UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE LA SOLUCIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE TRÁFICO WAN DEL ENLACE DE INTERNET DEDICADO CON ALTA DISPONIBILIDAD PARA UN CAMPUS UNIVERSITARIO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ABDEL VÍCTOR RAMÍREZ MARTÍNEZ

PROMOCIÓN
2008-I

LIMA-PERÚ
2011

DISEÑO DE LA SOLUCIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE TRÁFICO WAN DEL ENLACE DE INTERNET DEDICADO CON ALTA DISPONIBILIDAD PARA UN CAMPUS UNIVERSITARIO

A mis padres

Mis hermanos

Mis profesores

SUMARIO

El presente trabajo describe el diseño de la solución de seguridad y administración de tráfico WAN, del enlace de internet dedicado con alta disponibilidad, para un campus universitario.

Esta solución permite satisfacer las necesidades de acceso a internet de los usuarios de la universidad, en forma segura y optimizando el uso del recurso de ancho de banda digital adquirido por la universidad.

Esta solución es lograda mediante la implementación de una solución de seguridad perimetral informática y administración de trafico WAN, la cual es diseñada en función a las necesidades de la universidad expresada en los términos de referencia de las bases del concurso público de adquisición del servicio de internet. El diseño contempla los aspectos de seguridad, administración y disponibilidad, los cuales se aplican a los proyectos de networking en mayor o menor grado.

El informe se enfoca en la solución de ingeniería de networking, mas no en la planta externa. Por ello los aspectos conceptuales se enfocan a la topología de redes de datos y la seguridad de las mismas, al tráfico de internet, las redes virtuales de área local, y los protocolos de comunicaciones.

Luego de expuesta la solución de ingeniería de networking, se desarrollan los aspectos relacionados a los costos y cronograma de tareas. También se realiza el análisis de disponibilidad y se muestran los resultados obtenidos.

ÍNDICE

INTRODUCCIÓN

El presente trabajo surge por la necesidad de una institución universitaria de alto prestigio de contar con un acceso a internet que cubra las necesidades de su campus, que este siempre disponible, protegido ante las amenazas de una red abierta como internet, y además resuelva los problemas causados por no contar con una gestión del uso del recurso de ancho de banda digital de manera que, en las horas pico de acceso a internet se pueda asegurar el funcionamiento de las aplicaciones relacionadas a las actividades propias de la entidad (administrativas, lectivas, de investigación, etc.).

Lo explicado anteriormente es logrado mediante un diseño que incluye equipamiento de conectividad, seguridad perimetral informática, y administración de trafico WAN; acorde a las necesidades de la institución universitaria.

La solución se centra en la ingeniería de networking, es decir, en modificar la estructura de la plataforma de acceso a Internet de la entidad universitaria. Esta reestructuración involucra la definición de una nueva topología, además del análisis de costos y desempeño de los equipos de administración de tráfico y de seguridad. El propósito de la solución es satisfacer las necesidades de la universidad, la cual básicamente es hacer un uso adecuado del recurso de acceso de Internet, orientándose este al acceso para labores administrativas y educativas (investigación y desarrollo). El diseño incluye la configuración de los equipos con los respectivos protocolos de enlaces de comunicación, no se incluye la planta externa.

Para el desarrollo del informe se ha recurrido a diversas fuentes bibliográficas, relacionadas principalmente con las redes de computadoras, es decir, aspectos de seguridad en la red, tráfico multimedia, protocolos de comunicación, LAN virtuales, cálculos de confiabilidad. El informe se complementa con las hojas técnicas de los equipos usados en la implementación de la solución descrita.

El informe está dividido en cuatro capítulos principales:

- El primer capítulo, titulado "Planteamiento de Ingeniería del Problema", presenta una breve descripción del problema y el objetivo del proyecto mismo. Se hace una evaluación del problema y se precisan los alcances del informe, finalmente se hace una síntesis del trabajo realizado.
- El segundo capítulo, titulado "Marco Teórico Conceptual", exponen los conceptos más importantes relacionados al trabajo realizado. Los temas tratados son: Internet,

seguridad, dispositivos de red, protocolos de enlaces, disponibilidad, nodos y última milla.

