# UNIVERSIDAD MAYOR DE SAN ANDRES
## FACULTAD DE TECNOLOGÍA
## CARRERA ELECTRÓNICA Y TELECOMUNICACIONES


# "REDISEÑO DE LA RED LAN DE ACCESO A LA INFORMACIÓN DE LA CAJA NACIONAL DE SALUD REGIONAL POTOSÍ"

**PROYECTO DE GRADO presentado para obtener el grado de**

**Licenciatura en Electrónica y Telecomunicaciones**


## POSTULANTE: LUIS FERNANDO REYES LARREA

**TUTOR: LIC. JAVIER NICOLÁS YUJRA TARQUI**


**La Paz – Bolivia**

**2017**

Este trabajo está dedicado primeramente a mi Dios a quien le debo todo, mi vida no me alcanzara para poderle pagar todas las bendiciones y el conocimiento que el me da (DyC 109:7), y a mi familia que me apoyo en esta etapa de mi vida**.**

# INDICE

# TABLAS

## FIGURAS

## ANEXOS

**ANEXO11 - CONFIGURACIÓN REGIONAL1**

**ANEXO12 - CONFIGURACIÓN REGIONAL2**

**ANEXO13 - CONFIGURACIÓN FORTIWEB (WEB APPLICATION FIREWALL)**

**ANEXO14 - CONFIGURACIÓN FORTIGATE (FIREWALL)**

**ANEXO15 - CONFIGURACIÓN FORTIWAN (BALANCEADOR DE ENLACES)**

**ANEXO16 – CONFIGURACIÓN FORTIANALYZER (ANALIZADOR DE RED)**

# CAPITULO I

## INTRODUCCIÓN

### 1.1. ANTECEDENTES DEL PROYECTO

En estos últimos tiempos las tecnologías de la información están teniendo un gran crecimiento y mucha importancia en las redes LAN y en Internet debido a la gran necesidad de estar siempre conectados a diferentes servicios, estas redes actuales deben tener la capacidad de poder brindar integración de servicios tales como datos, audio, video y voz, ya sean locales y/o en internet, todo esto ha llevado a que las redes actuales tengan diferentes formas y a la vez tengan cierto tipo de sofisticación para su acceso, a todo esto se suma el crecimiento constante del número de usuarios finales y la generación de grandes cantidades de información y de tráfico de estos, lo cual hace que estas redes necesiten la capacidad de poder brindar un flujo de datos constantes y sin pérdidas y a la ves poder ser seguras para evitar intrusos en nuestra red.

La Caja Nacional de Salud regional Potosí, cuenta entre sus recursos informáticos, de redes y de almacenamiento con una topología tradicional, es decir la interacción entre todos estos recursos es a través de diferentes aplicaciones para usuarios finales. Su red actualmente cuenta con una cobertura a todos sus hospitales y oficinas los cuales consumen los datos generados por estas aplicaciones y a la vez utilizan internet para distintas actividades, a todo esto se suma la gran cantidad de usuarios finales que va en crecimiento, con lo que es muy necesario tener máxima seguridad para salvaguardar el tráfico de datos, además de la necesidad de tener un tráfico constante sin pérdidas grandes de la información. La virtualización de los clúster tradicionales están separadas de los recursos de computación y los de almacenamiento, siendo así que se requieran sistemas de almacenamiento costosos dependiendo de las aplicaciones, las cargas de trabajo en los servidores son sensibles a las variaciones de accesibilidad de los usuarios a dichas aplicaciones, lo que resulta en una excesiva lentitud en ciertos horarios picos, además que el crecimiento de los datos almacenados varía por temporadas lo cual hace que se tenga que

exagerar con la adquisición dichos recursos o en el peor de los casos la no accesibilidad a sus aplicaciones por falta de recursos, además de todo lo expuesto se suma la falta de documentación para la resolución de posibles inconvenientes en la red.

## 1.2. PLANTEAMIENTO CENTRAL DEL PROBLEMA

Debido al constante crecimiento de la red de la Caja Nacional de Salud Regional Potosí, esta tiene problemas para adaptarse a los cambios tecnológicos, cambios en el crecimiento que son afectados por el mal dimensionamiento de la red y los constantes ataques informáticos que estas sufren tanto a servidores como a usuarios finales, esto ha llevado a preguntarse a los encargados de red si ellos cuentan con una red que permita estar a la par de dichos cambios para poder evitar problemas de accesibilidad, escalabilidad, eficiencia y seguridad en sus redes, a esto se suma la poca documentación que se tiene debido al crecimiento constante de sus usuarios y los servicios que estos consumen.

Considerando el conjunto de debilidades identificadas en el diagnóstico realizado al sistema de información de la institución, el planteamiento de la problemática identificada es **¿Sistema de Información Institucional integrada, insuficiente y desactualizada que no responde a la demanda de los beneficiarios y/o usuarios que reciben sus beneficios de acceso a la información del sistema y aplicaciones de Salud en la Caja?**

## 1.3. OBJETIVOS DEL PROYECTO

### 1.3.1. OBJETIVO GENERAL

- Rediseñar la red LAN de acceso a la información de la Caja Nacional de Salud Regional Potosí

### 1.3.2. OBJETIVOS ESPECÍFICOS

- Diseñar diagramas de topología de la red
- Diseñar y configurar redundancia en las conexiones principales.
- Diseñar y reconfigurar el enrutamiento con OSPF.

- Reordenar VLANs.
- Diseñar y configurar Web Application Firewall para protección de acceso a servidores.
- Diseñar, configurar, ordenar y controlar el acceso a internet de los usuarios finales a través de un Firewall de siguiente Generación NGF
- Diseño y configuración de un balanceador de enlaces para acceso a internet.
- Diseño y configuración de un analizador de red.

## 1.4. JUSTIFICACIÓN DEL PROYECTO

### 1.4.1. JUSTIFICACIÓN TÉCNICA

Considerando el papel cada vez más importante de las tecnologías de la información en las empresas actuales, el buen funcionamiento de las redes es de vital importancia por no decir críticas en su funcionamiento, ya que un corte en los servicios de producción implica grandes pérdidas económicas, es por esa razón que las redes tanto de datos como de voz deben estar diseñadas de tal forma que puedan prevenir cualquier inconveniente, y a la ves poder brindar eficiencia, escalabilidad y seguridad.

Bajo estos argumentos un rediseño de la red actual de la Caja Nacional de Salud regional Potosí, Implicaría los siguientes beneficios técnicos a tomarse en cuenta:

- Contar con redundancia y protección contra fallas.
- Brindar seguridad en el flujo de datos tanto internamente como externamente.
- Brindar eficiencia en las aplicaciones sensibles al rendimiento, diferenciando el tráfico de estas, para tomar decisiones inteligentes sobre el uso compartido de carga cuando la red este temporalmente congestionada.
- Contar con documentación actualizada de la red

### 1.4.2. JUSTIFICACIÓN ECONÓMICA

Hoy en día, es imprescindible que la red evolucione para responder de manera inteligente a una nueva ola de objetivos comerciales y demandas de usuario, una arquitectura de red actual debe brindar al departamento de TI la flexibilidad que necesita para adaptarse a los cambios constantes.
Dadas estas características en las redes actuales, una red eficiente, escalable y actualizada ofrece las siguientes ventajas económicas:

- Mejora en la actualización de la red.
- Aumento en la productividad de los usuarios.
- Reducción de amenazas de infracciones de seguridad.
- En caso de adquirir nuevos equipos estos serán flexibles y soportaran el crecimiento de la red a futuro, reduciendo el costo de compras de equipos sin un adecuado dimensionamiento.
- Reducción del costo de contratar y capacitar personal técnico para redes.

### 1.4.3. JUSTIFICACIÓN SOCIAL

En la actualidad el acceso a la información es imprescindible desde cualquier lugar donde uno se encuentre, dependiendo del tipo de información que se requiera esta debe estar disponible de forma rápida y confiable, la Caja Nacional de Salud Regional Potosí es una institución dedicada a la salud de sus asegurados, como esta institución cuenta con 4 edificios a lo largo de la ciudad de potosí la información de registros de asegurados, historiales médicos, etc., debe estar disponible de forma rápida y confiable en los cuatro edificios que se cuentan, de esta forma el acceso a la información determina un gran impacto social en los asegurados para así poder contar con un servicio disponible, simple, rápido y óptimo.

### 1.4.4. JUSTIFICACIÓN INSTITUCIONAL

Para la caja Nacional de Salud Regional Potosí, es transcendente poder brindar un servicio eficaz, confiable y que no demande que el asegurado pierda su tiempo en espera de su atención, para este cometido el contar con una red

estable y libre de errores donde la información pueda fluir de extremo a extremo sin problemas es institucionalmente para la Caja un factor muy importante para poder brindar un servicio adecuado a sus asegurados.

## 1.5. ALCANCES Y LIMITACIONES

### 1.5.1. ALCANCES

- El presente proyecto abarcara el estudio de la red actual de la Caja Nacional de Salud Regional Potosí en sus componentes de Red LAN, en el consumo de sus aplicaciones de servicios internos, navegación y aplicaciones de internet de sus usuarios finales.
- Mediante este estudio se realizara una propuesta de rediseño de la red en todos los componentes detallados.

### 1.5.2. LIMITACIONES

- La falta de documentación y registros de la red actual.
- El presente proyecto requiere un periodo de tiempo de recolección de información de la red actual.
- El proyecto brindara una propuesta de rediseño de la red, que será puesta a consideración de la Caja Nacional de Salud Regional Potosí para su futura aplicación.

# CAPÍTULO II

## MARCO TEÓRICO

### 2.1. INTERNETWORK

Internetwork es la conexión de dos o más redes, estas redes están conectadas mediante un dispositivo de red que permite la comunicación entre estas redes

Aunque el uso de redes LAN o WAN tiene ventajas, la mayoría de las personas necesitan comunicarse con un recurso ubicado en otra red, fuera de la red local del hogar, el campus o la organización. Esto se logra mediante el uso de Internet. Internet es una colección mundial de redes interconectadas (abreviado: internetworks o internet), que colaboran para intercambiar información sobre la base de estándares comunes. A través de cables telefónicos, cables de fibra óptica, transmisiones inalámbricas y enlaces satelitales, los usuarios de Internet pueden intercambiar información de diversas formas.

Internet es un conglomerado de redes que no es propiedad de ninguna persona ni de ningún grupo. Para garantizar una comunicación eficaz en esta infraestructura heterogénea, se requiere la aplicación de tecnologías y estándares coherentes y comúnmente reconocidos, así como la cooperación de muchas entidades de administración de redes. Existen organizaciones que se desarrollaron con el fin de ayudar a mantener la estructura y la estandarización de los protocolos y los procesos de Internet. Entre estas organizaciones, se encuentran Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN) e Internet Architecture Board (IAB), entre muchas otras.

El término “internet” (con “i” minúscula) se utiliza para describir un conjunto de redes interconectadas. Para referirse al sistema global de redes de computadoras interconectadas, o World Wide Web, se utiliza el término “Internet” (con “I” mayúscula).[1]

1 Cisco CCNA1 V5 Pag.35

### 2.2.1. TIPOS DE INTERNETWORK

#### 2.2.1.1. LOCAL AREA NETWORK (LAN)

Las redes LAN están limitadas a un área local o una pequeña área geográfica, su extensión está limitada a un entorno de 200 metros como máximo, como ejemplo de red LAN se puede definir al conjunto de computadores o terminales finales conectadas entre sí en un departamento o área determinada, todos compartiendo y accediendo a recursos mediante dispositivos de red, una red LAN utiliza dispositivos tales como swtiches y/o hubs para interconectar a los dispositivos finales, para poder conectar a otras LANs o WANs se pueden utilizar Routers o Switches.

#### 2.2.1.2. WIDE AREA NETWORK (WAN)

Una red WAN puede cubrir más de un área geográfica, este tipo de red es ideal para oficinas en diferentes ciudades en un país o en el mundo, pueden cubrir distancias desde 100 a 1000 Km. Cada oficina puede estar conectada a otros sitios mediante un router.[2]

### 2.3. MODELO OSI

Inicialmente, el modelo OSI fue diseñado por la ISO para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas exclusivos.

En última instancia, la velocidad a la que fue adoptada Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos que se crearon mediante las especificaciones OSI se utilizan ampliamente en la actualidad, el modelo OSI de siete capas hizo más contribuciones al desarrollo de otros protocolos y productos para todo tipo de redes nuevas.

El modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa.

2 Cisco CCNA1 V5 Pag.33-34

También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Si bien el contenido de este curso está estructurado en torno al modelo de referencia OSI, el análisis se centra en los protocolos identificados en el modelo de protocolo TCP/IP. Haga clic en cada nombre de la capa para ver los detalles.

Mientras que a las capas del modelo TCP/IP se hace referencia solo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre. Por ejemplo, la capa física se conoce como capa 1 del modelo OSI.

**Tabla # 2.1: Capas Modelo OSI**
**Fuente: Elaboración Propia**

| NUMERO DE CAPA | NOMBRE DE CAPA |
|---|---|
| 7 | Aplicación |
| 6 | Presentación |
| 5 | Sesión |
| 4 | Transporte |
| 3 | Red |
| 2 | Datos |
| 1 | Física |

### 2.3.1 CAPA DE APLICACIÓN

Esta capa contiene varios protocolos que los usuarios requieren con frecuencia. Un protocolo de aplicación de amplio uso es HTTP (Protocolo de Transferencia de Hipertexto), que es la base de World Wide Web. Cuando un navegador desea una página Web, utiliza este protocolo para enviar al servidor el nombre de dicha página. A continuación, el servidor devuelve la página. Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico y noticias en la red.

Provee el interfaz de comunicación entre el usuario final y el software para cualquier aplicación. Además brinda las siguientes funcionalidades:

- Sincronización de aplicaciones cliente servidor.
- Control de errores e integridad de datos entre aplicaciones.
- Sistema independiente de procesos al usuario final.

### 2.3.2. CAPA DE PRESENTACIÓN

A diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso “en el cable”. La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto (por ejemplo, registros bancarios).

Provee la presentación de datos a la capa de aplicación y actúa como un traductor del formato de datos, esta traducción es necesaria para asegurar que los datos puedan ser leídos por las aplicaciones.

### 2.3.3. CAPA DE SESIÓN

Esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control de diálogo (dar seguimiento de a quién le toca transmitir), administración de token (que impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de una caída).

Se ocupan principalmente del control del diálogo entre dispositivos, en esta capa se determina el comienzo, el medio y el final de la sesión o conversación que ocurre entre aplicaciones.

### 2.3.4. CAPA DE TRANSPORTE

La función básica de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe hacer con eficiencia y de manera que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware.

La capa de transporte también determina qué tipo de servicio proporcionar a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de conexión de transporte más popular es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otros tipos de servicio de transporte posibles son la transportación de mensajes aislados, que no garantiza el orden de entrega, y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina cuando se establece la conexión. (Como observación, es imposible alcanzar un canal libre de errores; lo que se quiere dar a entender con este término es que la tasa de error es tan baja que se puede ignorar en la práctica.)

La capa de transporte es una verdadera conexión de extremo a extremo, en toda la ruta desde el origen hasta el destino. En otras palabras, un programa en la máquina de origen lleva a cabo una conversación con un programa similar en la máquina de destino, usando los encabezados de mensaje y los mensajes de control. En las capas inferiores, los protocolos operan entre cada máquina y sus vecinos inmediatos, y no entre las máquinas de los extremos, la de origen y la de destino, las cuales podrían estar separadas por muchos enrutadores.

Esta capa es la responsable de las conexiones end-to-end y la entrega de datos entre dos host o dispositivos finales, segmenta y re ensambla los datos como una funcionalidad de esta capa.

Provee las siguientes funcionalidades:

- Detección de fallas.
- Recuperación de errores.
- Establece, mantiene y restablece los circuitos virtuales.

La capa de transporte puede proveer una red confiable mediante:

- Acknowledgments
- Sequencing
- Flow Control

### 2.3.5. CAPA DE RED

Esta capa controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen a su destino. Las rutas

pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

Si hay demasiados paquetes en la subred al mismo tiempo, se interpondrán en el camino unos y otros, lo que provocará que se formen cuellos de botella. La responsabilidad de controlar esta congestión también pertenece a la capa de red, aunque esta responsabilidad también puede ser compartida por la capa de transmisión. De manera más general, la calidad del servicio proporcionado (retardo, tiempo de tránsito, inestabilidad, etcétera) también corresponde a la capa de red. Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red podría ser diferente del de la primera. La segunda podría no aceptar todo el paquete porque es demasiado largo. Los protocolos podrían ser diferentes, etcétera. La capa de red tiene que resolver todos estos problemas para que las redes heterogéneas se interconecten.

En las redes de difusión, el problema de enrutamiento es simple, por lo que la capa de red a veces es delgada o, en ocasiones, ni siquiera existe.

En resumen determina el mejor camino para devolver el paquete a través de la red, protocolos de ruteo como IP son usados para determinar direccionamiento lógico los cuales pueden determinar el destino del paquete. El más común dispositivo de red utilizado en esta capa es el Router, de todas maneras también existen switches de capa 3 que pueden ser implementados.

### 2.3.6. CAPA DE DATOS

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esta tarea haciendo que el emisor fragmente los datos de entrada en tramas de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción.

Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de las capas superiores) es cómo hacer que un transmisor rápido no sature de datos a un receptor lento. Por lo general se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese

momento. Con frecuencia, esta regulación de flujo y el manejo de errores están integrados. Las redes de difusión tienen un aspecto adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos, la subcapa de control de acceso al medio, se encarga de este problema.

La capa de datos provee una transferencia de datos a través de la red de forma segura desde la capa de red a la capa física.

Dos tipos de dominios determinan la confiabilidad de la capa de datos:

- Dominio de Broadcast
- Dominio de Colisión

Como dispositivos de red comúnmente utilizados en esta capa están los switches, bridges y los hubs.

### 2.3.7. CAPA FÍSICA

En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación. Los aspectos del diseño implican asegurarse de que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal, no como bit 0. Las preguntas típicas aquí son: ¿cuántos voltios se deben emplear para representar un 1 y cuántos para representar un 0?, ¿cuántos nanosegundos dura un bit?, ¿la transmisión se debe llevar a cabo en ambas direcciones al mismo tiempo?, ¿cómo se establece la conexión inicial y cómo se finaliza cuando ambos lados terminan?, ¿cuántos pines tiene un conector de red y para qué se utiliza cada uno? Los aspectos de diseño tienen que ver mucho con interfaces mecánicas, eléctricas y de temporización, además del medio físico de transmisión, que está bajo la capa física.

Como se mencionaba en esta capa se definen los parámetros eléctricos, mecánicos, de procesamiento y funcionamiento de la capa física, para la activación, mantenimiento, y desactivación de la conectividad física entre dispositivos.

En resumen sus características son:

- Especificación de voltaje, velocidad del cable, y cables pin-out.
- Capacidad de recibir y transmitir los datos de la señal.

Dadas las características de capa del modelo OSI podemos definir de qué manera se controla la información en cada capa respectiva:

**Tabla# 2.2: Encapsulamiento de la Información**
**Fuente: Elaboración Propia**

| CAPA OSI | CONTROL DE LA INFORMACION |
|---|---|
| APLICACIÓN<br>PRESENTACIÓN<br>SESIÓN | DATOS |
| TRANSPORTE | SEGMENTO |
| RED | PAQUETE |
| DATOS | TRAMA |
| FISICA | BIT |

Basados en el cuadro anterior podemos ver como la información es encapsulada para viajar a través de varias capas del modelo OSI.[3]

## 2.4. MODELO TCP/IP

El modelo de protocolo TCP/IP para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Como se muestra en la ilustración, define cuatro categorías de funciones que deben ocurrir para que las comunicaciones se lleven a cabo correctamente. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por lo tanto, el modelo de Internet es conocido normalmente como modelo TCP/IP.

La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de RFC disponibles al público. Las RFC contienen la especificación formal de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC también contienen documentos técnicos y organizacionales sobre Internet, entre los que se incluyen las especificaciones técnicas y los documentos de las políticas elaborados por el IETF.[4]

3 Cisco CCNA1 V5 Pag.140
3 Redes de computadoras Cuarta edición pag.37-40
4 Cisco CCNA1 V5 Pag.141

**Tabla# 2.3: Capas Modelo TCP/IP**
**Fuente: Elaboración Propia**

| MODELO OSI | MODELO TCP/IP |
|---|---|
| APLICACIÓN, PRESENTACIÓN Y SESIÓN | APLICACIÓN |
| TRANSPORTE | TRANSPORTE |
| RED | INTERNET |
| DATOS, FISICA | RED DE ACCESO |

Los siguientes protocolos son los que corresponden a cada capa del modelo TCP/IP:

**Tabla# 2.4: Protocolos Modelo TCP/IP**
**Fuente: Elaboración Propia**

| CAPAS TCP/IP | PROTOCOLOS |
|---|---|
| APLICACIÓN | TELNET, HTTP/HTTPS, FTP, TFTP DNS, SMTP, POP3, NFS NNTP, SNMP, NTP, DHCP |
| TRANSPORTE | TCP, UDP |
| INTERNET | ICMP, ARP, RARP, IP |
| INTERFACE DE RED | ETHERNET, FAST ETHERNET, TOKEN RING,FDDI |

## 2.5. MODELO JERARQUICO DE CISCO

La Guía de diseño para la tecnología LAN cableada en campus usa un modelo de diseño jerárquico para desglosarlo en grupos modulares o capas. Este desglose del diseño en capas permite a cada capa implementar funciones específicas, lo que simplifica el diseño de red y, por lo tanto, la implementación y administración de la red.

La modularidad en el diseño de red permite crear elementos de diseño que pueden replicarse en toda la red. La replicación ofrece una manera sencilla de ampliar la red, así como también un método de implementación homogéneo.

En arquitecturas de red mallada o plana, los cambios tienden a afectar a una gran cantidad de sistemas. El diseño jerárquico permite restringir los cambios operativos a un subgrupo de la red, lo que facilita la administración y mejora la recuperabilidad. La estructuración modular de la red en elementos pequeños y

fáciles de comprender también facilita la recuperabilidad mediante aislamiento de fallas mejorado.

El termino jerárquico permite a este modelo de Cisco realizar una clasificación de grupos de funciones o responsabilidades dentro de una capa lógica donde capa está subordinada por la capa superior, este modelo es el más efectivo a la hora de implementar una red moderadamente pequeña.

Una topología jerárquica típica es:

- Una capa central de routers y conmutadores de gama alta que están optimizados para la disponibilidad y el rendimiento.
- Una capa de distribución de enrutadores y conmutadores que implementan políticas. En las organizaciones pequeñas y medianas, las capas núcleo y distribución pueden combinarse.
- Una capa de acceso que conecta a los usuarios mediante conmutadores de gama baja y puntos de acceso inalámbricos.

**Tabla# 2.5: Dispositivos Modelo Jerárquico de Cisco**

**Fuente: Elaboración Propia**

| CAPA | DISPOSITIVO |
|---|---|
| NUCLEO | SWITCHES CAPA3, ROUTERS, GRANJA DE SERVIDORES |
| DISTRIBICIÓN | ROUTERS |
| ACCESO | SWITCHES CAPA 2, ESTACIONES DE TRABAJO |

### 2.5.1. CAPA DE ACCESO

La capa de acceso es por donde los dispositivos controlados por el usuario, dispositivos accesibles al usuario y otros dispositivos terminales se conectan a la red. La capa de acceso ofrece conectividad tanto inalámbrica como por cable y contiene características y servicios para garantizar seguridad y recuperabilidad para toda la red.

• **Conectividad de dispositivos:** la capa de acceso ofrece conectividad de dispositivos con ancho de banda de alta velocidad. A fin de hacer de la red una pieza transparente del trabajo diario del usuario final, la capa de acceso debe poder admitir ráfagas de tráfico de ancho de banda de alta velocidad cuando los usuarios realizan tareas de rutina, como enviar correos electrónicos pesados o abrir un archivo desde una página web interna.

Debido a que muchos tipos de dispositivos de los usuarios finales se conectan a la capa de acceso (equipos personales, teléfonos IP, puntos de acceso inalámbricos, y cámaras de videovigilancia mediante IP), la capa de acceso puede admitir muchas redes lógicas, con lo cual ofrece los beneficios de rendimiento, administración y seguridad.

• **Servicios de seguridad y recuperabilidad**: el diseño de la capa de acceso debe garantizar que la red esté disponible para todos los usuarios que la necesitan, cuando la necesitan. Como punto de conexión entre la red y los dispositivos clientes, la capa de acceso debe ayudar a proteger la red contra errores humanos y ataques maliciosos. Esta protección incluye garantizar que los usuarios tengan acceso solamente a servicios autorizados, con lo cual se evita que los dispositivos de usuario final se apoderen del rol de otros dispositivos en la red y, cuando es posible, se verifica que todos los dispositivos de usuario final están permitidos en la red.

