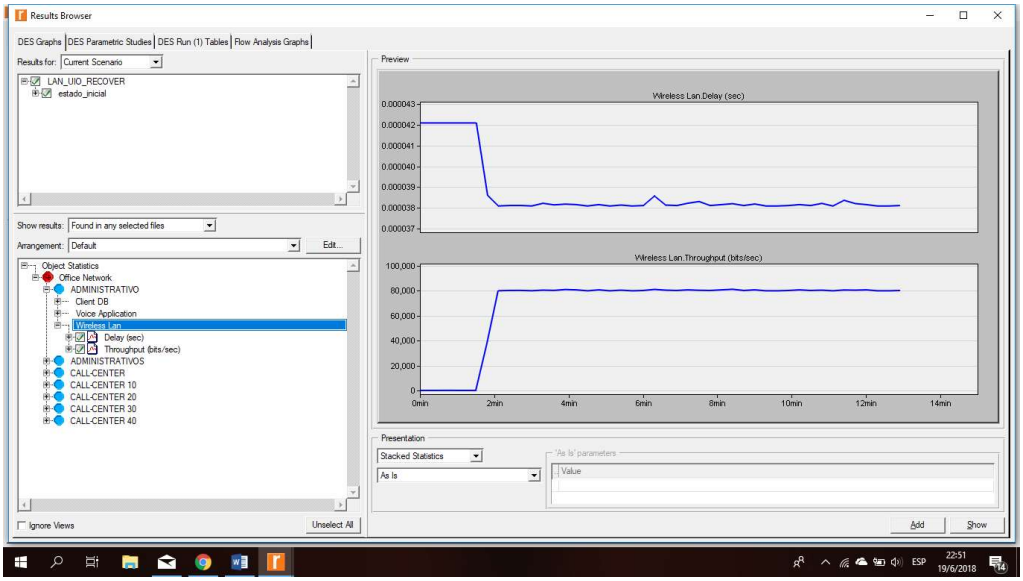

Figura 41. Wireless LAN.
Tomado de: (Opnet, 2018)

La Figura 41, muestra gráficas en las cuales se puede ver que el delay empieza en 0.000043 bytes/s y baja a 0.000038 bytes/s donde se estabiliza y se mantiene, el throughput llega a un tope de 80000 bytes/s en el cual se estabiliza y se mantiene, se puede verificar que al no poseer ningún control de ancho de banda o segmentación el mismo empezará a disminuir y la red inalámbrica se volverá lenta y su disponibilidad se reducirá conforme al número de usuarios concurrentes.

4.3. Comparativa entre parámetros de Red anterior a Red propuesta.

4.4. Análisis de QoS para Voz sobre IP

El tráfico generado por la red inalámbrica no está controlado ni maneja ningún tipo de segmentación de consumo de ancho de banda.