• **Funcionalidades de tecnología avanzada:** la capa de acceso ofrece un conjunto de servicios de red que admiten tecnologías avanzadas, como voz y video. La capa de acceso debe ofrecer acceso especializado para los dispositivos mediante el uso de tecnologías avanzadas, para garantizar que el tráfico de estos dispositivos no se vea afectado por el tráfico de otros dispositivos y, además, para garantizar la distribución eficiente del tráfico que necesitan muchos dispositivos en la red.

Los usuarios finales están conectados a esta capa, en esta capa pueden ser definidas VLANs, listas de acceso para permitir la comunicación mediante políticas implementadas en la capa de distribución, permitiendo el control de acceso a los recursos de la red para cada usuario.

### 2.5.2. CAPA DE DISTRIBUCIÓN

La capa de distribución admite muchos servicios importantes. En una red donde la conectividad debe atravesar la LAN completa, ya sea entre distintos dispositivos de la capa de acceso o desde un dispositivo de la capa de acceso a la WAN, la capa de distribución hace posible esta conectividad.

• **Escalabilidad:** en cualquier sitio con más de dos o tres dispositivos de capa de acceso, no resulta práctico interconectar todos los switches de acceso. La capa de distribución sirve como un punto de agregación para múltiples switches de la capa de acceso.

La capa de distribución puede reducir los gastos operativos haciendo que la red sea más eficiente, exigiendo menos cantidad de memoria, creando dominios de falla que compartimenten las fallas o los cambios en la red y procesando los recursos para dispositivos en cualquier otro lado en la red. La capa de distribución también aumenta la disponibilidad de red gracias a que contiene las fallas en dominios más pequeños.

• **Reducción de la complejidad y aumento de la recuperabilidad:** la Guía de diseño para la tecnología LAN cableada en campus usa una capa de distribución simplificada, en la cual un nodo de la capa de distribución se compone de una entidad lógica individual que puede implementarse usando un par de switches físicamente separados que funcionan como un dispositivo, o bien usando una pila física de switches que funcionan como un dispositivo. La recuperabilidad la aportan los componentes físicamente redundantes, como fuentes de alimentación, supervisores y módulos, así como también la conmutación activa para los planos de control lógico redundantes.

Este enfoque reduce la complejidad que supone configurar y operar la capa de distribución porque se requiere menor cantidad de protocolos. Se necesita muy poco o nada de ajuste para proporcionar convergencia en una fracción de segundo en torno a las fallas o interrupciones

En este modelo jerárquico, la capa de distribución es la capa que está en el medio del modelo, de esta manera la capa de distribución trabaja como un punto de reunión para los dispositivos de la capa de acceso, donde incluso pueden ser utilizados dispositivos de red tales como switches de capa 3 y routers para determinar cómo atraviesan los paquetes a la capa núcleo.

Para un efectivo control en esta capa se utilizan varias políticas para proveer manejo y seguridad en la red.

Como funciones principales de esta capa incluyen:

- Enrutamiento, determinación del mejor camino que tomara el paquete.
- Enrutamiento a través de VLANs.
- Filtrado, mediante listas de acceso, calidad de servicio, NAT y filtrado de rutas.
- Acceso a WAN
- Definición de dominios de broadcast y multicast
- Traducción entre diferentes tipos de medios (Ethernet, FO)

### 2.5.3. CAPA NUCLEO

En un entorno de LAN grande con frecuencia surge la necesidad de contar con varios switches de capa de distribución. Uno de los motivos es que cuando los switches de la capa de acceso se ubican en varios edificios geográficamente dispersos, puede ahorrarse la instalación de fibra óptica —potencialmente costosa— entre los edificios mediante la colocación de un switch de capa de distribución en cada uno de esos edificios. Dado que las redes crecen más allá de las tres capas de distribución en una sola ubicación, las organizaciones deberían usar una capa de núcleo central para optimizar el diseño.

Otro motivo para usar varios switches de capa de distribución es cuando la cantidad de switches de capa de acceso que se conectan a una sola capa de distribución excede los objetivos de rendimiento del diseñador de redes. En un diseño modular y escalable, puede colocar capas de distribución para el centro de datos, conectividad WAN o servicios periféricos de Internet.

En entornos en los que existen varios switches de capa de distribución próximos entre sí y en los que la fibra óptica ofrece capacidad de interconexión de ancho de banda de alta velocidad, la capa de núcleo central reduce la complejidad de la red.

La capa de núcleo central de la LAN es una pieza fundamental de la red escalable y, aun así, es una de las más simples de diseñar. La capa de distribución aporta los dominios de control y fallas, y el núcleo central representa la conectividad ininterrumpida, 24 horas al día, los 7 días de la semana todos los

días del año, entre ellos; las organizaciones deben contar con esto en entornos comerciales modernos en los que la conectividad a los recursos para realizar negocios sea crucial.

La capa de núcleo es el backbone de la red, la red se derrumbaría sin la estructura proporcionada por la capa de núcleo. Como lo mencionamos anteriormente la capa de distribución maneja el acceso al Core, esto hace posible que el Core se centre especialmente su trabajo en la velocidad y la confiabilidad. Este punto permite altas velocidades, rapidez y eficiencia siendo que de esta manera no se implementen políticas como en la capa de distribución. Redundancia y tolerancia a fallas son muy importantes tomar en cuenta en el diseño de esta capa, para que en circunstancias de caídas o errores en la red esta sea transparente para el usuario final. [5]

## 2.6. TOPOLOGIAS DE RED

El diseño lógico o físico de una red puede ser definido como una topología, típicamente una topología física es documentada mediante un diagrama de red, estos diagramas permiten tener una clara visión de toda la red y a la ves ayudar a resolver problemas generados en la red, o cambios que se puedan realizar en la red.

Una topología física consiste en la distribución de los dispositivos de red, cables, equipos finales dentro de la red.

Una topología lógica representa como la red esta comunicada actualmente entre sí.

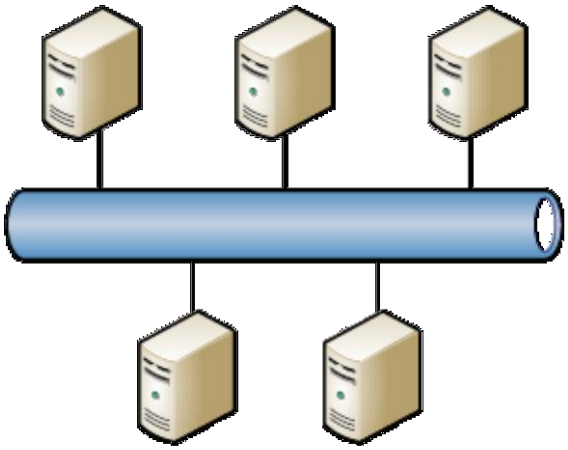
5 Top-Down Network Design Pag. 120

5 Campus Resumen de diseño Cisco Pag. 3-9

### 2.6.1. TOPOLOGIA BUS

Una topología Bus es referida a una topología linear, es decir que los nodos de la red están conectados a través de un cable (trunk o Backbone)

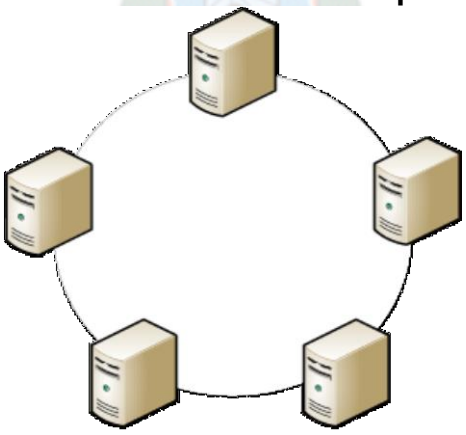
**Figura# 2.1: Topología Bus**
**Fuente: Elaboración Propia**



### 2.6.2. TOPOLOGIA ANILLO

Una topología en anillo permite que un dispositivo esté conectado directamente a otros dispositivos de la misma red. Cuando un dispositivo emite una señal de transmisión, la transmisión es enviada en una simple dirección hacia el siguiente dispositivo conectado, esta transmisión continua y pasa por todos los dispositivos sucesivamente hasta que vuelve al dispositivo original que transmitió, este método crea un anillo o loop.[6]

**Figura# 2.2: Topología Anillo**
**Fuente: Elaboración Propia**



6 Cisco CCNA1 V5 Pag.196

## 2.7. VIRTUAL LANs

Una LAN virtual (VLAN) es una emulación de una LAN estándar que permite que la transferencia de datos tenga lugar sin las restricciones físicas tradicionales colocadas en una red. Una VLAN es un conjunto de dispositivos LAN que pertenecen a un grupo administrativo. La pertenencia a estos grupos se basa en parámetros de configuración y políticas administrativas en lugar de la ubicación física. Los miembros de una VLAN se comunican entre sí como si estuvieran en el mismo cable o concentrador, cuando pudieran estar ubicados en diferentes segmentos físicos de LAN. Los miembros de una VLAN se comunican con los miembros en una VLAN diferente como si estuvieran en diferentes segmentos de LAN, incluso cuando estén ubicados en el mismo conmutador. Debido a que las VLAN se basan en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

En el comienzo de las VLAN a mediados de la década de 1990, hubo mucha conversación sobre el uso de VLAN para agrupar a los usuarios que trabajan en un proyecto junto, aunque no estuvieran físicamente juntos. Con VLANs, la ubicación física de un usuario no importa. Un administrador de red puede asignar un usuario a una VLAN independientemente de la ubicación del usuario. En teoría, la asignación de VLAN puede basarse en aplicaciones, protocolos, requisitos de rendimiento, requisitos de seguridad, características de carga del tráfico u otros factores.

VLANs permite segmentar dominios de broadcast de capa 2 sin tener un router, cada VLAN creada en un switch o varios puertos del switch representan grupos lógicos dentro de los dispositivos teniendo su propio dominio de broadcast, por lo tanto podemos decir que a la hora del diseño cada VLAN puede representar a un determinado departamento y este puede diferenciar su tráfico de otros departamentos que tengan sus propias VLANs.[7]

### 2.7.1. MANAGEMENT VLAN

Por defecto cada equipo viene configurado con una VLAN management en sus puertos de acceso para la administración de dicho equipo la cual tiene una dirección IP para este propósito.

7 Top-Down Network Design Pag. 141

### 2.7.2. CONFIGURACIÓN DE VLANs

Por defecto todos los interfaces de un switch vienen con la VLAN 1, para poder crear nuevas VLANs se debe seguir el siguiente procedimiento:

- Crear la VLAN, usando un numero identificativo ID de 2 al 1001
- Definir un nombre para la VLAN.
- Asignar a un puerto del switch.

### 2.7.3. VLAN TRUNKING

Una de las características de las VLANs es que pueden abarcar múltiples redes interconectadas entre switches, este tráfico de switch a switch es pasado por un interfaz denominado TRUNK, este interfaz Trunk debe tener al menos una velocidad de transmisión igual o mayor a 100Mbps.

Los Puertos Trunk esencialmente tienen todas las VLANs asignadas para poder pasar a otro switch el tráfico correspondiente de cada VLAN.

### 2.7.4. VLAN NATIVA

Otra característica principal de las VLANs es el concepto de VLAN nativa, el tráfico procedente de puertos de acceso que comparte la misma VLAN estas no se etiquetan en el enlace troncal. Por lo tanto cualquier trama que no esté etiquetada es recibida por el puerto trunk es considerada como una VLAN nativa.

## 2.8. PROTOCOLOS DE ENRUTAMIENTO

Un Protocolo de enrutamiento permite que los routers determinen cuál es la ruta que se debe usar para enviar los datos. Esto lo hace mediante un concepto denominado vector-distancia. Se contabiliza un salto cada vez que los datos atraviesan un router es decir, pasan por un nuevo número de red, esto se considera equivalente a un salto. Una ruta que tiene un número de saltos igual a 4 indica que los datos que se transportan por la ruta deben atravesar cuatro routers antes de llegar a su destino final en la red. Si hay múltiples rutas hacia un destino, la ruta con el menor número de saltos es la ruta seleccionada por el router.[9]

9 Top-Down Network Design Pag. 209

### 2.8.1. PROTOCOLOS DE ENRUTAMIENTO ESTATICOS

Son de configuración manual, todas las rutas estáticas que se le ingresen manualmente son las que el router las tendrá en sus tablas de enrutamiento por lo tanto sabrá en rutar paquetes hacia dichas redes.

### 2.8.2. PROTOCOLOS DE ENRUTAMIENTO DINAMICOS

El administrador de red sólo se encarga de configurar el protocolo de enrutamiento mediante comandos IOS, en todos los routers de la red y estos automáticamente intercambiarán sus tablas de enrutamiento con sus routers vecinos, por lo tanto cada router conoce la red gracias a las publicaciones de las otras redes que recibe de otros routers. Los protocolos de enrutamiento dinámicos se dividen en vector distancia y estado de enlace:

#### 2.8.2.1. VECTOR DISTANCIA

Su métrica se basa en Numero de Saltos, es decir la cantidad de routers por los que tiene que pasar el paquete para llegar a la red destino, la ruta que tenga el menor número de saltos es la más óptima y la que se publicará.

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

#### 2.8.2.2. ESTADO DE ENLACE

Su métrica se basa el retardo, ancho de banda, carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo prefiere una ruta por sobre otra. Estos protocolos utilizan un tipo de publicaciones llamadas Publicaciones de estado de enlace (LSA), que intercambian entre los routers, mediante estas publicaciones cada router crea una base datos de la topología de la red completa.

- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermadiate System (IS-IS)

**Tabla# 2.6: Protocolos de Enrutamiento**
**Fuente: Elaboración Propia**

| PROTOCOLO DE ENRUTAMIENTO | TIPO | IGP/EGP |
|---|---|---|
| RIP | VECTOR DISTANCIA | IGP |
| EIGRP | VECTOR DISTANCIA | IGP |
| OSPF | ESTADO DE ENLACE | IGP |
| IS-IS | ESTADO DE ENLACE | IGP |
| BGP | VECTOR DISTANCIA | EGP |

## 2.9. FIREWALL

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente, y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

Un firewall puede ser hardware, software o ambos.[10]

### 2.9.1. TIPOS DE FIREWALLS

#### 2.9.1.1. FIREWALL PROXY

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir.

10 Top-Down Network Design Pag. 244

### 2.9.1.2. FIREWALL DE INSPECCION ACTIVA

Un firewall de inspección activa, ahora considerado un firewall “tradicional”, permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Este firewall monitorea toda la actividad, desde la apertura de una conexión hasta su cierre. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

### 2.9.1.3. FIREWALL DE ADMINISTRACION UNIFICADA DE AMENAZAS (UTM)

Un dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.

### 2.9.1.4. FIREWALL DE PROXIMA GENERACION (NGFW)

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:

- Funcionalidades de firewall estándares, como la inspección con estado
- Prevención integrada de intrusiones
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas
- Rutas de actualización para incluir fuentes de información futuras
- Técnicas para abordar las amenazas de seguridad en evolución.

## 2.10. WEB APPLICATION SECURITY (WAF)

Las aplicaciones web que se exponen externamente son vulnerables a ataques como cross site scripting, inyección de SQL y Layer 7 Denial of Service (DoS). Las aplicaciones web internas son aún más fáciles de atacar, el atacante es

capaz de acceder a una red interna donde muchas de las organizaciones piensan que están protegidas por su defensa red perimetral.

El código personalizado es generalmente el eslabón más débil, los equipos tienen la imposible tarea de mantenerse al tanto de cada tipo de ataque, sin embargo incluso el código comercial es vulnerable, las organizaciones no tienen los recursos para aplicar nuevos parches y seguridad para solucionar tan pronto como estén disponibles, además de tener un ejército de desarrolladores para proteger sus sistemas, los ataques de Día-Cero puede dejarte indefenso y solo capaz de responder después de que el ataque ha ocurrido.

Un equipo WAF Provee seguridad completa de manera externa e interna en su red:

- IP Reputation
- Botnets
- DoS Detection
- Layer 7 DoS Attacks
- SQL Inyection
- Web Defacement
- Data leak
- Cookie Poison
- Brute Force

## 2.11. METODOLOGIA DE DISEÑO DE REDES

Una red creada con cierta complejidad con bastante frecuencia no funciona en cuanto a desempeño como hubiésemos esperado, no es escalable a medida que la necesidad de crecimiento se evidencia que es algo normal que suceda y lo más crítico es que no satisface la totalidad de los requerimientos del cliente.

La metodología del diseño ha sido una constante en la búsqueda de soluciones A través de la experiencia acumulada en el diseño de productos, la teoría general de sistemas provee otra aproximación al diseño, y permite hacer frente a problemas de diferentes orígenes. Básicamente en una metodología sistemática permite vincular los diferentes subsistemas mediante el uso de variables.

Tradicionalmente dos alternativas de diseño existen actualmente: Top Down y Buttom up, han sido empleadas en el desarrollo de nuevos productos.

En la metodología Top Down, el diseño comienza desde el nivel superior. Las especificaciones son definidas en términos del estado del sistema global y cada componente individual debe ser estimado con suficiente tiempo.[11]

## 2.12. ANALIZAR LOS REQUERIMIENTOS

Para poder entender los requerimientos del diseño de una red, primeramente es necesario conocer a fondo a la organización con la cual se trabajara en esto, conocer en que rubro es su trabajo, que productos manejan, que servicios brindan, conocer la estructura organizativa y jerárquica de la compañía, para esto es necesario tener una reunión con ellos para obtener toda esta información, mediante preguntas tales como: ¿Por qué la compañía se está embarcando en este nuevo proyecto de diseño de red?, ¿Para qué seria usada la nueva red?, ¿Cómo le ayudaría la nueva red a la compañía para que tenga más éxito en su negocio?.

Una vez definidos estos componentes necesarios podemos avanzar en el diseño de la red.

## 2.13. ANALISIS TECNICO DE OBJETIVOS Y COMPENSACIONES

En un análisis técnico típicamente de incluyen los siguientes objetivos:

- Escalabilidad
- Disponibilidad
- Performance de la red
- Seguridad
- Manejabilidad
- Usabilidad
- Adaptabilidad
- Asequibilidad

Definiendo, analizando y entendiendo estos conceptos podremos tener una visión más clara acerca de las necesidades técnicas de la compañía.

11 Top-Down Network Design Pag. 119

## 2.14. CARACTERIZAR LA RED Y LOS SITIOS EXISTENTES

Un importante paso en el diseño de red es el examinar la red actual de la compañía para así tener un mejor juicio y conocer las expectativas de la compañía en cuanto a escalabilidad, performance y disponibilidad de la red.

En este paso incluye aprender acerca de la topología y estructura física, evaluando el desempeño de la red actual. Es necesario poder documentar cualquier anormalidad presentada durante este análisis como ser cuellos de botella, problemas de performance en la red, además de identificar dispositivos de red que estén trabajando actualmente, si estos necesitan ser reemplazados o mejorar la configuración que tienen, el número de puertos que están trabajando, si su capacidad es suficiente o insuficiente, para así una vez identificado estos objetivos dar solución en el nuevo diseño.

## 2.15. DISEÑO DE TOPOLOGIA DE RED

Un mapa topológico de una red permite poder identificar segmentos de red, puntos de interconexión y las comunicaciones de los usuarios. A pesar de que sitios geográficos pueden aparecer en el mapa, el propósito del mapa es mostrar la geometría de la red, no así la geometría física o la implementación técnica. El mapa es un plano de alto nivel análogo a un dibujo arquitectónico que muestra la ubicación y tamaño de las habitaciones de un edificio, pero no los materiales de construcción para fabricar las habitaciones.

Diseñar una red topológica es el primer paso en la fase de un diseño lógico, conociendo los requerimientos de la compañía para escalabilidad y adaptabilidad, es importante diseñar una topología lógica antes de seleccionar productos físicos o tecnologías.

Durante la fase de diseño topológico se deben identificar la red y los puntos de interconexión, el tamaño y el alcance de la red, y los tipos de dispositivos de red que van a ser requeridos.

### 2.15.1. DISEÑO DE TOPOLOGIA DE RED REDUNDANTE

El diseño de una red redundante permite que se conozca los requerimientos para una red disponible mediante la duplicación de elementos en la red. La redundancia permite eliminar cualquier simple punto de falla en la red. El objetivo es duplicar cualquier componente requerido cuyo fallo podría deshabilitar

aplicaciones críticas, así poner contar con la disponibilidad de estas aplicaciones sin cortes.

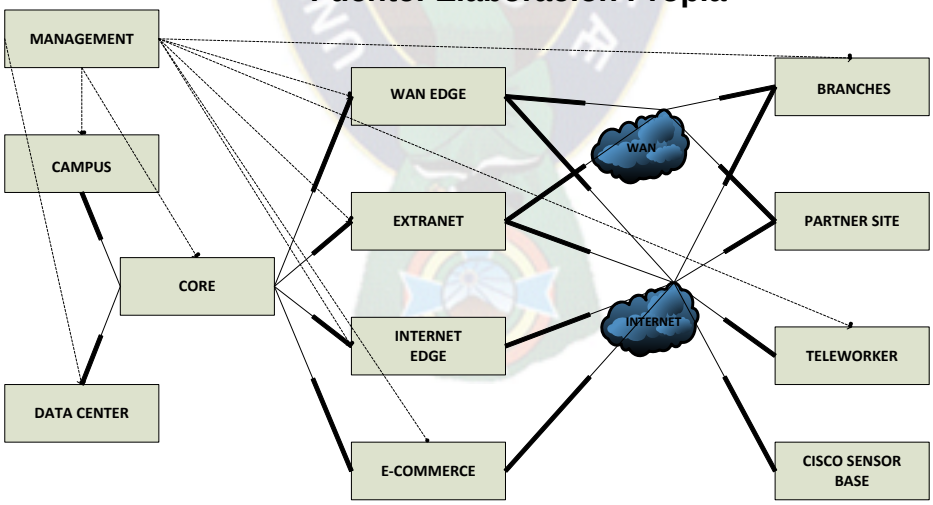
### 2.15.2. DISEÑO DE RED MODULAR

Grandes proyectos de diseño de redes y grandes redes en general, constan de diferentes áreas o módulos. Cada área debe diseñarse utilizando un enfoque sistemático de arriba hacia abajo, aplicando la jerarquía y la redundancia cuando sea apropiado. Las soluciones y servicios de red se pueden seleccionar en una base por módulo, pero se validan como parte del diseño general de la red.

## 2.16. ARQUITECTURA DE REFERENCIA DE SEGURIDAD CISCO SAFE

SAFE es la referencia de arquitectura que usan los diseñadores de red para simplificar la complejidad de una red grande. Esta arquitectura permite aplicar un enfoque modular a una red. Con SAFE se puede analizar el funcionamiento, lógica, y física de los componentes de la red simplificando así el proceso de diseño de una red empresarial global.[12]

**Figura# 2.3: Diagrama Cisco SAFE**
**Fuente: Elaboración Propia**

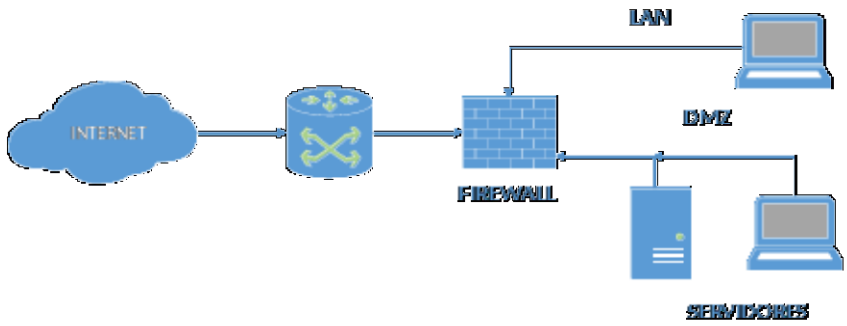



12 Cisco SAFE Reference Guide Pag.1-2

## 2.17. DISEÑO TOPOLOGICO DE RED SEGURA

Cuando se desarrolla el diseño lógico topológico de una red, se debe comenzar con tener la idea de donde el equipamiento debe ser instalado. Se debe empezar a trabajar sabiendo donde se instalara el equipamiento físicamente, ya que es muy crítico y necesita estar protegido de accesos no autorizados, robos, vandalismos y desastres naturales, esto no es un aspecto a considerar dentro
De un diseño lógico de la red pero es mencionado aquí porque en el diseño lógico topológico puede tener un gran impacto, y porque en el planeamiento para la seguridad física se debe empezar considerando este punto.

**Figura# 2.4: Diagrama Topológico de Red**
**Fuente: Elaboración Propia**




## 2.18. DISEÑO DE MODELOS PARA DIRECCIONAMIENTO Y NUMERACIÓN

El diseño de direccionamiento y numeración permite asignar esto a los componentes de red, incluyendo redes, subredes, y sistemas finales, a partir del protocolo IP.

Las direcciones de capa de red deben ser planeadas, manejadas y documentadas. Es posible que los sistemas finales puedan aprender estas direcciones dinámicamente.[13]

La siguiente lista provee simples reglas para el direccionamiento:

- Diseñar un modelo estructurado para el direccionamiento, esto es antes de asignar cualquier dirección.
- Dejar un campo para el crecimiento en el modelo de direccionamiento.
- Asignar bloques de direcciones jerárquicas para posibilitar la escalabilidad y disponibilidad.

13 Top-Down Network Design Pag. 189

- Asignar bloques de direcciones basadas en la red física
- Si el nivel de manejo de la red esta regionalizado en oficinas regionales, es posible delegar el direccionamiento.
- Para maximizar la flexibilidad y minimizar la configuración, se debe usar direccionamiento dinámico para sistemas finales.
- Para maximizar la seguridad y adaptabilidad se debe usar direcciones privadas con NAT.

## 2.19. SELECCIONAR PROTOCOLOS DE SWITCHING Y ROUTING

Se deben seleccionar correctamente los protocolos de Switching y Routing para un correcto diseño de la red, esta selección va depender de las necesidades de la compañía, algunos atributos necesarios que deben cumplir estos protocolos son los siguientes:

- Características de tráfico de red.
- Ancho de Banda, memoria y utilización de CPU.
- Número aproximado de routers o switches soportados.
- Capacidad de adaptación rápida cuando existen cambios en la red.
- Capacidad para autenticar actualizaciones de ruta por razones de seguridad. [14]

14 Top-Down Network Design Pag. 20

**Tabla# 2.7: Atributos Protocolos Switching & Routing**
**Fuente: Elaboración Propia**

| | CRITICO | | | OTROS | | |
|---|---|---|---|---|---|---|
| | ADAPTABILIDAD- SE DEBE ADAPTAR A CAMBIOS EN UNA RED GRANDE EN SEGUNDOS | DEBE SER ESCALABLE EN GRANDES REDES (MUCHOS ROUTERS) | DEBE SER UN ESTANDAR EN LA INDUSTRIA Y COMPATIBLE CON LOS EQUIPOS EXISTENTES | NO DEBE CREAR MUCHO TRAFICO | DEBE CORRER EN ROUTERS INEXPENSIVOS | DEBER FACIL DE CONFIGURAR Y MANEJAR |
| BGP | X* | X | X | 8 | 7 | 7 |
| OSPF | X | X | X | 8 | 8 | 8 |
| IS-IS | X | X | X | 8 | 6 | 6 |
| IGRP | X | X | | | | |
| EIGRP | X | X | | | | |
| RIP | | | X | | | |
| X*= Muy crítico. 1=bajo. 10=alto | | | | | | |

**Tabla# 2.8: Comparación Protocolos de Ruteo**
**Fuente: Elaboración Propia**

| COMPARACION DE PROTOCOLOS DE RUTEO | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **VECTOR DISTANCIA/ ESTADO DE ENLACE** | **INTERIOR/ EXTERIOR** | **CLASSFULL/ CLASSLESS** | **METRICA SOPORTADA** | **ESCALABILIDAD** | **TIEMPO DE CONVERGENCIA** | **RECURSOS** | **SOPORTA SEGURIDAD? RUTAS AUTENTICADAS?** | **FACIL DISEÑO, CONFIGURACION Y TROUBLESHOOTING** |
| **RIPv1** | VECTOR DISTANCIA | INTERIOR | CLASSFULL | CONTEO DE SALTOS | 15 SALTOS | PUEDE SER LARGO (SINO TIENE BALANCEO DE CARGA | MEMORIA:BAJO CPU:BAJO ANCHO DE BANDA:ALTO | NO | FACIL |
| **RIPv2** | VECTOR DISTANCIA | INTERIOR | CLASSLESS | CONTEO DE SALTOS | 15 SALTOS | PUEDE SER LARGO (SINO TIENE BALANCEO DE CARGA | MEMORIA:BAJO CPU:BAJO ANCHO DE BANDA:ALTO | SI | FACIL |
| **IGRP** | VECTOR DISTANCIA | INTERIOR | CLASSFULL | ANCHO DE BANDA RETRASO ADAPTABILIDAD CARGA | 255 SALTOS (POR DEFECTO 100) | RAPIDO (USA ACTUALIZACIONES Y ENVENENAMIENTO EN REVERSA) | MEMORIA:BAJO CPU:BAJO ANCHO DE BANDA:ALTO | NO | FACIL |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **EIGRP** | VECTOR DISTACIA AVANZADO | INTERIOR | CLASSLESS | ANCHO DE BANDA RETRASO ADAPTABILIDAD CARGA | 1000s ROUTERS | MUY RAPIDO (USA ALGORITMO DUAL) | MEMORIA:MODERADA CPU:BAJO ANCHO DE BANDA:BAJO | SI | FACIL |
| **OSPF** | ESTADO DE ENLACE | INTERIOR | CLASSLESS | COST (100 MILLONES DIVIDIDOS POR EL ANCHO DE BANDA EN CISCO ROUTERS) | MENOR A 1000 ROUTERS POR AREA , MENOR A 1000 AREAS | RAPIDO (USA LSAs Y PAQUETES HELLO) | MEMORIA:ALTA CPU:ALTO ANCHO DE BANDA:BAJO | SI | MODERADO |
| **BGP** | PATH VECTOR | EXTERIOR | CLASSLESS | MUCHOS ATRIBUTOS Y OTRO VALORES CONFIGURABLES | 1000s ROUTERS | RAPIDO (USA ACTUALIZACIONES Y PAQUETES KEEPALIVE Y WITHDRAWS ROUTERS) | MEMORIA:ALTA CPU:ALTA ANCHO DE BANDA:BAJO | SI | MODERADO |
| **IS-IS** | ESTADO DE ENLACE | INTERIOR | CLASSLESS | CONFIGURA VALORES PATH, PLUS DELAY EXPENSE Y ERRORES | MILES DE ROUTERS POR AREA MENOR DE MIL AREAS | RAPIDO (USA LSAs) | MEMORIA:ALTA CPU:ALTA ANCHO DE BANDA:BAJO | SI | MODERADO |

## 2.20. DISEÑO DE SEGURIDAD DE RED

En el proceso de seguridad en el diseño de una red se deben seguir los siguientes pasos para una eficiencia a la hora de ejecutar un plan de seguridad:

- Identificar los dispositivos de red
- Analizar los riesgos de seguridad
- Analizar los requerimientos de seguridad
- Desarrollar un plan de seguridad
- Definir políticas de seguridad
- Desarrollar procedimientos para aplicar las políticas de seguridad
- Desarrollar una estriega de implementación técnica
- Lograr la aceptación de los usuarios, gerentes y personal técnico
- Entrenar a los usuarios, gerentes y personal técnico
- Implementar estrategias técnicas y procedimientos de seguridad
- Probar la seguridad y actualizar este si presenta problemas
- Mantener la seguridad [15]

15 Top-Down Network Design Pag. 234

## 2.21. DESARROLLO DE ESTRATEGIAS DE GESTIÓN DE REDES

La gestión de redes es uno de los aspectos más importantes en el desarrollo lógico de una red. A menudo, la administración o gestión es analizada durante el diseño de una red, ya que se considera un problema operacional más que un problema de diseño. Sin embargo, si considera la administración o gestión desde el principio, puede evitar problemas de escalabilidad y rendimiento que se producen cuando se agrega administración a un diseño una vez que el diseño se ha completado.[16]

### 2.21.1. DISEÑO DE GESTIÓN DE RED

Los sistemas de gestión de redes pueden ser caros. También pueden tener un efecto negativo en el rendimiento de la red.

Preste atención al principio de incertidumbre de Heisenberg, que establece que el acto de observar algo puede alterar lo que se observa. Algunos sistemas de gestión de red analizan estaciones remotas regularmente. La cantidad de tráfico causada por el análisis puede ser significativa.

Estudiar el entorno para determinar qué recursos debe ser monitoreado y que métricas se utilizarán al medir el rendimiento de los dispositivos. Elija cuidadosamente los datos que desea recopilar. Salvar demasiados datos puede resultar muy costoso en el consumo de recursos proceso y almacenamiento de los datos. [17]

### 2.21.2. GESTIÓN DE PROCESOS DE RED

En general, la mayoría de las compañías tienen la necesidad de desarrollar procesos de administración de red que les ayuden a administrar la implementación y operación de la red, diagnosticar y solucionar problemas, optimizar el rendimiento y planificar mejoras.[18]

- Gestión de fallas
- Gestión de configuración
- Gestión de cuentas
- Gestión de rendimiento
- Gestión de seguridad

16 Top-Down Network Design Pag. 269

17 Top-Down Network Design Pag. 263

18 Top-Down Network Design Pag. 271

# CAPITULO III

## METODOLOGÍA DE DESARROLLO DEL PROYECTO

Por todo lo mencionado en los capítulos anteriores, el siguiente proyecto plantea la revisión, análisis y rediseño de la red actual de la Caja Nacional de Salud Regional Potosí. La metodología de investigación para el desarrollo del proyecto de grado abarcara los alcances de investigaciones descriptiva, correlacional y explicativa.

### 3.1. INVESTIGACION DESCRIPTIVA

Con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas.

Así como los estudios exploratorios sirven fundamentalmente para descubrir y prefigurar, los estudios descriptivos son útiles para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación. En esta clase de estudios el investigador debe ser capaz de definir, o al menos visualizar, qué se medirá (qué conceptos, variables, componentes, etc.) y sobre qué o quiénes se recolectarán los datos (personas, grupos, comunidades, objetos, animales, hechos). Por ejemplo, si vamos a medir variables en escuelas, es necesario indicar qué tipos habremos de incluir (públicas, privadas, administradas por religiosos, laicas, de cierta orientación pedagógica, de un género u otro, mixtas, etc.). Si vamos a recolectar datos sobre materiales pétreos, debemos señalar cuáles. La descripción puede ser más o menos profunda, aunque en cualquier caso se basa en la medición de uno o más atributos del fenómeno de interés.[1]

1 Metodología de la Investigación Sexta edición - Sampieri Cap. 5, pág. 92

## 3.2. INVESTIGACION CORRELACIONAL

Los estudios correlacionales pretenden responder a preguntas de investigación como las siguientes: ¿aumenta la autoestima de los pacientes conforme reciben una psicoterapia gestáltica? ¿A mayor variedad y autonomía en el trabajo corresponde mayor motivación intrínseca respecto de las tareas laborales? ¿Hay diferencias entre el rendimiento que otorgan las acciones de empresas de alta tecnología computacional y el rendimiento de las acciones de empresas pertenecientes a otros giros con menor grado tecnológico en la Bolsa de Comercio de Buenos Aires? ¿Los campesinos que adoptan más rápidamente una innovación son más cosmopolitas que los campesinos que la adoptan después? ¿La lejanía física entre las parejas de novios tiene una influencia negativa en la satisfacción en la relación? (Todas en un contexto específico).

Este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto en particular. En ocasiones sólo se analiza la relación entre dos variables, pero con frecuencia se ubican en el estudio vínculos entre tres, cuatro o más variables.

La utilidad principal de los estudios correlacionales es saber cómo se puede comportar un concepto o una variable al conocer el comportamiento de otras variables vinculadas. Es decir, intentar predecir el valor aproximado que tendrá un grupo de individuos o casos en una variable, a partir del valor que poseen en las variables relacionadas.

Los estudios correlacionales se distinguen de los descriptivos principalmente en que, mientras que estos últimos se centran en medir con precisión las variables individuales (algunas de las cuales se pueden medir con independencia en una sola investigación), los primeros evalúan, con la mayor exactitud que sea posible, el grado de vinculación entre dos o más variables, pudiéndose incluir varios pares de evaluaciones de esta naturaleza en una sola investigación (comúnmente se incluye más de una correlación).[2]

2 Metodología de la Investigación Sexta edición - Sampieri Cap. 5, pág. 93-94

## 3.3. INVESTIGACION EXPLICATIVA

Los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables.

Las investigaciones explicativas son más estructuradas que los estudios con los demás alcances y, de hecho, implican los propósitos de éstos (exploración, descripción y correlación o asociación); además de que proporcionan un sentido de entendimiento del fenómeno a que hacen referencia.[3]

## 3.4. DISEÑO DE INVESTIGACIÓN

El enfoque de nuestra investigación es cuantitativo. Además no es necesario realizar una investigación experimental, como el objetivo del presente trabajo de grado es realizar una propuesta para el rediseño de una red LAN, esto nos permitirá realizar tres distintos tipos de investigaciones por etapas, siendo la primera una *investigación descriptiva* dado que se observara los eventos que están ocurriendo en la red actualmente mediante un monitoreo y documentación existente. La segunda etapa de investigación permitirá realizar una *investigación correlacional* ya que se evaluara el comportamiento de las variables tomadas en la investigación descriptiva y por último una investigación explicativa ya que se dará soluciones a los problemas encontrados, para poder mejorar estas variables en el rediseño.

## 3.5. SELECCIÓN DE LA MUESTRA

El estudio se llevara a cabo en la Caja Nacional de Salud Regional Potosí, en el departamento de Potosí. La investigación se realizara en los cuatro sitios o edificios que comprenden la red LAN de la Caja Nacional de Salud Regional Potosí para poder obtener información necesaria de la red, poder analizarla y mejorarla.

3 Metodología de la Investigación Sexta edición - Sampieri Cap. 5, pág. 95-96

El tipo de muestra es *probalistica* pues nuestra elección no es al azar sino por las características de la investigación mencionada anteriormente se tomaron muestras del comportamiento de la red LAN en diferentes horarios, diferentes dispositivos, usuarios, etc., teniendo así una muestra variada del comportamiento de la red LAN, para que mediante estas muestras poder encontrar similitudes y diferencias, patrones y coincidencias.

### 3.6. RECOLECCIÓN DE DATOS

El enfoque de la presente investigación es cuantitativo ya que obtendremos información a partir de eventos que se generan en la red LAN para después poder medir y mejorar las variables involucradas en dichos eventos.

Los Instrumentos necesarios para poder realizar la recolección de datos van desde entrevistas con los funcionarios, documentos actualmente existentes, diagramas de red y herramientas de medición de tráfico.

# CAPITULO IV

## DIAGNOSTICO TÉCNICO

## MODELADO DE LE RED LAN DE LA CAJA NACIONAL DE SALUD REGIONAL POTOSI

### 4.1. ANTEDEDENTES DE LA CAJA NACIONAL DE SALUD REGIONAL POTOSI

La Caja Nacional de Salud, es una institución descentralizada de derecho público sin fines de lucro, con personalidad jurídica, autonomía de gestión y patrimonio independiente, encargada de la gestión, aplicación y ejecución del régimen de Seguridad Social a corto plazo (Enfermedad, Maternidad y Riesgos Profesionales).

### 4.2. HISTORIA DE LA EMPRESA

La Caja Nacional de Salud (CNS), inicia sus actividades como Caja Nacional de Seguridad Social (CNSS), etapa que abarca de diciembre de 1956 hasta marzo de 1987 y comprende la promulgación del Código de Seguridad Social en fecha 14 de diciembre de 1956 y la de su Decreto Reglamentario o Reglamento del Código de Seguridad Social el 30 de septiembre de 1959.

En esta etapa también están comprendidos el Decreto Ley de Racionalización de Aportes de 28 de marzo de 1972, el Decreto Ley de Reformas al Código de Seguridad Social y el Decreto Ley de Complementación de Reformas de 3 de junio de 1977.

La promulgación del Código de Seguridad Social significó un avance de la Seguridad Social Boliviana con relación a los demás países latinoamericanos. Sin embargo, desde su inicio la administración de los seguros establecidos en el citado Código no cumplieron con el principio de unidad de gestión, por cuanto se encargó la gestión del Seguro Social Obligatorio a varias instituciones, siendo la más importante, la Caja Nacional de Seguridad Social, entidad matriz gestora del Seguro Social Obligatorio integral, con más del 80% de asegurados activos y pasivos, pertenecientes a la mayoría de las ramas de actividad económica.

Las prestaciones señaladas en el Código de Seguridad Social comprendían los regímenes de enfermedad, maternidad, riesgos profesionales, invalidez, vejez, muerte y el régimen especial de asignaciones familiares.

Después de 30 años de administración integral del Seguro Social, el 15 de abril de 1987 se promulga la Ley Financial 0924, que en su artículo tercero afecta los esquemas administrativo y financiero del sistema de Seguridad Social, procediéndose a la separación de los seguros, administrados integralmente hasta ese entonces. Dejándose a las Cajas la administración de los seguros a corto plazo: Enfermedad, Maternidad y Riesgos Profesionales a corto plazo y a los Fondos Complementarios la administración de las prestaciones a largo plazo: Invalidez, Vejez y Muerte, aspectos que son ratificados por su Decreto Reglamentario No. 21637 del 25 de junio de 1987.

En consecuencia la Caja Nacional de Seguridad Social que hasta marzo de 1987 administraba el seguro integral, se convierte en la Caja Nacional de Salud, institución descentralizada de derecho público sin fines de lucro, con personalidad jurídica, autonomía de gestión y patrimonio independiente, encargada de la gestión aplicación y ejecución del régimen de Seguridad Social a Corto Plazo: Enfermedad, Maternidad y Riesgos Profesionales, instituidos por el Código de Seguridad Social, su Reglamento, la Ley Financial 924, el Decreto Supremo 21637 y demás disposiciones legales conexas.

### 4.3. PROCESOS QUE REALIZA LA CAJA NACIONAL DE SALUD REGIONAL POTOSI

Optimizar la gestión de recursos humanos asignando y utilizando personal médico, paramédico, administrativos y de servicios en función de parámetros e indicadores estándar.

Remodelar, refuncionalizar y construir hospitales además de policlínicos, acorde a los niveles de la demanda.

Brindar atenciones en salud con calidad a la población asegurada con la implementación de planes, programas y control de calidad.

Lograr el equilibrio financiero, incrementando los ingresos y optimizando el gasto.

Incrementar la población cubierta y disminuir el nivel de desafiliaciones.

Refuncionalizar el modelo de atención en salud (Medicina Familiar y Comunitaria) hasta alcanzar niveles óptimos de eficacia, eficiencia y economía.

Implementar por fases, un modelo de administración con desconcentración administrativa, financiera y técnica.

Proveer a los centros médicos de manera oportuna, suficientes medicamentos, insumos, materiales y equipo médico.

Mejorar los índices de productividad y rendimiento (salud y administración) hasta cubrir la demanda insatisfecha.

## 4.4. DECLARACION DE MISION Y VISION DE LA CAJA NACIONAL DE SALUD REGIONAL POTOSI

### Misión

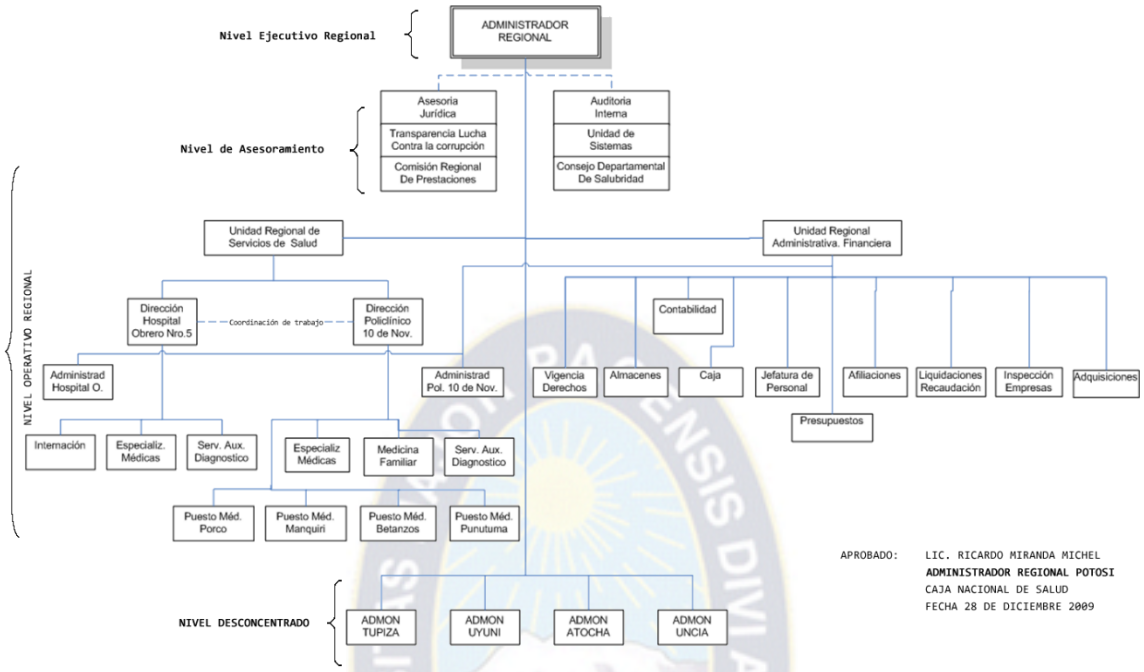
La misión de la Caja Nacional de Salud a través de sus Administraciones Regionales y Agencias Distritales es brindar protección integral en el campo de la salud a toda su población protegida, como parte activa y componente de la población boliviana. Se rige por los principios de Universalidad, Solidaridad, Unidad de Gestión, Economía, Oportunidad y Eficacia en el otorgamiento de las prestaciones de salud, optimizando el uso de recursos y buscando ampliar el nivel de cobertura.

### Visión

La Caja Nacional de Salud busca mantener el liderazgo nacional en la provisión de seguros de corto plazo, con efectividad, equidad y calidad probada.

## 4.5. ORGANIGRAMA DE LA CAJA NACIONAL DE SALUD REGIONAL POTOSI

**Figura# 4.1: Organigrama de la Caja Nacional de Salud Regional Potosí**
**Fuente: CNS Regional Potosí**

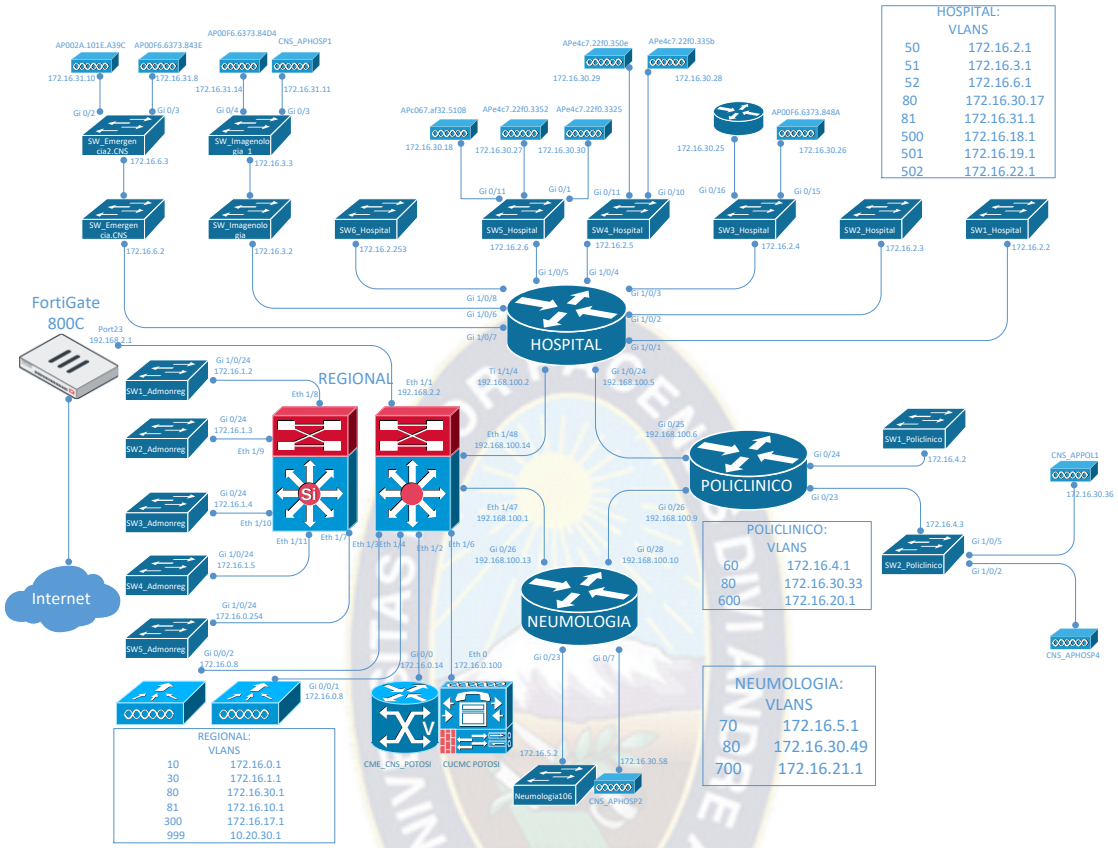



## 4.6. ANALISIS DE LA RED LAN ACTUAL

La red LAN que actualmente tiene la institución está formada principalmente por cuatro routers que se unen entre sí mediante conexiones punto a punto con fibra óptica, estos cuatro routers conforman un anillo de red, cada router esta físicamente presente en cada uno de los cuatro edificios que comprenden la red, y estos a la ves tienen conectados switches de acceso a los usuarios finales, siendo el edificio principal donde se genera la mayor cantidad de trafico el edificio Regional donde se encuentran todos los servicios y aplicaciones que se consumen en la red.