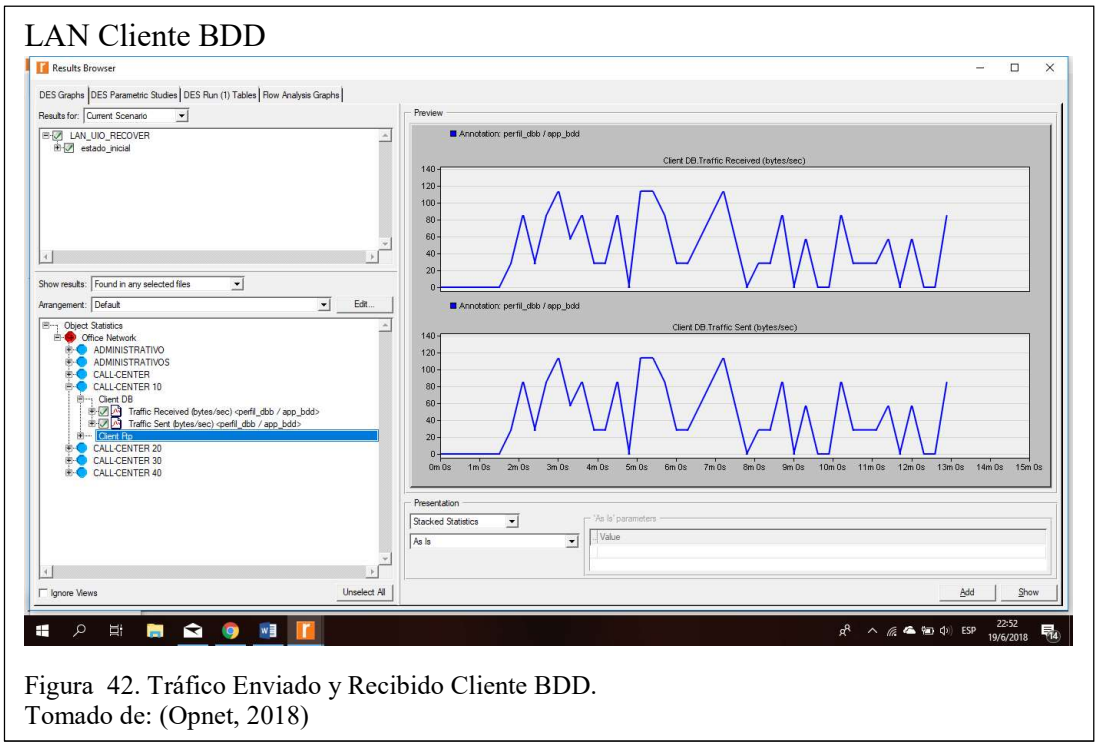

Figura 42. Tráfico Enviado y Recibido Cliente BDD.
Tomado de: (Opnet, 2018)

En la Figura 42, el Cliente de Base de Datos genera un tráfico Enviado y Recibido que llega a tener varios puntos altos de los cuales el máximo 118 bytes/s, se puede determinar que en base a las peticiones generadas por el cliente el canal tendrá la tendencia a saturarse con la falta de priorización del tráfico, generando una pérdida de paquetes y lentitud en la red.

LAN Cliente FTP

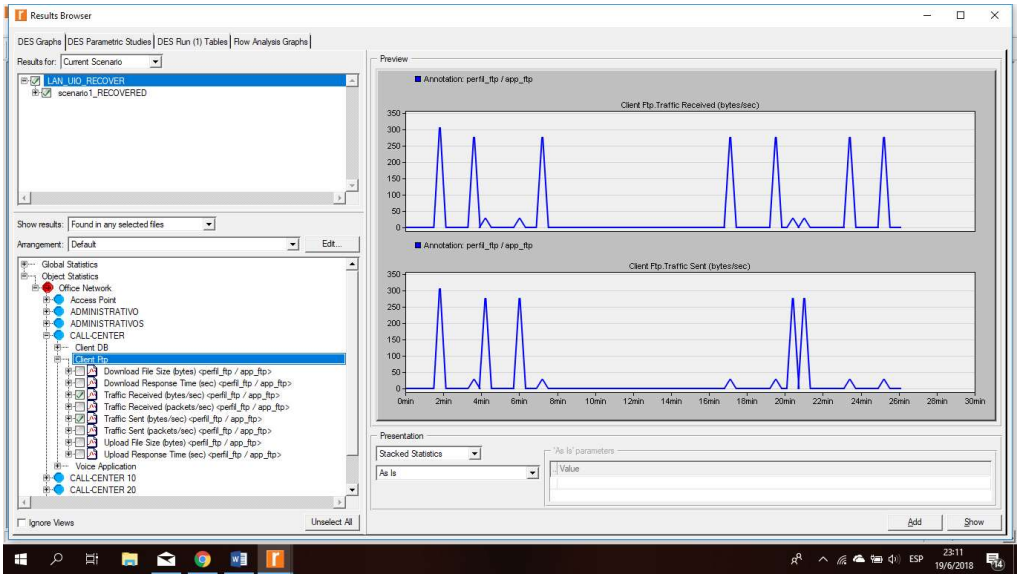

Figura 43. Tráfico Enviado y Recibido Cliente Ftp.
Tomado de: (Opnet, 2018)

En la Figura 43, se muestra el servicio FTP el cual es importante ya que este representa él envió concurrente de archivos entre Recover y sus clientes, el tráfico enviado y recibido como muestra la figura 43 tiene puntos altos de consumo en los cuales el pico más alto es de 300bytes/s, este proceso de recepción de archivos es generado en horas no laborables lo cual no afecta a la producción, sin embargo, existen determinados archivos que no tienen un horario establecido y que llegan en horas laborables lo que generaría una lentitud en la transferencia e incluso en los gestores que se encuentren cargando algún archivo en el Servidor FTP.