## 4.7. DIAGRAMA LOGICO DE LA RED ACTUAL

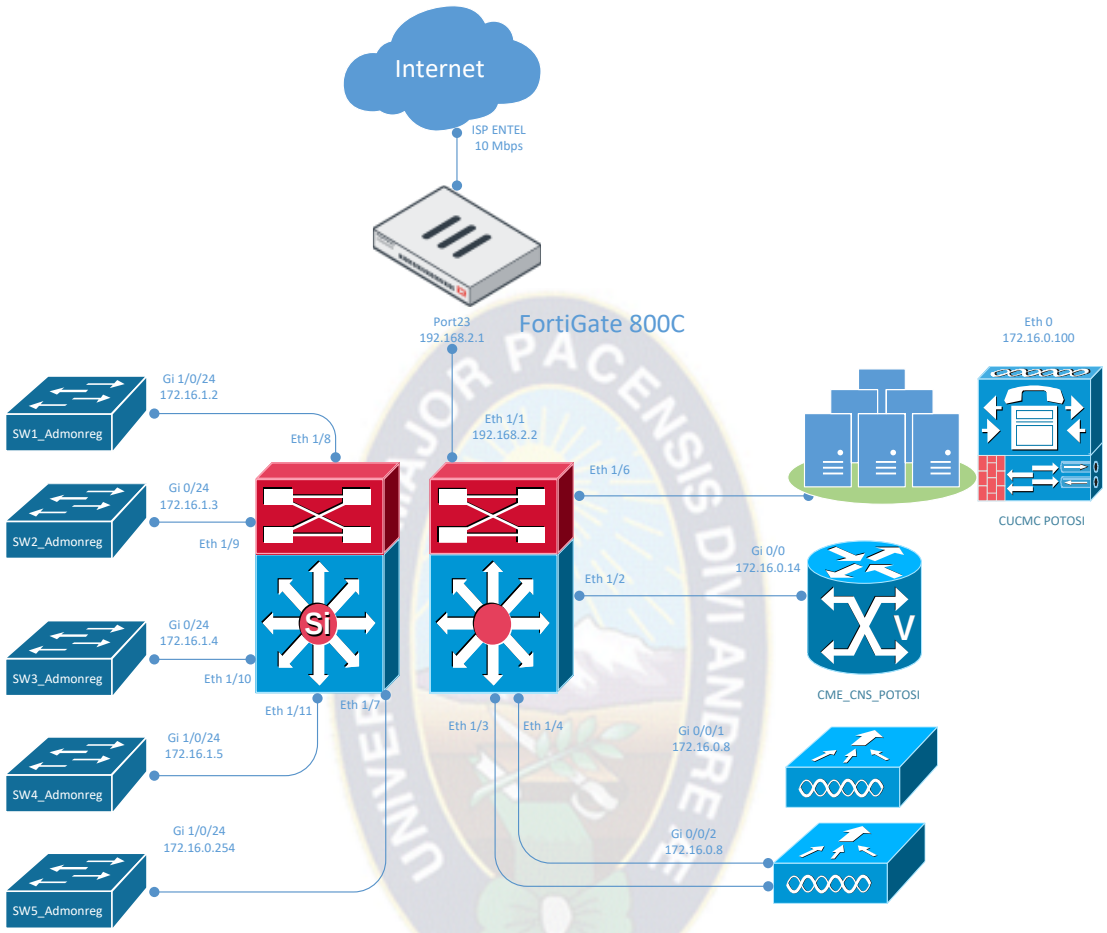
**Figura# 4.2: Diagrama lógico de red actual**
**Fuente: Elaboración Propia**




La figura 4.2 muestra el diagrama lógico de la red actual en su totalidad, siendo comprendido por distintos segmentos de redes organizadas en VLANs en cada sitio, todo el tráfico de servicios, aplicaciones internas, aplicaciones externas y navegación a internet se realiza a través del sitio Regional, siendo este el principal en toda la red dadas las características mencionadas, toda la red tiene un solo enlace de Internet que está conectado a un firewall de borde de red el cual gestiona toda la navegación.

## 4.8. DIAGRAMA LOGICO DE RED SITIO REGIONAL

**Figura# 4.3: Diagrama lógico de red sitio Regional**
**Fuente: Elaboración Propia**




Como se mencionó anteriormente el sitio Regional es el principal edificio dentro de la red LAN de la Caja Nacional de Salud Regional Potosí, el cual contiene dentro de sus instalaciones el conjunto de aplicaciones y servicios que son consumidos por la red LAN, además también es el gateway hacia internet para toda la red, teniendo como ISP a Entel con un ancho de banda de 10 Mbps para navegación y publicación de servicios.

A continuación se detalla la granja de servidores que están en este sitio:

**Tabla# 4.1: Aplicaciones de la granja de servidores**
**Fuente: Elaboración Propia**

| Nombre de la Aplicación | Tipo de aplicación | Es una aplicación nueva? (si o no) | Criticidad |
|---|---|---|---|
| SIAIS | Cliente - servidor/gestión | No | 100% |
| SHIF-ND | Cliente Servidor/financiera | No | 100% |
| SINBIOS | Cliente - Servidor/ bioestadística | No | 100% |
| ERP | WEB/administrativa | SI | 100% |
| CAMARAS IP | Comunicación | No | 100% |
| TELEFONIA IP | Comunicación | No | 100% |
| WIRELESS | Comunicación | No | 100% |

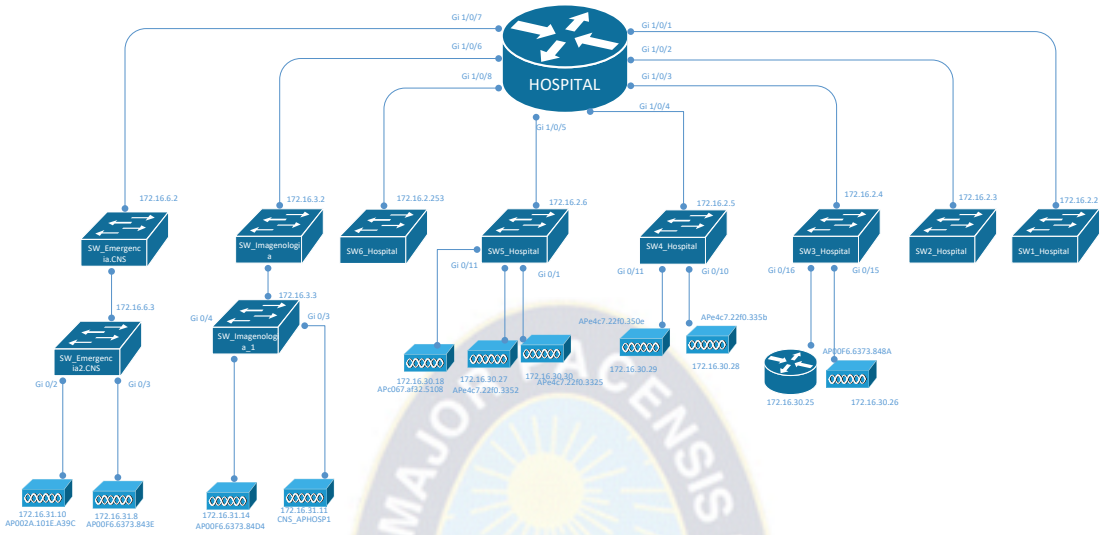
A continuación se detallan los equipos en el sitio Regional:

**Tabla# 4.2: Listado de equipos sitio Regional**
**Fuente: Elaboración Propia**

| REGIONAL | |
|---|---|
| **EQUIPO** | **VERSION** |
| cisco Nexus9000 C9372PX | version 6.1(2)I3(3a) |
| cisco WS-C3650-24PS | Version 03.03.03SE |
| cisco WS-C3560X-24P | Version 12.2(55)SE3 |
| cisco WS-C3560X-24P | Version 12.2(55)SE3 |
| cisco WS-C2960X-24PS-L | Version 15.0(2)EX5 |
| cisco WS-C2960X-24PS-L | Version 15.0(2)EX5 |
| FGT800C | v5.2.4,build688 (GA) |

## 4.9. DIAGRAMA LOGICO DE RED SITIO HOSPITAL

**Figura# 4.4: Diagrama lógico de red sitio Hospital**
**Fuente: Elaboración propia**




El sitio Hospital es el cual presenta la mayor cantidad de usuarios finales, como se ve en la gráfica cuenta con la mayor cantidad de switches que cualquier otro sitio.

A continuación se detallan los equipos en el sitio Hospital:

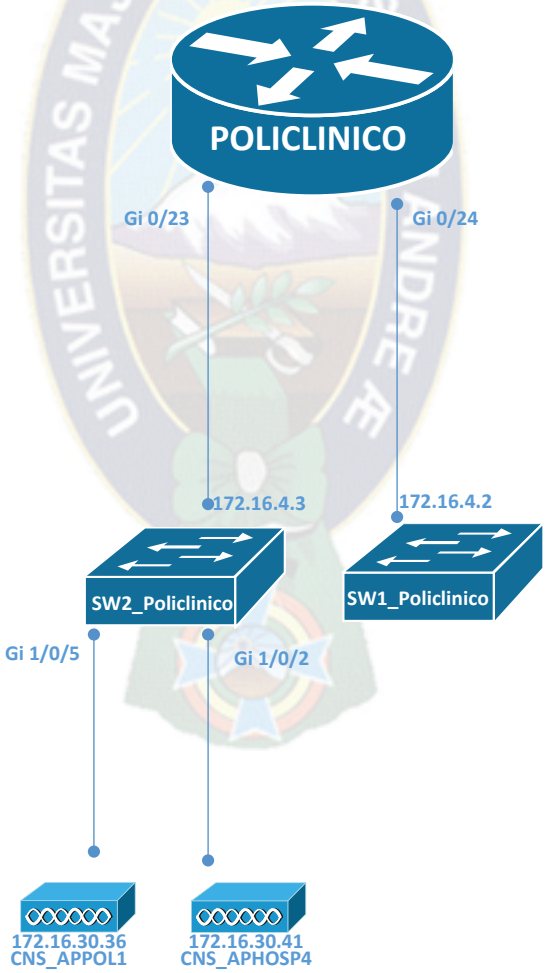
**Tabla# 4.3: Listado de equipos sitio Hospital**
**Fuente: Elaboración Propia**

| HOSPITAL | |
|---|---|
| **EQUIPO** | **VERSION** |
| cisco WS-C3850-24S | Version 03.03.05SE |
| cisco WS-C3560X-24P | Version 12.2(55)SE1 |
| cisco WS-C3560X-24P | Version 12.2(55)SE1 |
| cisco WS-C3560X-24P | Version 12.2(55)SE3 |
| cisco WS-C2960X-24PS-L | Version 15.2(2)E5 |
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |

| | |
|---|---|
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |
| cisco WS-C3560X-24P | Version 12.2(55)SE1 |
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |

## 4.10. DIAGRAMA LOGICO DE RED SITIO POLICLINICO

**Figura# 4.5: Diagrama lógico de red sitio Policlínico**
**Fuente: Elaboración Propia**



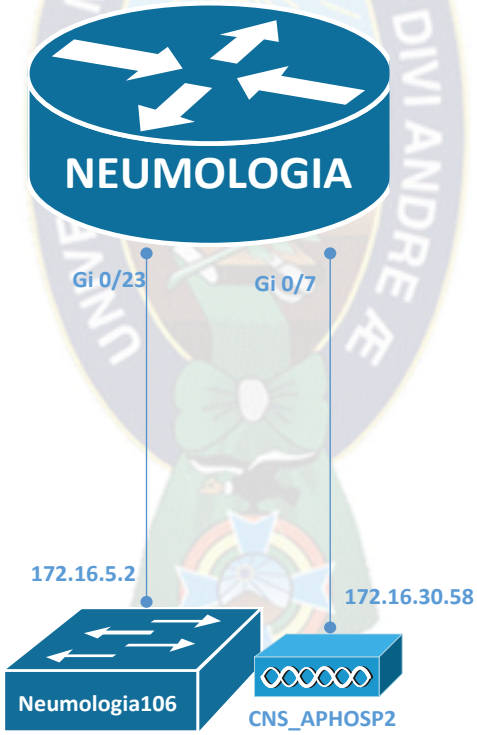
A continuación se detallan los equipos en el sitio Policlínico:

**Tabla# 4.4: Listado de equipos sitio Policlínico**
**Fuente: Elaboración Propia**

| POLICLINICO | |
|---|---|
| **EQUIPO** | **VERSION** |
| cisco WS-C3650-24PD | Version 03.06.04.E |
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |
| cisco WS-C3650-24PS | Version 03.03.03SE |

## 4.11. DIAGRAMA LOGICO DE RED SITIO NEUMOLOGIA

**Figura# 4.6: Diagrama lógico de red sitio Neumología**
**Fuente: Elaboración Propia**



A continuación se detallan los equipos en el sitio Neumología:

**Tabla# 4.5: Listado de equipos sitio Neumología**
**Fuente: Elaboración Propia**

| NEUMOLOGIA | |
|---|---|
| **EQUIPO** | **VERSION** |
| cisco WS-C3650-24PD | Version 03.06.04.E |
| cisco WS-C3560G-24PS | Version 12.2(35)SE5 |

## 4.12. GESTIÓN DE RIESGOS

Para evaluar los riesgos asociados a la red actual de la Caja Nacional de Salud regional Potosí, primero podemos agrupar los mismos en cuatro puntos principales:

- **Fallos intencionales:** Empleados o gente externa, Hackers.
- **Fallas por el medio ambiente:** Fenómenos naturales, terremotos, incendios, inundaciones, etc.
- **Fallas mecánicas:** Fallas de hardware en equipos, corte brusco de suministro eléctrico, etc.
- **Fallos fortuitos o Accidentes:** Empleados con poca capacitación, descuidos, etc.

Elementos necesarios en el diseño de la red:

- **Disponibilidad:** Tener la información necesaria.
- **Integridad:** No accesos a la información por personas no autorizadas.
- **Confidencialidad:** Información solo disponible o vista por personal autorizado.

No tomar en cuenta los aspectos mencionados en el diseño de la red puede resultar en:

- Pérdida económica para la Caja Nacional de Salud regional Potosí.
- Pérdida en productividad.

- Pérdida de Confianza.
- Pérdida de oportunidades de negocio.

Mediante un diseño correcto de la red tocando los aspectos mencionados anteriormente, se verán las acciones de mitigación para evitar los problemas. Para tener un equilibrio entre riesgo y confianza. El sistema que se evaluará es la red actual donde el riesgo es igual a la probabilidad de que ocurra algo por el impacto que produce.

**Evaluación de Riesgos:**

- Circunstancias Políticas.
- Aspectos comerciales y legales.
- Circunstancias Económicas.
- Eventos naturales.
- Aspectos tecnológicos y técnicos Comportamiento humano.

De acuerdo a lo mencionado podemos listar los riesgos más importantes asociado al rediseño de la red, tomando en cuenta una escala del 1 al 5, siendo el 5 la máxima probabilidad de que ocurra un suceso.

**Tabla# 4.6: Gestión de riesgos**
**Fuente: Elaboración Propia**

| | AMENAZA | PROBABILIDAD | IMPACTO | RIESGO |
|---|---|---|---|---|
| **1** | PERDIDA DE INFOMACION POR CAUSAS NATURALES | 2 | 4 | 8 |
| **2** | AUSENCIA DE RESPONSABILIDAD, INCUMPLIMIENTO DE OBJETIVOS | 4 | 3 | 12 |
| **3** | PERDIDA DE INFORMACION, ATAQUES INFORMATICOS, ROBOS | 4 | 5 | 20 |
| **4** | ADMINISTRADORES DE RED NO ESTABLES EN SUS FUNCIONES | 4 | 3 | 12 |
| **5** | FALTA DE DOCUMENTACION | 5 | 4 | 20 |

| | | | | |
|---|---|---|---|---|
| **6** | FALTA DE CONTROL Y SEGUIMIENTO EN LOS INCIDENTES | 4 | 4 | 16 |
| **7** | CALCULOS ERRONEOS EN EL CRECIMIENTO DE PERSONAL | 4 | 4 | 16 |
| **8** | CAUSAS POLITICAS Y DESACUERDOS | 4 | 4 | 16 |
| **9** | DIMENCIONAMIENTO ERRONEO EN DISPOSITIVOS DE RED | 3 | 4 | 12 |
| **10** | POLITICAS DE ESTADO PARA LA DEPENDENCIA DE PRODUCTOS | 4 | 3 | 12 |

**Tabla# 4.7: Matriz de riesgos**
**Fuente: Elaboración Propia**

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | **5** | **4** | **3** | **2** | **1** |
| **PROBABILIDAD** | **5** | | 5 | | | |
| | **4** | 3 | 6_7_8 | 2_4_10 | | |
| | **3** | | 9 | | | |
| | **2** | | 1 | | | |
| | **1** | | | | | |

Acciones a realizar contra los riesgos mostrados anteriormente:

**Tabla# 4.8: Acciones de mitigación**
**Fuente: Elaboración Propia**

| | AMENAZA | MITIGACION |
|---|---|---|
| **1** | PERDIDA DE INFOMACION POR CAUSAS NATURALES | CONTAR CON UN BACKUP ACTUALIZADO |
| **2** | AUSENCIA DE RESPONSABILIDAD, INCUMPLIMIENTO DE OBJETIVOS | ESTRUCTURAR FUNCIONES LABORALES |
| **3** | PERDIDA DE INFORMACION, ATAQUES INFORMATICOS, ROBOS | IMPLEMENTAR SITIOS REMOTOS ALTERNATIVOS CON BACKUP DE LA INFORMACION |

| | | |
|---|---|---|
| **4** | ADMINISTRADORES DE RED NO ESTABLES EN SUS FUNCIONES | INSTITUCIONALIZACION DEL PERSONAL |
| **5** | FALTA DE DOCUMENTACION | GENERACION DE LA DOCUMENTACION |
| **6** | FALTA DE CONTROL Y SEGUIMIENTO EN LOS INCIDENTES | IMPLEMENTACION DE SISTEMAS DE CONTROL Y SEGUIMIENTO DE SUCESOS |
| **7** | CALCULOS ERRONEOS EN EL CRECIMIENTO DE PERSONAL | SE ASUME LA AMENAZA |
| **8** | CAUSAS POLITICAS Y DESACUERDOS | BACKUP DE LA INFORMACION |
| **9** | DIMENCIONAMIENTO ERRONEO EN DISPOSITIVOS DE RED | DIAGNOSTICO DEL DESEMPEÑO DE EQUIPOS |
| **10** | POLITICAS DE ESTADO PARA LA DEPENDENCIA DE PRODUCTOS | MAYOR FLEXIBILIDAD |

Dadas las soluciones presentadas podemos volver a calcular el riesgo:

**Tabla# 4.9: Gestión de riesgos con mitigación**
**Fuente: Elaboración Propia**

| | AMENAZA | PROBABILIDAD | IMPACTO | RIESGO |
|---|---|---|---|---|
| **1** | PERDIDA DE INFOMACION POR CAUSAS NATURALES | 2 | 3 | 8 |
| **2** | AUSENCIA DE RESPONSABILIDAD, INCUMPLIMIENTO DE OBJETIVOS | 4 | 3 | 12 |
| **3** | PERDIDA DE INFORMACION, ATAQUES INFORMATICOS, ROBOS | 4 | 4 | 20 |
| **4** | ADMINISTRADORES DE RED NO ESTABLES EN SUS FUNCIONES | 4 | 3 | 12 |
| **5** | FALTA DE DOCUMENTACION | 5 | 3 | 20 |
| **6** | FALTA DE CONTROL Y SEGUIMIENTO EN LOS INCIDENTES | 4 | 3 | 16 |

| | | | | |
|---|---|---|---|---|
| **7** | CALCULOS ERRONEOS EN EL CRECIMIENTO DE PERSONAL | 4 | 3 | 16 |
| **8** | CAUSAS POLITICAS Y DESACUERDOS | 4 | 3 | 16 |
| **9** | DIMENCIONAMIENTO ERRONEO EN DISPOSITIVOS DE RED | 3 | 3 | 12 |
| **10** | POLITICAS DE ESTADO PARA LA DEPENDENCIA DE PRODUCTOS | 4 | 2 | 12 |

**Tabla# 4.10: Matriz de riesgos con mitigación**
**Fuente: Elaboración Propia**

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | **5** | **4** | **3** | **2** | **1** |
| **PROBABILIDAD** | **5** | | | 5 | | |
| | **4** | | 3 | 2_4_6_7_8 | 10 | |
| | **3** | | | 9 | | |
| | **2** | | | 1 | | |
| | **1** | | | | | |

## 4.13. ANALISIS DE FLUJO DE DATOS

Como se mencionó anteriormente el sitio Regional es el que alberga todos los servicios y aplicaciones dentro de la red LAN de la Caja Nacional de Salud regional Potosí, y a la ves proporciona la salida a internet para todos los usuarios, de esta manera se tomaron las siguientes tablas de flujo de tráfico que se genera en la totalidad de la red LAN:

**Tabla# 4.11: Top Aplicaciones por ancho de banda**
**Fuente: Elaboración Propia**

**Top de Aplicaciones por ancho de banda**

| Aplicación | Trafico | % |
|---|---|---|
| YouTube | 533.86 GB | 89.78% |
| HTTP.BROWSER | 36.99 GB | 44.23% |
| Google.Services | 36.33 GB | 46.47% |
| QUIC | 6.18 GB | 36.26% |
| Microsoft.Portal | 5.77 GB | 43.21% |
| Mega | 7.43 GB | 56.31% |
| Kaspersky.Update | 6.59 GB | 59.34% |
| Microsoft.Outlook | 1.38 GB | 82.76% |
| Amazon.AWS_S3 | 370.71 MB | 47.73% |
| Andromeda.Botnet | 640.10 MB | 89.92% |
| Moodle | 226.91 MB | 49.76% |
| Apple.iPhone | 362.05 MB | 83.23% |
| Facebook | 163.00 MB | 43.12% |
| TeamViewer | 26.20 MB | 68.43% |
| Psiphon | 18.35 MB | 70.77% |
| Viber | 947.59 KB | 71.87% |
| Xbox | 363.10 KB | 70.88% |
| Thunder.Xunlei | 82.34 KB | 32.07% |

**Tabla# 4.12: Top de categorías de aplicaciones por ancho de banda**
**Fuente: Elaboración Propia**

**Top de categorías de aplicaciones por ancho de banda**

| Categoría de Aplicación | Trafico | % |
|---|---|---|
| Video/Audio | **594.64 GB** | **72.91%** |
| Web.Others | **83.63 GB** | **10.25%** |
| General.Interest | **78.19 GB** | **9.59%** |

| | | |
|---|---|---|
| Network.Service | **17.05 GB** | **2.09%** |
| Collaboration | **13.35 GB** | **1.64%** |
| Storage.Backup | **13.19 GB** | **1.62%** |
| Update | **11.11 GB** | **1.36%** |
| Email | **1.67 GB** | **0.20%** |
| Cloud.IT | **776.73 MB** | **0.09%** |
| Botnet | **711.86 MB** | **0.09%** |
| Business | **456.01 MB** | **0.05%** |
| Mobile | **434.99 MB** | **0.05%** |
| Social.Media | **378.02 MB** | **0.05%** |
| Remote.Access | **38.29 MB** | **0.00%** |
| Proxy | **25.92 MB** | **0.00%** |
| VoIP | **1.29 MB** | **0.00%** |
| Game | **512.25 KB** | **0.00%** |
| P2P | **256.74 KB** | **0.00%** |

**Tabla# 4.13: Top sitios web por ancho de banda**
**Fuente: Elaboración propia**

**Top de sitios web por ancho de banda**

| Sitio Web | Trafico | % |
|---|---|---|
| osxapps.itunes.apple.com | 5.70 GB | 9.90% |
| safebrowsing-cache.google.com | 9.38 GB | 33.29% |
| s.ytimg.com | 1.92 GB | 7.76% |
| gfs270n087.userstorage.mega.co.nz | 3.43 GB | 15.00% |
| *.c.docs.google.com | 8.55 GB | 98.64% |
| r4---sn-xouxacv-a2ce.googlevideo.com | 1.09 GB | 17.39% |
| www.la-razon.com | 1.25 GB | 24.47% |
| tpc.googlesyndication.com | 866.58 MB | 17.53% |
| video-atl3-1.xx.fbcdn.net | 1.53 GB | 34.32% |
| play.cdn08.fx.fastcontentdelivery.com | 917.65 MB | 23.09% |

| | | |
|---|---|---|
| www.roadblockspringdenver.com | 622.74 MB | 18.14% |
| i_mp3-es_GTA-IV--San-Andreas-Beta-3.fawedixarfores.com | 1.86 GB | 70.73% |
| seriesblanco.com | 1.93 GB | 99.97% |
| bioimagenologia.fcts-usfx.com | 130.52 MB | 7.27% |
| www1.hospitalitaliano.org.ar | 106.22 MB | 6.01% |
| erp.cns.gob.bo | 256.00 MB | 15.51% |
| outlook.live.com | 1.11 GB | 73.65% |
| download.skype.com | 526.94 MB | 42.69% |
| www.cinedirecto.net | 261.65 MB | 22.90% |
| mmg.whatsapp.net | 539.11 MB | 48.19% |

**Tabla# 4.14: Top categorías sitios web por ancho de banda**
**Fuente: Elaboración Propia**

**Top de Categorías de sitios web por ancho de banda**

| Categoría Web | Trafico | % |
|---|---|---|
| Information Technology | **57.60 GB** | **30.28%** |
| Search Engines and Portals | **28.17 GB** | **14.81%** |
| Content Servers | **24.70 GB** | **12.99%** |
| File Sharing and Storage | **22.83 GB** | **12.00%** |
| Web-based Applications | **8.67 GB** | **4.56%** |
| Streaming Media and Download | **6.29 GB** | **3.31%** |
| News and Media | **5.11 GB** | **2.69%** |
| Advertising | **4.83 GB** | **2.54%** |
| Social Networking | **4.45 GB** | **2.34%** |
| Business | **3.88 GB** | **2.04%** |
| Unrated | **3.35 GB** | **1.76%** |
| Others | **2.64 GB** | **1.39%** |
| Illegal or Unethical | **1.93 GB** | **1.01%** |
| Health and Wellness | **1.73 GB** | **0.91%** |
| Government and Legal Organizations | **1.61 GB** | **0.85%** |

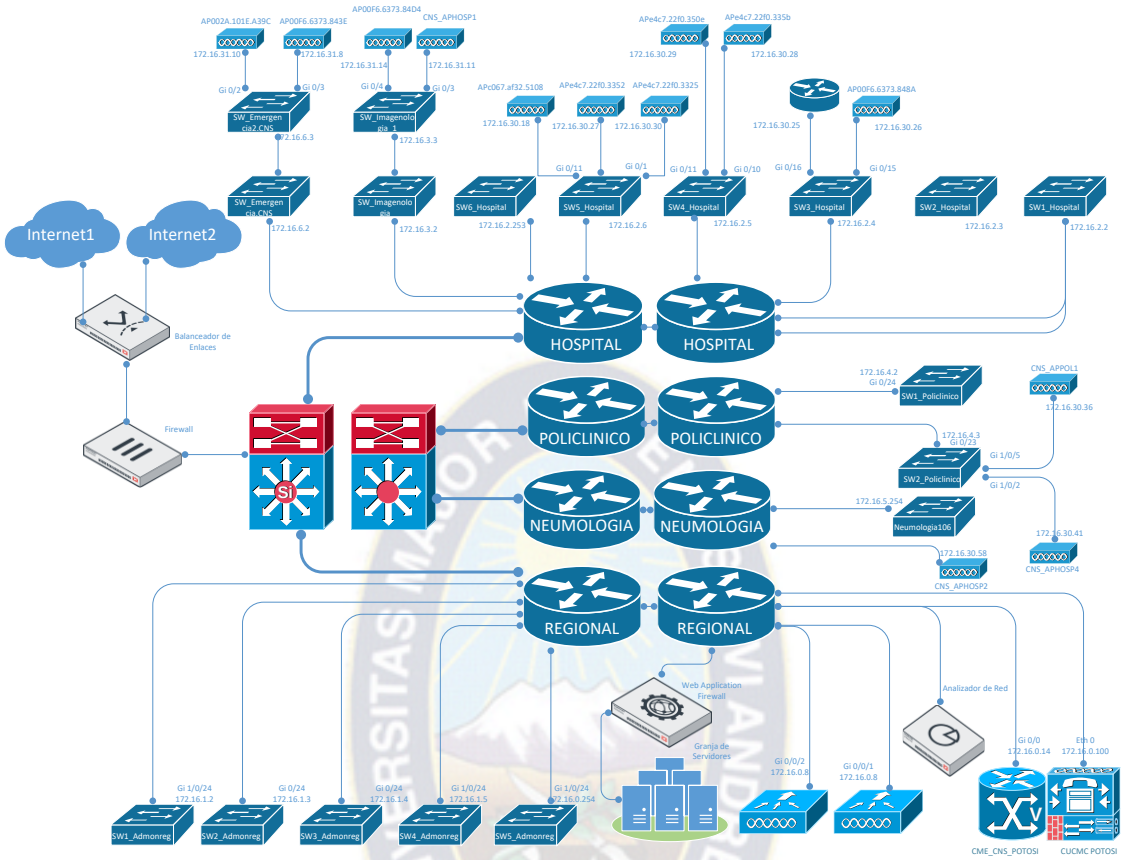
| | | |
|---|---|---|
| Web-based Email | **1.50 GB** | **0.79%** |
| Internet Telephony | **1.21 GB** | **0.63%** |
| Entertainment | **1.12 GB** | **0.59%** |
| Instant Messaging | **1.09 GB** | **0.57%** |

## 4.14. DIAGRAMAS DE TRAFICO POR SITIOS

## 4.15. REDISEÑO DEL DIAGRAMA DE RED LOGICO PARA LA CNS REGIONAL POTOSI

El rediseño propuesto se basó en el modelo de estructura jerárquica por capas, con redundancia a nivel de equipos en las capas de core y distribución, esta estructura está compuesta básicamente por dos Switches Nexus en el Core, en la capa de distribución dos switches capa tres en cada sitio con redundancia y en la capa de acceso se tienen switches de capa dos dependiendo de la cantidad de usuarios finales. Dado el tamaño de la red y tomando en cuenta que debe soportar tráfico a nivel nacional y local; en el mismo se tomó en cuenta el entorno a ser implementado, para este caso el sitio Regional es el lugar central de toda la topología, donde se encuentran la granja de servidores y accesos a internet de toda la red de la Caja Nacional de Salud Regional Potosí, siendo este sitio estratégico para los fines deseados en el rediseño.

**Figura# 4.7: Rediseño de diagrama de red lógico**
**Fuente: Elaboración propia**




Para el diseño planteado se tomaron en cuenta los siguientes aspectos fundamentales:

- **ESCALABILIDAD:** La red es escalable, es decir poder crecer a futuro sin la necesidad de perder el control o la manejabilidad, ya que es una red Jerárquica esta soporta el crecimiento y el control adecuado.
- **DISPONIBILIDAD:** La red tendrá un alto porcentaje de disponibilidad, de manera que los usuarios no puedan notar la existencia de algún corte en la red, ya que del rediseño cuenta con alta disponibilidad en las capas criticas da la red se estima tener una disponibilidad del 99.999%.
- **PERFORMANCE:** Ya que el rendimiento de la red está estrechamente vinculado a la escalabilidad, al ser esta una red escalable debido al diseño jerárquico esta tiene un alto rendimiento en ancho de banda en sus enlaces entre equipos, estos equipos a la vez presentan características

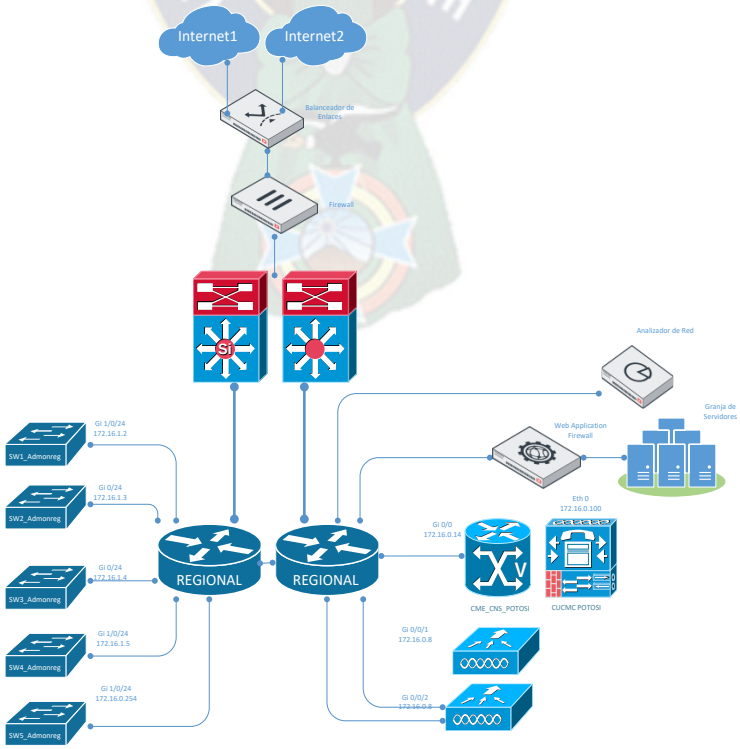
elevadas en throughput o umbrales en la transferencia de información a través de ellos, con esto disminuyendo la latencia en el tráfico de datos en la red y aumentando el tiempo de respuesta a las solicitudes de los servicios consumidos por los usuarios.

- **SEGURIDAD:** Siendo la seguridad uno de los aspectos más importantes en el diseño de red, se tomaron en cuenta la seguridad en borde como dentro de la red, teniendo una granja de servidores en el sitio Regional, la cual brinda servicios internos como externos a través de internet se tomaron las medidas necesarias para el seguro acceso desde internet a estos servicios, prevenir ataques informáticos a los servidores como denegación de servicio, ataques de fuerza bruta, etc., también la seguridad en la navegación a internet de los usuarios finales de cada sitio, teniendo un monitoreo constante de la actividad de cada uno de ellos.

## 4.16. REDISEÑO DIAGRAMA LOGICO DE RED SITIO REGIONAL

A nivel local del sitio Regional se propone el siguiente diseño de red, siendo este un sistema con redundancia en sus routers de administración que se conectan al core de la red mediante fibra óptica.

**Figura# 4.8: Rediseño diagrama lógico de red sitio Regional**
**Fuente: Elaboración propia**

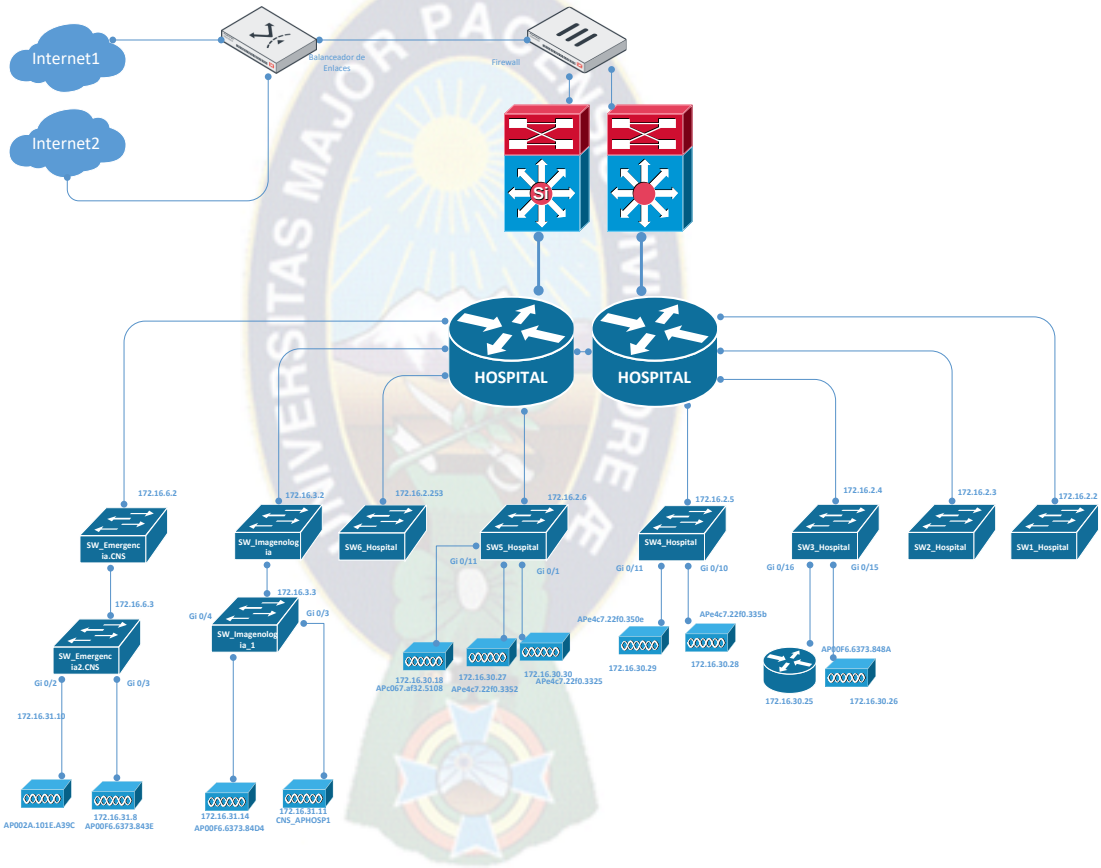


Como se mencionaba este sitio es el principal dentro de la red ya que alberga todos los servidores y servicios locales de la Caja Nacional de Salud Regional Potosí.

## 4.17. REDISEÑO DIAGRAMA LOGICO DE RED SITIO HOSPITAL

De la misma manera que el sitio Regional, este sitio está diseñado con un sistema redundante en los routers de administración que están conectados a través de fibra óptica al core de la red.

**Figura# 4.9: Rediseño diagrama lógico de red sitio Hospital**
**Fuente: Elaboración propia**

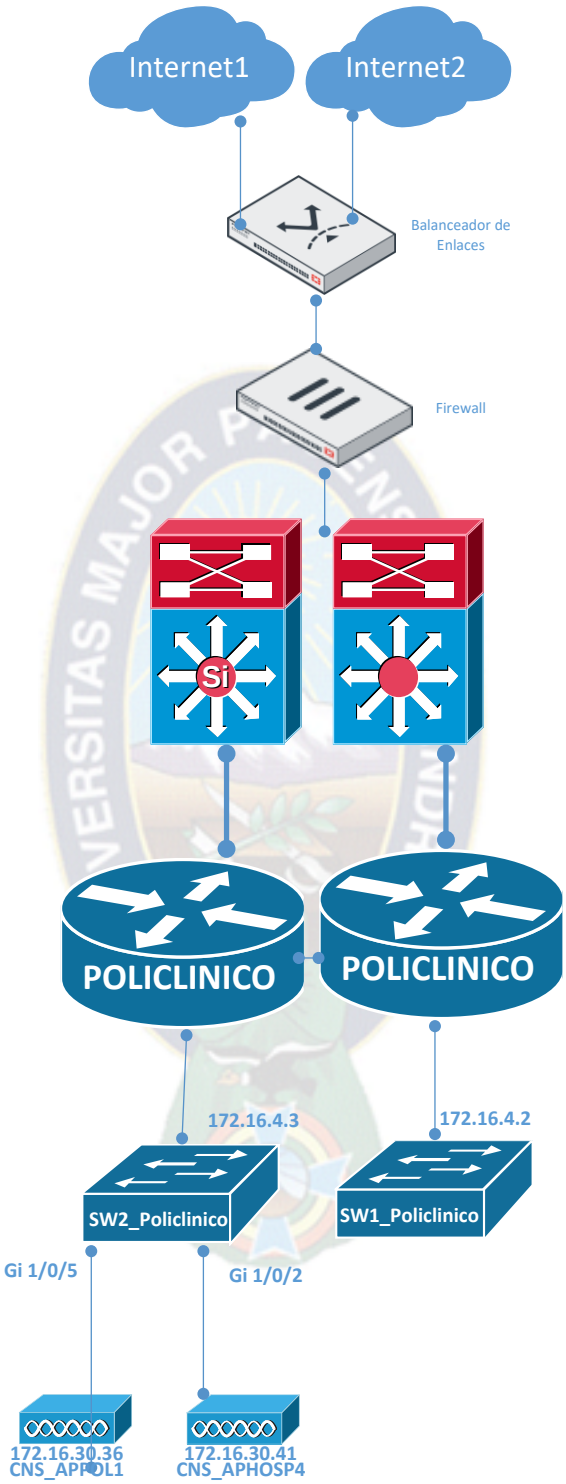



El sitio Hospital es el que contiene la mayor cantidad de usuarios finales, debido a esta situación se tiene la mayor cantidad de switches de acceso de la red.

## 4.18. REDISEÑO DIAGRAMA LOGICO DE RED SITIO POLICLINICO

El sitio Policlínico de la misma manera cuenta con un sistema redundante a nivel de distribución que está conectado mediante fibra óptica al core de la red.

**Figura# 4.10: Rediseño diagrama lógico de red sitio Policlínico**
**Fuente: Elaboración Propia**

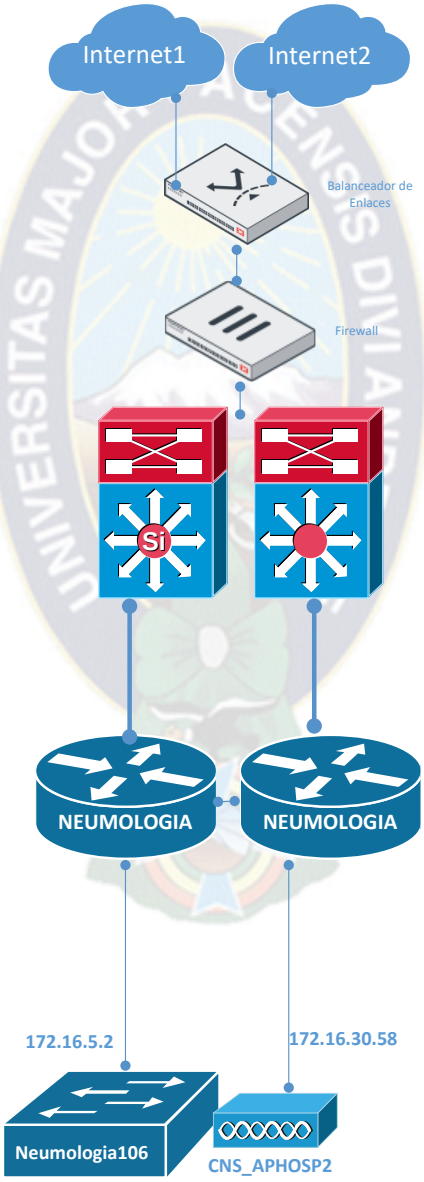


La cantidad de switches de acceso es menor en este sitio.

## 4.19. REDISEÑO DIAGRAMA LOGICO DE RED SITIO NEUMOLOGIA

El ultimo sitio de la red es el de Neumología de la misma manera que los demás también está diseñado con un sistema redundante en la capa de distribución y también está conectado mediante fibra óptica al core de la red.

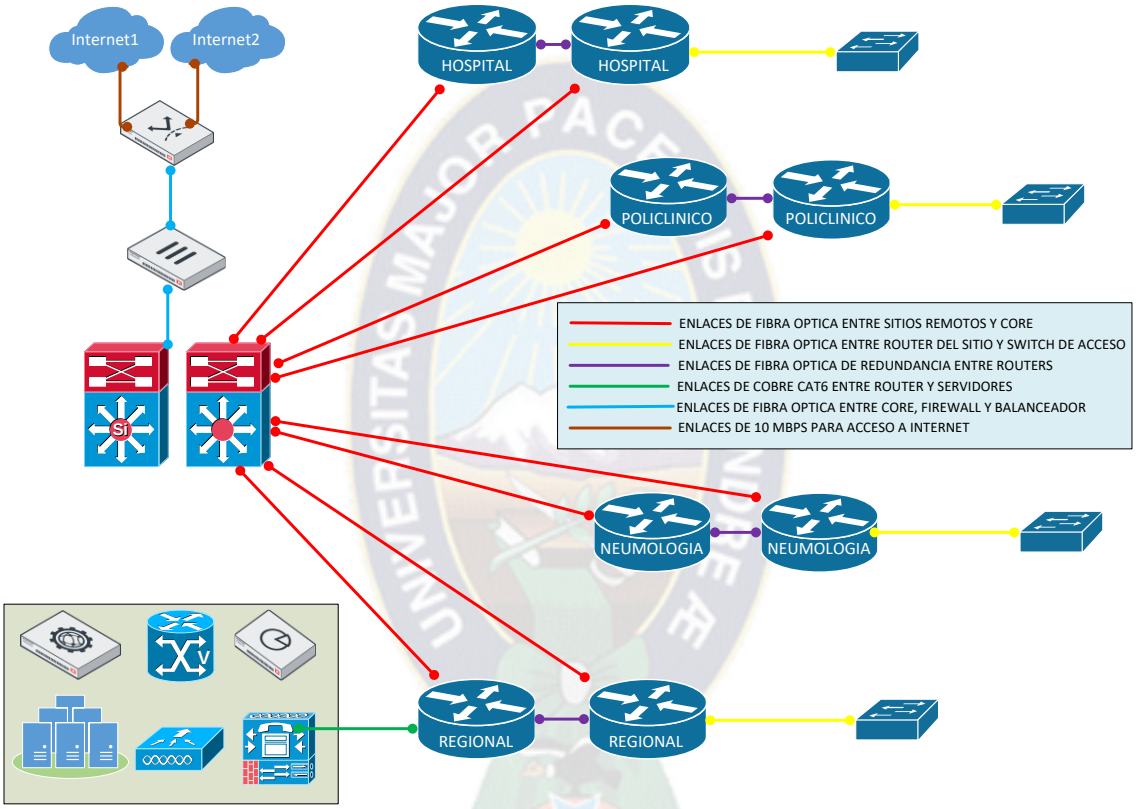
**Figura# 4.11: Rediseño diagrama lógico de red sitio Neumología**
**Fuente: Elaboración Propia**



## 4.20. REDISEÑO DIAGRAMA DE RED FISICO PARA LA CNS REGIONAL POTOSI

El siguiente diagrama físico de la red se lo realizo en base a la solución propuesta y utilizando el equipamiento existente de la red de la Caja Nacional de Salud Regional Potosí:

**Figura# 4.12: Rediseño diagrama físico de red**
**Fuente: Elaboración propia**




Cabe mencionar que el core de la red esta físicamente ubicado en el sitio regional de la red.

## 4.21. ESTUDIO DE FACTIBILIDAD

## 4.22. FACTIBILIDAD OPERACIONAL

Terminado el rediseño de la red propuesta para la Caja Nacional de Salud Regional Potosí, y determinados los límites de las áreas a trabajar, hacemos notar que la institución cuenta con una unidad de Tecnologías de la Información

dirigida por el Licenciado Javier Pinto Mamani. Esta unidad a la ves está dividida por áreas de especialidad como son: telefonía, redes, servidores, seguridad soporte técnico. Todas estas áreas serán involucradas en cada una de las etapas del proyecto de rediseño, siendo de manera inicial y con mayor prioridad el trabajo con el área de redes.

Por todo lo expuesto se puede concluir que el proyecto de rediseño es factible operacionalmente y se continuara con el rediseño.

### 4.23. FACTIBILIDAD TÉCNICA

El rediseño de red para la Caja Nacional de Salud Regional Potosí, incluye equipamiento de redes a nivel corporativo, este equipamiento está disponible actualmente en Bolivia, es distribuido por varias empresas a nivel nacional que cuentan con todas las garantías legales, es decir licencias, soporte de fábrica y local, dadas estas condiciones es factible técnicamente conseguir el equipamiento necesario para el rediseño de la red.

De esta manera también cabe resaltar que la Caja Nacional de Salud Regional Potosí, ya cuenta con una red de cableado estructurado en parte categoría 5e y categoría 6 en el sitio Regional. Con conexiones de fibra óptica entre los cuatro sitios y conexiones ADSL de internet para conexiones VPN sitio a sitio con las otras regionales de Bolivia.

Con todos estos detalles concluimos que el rediseño es factible de implementar técnicamente.