LAN Aplicación de Voz

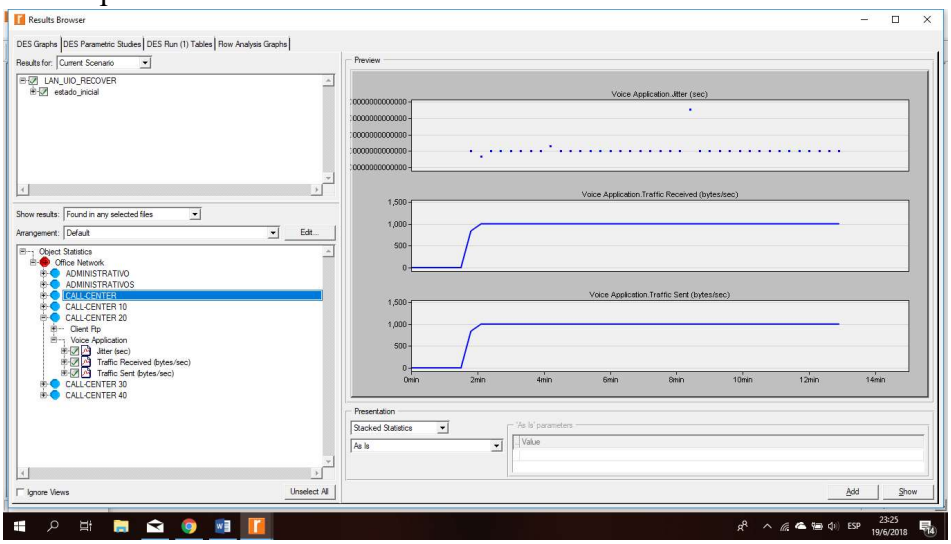

Figura 44. Tráfico Enviado y Recibido de Aplicación de Voz
Tomado de: (Opnet, 2018)

La Figura 44, muestra que el Servicio de Voz Ip genera un tráfico enviado y recibido que llega a un punto de 1000 bytes/s donde se estabiliza y se mantiene hasta el final de la simulación, se debe mencionar que la calidad de voz no es garantizada ya que el momento de haber una saturación en el canal ocasionado por cualquier otro tipo de tráfico puede resultar en intermitencias y mala calidad en las llamadas.

4.2.2. Graficas de Rediseño Propuesto

WLAN Cliente BDD

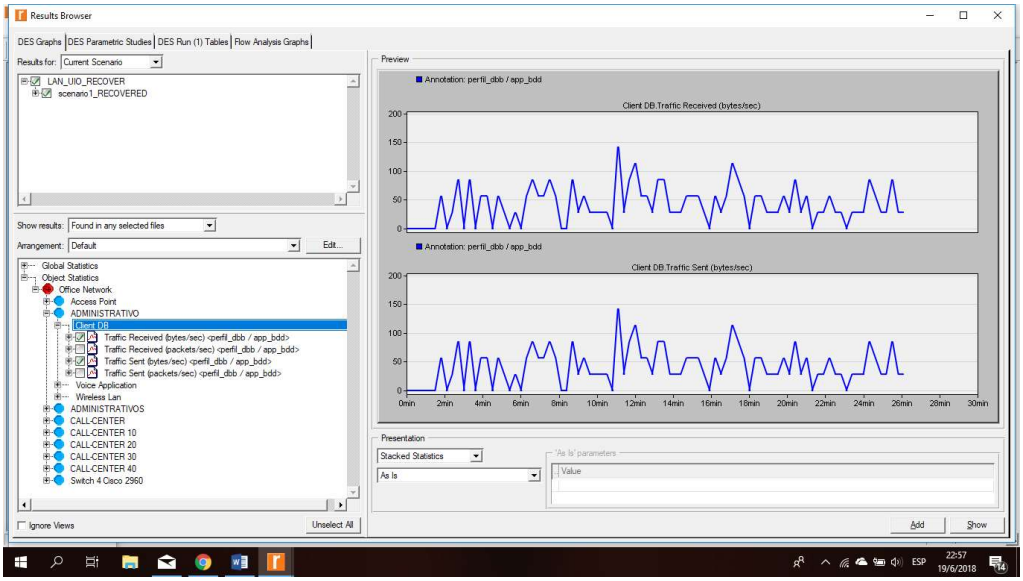

Figura 45. Tráfico Enviado y Recibido de Cliente BDD.
Tomado de: (Opnet, 2018)

En la Figura 45, se muestra el tráfico generado por el Cliente de Base de datos en similar al del estado inicial sin embargo se puede verificar que posee un solo punto que llega a 140 bytes/s mientras que al simular por mayor tiempo se el tráfico se estabiliza con un promedio de 80 bytes/s con lo cual se mejora en un 40%.

Tomando en cuenta también el control por medio de Listas de Control de Acceso los usuarios que podrán tener acceso genera un tráfico controlado en cuanto a lo generado por la o las bases de datos.

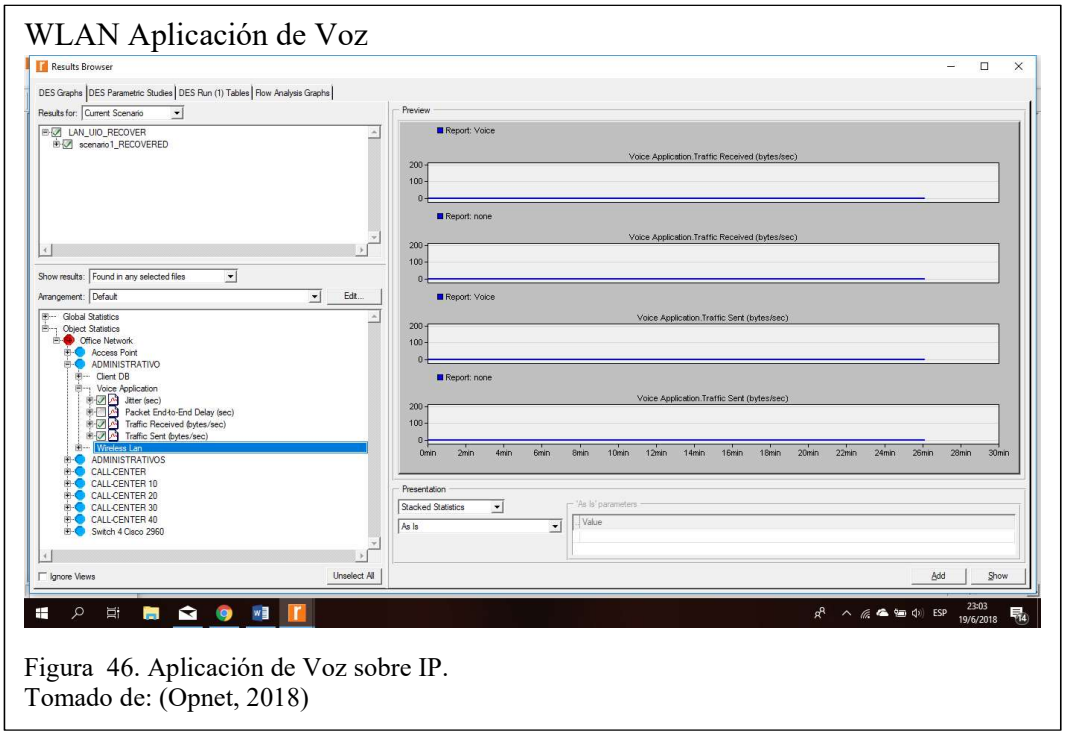

Figura 46. Aplicación de Voz sobre IP.
Tomado de: (Opnet, 2018)

En la Figura 46, el tráfico generado por la voz en el rediseño propuesto a diferencia del estado inicial no llega ni a los 10 bytes/s mientras que en el estado inicial llegaba a los 2000 bytes/s lo cual demuestra que su mejora en un 90% considerando la señalización por QoS propuesta en la Tabla 16.