# CAPITULO V

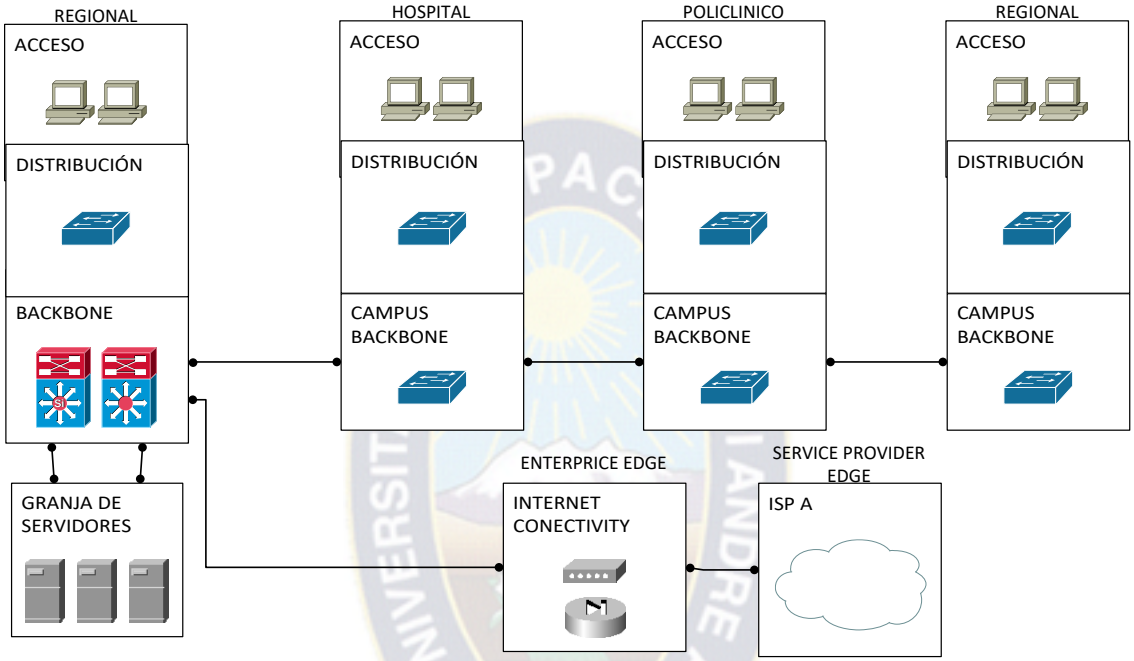
## INGENIERIA DEL PROYECTO

## “REDISEÑO DE LA RED LAN DE LA CAJA NACIONAL DE SALUD REGIONAL POTOSI”

### 5.7. PROPUESTA DE REDISEÑO

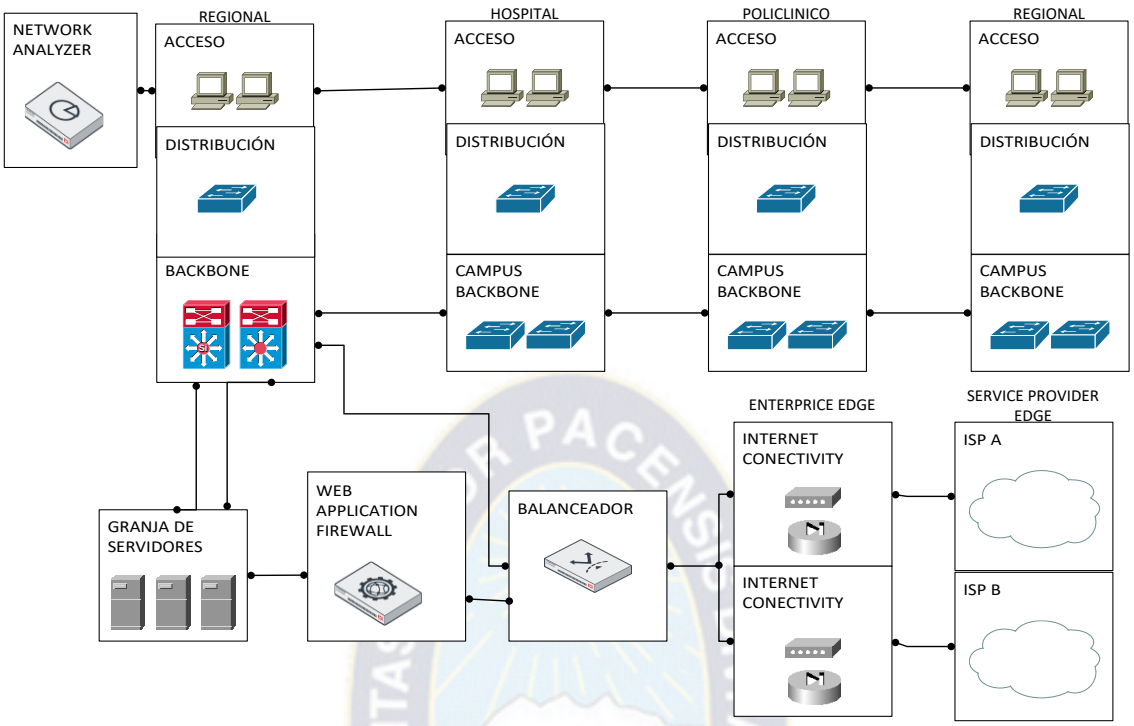
**Figura#5.1. Diagrama Modular de la Red Actual**

**Fuente: Elaboración Propia**



**Figura#5.2. Diagrama Modular de la Propuesta de Rediseño de la Red**

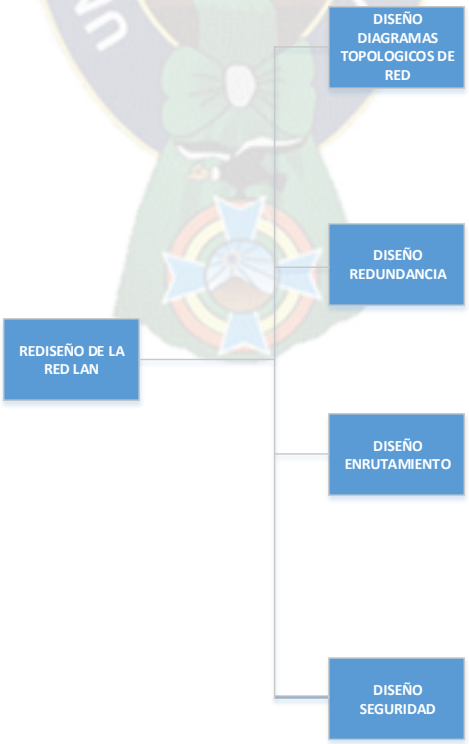
**Fuente: Elaboración Propia**




La propuesta de rediseño comprende las siguientes mejoras en la red actual:

**Figura#5.3. Diagrama de Flujo Rediseño**

**Fuente: Elaboración Propia**



- **DISEÑO DIAGRAMAS DE TOPOLOGIA DE LA RED:**
  Diseñar diagramas Lógico y Físico
- **DISEÑO Y CONFIGURACION DE LAS CONEXIONES PRINCIPALES:**
  Para evitar cortes en el flujo de tráfico debido a fallas en las conexiones principales de la red.
- **DISEÑO Y RECONFIGURACION DE ENRUTAMIENTO OSPF:**
  Reconfiguración de enrutamiento a OSPF para mejorar la distribución de enrutamiento de la información.
- **REORDENAMINETO DE VLANs:**
  Ordenar de tal forma que se maneje un estándar en los IDs e IPs en todos los sitios de la red, para mejorar la administración.
- **DISEÑAR Y CONFIGURAR WEB APPLICATION FIREWALL:**
  Proteger los la granja de servidores de ataques externos.
- **DISEÑAR, CONFIGURAR, ORDENAR Y CONTROLAR EL ACCESO A INTERNET DE USUARIOS FINALES:**
  Mejorar y proteger la navegación de usuarios finales para un mejor uso de ancho de banda de acceso a internet.
- **DISEÑAR Y CONFIGURAR UN BALANCEADOR DE ENLACES A INTERNET:**
  Obtener un segundo enlace a internet y poder brindar eficiencia y redundancia en el uso de ancho de banda.
- **DISEÑAR Y CONFIGURAR ANALIZADOR DE RED:**
  Identificar que tráfico de red se está generando en los usuarios finales.

### 5.2. PLAN DE TRABAJO

Se propone desarrollar la totalidad del proyecto de grado en 7 (siete) etapas:

1. La primera etapa corresponde al diseño de diagramas de topología de la red y redundancia.
2. En la segunda etapa se realizara el rediseño del enrutamiento en base al protocolo OSPF
3. Como tercera etapa se reordenara todas las VLANs existentes
4. En la cuarta etapa se diseñara y configurara el Web Application Firewall para protección de los servidores.

5. En esta quinta etapa se procederá a realizar el diseño, configuración, dar orden y controlar el acceso a internet de los usuarios finales para optimizar el ancho de banda de acceso a internet
6. Como sexta etapa se diseñara y configurara el balanceo de acceso a internet mediante un balanceador de enlaces.
7. Como séptima y última etapa se diseñara y configurara un analizador de red para poder observar las actividades que realizan los usuarios finales.

## 5.3. REQUERIMIENTOS PARA EL REDISEÑO DE LA RED

Basados en los análisis y los problemas planteados anteriormente pasaremos a enlistar los siguientes requerimientos a tomar en cuenta en el rediseño de la red:

- Comunicaciones de red entre todos los sitios en la regional.
- Comunicaciones de red entre los distintos sistemas informáticos de la red de la caja Nacional de Salud regional Potosí.
- Comunicaciones de red para acceder a servicios de Internet y aplicaciones.
- Todas las áreas de trabajo de la regional deben estar integradas en un solo proyecto que contengan productos, elementos y soluciones que brinden una integración global de la red.
- Se recomienda utilizar una a dos marcas de equipamiento de red y seguridad, así de esta manera poder contar con una fácil resolución de problemas si se presentasen, además eliminar posibles inconvenientes en incompatibilidades de muchas marcas.
- Todos los equipos y las configuraciones deben estar sujetos a los estándares internacionales determinados para este tipo soluciones.
- El core del rediseño está ubicado en el sitio Regional, donde se encuentran todos los servicios de la red.
- Debido a la importancia del acceso fluido a internet, se deberá adquirir un enlace extra a internet, y con esto poder implementar un mecanismo que brinde redundancia y balanceo para todas las salidas a internet, de esta manera poder evitar el corte en el servicio de internet, dicho mecanismo deberá ser transparente para los usuarios finales, de tal forma que deberá ser automático sin la intervención de los administradores de la red.

- La seguridad se implementará en el borde de la red para protección de ataques de borde, navegación segura de usuarios finales y seguridad interna a nivel de DMZ para protección de la granja de servidores, además del monitoreo y por consiguiente los reportes respectivos.

### 5.4. DIMENCIONAMIENTO Y SELECCIÓN DE EQUIPAMIENTO

En el rediseño de la red de la Caja Nacional de Salud Regional Potosí, se propone poder trabajar con las marcas **Cisco** para Switching & Routing y **FortiNet** para Seguridad, por las siguientes razones:

- **Estabilidad y estandarización de la red:** La mayoría de las redes actuales son móviles y visuales, las soluciones de Cisco ofrecen en forma constante una experiencia de red de alta calidad, además de ser una marca que maneja los principales estándares y protocolos mundiales.
- **Escalabilidad:** Siendo Cisco una marca reconocida mundialmente, esta brinda una variedad de soluciones tanto en datos, voz y video, de tal manera que sus soluciones se adaptan para poder permitir que la red sea escalable con los constantes cambios que ocurren en las redes actuales.
- **Costos energéticos y consumo de recursos:** Las soluciones Cisco permite reducir los costos energéticos y de recursos mediante diseños de ahorro de energía, optimizaciones de video y voz, brindando vida útil extendía en sus equipos.
- **Seguridad sin compromisos:** FortiNet brinda a las organizaciones una protección adecuada que responde a las amenazas que pasan a través de su red. FortiNet es la única empresa que se especializa en la seguridad para redes, puntos finales, aplicaciones, centros de datos y acceso a la nube para poder trabajar juntos en manera integrada y colaborativa.
- **Capacitación y soporte constantes:** Tanto Cisco como FortiNet son marcas que cuentan con capacitaciones y certificaciones mundiales de los productos que comercializan, siendo este punto una gran ventaja con sus competidores más cercanos al no tener personal calificado con certificaciones que puedan representar la correcta instalación, configuración y administración de sus equipos.

Por estos puntos mencionados se procedió con el rediseño de la red de la Caja Nacional de Salud Regional Potosí como se detalla a continuación:

**5.5. EQUIPAMIENTO**

Siendo el sitio Regional el core principal de la red, este sitio es el que presentara la mayor cantidad de nuevos dispositivos sugeridos para el rediseño físico de la red.

Dentro del rediseño físico de la red se proponen los siguientes equipos en los diferentes sitios:

**Tabla# 5.1: Detalle Modelos Rediseño**
**Fuente: Elaboración Propia**

| REGIONAL | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco Nexus9000 C9372PX | 1 | Para brindar alta redundancia en el core de la red |
| 2 | cisco WS-C3650-24S | 2 | Para brindar alta redundancia en distribución de la red |
| 3 | FortiWan 200B | 1 | Balanceador de enlaces WAN |
| 4 | FortiWeb 1000D | 1 | Web Application Firewall para proteger a los servidores de la DMZ |
| 5 | FortiAnalyzer VM | 1 | Analizador de trafico de red |

| HOSPITAL | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco WS-C3850-24S | 1 | Para brindar alta redundancia en distribución de la red |

| POLICLINICO | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco WS-C3650-24PD | 1 | Para brindar alta redundancia en distribución de la red |

| NEUMOLOGIA | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco WS-C3650-24PD | 1 | Para brindar alta redundancia en distribución de la red |

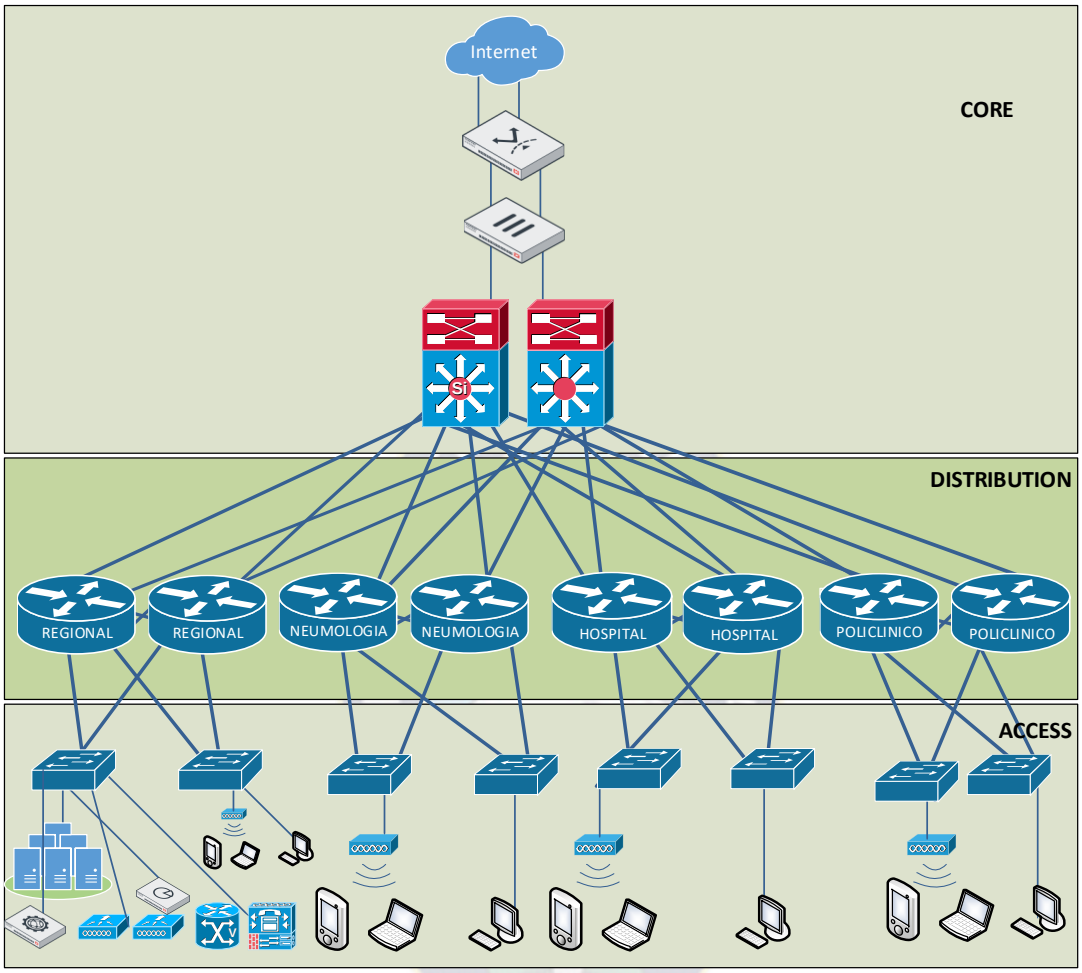
## 5.6. REDISEÑO DIAGRAMA TOPOLOGICO DE LA RED

La red actual presenta una topología semi jerárquica ya que presenta su punto de core en el sitio regional, pero este punto a la ves es donde están alojados los servicios consumidos por la red, por lo tanto para poder brindar a la red una topología jerárquica es necesario poder contar con una capa de core exclusiva y así poder aprovechar todas las grandes ventajas que tiene una red jerárquica:

- Menos carga de trabajo requerida para los CPUs de los dispositivos.
- Una metodología de diseño de red jerárquica le permite diseñar una topología modular que limita el número de routers de comunicación.
- El uso de un modelo jerárquico ayuda a minimizar los costos.
- El diseño modular del modelo jerárquico permite una planificación precisa de la capacidad dentro de cada capa de la jerarquía, reduciendo así la pérdida de ancho de banda.
- El concepto de modularidad le permite mantener cada elemento de diseño simple y fácil de entender.
- La simplicidad de un modelo jerárquico minimiza la necesidad de una capacitación extensiva para el personal de operaciones de red y agiliza la implementación de un diseño.
- El reconocimiento de fallas y su solución se simplifica porque los administradores de red pueden reconocer fácilmente los puntos de transición en la red, también esto ayuda a aislar posibles puntos de fallo.
- Si la escalabilidad es un objetivo principal, se recomienda una topología jerárquica porque la modularidad en un diseño permite crear elementos de diseño que se pueden replicar a medida que crece la red.

A continuación en la figura 5.4 se muestra el rediseño del diagrama de red en un modelo jerárquico:

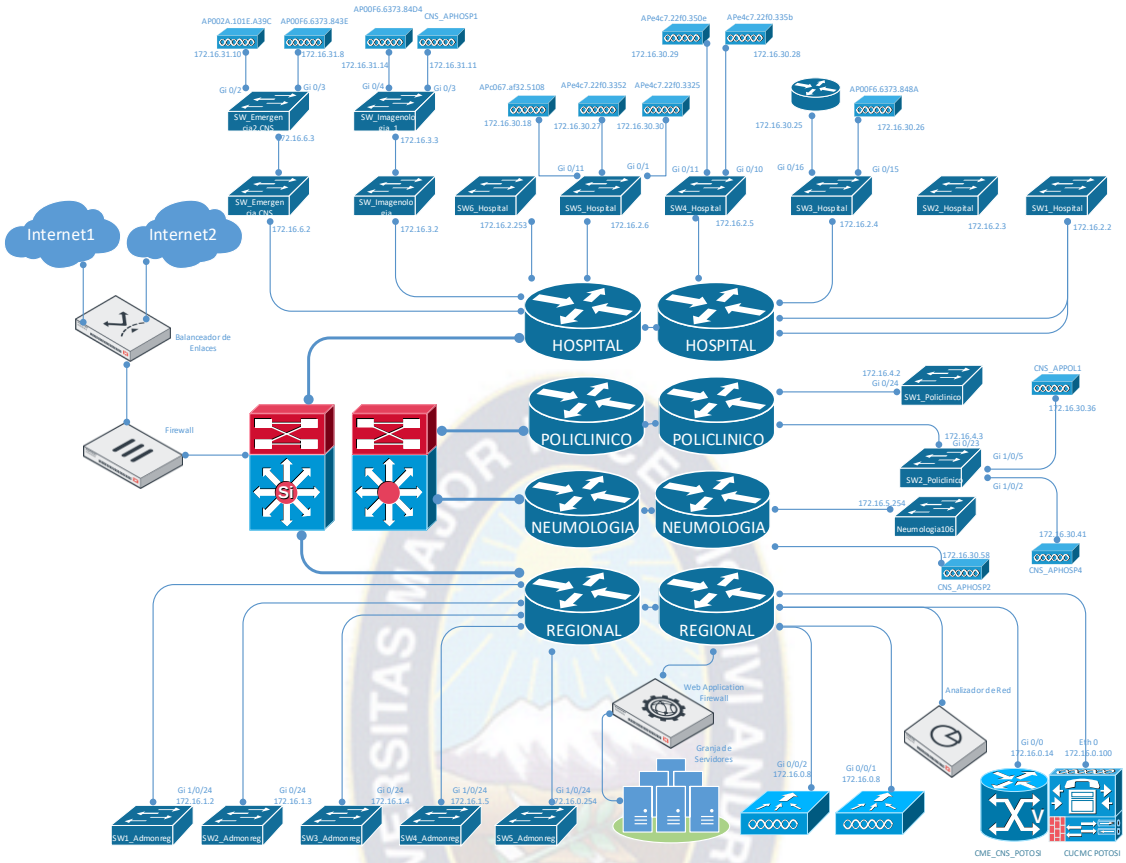
**Figura# 5.4: Rediseño Diagrama Topológico Modelo Jerárquico**
**Fuente: Elaboración Propia**




Cabe resaltar que la capa de core del rediseño jerárquico está ubicado en el sitio Regional.

A continuación en la figura 5.5 se muestra el diagrama topológico modelo jerárquico detallado de la red de la Caja Nacional de Salud Regional Potosí:

**Figura# 5.5: Diagrama Topológico Modelo Jerárquico Detallado**
**Fuente: Elaboración Propia**




## 5.7. REDISEÑO Y CONFIGURACION DE REDUENDANCIA CAPA DE DISTRIBUCION

Como se puede observar en las figuras x, y la capa de distribución del modelo jerárquico contiene dispositivos que se encargan del enrutamiento a los diferentes sitios de la red y estos están rediseñados en alta redundancia para poder contar con tolerancia a fallas por diferentes motivos como pueden ser en hardware o en software.

**Tabla# 5.2: Dispositivos en Alta Redundancia**
**Fuente: Elaboración Propia**

| REGIONAL | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco Nexus9000 | 2 | Para brindar alta redundancia en el core de la red |
| 1 | cisco WS-C3650-24S | 2 | Para brindar alta redundancia en distribución de la red |

| HOSPITAL | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco WS-C3850-24S | 2 | Para brindar alta redundancia en distribución de la red |

| POLICLINICO | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco WS-C3650-24PD | 2 | Para brindar alta redundancia en distribución de la red |

| NEUMOLOGIA | | | |
|---|---|---|---|
| **ID** | **NOMBRE** | **CANTIDAD** | **OBSEVACIONES** |
| 1 | cisco WS-C3650-24PD | 2 | Para brindar alta redundancia en distribución de la red |

El alcance pretendido para este rediseño en la parte de alta redundancia comprenderá todos los sitios de la red, es decir Regional, Hospital, Policlínico y Neumología en la capa de distribución del modelo jerárquico, también en la capa de core de la red, para esto se utilizara HSRP en todos los dispositivos mencionados en las tablas anteriores.

El rediseño de alta redundancia cuenta a nivel general con las funcionalidades:

- Proporcionar alta disponibilidad de red al proporcionar redundancia de primer salto para usuarios que tengan una puerta de enlace predeterminada (First-hop Redundancy).
- Debe Trabajar en Cluster o grupo de dispositivos (Maestro y Esclavo).
- No depender de la disponibilidad de un único enrutador.
- Diferenciados por grupos para evitar conflicto de IPs virtuales.

### 5.7.1 CONFIGURACIÓN HSRP

A continuación se detalla un ejemplo de configuración de HSRP para uno de los dispositivos de la red:

*enable*
*configure terminal*
*interface FastEthernet0/0*
*ip address 192.168.100.2 255.255.255.248*
*standby 1 ip 192.168.100.1*
*standby 1 priority 120*
*standby 1 preempt*

A continuación haremos una breve explicación de cada comando:

**Enable:** Se habilita el modo de acceso privilegiado al dispositivo.

**Configure Terminal:** Para ingresar en el modo de configuración global.

**Interface:** Ingresar al modo de configuración del interfaz.

**Ip address:** Configurar la IP del interfaz

**Standby 1:** Activa HSRP en el interfaz, el numeral 1 indica el número grupo HRSP.

**Standby 1 ip 192.168.100.1:** ip nos da la opción de configurar la ip virtual en el dispositivo virtual.

**Standby 1 priority 120:** Priority determina cual dispositivo tendrá mayor prioridad, es decir que sea el dispositivo activo.