WLAN

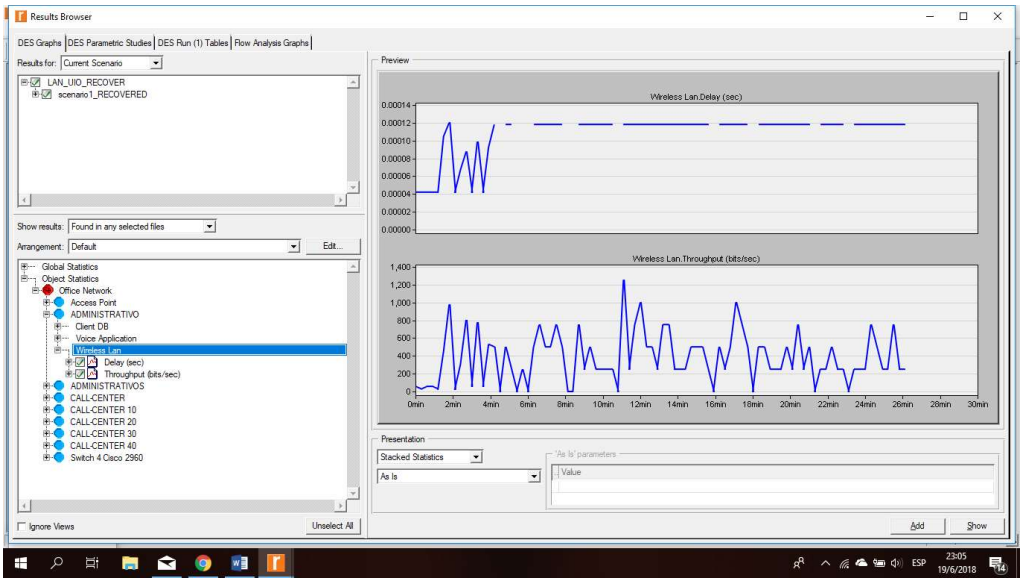

Figura 47. Wireless LAN.
Tomado de: (Opnet, 2018)

En la Figura 47, se puede observar que el delay llega a los 0.00012 bytes/s que en comparación al estado inicial aumenta debido al control de ancho de banda asignado en el Wireless Controler lo que genera un delay controlado y una mejora de un 5% en el throughput de cada usuario.

LAN Cliente BDD

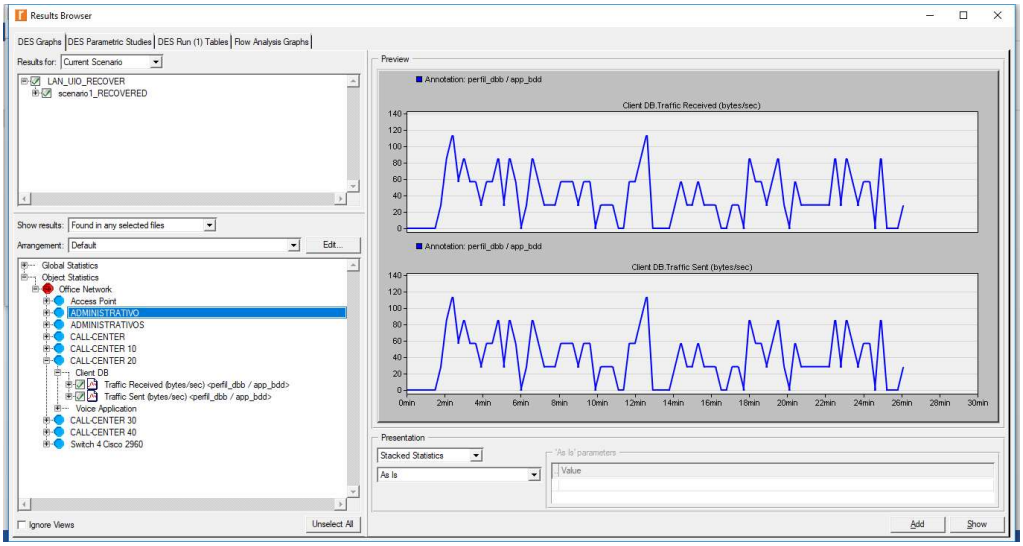

Figura 48. Tráfico Enviado y Recibido de Cliente de BDD
Tomado de: (Opnet, 2018)

En la Figura 48, el Cliente de Base de Datos genera un tráfico enviado y recibido con un tope máximo de 110 bytes/s, esto que mejora en un 9% en cuanto al tráfico generado por consumo de las bases de datos sin contar con el control y prioridad dada por medio del QoS propuesto en la Tabla 16.