**Standby 1 preempt:** Preempt habilita que el dispositivo con la prioridad más alta siempre sea el dispositivo activo.

A continuación en la tabla 5.3 se muestra las asignaciones de IPs para HSRP, con sus respectivos grupos e IPs virtuales:

**Tabla#5.3: Asignación IPs HSRP**

**Fuente: Elaboración Propia**

| HSRP | | | | |
|---|---|---|---|---|
| **Dispositivo** | **IP** | **Grupo** | **VIP** | **Observaciones** |
| Core1 | 192.168.100.2/255.255.255.248 | 1 | 191.168.100.1/255.255.255.248 | Core a Internet |
| Core2 | 192.168.100.3/255.255.255.248 | | | |

| | | | | |
|---|---|---|---|---|
| Core1 | 192.168.100.10/255.255.255.248 | 2 | 192.168.100.9/255.255.255.248 | Core a Regional |
| Core2 | 192.168.100.11/255.255.255.248 | | | |
| Core1 | 192.168.100.18/255.255.255.248 | 3 | 192.168.100.17/255.255.255.248 | Core a Hospital |
| Core2 | 192.168.100.19/255.255.255.248 | | | |
| Core1 | 192.168.100.26/255.255.255.248 | 4 | 192.168.100.25/255.255.255.248 | Core a Neumología |
| Core2 | 192.168.100.27/255.255.255.248 | | | |
| Core1 | 192.168.100.34/255.255.255.248 | 5 | 192.168.100.33/255.255.255.248 | Core a Policlínico |
| Core2 | 192.168.100.35/255.255.255.248 | | | |
| Regional1 | 192.168.100.13/255.255.255.248 | 6 | 192.168.100.12/255.255.255.248 | Regional a Core |
| Regional2 | 192.168.100.14/255.255.255.248 | | | |
| Regional1 | 172.16.10.2/255.255.255.0 | 7 | 172.16.10.1/255.255.255.0 | VLAN10 |
| Regional2 | 172.16.10.3/255.255.255.0 | | | |
| Regional1 | 172.16.20.2/255.255.255.0 | 8 | 172.16.20.1/255.255.255.0 | VLAN20 |
| Regional2 | 172.16.20.3/255.255.255.0 | | | |
| Regional1 | 172.16.30.2/255.255.255.0 | 9 | 172.16.30.1/255.255.255.0 | VLAN30 |
| Regional2 | 172.16.30.3/255.255.255.0 | | | |
| Regional1 | 172.16.40.2/255.255.255.192 | 10 | 172.16.40.1/255.255.255.192 | VLAN40 |
| Regional2 | 172.16.40.3/255.255.255.192 | | | |
| Regional1 | 172.16.50.2/255.255.255.0 | 11 | 172.16.50.1/255.255.255.0 | VLAN50 |
| Regional2 | 172.16.50.3/255.255.255.0 | | | |
| Hospital1 | 192.168.100.21/255.255.255.248 | 12 | 192.168.100.20/255.255.255.248 | Hospital a Core |
| Hospital2 | 192.168.100.22/255.255.255.248 | | | |
| Hospital1 | 172.16.21.2/255.255.255.0 | 13 | 172.16.21.1/255.255.255.0 | VLAN20 |
| Hospital2 | 172.16.21.3/255.255.255.0 | | | |
| Hospital1 | 172.16.31.2/255.255.255.0 | 14 | 172.16.31.1/255.255.255.0 | VLAN30 |
| Hospital2 | 172.16.31.3/255.255.255.0 | | | |
| Hospital1 | 172.16.40.66/255.255.255.192 | 15 | 172.16.40.65/255.255.255.192 | VLAN40 |
| Hospital2 | 172.16.40.67/255.255.255.192 | | | |
| Hospital1 | 172.16.51.2/255.255.255.0 | 16 | 172.16.51.1/255.255.255.0 | VLAN50 |
| Hospital2 | 172.16.51.3/255.255.255.0 | | | |
| Neumología1 | 192.168.100.29/255.255.255.248 | 17 | 192.168.100.28/255.255.255.248 | Neumología a Core |
| Neumología2 | 192.168.100.30/255.255.255.248 | | | |
| Neumología1 | 172.16.22.2/255.255.255.0 | 18 | 172.16.22.1/255.255.255.0 | VLAN20 |
| Neumología2 | 172.16.22.3/255.255.255.0 | | | |
| Neumología1 | 172.16.32.2/255.255.255.0 | 19 | 172.16.32.1/255.255.255.0 | VLAN30 |
| Neumología2 | 172.16.32.3/255.255.255.0 | | | |
| Neumología1 | 172.16.40.130/255.255.255.192 | 20 | 172.16.40.129/255.255.255.192 | VLAN40 |
| Neumología2 | 172.16.40.131/255.255.255.192 | | | |
| Neumología1 | 172.16.52.2/255.255.255.0 | 21 | 172.16.52.1/255.255.255.0 | VLAN50 |

| | | | | |
|---|---|---|---|---|
| Neumologia2 | 172.16.52.3/255.255.255.0 | | | |
| Policlinico 1 | 192.168.100.37/255.255.255.248 | 22 | 192.168.100.36/255.255.255.248 | Policlínico a Core |
| Policlinico 2 | 192.168.100.38/255.255.255.248 | | | |
| Policlinico 1 | 172.16.23.2/255.255.255.0 | 23 | 172.16.23.1/255.255.255.0 | VLAN20 |
| Policlinico 2 | 172.16.23.3/255.255.255.0 | | | |
| Policlinico 1 | 172.16.33.2/255.255.255.0 | 24 | 172.16.33.1/255.255.255.0 | VLAN30 |
| Policlinico 2 | 172.16.33.3/255.255.255.0 | | | |
| Policlinico 1 | 172.16.40.194/255.255.255.192 | 25 | 172.16.40.193/255.255.255.192 | VLAN40 |
| Policlinico 2 | 172.16.40.195/255.255.255.192 | | | |
| Policlinico 1 | 172.16.53.2/255.255.255.0 | 26 | 172.16.53.1/255.255.255.0 | VLAN50 |
| Policlinico2 | 172.16.53.3/255.255.255.0 | | | |

## 5.8. REDISEÑO Y RECONFIGURACIÓN ENRUTAMIENTO CON OSPF

Considerando que la red de la Caja Nacional de Salud Regional Potosí esta rediseñada en una topología jerárquica, podemos realizar el rediseño y la reconfiguración del enrutamiento a OSPF Jerárquico bajo las siguientes ventajas:

- OSPF es un estándar de la IETF, por lo tanto es compatible con todos los dispositivos de red que lo soportan.
- Con enrutamiento OSPF no hay limitación para el conteo de saltos, teniendo en cuenta que la red de la Caja Nacional de Salud Regional Potosí cuenta con una topología jerárquica, los saltos desde la capa de distribución hasta el destino final ya sea la red local o navegación a internet son de dos a tres saltos.
- OSPF utiliza VLSM, en la red de la Caja Nacional de Salud Regional Potosí están asignadas a varias direcciones IP con subredes mediante VLANs, las cuales corresponden a cada sitio en la red, por lo tanto OSPF trabaja con todas estas subredes sin ningún problema.
- Utilizando el enrutamiento OSPF la multidifusión IP evita las actualizaciones de estado de enlace. Con esto podemos garantizar un menor procesamiento en los routers de la red que no están a la escucha

de paquetes OSPF. Siendo también que las actualizaciones sólo se envían en caso de cambios de enrutamiento en la red y no de manera periódica. Todo esto garantiza un mejor uso del ancho de banda, es decir el router configurado con OSPF conoce toda la topología de la red con los enlaces que unen a cada dispositivo y sus respectivos estados. Siendo de esta manera que OSPF sea un protocolo un tanto lento en su convergencia ya que tiene que alertar en todas las bases de datos de todos su routers los cambios producidos, para poder mejorar este aspecto OSPF está configurado con múltiples áreas, así cuando exista un cambio en la red, este cambio solo se propaga dentro del área correspondiente.

### 5.8.1 CONFIGURACIÓN OSPF

A continuación se detalla un ejemplo de configuración de HSRP para uno de los dispositivos de la red:

```
enable
configure terminal
router ospf 100
 router-id 0.0.0.1
 log-adjacency-changes
 area 1 virtual-link 0.0.0.3
 area 2 virtual-link 0.0.0.5
 area 3 virtual-link 0.0.0.7
 area 4 virtual-link 0.0.0.9
 network 192.168.100.0 0.0.0.7 area 0
 network 192.168.100.8 0.0.0.7 area 1
 network 192.168.100.16 0.0.0.7 area 2
 network 192.168.100.24 0.0.0.7 area 3
 network 192.168.100.32 0.0.0.7 area 4
```

A continuación haremos una breve explicación de cada comando:

**Enable:** Se habilita el modo de acceso privilegiado al dispositivo.
**Configure Terminal:** Para ingresar en el modo de configuración global.

**router ospf 100**: Habilita el ruteo OSPF e ingresa al modo de configuración de router. El argumento 100 (process-id) identifica el proceso OSPF.

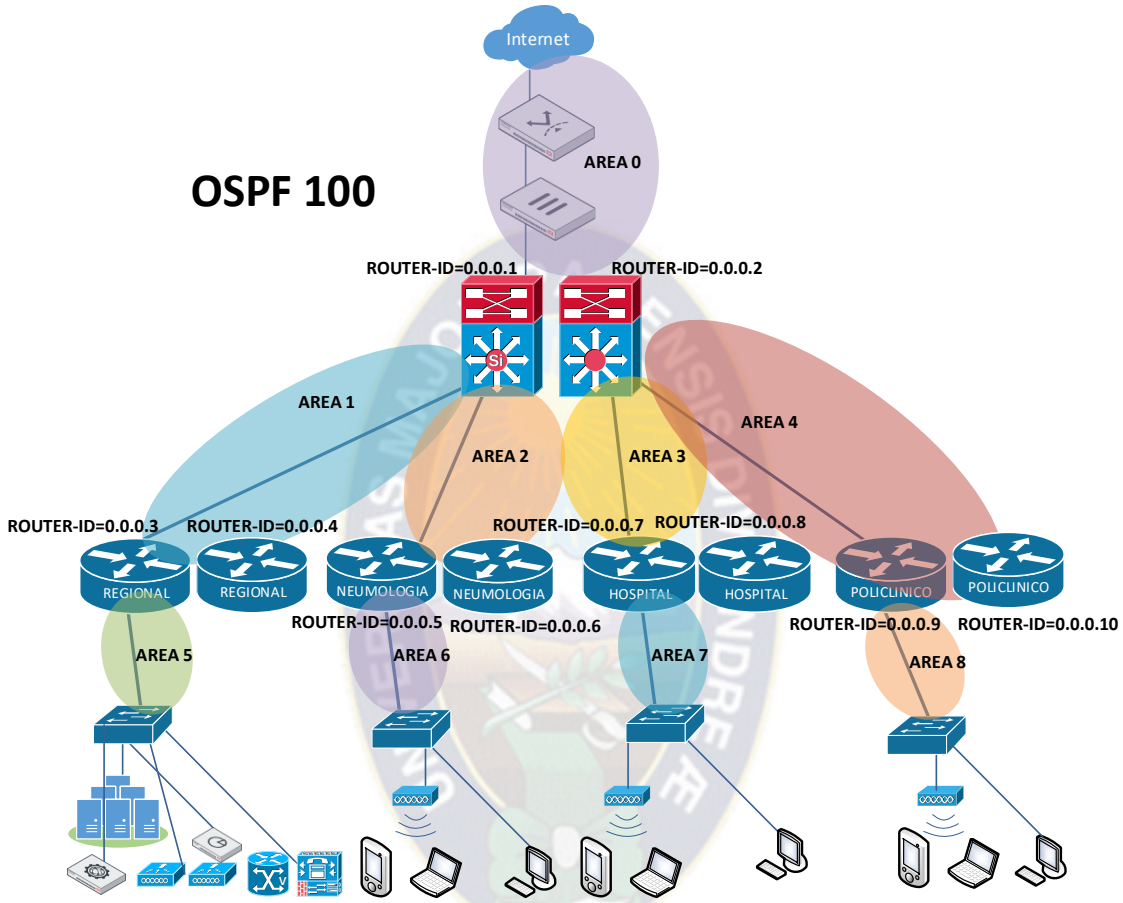
**router-id 0.0.0.1:** Para obligar a OSPF a utilizar el funcionamiento del anterior ID del enrutador OSPF.

**area 1 virtual-link 0.0.0.3:** área 1 identifica ID asignado al área, virtual-link identifica al link virtual por donde se transitara a las áreas que correspondan.

**network 192.168.100.0 0.0.0.7 area 0:** Con network OSPF anuncia interfaces, no redes. Utiliza la máscara de comodín para determinar qué interfaces publicitar. El area 0 es el ID del area del dispositivo OSPF.

A continuación en el diagrama 5.6 se puede ver el enrutamiento con OSPF Jerárquico inter área.

**Figura# 5.6: Diagrama Enrutamiento OSPF Jerárquico Inter área**
**Fuente: Elaboración Propia**




A continuación en la tabla 5.4 se detallan las áreas dentro del proceso OSPF 100:

**Tabla# 5.4: Áreas OSPF**
**Fuente: Elaboración Propia**

| OSPF 100 | | |
|---|---|---|
| **DISPOSITIVO** | **ID** | **AREA** |
| CORE1 | 0.0.0.1 | AREA 0 |
| CORE2 | 0.0.0.2 | AREA 0 |
| REGIONAL1 | 0.0.0.3 | AREA 1 - AREA 5 |
| REGIONAL2 | 0.0.0.4 | AREA 1 - AREA 5 |
| NEUMOLOGIA1 | 0.0.0.5 | AREA 2 - AREA 6 |
| NEUMOLOGIA2 | 0.0.0.6 | AREA 2 - AREA 6 |
| HOSPITAL1 | 0.0.0.7 | AREA 3 - AREA 7 |
| HOSPITAL2 | 0.0.0.8 | AREA 3 - AREA 7 |

| | | |
|---|---|---|
| POLICLINICO1 | 0.0.0.9 | AREA 4 - AREA 8 |
| POLICLINICO2 | 0.0.0.10 | AREA 4 - AREA 8 |

Como se puede apreciar la configuración en el proceso OSPF 100 está definida por interareas, siendo la capa de Distribución la que contiene la mayor cantidad de áreas.
A continuación en la tabla 5.5 se detalla los virtual links que permiten la conexión de las áreas en el proceso OSPF 100:

**Tabla# 5.5: Virtual Links OSPF**
**Fuente: Elaboración Propia**

| OSPF 100 VIRTUAL LINKS | | |
|---|---|---|
| **DISPOSITIVO** | **AREA** | **LINK** |
| CORE1 | AREA 1 | 0.0.0.3 |
| CORE1 | AREA 2 | 0.0.0.5 |
| CORE1 | AREA 3 | 0.0.0.7 |
| CORE1 | AREA 4 | 0.0.0.9 |
| CORE2 | AREA 1 | 0.0.0.4 |
| CORE2 | AREA 2 | 0.0.0.6 |
| CORE2 | AREA 3 | 0.0.0.8 |
| CORE2 | AREA 4 | 0.0.0.10 |
| REGIONAL1 | AREA 1 | 0.0.0.1 |
| REGIONAL2 | AREA 1 | 0.0.0.2 |
| NEUMOLOGIA1 | AREA 2 | 0.0.0.1 |
| NEUMOLOGIA2 | AREA 2 | 0.0.0.2 |
| HOSPITAL1 | AREA 3 | 0.0.0.1 |
| HOSPITAL2 | AREA 3 | 0.0.0.2 |
| POLICLINICO1 | AREA 4 | 0.0.0.1 |
| POLICLINICO2 | AREA 4 | 0.0.0.2 |

## 5.9. REDISEÑO VLANS

En el rediseño del direccionamiento y asignación de direcciones IPs se definieron distintas redes tanto en datos, acceso inalámbrico y voz a través de VLANs para cada uno de los sitios de la red de la Caja Nacional de Salud Regional Potosí, esto para poder diferenciar y brindar seguridad al tráfico de cada uno de los sitios, haciendo una diferenciación de cierto trafico sensible de la red, mejorar el rendimiento en la red reduciendo el trafico innecesario que se generan por

dominios de difusión, además de brindar una administración más simple de la red cuando se necesite asignar nuevos usuarios o servicios.

La siguiente tabla 5.6 se muestra la asignación de IPs de la red y sus respectivas VLANs:

**Tabla# 5.6: Direccionamiento y asignación de IPs con VLANs**
**Fuente: Elaboración Propia**

| DIRECCIONAMIENTO RED CAJA NACIONAL DE SALUD REGIONAL POTOSI | | |
|---|---|---|
| **VLAN** | **IP/MASK** | **SITE** |
| 10 Datos_Sistemas | VLAN10 – 172.16.10.0/24 | REGIONAL |
| 20 Datos_Regional | VLAN20 – 172.16.20.0/24 | REGIONAL |
| 30 Wireless_Regional | VLAN30 – 172.16.30.0/24 | REGIONAL |
| 40 Aps_Regional | VLAN40 – 172.16.40.0/26 | REGIONAL |
| 50 Voz_Regional | VLAN50 – 172.16.50.0/24 | REGIONAL |
| **VLAN** | **IP/MASK** | **SITE** |
| 20 Datos_Hospital | VLAN20 – 172.16.21.0/24 | HOSPITAL |
| 30 Wireless_Hospital | VLAN30 – 172.16.31.0/24 | HOSPITAL |
| 40 Aps_Hospital | VLAN40 – 172.16.40.64/26 | HOSPITAL |
| 50 Voz_Hospital | VLAN50 – 172.16.51.0/24 | HOSPITAL |
| **VLAN** | **IP/MASK** | **SITE** |
| 20 Datos_Neumologia | VLAN20 – 172.16.22.0/24 | NEUMOLOGIA |
| 30 Wireless_Neumologia | VLAN30 – 172.16.32.0/24 | NEUMOLOGIA |
| 40 Aps_Hospital | VLAN40 – 172.16.40.128/26 | NEUMOLOGIA |
| 50 Voz_Hospital | VLAN50 – 172.16.52.0/24 | NEUMOLOGIA |
| **VLAN** | **IP/MASK** | **SITE** |
| 20 Datos_Policlinico | VLAN20 – 172.16.23.0/24 | POLICLINICO |
| 30 Wireless_Policlinico | VLAN30 – 172.16.33.0/24 | POLICLINICO |

| | | |
|---|---|---|
| 40 Aps_Policlinico | VLAN40 – 172.16.40.192/24 | POLICLINICO |
| 50 Voz_Policlinico | VLAN50 – 172.16.53.0/24 | POLICLINICO |

### 5.9.1 CONFIGURACIÓN DE VLANs

A continuación se detalla un ejemplo de configuración de una VLAN para uno de los dispositivos de la red:

```
enable
configure terminal
interface Vlan10
name Datos_Sistemas

enable
configure terminal
interface FastEthernet0/1
switchport mode trunk

enable
configure terminal
interface FastEthernet2/1
switchport access vlan 10
switchport mode Access
```

A continuación haremos una breve explicación de cada comando:

**Enable:** Se habilita el modo de acceso privilegiado al dispositivo.

**Configure Terminal:** Para ingresar en el modo de configuración global.

**interface Vlan10**: Permite crear una SVI (Switch Virtual Interface) asociada a la VLAN cuyo ID (10) se aplica, e ingresar al modo de configuración de esa interfaz.

**name Datos_Sistemas:** Configura la etiqueta a la VLAN 10.

**Interface FastEthernet0/1:** Ingresar al modo de configuración del interfaz.

**switchport mode trunk:** Configura la interface en el modo troncal.

**switchport mode Access:** Configura la interface en el modo de acceso.

**switchport access vlan 10:** Asigna la VLAN 10 en el interfaz en modo de acceso.

### 5.10. DISEÑO Y CONFIGURACION DE WEB APPLICATION FIREWALL

La Caja Nacional de Salud Regional Potosí, cuenta con una granja de servidores ubicada en el sitio Regional, donde se albergan todos los servicios consumidos tanto localmente como externamente, a continuación en la tabla 5.7 se detallan:

**Tabla# 5.7: Granja de Servidores**
**Fuente: Elaboración Propia**

| Granja de Servidores<br>Caja Nacional de Salud Regional Potosí | | |
|---|---|---|
| **Servidor** | **Tipo de Servicio** | **Uso** |
| SIAIS | Cliente Servidor/Gestión | Interno |
| SHIF-ND | Cliente Servidor/Financiera | Interno |
| SINBIOS | Cliente Servidor/ Bioestadística | Interno |
| ERP | WEB/Administrativa | Interno/externo |
| CAMARAS IP | Comunicación | Interno |
| TELEFONIA IP | Comunicación | Interno/externo |
| WEB | Página Web | Interno/externo |

Dado que el funcionamiento de los servicios de la Granja de Servidores debe ser constante y libre de ataques, el rediseño contempla la protección de los servicios de aplicaciones de esta mediante un Web Application Firewall que cuenta con las siguientes funcionalidades de protección para los servicios mencionados:

- Protección contra cualquier vulnerabilidad conocida o desconocida. Una vez que se define una política de ingreso local o externo para cualquier aplicación o servicio web de la Caja Nacional de Salud regional Potosí, el dispositivo comienza a analizar y monitorizar todo el flujo de tráfico dirigido hacia esa aplicación que se encuentra en la granja de servidores. Basándose en una tecnología de análisis del comportamiento denominada Auto-Learn. Analizando el comportamiento de los usuarios que consumen la aplicación, el equipo es capaz de entender y determinar cómo debe accederse a la aplicación web. La funcionalidad de Auto-Learn es totalmente transparente y no requiere de ningún cambio en las aplicaciones web o en la arquitectura de red. Usando Auto-Learn, el equipo no escanea la aplicación para determinar el perfil, sino que analiza de forma exhaustiva todo el tráfico que se dirige hacia la aplicación. De esta forma, creando un perfil de seguridad inteligente y adaptado a cada aplicación FortiWeb es capaz de proteger frente a cualquier vulnerabilidad conocida o desconocida, ataques “zero day” como SQL Injection, Cross Site Scripting y cualquier otro ataque a nivel de aplicación.

- Dado que la red de la Caja Nacional de Salud Regional Potosí es una red que va en gran crecimiento, con proyectos futuros de alojamientos compartidos webs, es útil la función de ADOM's, o dominios administrativos, la cual nos permite separar conjuntos de políticas, de forma que tengamos administradores en cada dominio. Estos administradores podrán iniciar sesión y acceder directamente a su dominio, como si se tratara de un dispositivo FortiWeb aparte.
- La red cuenta con una granja de servidores y estos son los que comparten los servicios y aplicaciones, con el dispositivo tendremos la opción de repartir las conexiones que se dirijan a estos. Especificando el servidor o los servidores que contenga la aplicación a consumir, FortiWeb, mediante el algoritmo que hayamos seleccionado, repartirá las sesiones.

Los algoritmos de balanceo son en el caso que exista redundancia a nivel de servidores:

- Round Robin: Distribuye las sesiones igualmente a cada miembro de la granja.
- Weighted Round Robin: Distribuye las sesiones basándonos en pesos que hayamos establecido para cada miembro.
- Least Connection Manda las conexiones al miembro de la granja que menos conexiones haya recibido.

En el caso de que la aplicación sea una que no tenga que cortar la sesión con la que se inició el equipo está configurado de tal forma que provea persistencia de sesiones para que todas las peticiones HTTP o HTTPS que haga un cliente se realicen contra el mismo servidor.

Las persistencias soportadas son:

- Persistent IP
- Persistent Cookie
- Insert Cookie
- ASP Session ID
- PHP Session ID
- JSP Session ID

Para verificar si algún servidor ha sufrido algún inconveniente se habilito la opción de heath check, mediante la cual podremos comprobar el estado del

servidor, y en el caso de que este no esté operativo redirigir sus sesiones a otro servidor.

El equipo posee una protección contra una amplia gama de ataques:

- Cross Site Scripting
- Inyección SQL
- Secuestro de sesiones
- Alteración /Envenenamiento de cookies
- Falsificación de solicitudes entre sitios
- Inyección de comandos
- Inclusión remota de archivos
- Alteración de formularios
- Manipulación de campos ocultos
- Pérdida de datos salientes
- Contrabando de solicitudes HTTP
- Inclusión remota de archivos
- Ataques de codificación
- Control de acceso roto
- Navegación forzada
- Directorio transversal
- Reconocimiento de sitios
- Piratería de motores de búsqueda
- Ataque de fuerza bruta
- Control de velocidad de acceso
- Envenenamiento de esquemas
- Alteración de parámetros XML
- Prevención de Intrusos XML
- Escaneo WSDL
- Carga útil recursiva
- Ataque de entidades externas
- Desbordamientos del Búfer
- Denegación de Servicio

A continuación la tabla 5.8 muestra los servidores protegidos por el WAF, con sus IPs Reales, IPs Virtuales y el puerto de servicio que utilizan:

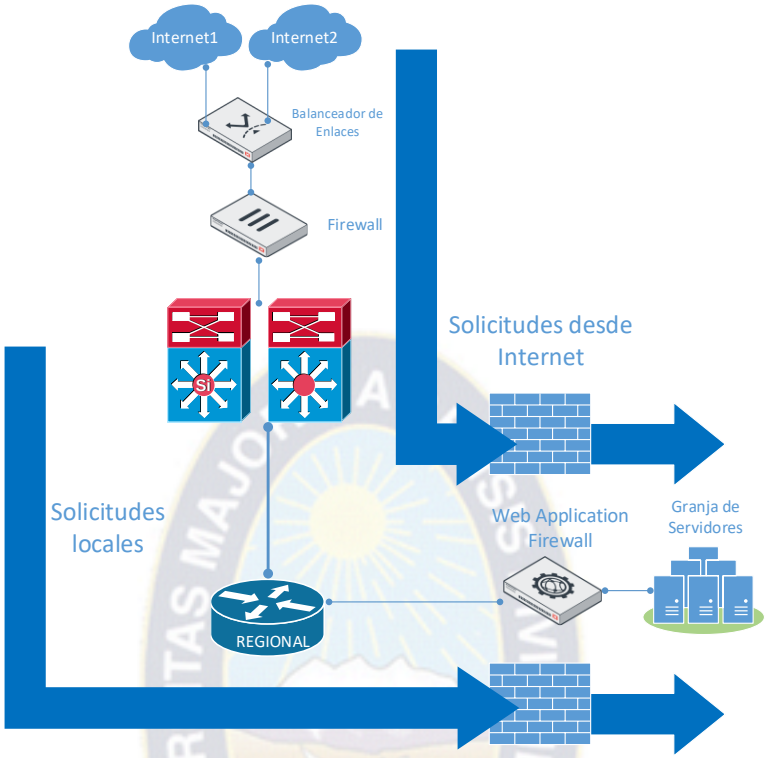
**Tabla# 5.8: Servidores Protegidos WAF**
**Fuente: Elaboración Propia**

| Servidores Protegidos | | | | |
|---|---|---|---|---|
| **Servidor** | **Tipo de Servicio** | **IP Real** | **IP Virtual** | **Puerto** |
| SIAIS | Cliente Servidor/Gestión | 172.16.5.14 | 172.16.10.14 | 80 |
| SHIF-ND | Cliente Servidor/Financiera | 172.16.5.13 | 172.16.10.13 | 80 |
| SINBIOS | Cliente Servidor/ Bioestadística | 172.16.5.12 | 172.16.10.12 | 80 |
| ERP | WEB/Administrativa | 172.16.5.11 | 172.16.10.11 | 80/443 |
| WEB | Página Web | 172.16.5.10 | 172.16.10.10 | 80/443 |

En el caso de los servidores WEB y ERP estos manejan dos puertos para su acceso web que son el 80 (http) y el 443 (https), pero por seguridad en estas conexiones externas se realiza un re direccionamiento de puerto, es decir el WAF se encarga de re direccionar todas las solicitudes del puerto http al puerto seguro https.

A continuación en la figura 5.7 se muestra el diagrama topológico del rediseño de la protección WAF en el sitio Regional:

**Figura# 5.7: Diagrama Topológico WAF**
**Fuente: Elaboración Propia**




El detalle de toda la configuración del Web Application Firewall esta detallada en el anexo 3.

## 5.11. REDISEÑO ACCESO A INTERNET USUARIOS FINALES

Mediante el Firewall de borde todos los usuarios acceden a internet, en el rediseño se reordeno todas las salidas a internet de todos los usuarios de la red con el objeto de poder conseguir las siguientes mejoras en el uso del acceso a internet:

- Mejor distribución del ancho de banda a usuarios, es decir mayor fluidez en el acceso a internet para usuarios que necesiten consumir aplicaciones en la nube.
- Seguridad en la navegación de usuarios hacia páginas no deseadas, por ende la red estará más segura ante amenazas generadas desde internet.
- Control de la navegación de los usuarios
- Control en las aplicaciones de los usuarios.
- Mayor rendimiento en la red.

Bajo estos beneficios se procedió a realizar las siguientes agrupaciones de usuarios por segmentos de IPs según la necesidad de acceso a internet:

**Tabla# 5.9: Restricciones navegación por usuario**
**Fuente: Elaboración Propia**

| RESTRICCIONES NAVEGACIÓN POR USUARIO | | | | |
|---|---|---|---|---|
| **SEGMENTO** | **GRUPO** | **PERFIL DE NAVEGACIÓN** | **PERFIL DE APLICACIÓN** | **SITIO** |
| 172.16.10.2-172.16.10.200 | SISTEMAS | NAVEGACIÓN TOTAL | BÁSICO | REGIONAL |
| 172.16.10.201-172.16.10.254 | GERENTES Y JEFES | NAVEGACIÓN TOTAL | BÁSICO | REGIONAL |
| 172.16.20.20-172.16.20.200 | ADMINISTRATIVOS_R | NAVEGACIÓN MEDIA | MEDIO | REGIONAL |
| 172.16.20.201-172.16.20.254 | DOCTORES Y ENFERMERAS_R | NAVEGACIÓN BASICA | MEDIO | REGIONAL |
| 172.16.30.10-172.16.30.200 | USUARIOS WIFI_R | NAVEGACIÓN WIFI | MEDIO | REGIONAL |
| 172.16.30.201-172.16.30.254 | INVITADOS WIFI_R | NAVEGACIÓN BAJA | BAJO | REGIONAL |
| 172.16.21.20-172.16.21.200 | ADMINISTRATIVOS_H | NAVEGACIÓN MEDIA | MEDIO | HOSPITAL |
| 172.16.21.201-172.16.21.254 | DOCTORES Y ENFERMERAS_H | NAVEGACIÓN BASICA | BÁSICO | HOSPITAL |
| 172.16.31.10-172.16.31.200 | USUARIOS WIFI_H | NAVEGACIÓN WIFI | MEDIO | HOSPITAL |
| 172.16.31.201-172.16.31.254 | INVITADOS WIFI_H | NAVEGACIÓN BAJA | BAJO | HOSPITAL |
| 172.16.22.20-172.16.22.200 | ADMINISTRATIVOS_N | NAVEGACIÓN MEDIA | MEDIO | NEUMOLOGIA |
| 172.16.22.201-172.16.22.254 | DOCTORES Y ENFERMERAS_N | NAVEGACIÓN BASICA | BÁSICO | NEUMOLOGIA |
| 172.16.32.10-172.16.32.200 | USUARIOS WIFI_N | NAVEGACIÓN WIFI | MEDIO | NEUMOLOGIA |
| 172.16.32.201-172.16.32.254 | INVITADOS WIFI_N | NAVEGACIÓN BAJA | BAJO | NEUMOLOGIA |
| 172.16.23.20-172.16.23.200 | ADMINISTRATIVOS_P | NAVEGACIÓN MEDIA | MEDIO | POLICLINICO |
| 172.16.23.201-172.16.23.254 | DOCTORES Y ENFERMERAS_P | NAVEGACIÓN BASICA | BÁSICO | POLICLINICO |
| 172.16.33.10-172.16.33.200 | USUARIOS WIFI_P | NAVEGACIÓN WIFI | MEDIO | POLICLINICO |

| | | | | |
|---|---|---|---|---|
| 172.16.33.201 - 172.16.33.254 | INVITADOS WIFI_P | NAVEGACIÓN BAJA | BAJO | POLICLINICO |

Para los perfiles de navegación se tomaron en cuenta los siguientes parámetros:

**Tabla# 5.10: Perfiles de Navegación**
**Fuente: Elaboración Propia**

| Perfiles de Navegación a Internet | |
|---|---|
| **Perfil de Navegación** | **Restricciones** |
| Navegación Total | Contenido para adultos<br>Contenido riesgoso para la seguridad |
| Navegación Media | Contenido para adultos<br>Contenido riesgoso para la seguridad<br>Descargas<br>Contenido multimedia<br>Juegos<br>Redes sociales |
| Navegación Básica | Contenido para adultos<br>Contenido riesgoso para la seguridad<br>Juegos |
| Navegación WiFi | Contenido para adultos<br>Contenido riesgoso para la seguridad<br>Descargas<br>Contenido multimedia<br>Juegos<br>Redes sociales<br>Actualizaciones |
| Navegación Baja | Contenido para adultos<br>Contenido riesgoso para la seguridad<br>Descargas<br>Contenido multimedia<br>Juegos<br>Redes sociales<br>Actualizaciones<br>Correo<br>Radio y TV por internet |

Para las restricciones de aplicaciones de internet se tomaron en cuenta los siguientes perfiles:

**Tabla# 5.11: Perfiles de Aplicación**
**Fuente: Elaboración Propia**

| Perfiles de Aplicación | |
|---|---|
| **Perfil de Aplicación** | **Restricciones** |
| Basico | Botnet<br>Proxy |
| Medio | Botnet<br>Proxy<br>Game<br>P2P<br>Storage & Backup<br>Update |
| Bajo | Botnet<br>Proxy<br>Game<br>P2P<br>Storage & Backup<br>Remote Access<br>Network Service<br>Update<br>Video & Audio<br>Social Media |

Las publicaciones de los servicios de los dos servidores a los que se acceden desde fuera de la red son las siguientes:

**Tabla# 5.12: Virtual IPs FortiGate**
**Fuente: Elaboración Propia**

| Publicaciones Virtual IP | | | | |
|---|---|---|---|---|
| **External IP** | **Interfaz** | **Mapped IP** | **Interfaz** | **Puerto** |
| 10.10.10.1 | Wan1 | 172.16.10.10 | LAN | 80 |
| 10.10.10.1 | Wan1 | 172.16.10.10 | LAN | 443 |
| 10.10.10.3 | Wan1 | 172.16.10.11 | LAN | 80 |
| 10.10.10.3 | Wan1 | 172.16.10.11 | LAN | 443 |

Las External IPs son recibidas desde el equipo FortiWan el cual es el que gestiona las IPs públicas de Internet, el firewall recibe estas IPs y las envía a su respectiva VLAN.

El detalle de la configuración del firewall FortiGate se detalla en el anexo 4.

## 5.12. DISEÑO Y CONFIGURACION BALANCEADOR DE ENLACES

Dado que la red actual cuenta con solo un enlace hacia internet de 8 Mbps del ISP ENTEL, el rediseño contempla poder adquirir un enlace más hacia internet, esto para contar con una tolerancia a fallas a nivel de enlaces WAN, tanto para navegación de los usuarios finales como también para las publicaciones que se hacen desde la DMZ.

A continuación se detallan los enlaces del rediseño:

**Tabla# 5.13: Enlaces WAN**
**Fuente: Caja Nacional de Salud**

| Enlaces WAN | | | | |
|---|---|---|---|---|
| **Tipo de acceso ADSL** | **Velocidad** | **ISP** | **Red** | **Mascara** |
| Banda Ancha Empresarial | 8.192 Kbps | ENTEL | 200.200.100.0 | 255.255.255.248 |
| Banda Ancha Empresarial | 8.192 Kbps | ENTEL | 200.200.200.0 | 255.255.255.248 |

Para que los dos enlaces puedan brindar una tolerancia a fallas y balanceo el rediseño contempla la configuración de un equipo Balanceador de enlaces, brindando las siguientes mejoras:

- Acceso a recursos de Internet desde la Caja Nacional de Salud Regional Potosí, es decir los usuarios finales tendrán una mayor experiencia en la navegación.
- Acceso a recursos empresariales desde internet, a través del equipo poder determinar los recursos que se consumirán desde fuera de la red, brindando seguridad a nivel de IP o puertos.
- Balanceo de servicios de internet solicitados por los usuarios, definiendo que servicios son más críticos a la hora de su consumo, el equipo puede priorizar estos para una mejora en el acceso.
- Optimización y distribución del tráfico a través de enlaces disponibles, en caso de la caída o falla de uno de los enlaces el otro disponible trabajaría sin notarse una interrupción. Esta situación incrementa la confiabilidad de la red, siendo tolerable a fallas que puedan presentarse.
- Además el equipo brinda el servicio de publicación de servidores “Virtual Servers”, siento FortiWan quien recibe las IPs públicas, este además de balancear gestiona estas para ser utilizadas en los servicios que se consumen desde fuera de la red es decir desde internet, a continuación la

tabla muestra la asignación de estas IPs y su mapeo a las IPs de la red de la Caja Nacional de Salud regional Potosí:

La tabla 5.14 muestra las publicaciones de los servicios a partir de las IPs públicas que se tiene.

**Tabla# 5.14: Virtual Server FortiWan**

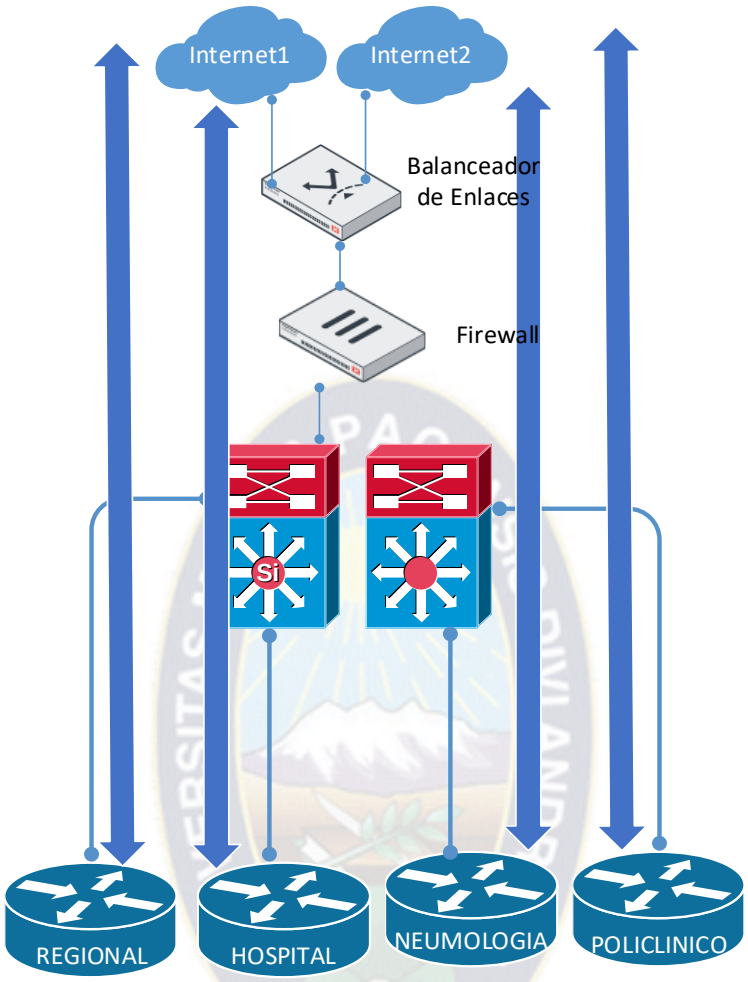
**Fuente: Elaboración Propia**

| Publicaciones Virtual Server | | | | |
|---|---|---|---|---|
| **IP** | **Interfaz** | **IP Virtual** | **Interfaz** | **Puerto** |
| 200.200.100.2 | Wan1 | 10.10.10.1 | LAN | 80 |
| 200.200.200.2 | Wan2 | 10.10.10.1 | LAN | 443 |
| 200.200.100.3 | Wan1 | 10.10.10.3 | LAN | 80 |
| 200.200.200.3 | Wan2 | 10.10.10.3 | LAN | 443 |

La figura 5.8 muestra el rediseño con el balanceador de enlaces realizando el balanceo de los dos enlaces hacia internet.

En el anexo 5 se detalla la configuración del Balanceador de enlaces.

**Figura# 5.8: Diseño Balanceo de Enlaces**
**Fuente: Elaboración Propia**




La tabla 5.15 muestra la distribución de rutas que el equipo realiza para la navegación de los usuarios, además de brindar el balanceo y tolerancia a fallas en los interfaces de Internet:

**Tabla # 5.15: Auto Routing**
**Fuente: Elaboración Propia**

| Auto Routing | | | |
|---|---|---|---|
| **Policy** | **Interfaz** | **Algorithm** | **Fail-Over Policy** |
| Policy1 | Wan1/Wan2 | Optimum Route | Next-Match |
| Policy2 | Wan1 | Fixed | Next-Match |
| Policy3 | Wan2 | Fixed | Next-Match |

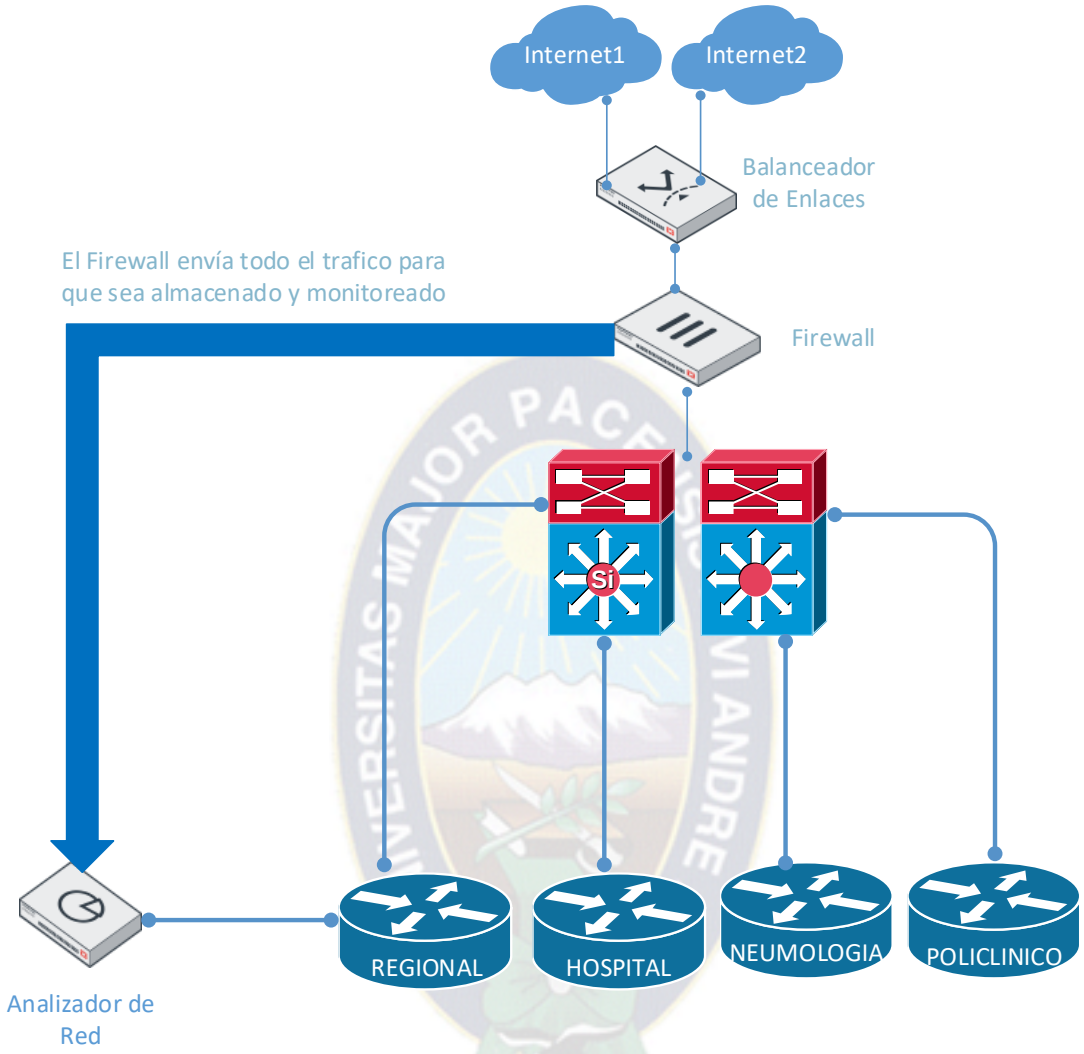
## 5.13. DISEÑO Y CONFIGURACIÓN DE UN ANALIZADOR DE RED

Dado que la red contiene una gran cantidad de usuarios y estos en su mayoría tienen acceso a internet, es necesario poder contar con un dispositivo capaz de poder monitorear el tráfico que generan cada uno de estos usuarios y a la ves poder guardar toda esta información, el rediseño comprende la configuración de un equipo analizador de red que cumple con las siguientes características en su funcionamiento:

- El equipo trabaja a través de un FortiGate para colectar la información generada en el tráfico de la red.
- Permite analizar, reportar y almacenar eventos de seguridad, tráfico de la red y contenido web, para que se cumplan las políticas establecidas en la red de la Caja Nacional de Salud Regional Potosí.
- El equipo puede generar más de 550 informes en distintos idiomas, estos informes pueden contener gráficos y tablas que son completamente configurables.
- Genera informes de la capacidad y utilización de la red, con lo cual conseguimos tener una gestión de la red en forma planificada y eficiente.
- El equipo es escalable ya que puede funcionar en modo colector o analizador optimizando el procesamiento de logs.

La figura 5.9 nos muestra el rediseño del analizador de red FortiAnalyzer.

**Figura# 5.9: Diseño Analizador de red**
**Fuente: Elaboración Propia**




Como se mencionó anteriormente el equipo trabaja a través de un FortiGate para recibir la información del tráfico que se genera en la red, FortiAnalyzer almacena todos estos logs en su base de datos para poder consultarlos cuando asi se lo requiera, esta información puede ser representada en Reportes tanto por defecto del equipo o personalizados como se detalla a continucacion algunos:

- Admin and System Events Report
- Application Risk and Control
- Bandwidth and Applications Report
- Client Reputation
- Cyber Threat Assessment
- Data Loss Prevention Detailed Report

- Detailed Application Usage and Risk
- Email Report
- IPS Report
- Security Analysis
- User Security Analysis
- Web Usage Report

Estos reportes pueden ser generados al momento que se los requiera o programar un día específico, esto puede ser repetitivo o solo a demanda.

También es posible obtener el reporte de acuerdo al tiempo, es decir reportes anuales, mensuales, semanales, diarios y/o de una fecha específica.

A continuación en la tabla 5.16 se detalla las IPs con las que están conectados los equipos FortiGate y FortiAnalyzer:

**Tabla# 5.16: Conexión FortiAnalyzer**
**Fuente: Elaboración Propia**

| Conexión FortiAnalyzer | |
|---|---|
| **IP** | **Equipo** |
| 172.16.10.15 | FortiAnalyzer |
| 172.16.10.10 | FortiGate |

## CONCLUCIONES

Terminado el proceso en el análisis y rediseño de la red LAN de la Caja Nacional de Salud Regional Potosí. Se puede llegar a las siguientes conclusiones del proyecto:

- Se hizo el fundamento teórico de todo el rediseño de la red LAN. Se realizó el análisis y diagnóstico de la red actual de la Caja Nacional de Salud Regional Potosí, mediante técnicas de observación y análisis de flujo de tráfico de sus datos.
- Se rediseño en base al modelo de red jerárquico para que la red sea convergente entre todos sus sitios que comprende la Caja Nacional de Salud Regional Potosí.
- Se validó el rediseño del modelo de red sugerido mediante un análisis teórico y mediante herramientas de simulación la redundancia, escalabilidad y estabilidad de la red LAN de la Caja Nacional de Salud Regional Potosí.

## RECOMENDACIONES

Una vez terminado el presente proyecto, se recomienda lo siguiente:

- El rediseño contempla un funcionamiento óptimo, se recomienda realizar la implementación a mediano plazo, dadas las observaciones en red y seguridad que se obtuvieron en el diagnóstico de la red actual de la Caja Nacional de Salud Regional Potosí.

# BIBLIOGRÁFIA


| | |
|---|---|
| **Mario Tamayo y Tamayo** | El proceso de la investigación científica Cuarta Edición (2003) |
| **Roberto Hernandez Sampieri** | Metodología de la Investigación Sexta edición (2014) |
| **William Stallings** | Guía de diseño base Comunicaciones y redes de Computadoras Séptima edición (2004) |
| **Santiago Cristobal Pérez** | Metodología de análisis de comportamiento De redes LAN (2014) |
| **Andrew S. Tanenbaum** | Redes de computadoras Quinta edición (2012) |
| **Unión Internacional de Telecomunicaciones** | Manual sobre redes basadas en el Protocolo Internet (IP) y asuntos conexos (2005) |
| **Cisco** | Smart Business Architecture Borderless Networks para organizaciones medianas (2011) |
| **Cisco** | Cisco Catalyst 3650 Series Switches (2017) |
| **Cisco** | Cisco Nexus 9300 Platform Switches (2017) |
| **Cisco** | Campus Resumen de diseño (2014) |
| **Cisco** Configuration | First Hop Redundancy Protocols Guide, Cisco IOS XE (2017) |
| **Cisco** | IP Routing: OSPF Configuration Guide (2011) |
| **Cisco** Switches | Cisco Catalyst 2960-S and 2960 Series with LAN Lite Software (2014) |
| **Cisco** | Cisco SAFE Reference Guide (2010) |
| **Cisco** | Top-Down Network Desing (2011) |
| **Cisco** | CCNA V5 (2015) |

**FortiNet** FortiAnalyzer Resumen de funcionalidades (2015)

**FortiNet** FortiWeb Resumen de funcionalidades (2015)

**FortiNet** DOCUMENTO DESCRIPTIVO FORTIGATE Resumen de funcionalidades (2015)

**FortiNet** FortiWAN Handbook (2017)

**FortiNet** www.fortinet.com

**Cisco** www.cisco.com

**CNS** www.cnspotosi.gob.bo

**Wikipedia** es.wikipedia.org