LAN Cliente FTP

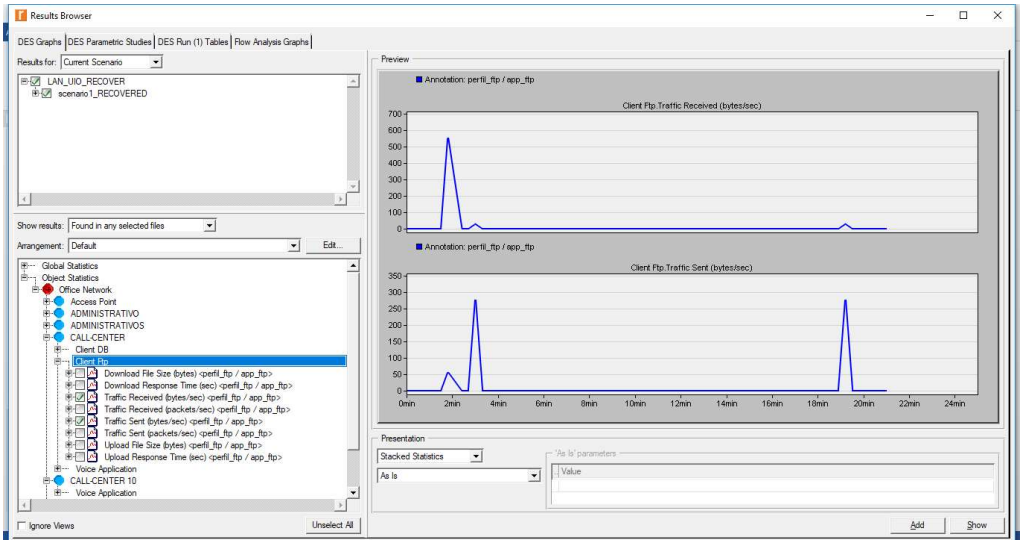

Figura 49. Trafico Enviado y Recibido de Cliente FTP.
Tomado de: (Opnet, 2018)

El trafico FTP con la propuesta llega a tener a penas un punto máximo en la gráfica de Figura 49, de 550 bytes/s y luego se estabiliza y consume de acuerdo a la prioridad asignada en el QoS en la Tabla 16.

LAN Aplicación de Voz

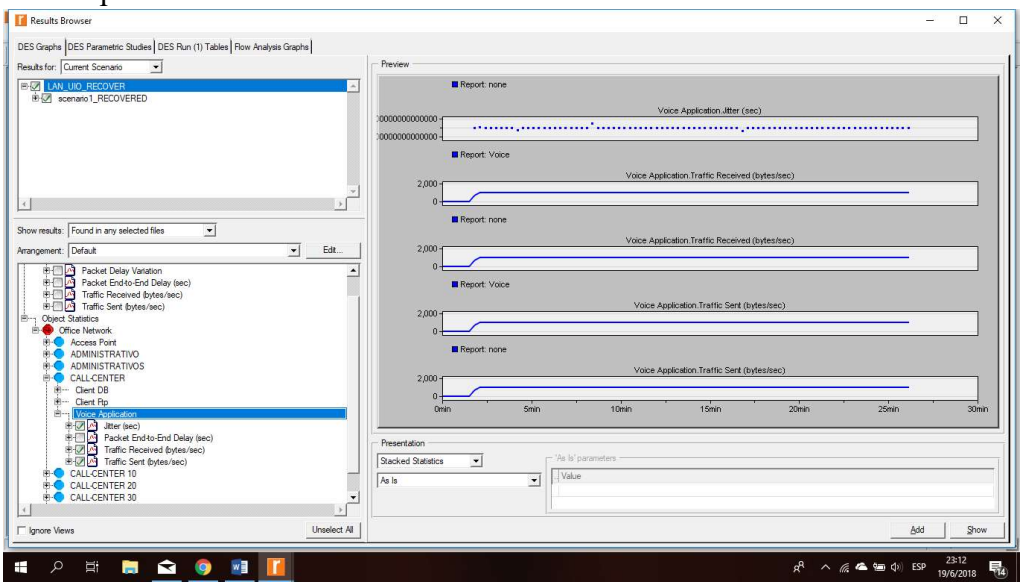

Figura 50. Tráfico Enviado y Recibido de Voz IP.
Tomado de: (Opnet, 2018)

El tráfico de voz IP se mantiene en su consumo al igual que la situación inicial ya que es el tráfico que tiene la mayor prioridad en el QoS propuesto en la Tabla 16.

4.3. Análisis Comparativo

En las gráficas anteriormente detalladas se pueden observar datos que demuestran que el rediseño propuesto además de utilizar herramientas y equipos capaces de manejar Seguridad y QoS le dan a la red una mejora de consumo de ancho de banda en un 40% en WLAN, mientras que el rendimiento con el QoS genera una pérdida de paquetes de un 9% menos al estado inicial, los servidores que son críticos al tener enlaces con mayor capacidad de ancho de banda generan un canal 10 veces mayor al actual evitando los cuellos de botella y mejorando en un 90% el throughput y en el caso de la red inalámbrica su seguridad aumenta en un 80% gracias al Wireless Controler que permite un control que en el estado inicial es totalmente libre y sin ninguna supervisión.

La red inicial no posee ningún mecanismo de seguridad interna por lo cual se mejora en un 80% el control y confidencialidad de la información, es necesario aclarar que no se puede manejar un mejor porcentaje debido a que para tener un control o una seguridad bien implementada es necesario tener procesos y políticas establecidas en el departamento de TI, las mismas que deben ser consensuadas con las Gerencias y Departamentos que forman parte de la Empresa y por ende de la Red.

CONCLUSIONES

- Se procedió con una investigación a detalle del estado actual de la empresa, lo que permitió tomar decisiones claras para el rediseño en base a las metas planteadas por la misma, dando como resultado una solución que mejora en un 80% el comportamiento actual de red inalámbrica por medio de un Control que garantiza la seguridad y la disponibilidad, evitando cuellos de botella como resultante de la segmentación de ancho de banda y control de usuarios.
- La Empresa carece de Procesos y Políticas en el departamento de TI lo cual evita que la Seguridad Propuesta por medio de ACL garantice que el usuario final este protegido en un porcentaje mayor al 80%, al establecer políticas se procederá a quitar varios accesos y como resultante el porcentaje de seguridad aumentara hasta llegar a una seguridad mayor al 90%.
- La infraestructura actual se encuentra limitada, debido a, que ha crecido conforme la empresa lo ha requerido de manera inmediata esto sumado a la falta de conocimiento en networking genera que el control y administración centralizada no sea posible por los distintos protocolos que manejan determinadas marcas, el rediseño propone una estandarización de equipos y adicional un modelo jerárquico que garantiza el funcionamiento y el tiempo de vida de los dispositivos.
- El diseño propuesto despliega resultados que evidencian un mejor funcionamiento de las aplicaciones y servicios, además de ser una solución sostenible por la garantía de marca CISCO.
- El rediseño permite manejar en la capa de núcleo QoS de manera que garantice que el tráfico de voz y datos consuma los recursos necesarios y no saturen la red.

- Recover busca tener a futuro certificaciones que le generen un mayor reconocimiento a nivel nacional e internacional motivo por el cual se plantea mejorar su infraestructura de red, tomando en cuenta el costo beneficio que esto representa, garantizando así a sus clientes un buen servicio sustentado y garantizado en base a la infraestructura propuesta.

RECOMENDACIONES

- Uso del Enlace de Fibra entre Recover e ICESA con la finalidad de reducir costos y garantizar un menor consumo en el ancho de banda con respecto a la sucursal de Guayaquil que hace uso del mismo canal para comunicación con ICESA e Internet.
- Hacer uso de la Infraestructura Virtual aprovechando las características y beneficios que esta posee para generar Servidores de Archivos, Pruebas y Desarrollo.
- Mejorar la Seguridad en el acceso al Data Center ya que es solo una perilla la cual separa a cualquier persona del ingreso al mismo.

LISTA DE REFERENCIAS

Arquez, J. B.-D. (2008). Mecanismo de Manejo de Cola en Redes IP. *UNIVERSIDAD TECNOLOGICA DE BOLIVAR*, 26. Obtenido de http://biblioteca.unitecnologica.edu.co/notas/tesis/0045090.pdf

Bleda, D. F. (30 de Mayo de 2004). *Seguridad en Redes Convergentes.* Obtenido de isecauditors: https://www.isecauditors.com/sites/default/files/files/seguridad-redes-convergentes-W04H.pdf

Butler, J. Z. (2013). *Redes inalámbricas en los países en desarrollo* (Tercera ed.). Copenhagen.

CAPACITY. (21 de Julio de 2014). *capacityacademy*. Obtenido de http://blog.capacityacademy.com/2014/07/21/11009-2/

Capacity Academy. (6 de Junio de 2014). *Cisco CCNA Internetworking*. Obtenido de https://es.slideshare.net/CapacityAcademy/cisco-ccna-internetworking-curso-online

Cisco Networking Academy . (2015). Fundamentos de enrutamiento y conmutación (Routing and Switching Essentials).

Cisco Networking Academy. (2010). CCNA 1 AND 2. En *Cisco Networking Academy* (pág. 24).

Comunicaciones y Redes de Computadores. (s.f.). En W. Stalling. Prentice Hall.

D.Terán. (2011). *Redes Convergentes: Diseño e Implementación.* Barcelona: Marcombo S.A.

DGTIC. (2014). GUIA PARA APLICAR LA NORMA TIA/EIA 568 PARA CABLEADO ESTRUCTURADO. *Gobierno del Estado de Tabasco*.

Dominguez, C. V.-L. (2002). Redes Inalámbricas. *Escuela Técnica Superior de Ingeniería Informática*. Obtenido de https://blyx.com/public/wireless/redesInalambricas.pdf

Fajardo, Á. M. (13 de Junio de 2004). *Redes Convergentes.* Obtenido de redalyc: http://www.redalyc.org/html/911/91101407/

GARTNER. (2016). *Dara Center Networking.*

Guerra, P. F. (2016). PROPUESTA DE METODOLOGIA PARA LA IMPLETACIÓN DE PROYECTOS DE REDES - CASO DE ESTUDIO INSTITUCION FINANCIERA LOCAL. *Pontifica Universidad Catolica del Ecuador*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/13491/Tesis%20Pablo%20Erazo%20Guerra.pdf?sequence=1&isAllowed=y

Joskowicz, I. (2013). VOZ, VIDEO Y TELEFONIA SOBRE IP. En I. J. Joskowicz, *Instituto de Ingeniería Eléctrica, Facultad de Ingeniería* (págs. 27-28). Obtenido de

http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Voz%20Video%20y%20Telefonia%20sobre%20IP.pdf

Martinez, J. J. (Enero de 2016). *todosobreredesdedatos*. Obtenido de blogspot: http://todosobreredesdedatos.blogspot.com/p/stp_5.html

Opnet. (2018). Simulacion. Quito, Ecuador.

ORION. (2018). *Monitoreo de Enlaces.* Quito.

Padilla, L. P. (2016). REDISEÑO DE UNA RED LAN MULTISERVICIOS PARA EL MUNICIPIO DE TULCAN. *UDLA*.

PRTG. (2018). *Monitoreo Aplicacion Web.* Quito.

PRTG. (2018). *Monitoreo de Base de Datos.* Quito.

PRTG. (2018). *Monitoreo DNS.* Quito.

Recover. (2015).

Recover. (2018).

Salazar, G. (30 de Septiembre de 2016). *supportforums.cisco.com*. Obtenido de https://supportforums.cisco.com/t5/routing-y-switching-blogs/fundamentos-de-qos-calidad-de-servicio-en-capa-2-y-capa-3/ba-p/3103715