- El tercer capítulo, titulado "Metodología para la Solución del Problema", describe la ingeniería del proyecto. Preliminarmente se hace el análisis de la solución considerando la situación inicial y los requerimientos de la universidad, luego se describe el sistema implementado.

- El cuarto capítulo, titulado "Análisis y Presentación de Resultados", desarrolla los temas involucrados al presupuesto, al cronograma, al análisis de la disponibilidad y a la presentación de resultados.

Finalmente se presentan las conclusiones.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primeramente se describe el problema y luego se expone el objetivo del trabajo, también se evalúa el problema y se precisan los alcances del informe, para finalmente presentar una síntesis del diseño realizado.

1.1 Descripción del problema

Inexistencia de una gestión y seguridad en el uso del recurso de ancho de banda digital, para el acceso a Internet, orientado a cubrir las necesidades del campus de una institución universitaria.

El tráfico de Internet de la institución universitaria tiene cómo objetivo satisfacer los procesos relacionados con los servicios académicos, la investigación y las tareas administrativas.

Los requerimientos de capacidad de acceso a Internet aumentaron y además era necesario optimizar su uso dando prioridad a las actividades ya mencionadas, y restringiendo la navegación a páginas que desperdician este recurso. La óptima gestión del recurso de ancho de banda debía orientarse a la asignación de cuotas, de acuerdo a la importancia de los usuarios. El esquema de seguridad está también asociado a la optimización de este recurso por cuanto cuenta con políticas de seguridad que bloquean tráfico malicioso y también no orientado a las actividades de la universidad.

1.2 Objetivos del trabajo

Diseñar una solución que brinde una óptima seguridad y administración del tráfico WAN del enlace de Internet dedicado, asegurando una alta disponibilidad de la misma.

La solución es lograda mediante la reestructuración de la plataforma de acceso a Internet, la cual debe ser conformada por un equipo de administración de tráfico y un equipo de seguridad (Firewall avanzado), en una topología redundante la cual es optimizada mediante el uso de diversos protocolos de enlaces de comunicación.

1.3 Evaluación del problema

Las actividades de la institución universitaria se pueden dividir en Tareas administrativas, servicios académicos e Investigación, en las cuales se consideran diversas áreas, entre las cuales se pueden mencionar a: Autoridades, áreas de soporte administrativo, Biblioteca Central, Facultades, etc.

Todas ellas deben hacer uso del tráfico de Internet para las tareas relacionadas a su gestión, por lo que un uso inapropiado es considerado un desperdicio del ancho de banda digital (cantidad de datos que se pueden transmitir por segundo). Además cada área tiene su propio requerimiento de navegación, es decir que si no existe una administración de este recurso, todas las áreas estarían compitiendo sin restricción.

Previa a la solución implantada, la universidad contaba con un máximo de 50 Mbps los cuales no eran administrados. Esto hacía que los usuarios apreciaran la lentitud de sus servicios, por ello se vio que era necesaria, no sólo aumentar la capacidad de tráfico de Internet, sino también asignar cuotas y prioridades de acuerdo a la función de cada usuario. Se consideraba también establecer una reserva suficiente para situaciones especiales (eventos, video conferencias) y crecimiento futuro (red inalámbrica, aumento de usuarios).

Cómo ejemplo del mal uso de la capacidad de acceso a Internet se puede mencionar que durante la etapa de prueba de los 200 Mbps (sin políticas ni cuotas de restricción aplicadas) un día feriado los alumnos residentes coparon el ancho de banda digital con trafico de Internet ajena a las actividades especificadas, es decir You Tube, descarga de películas y series televisivas, y otras de similar índole.

Los argumentos mencionados justificaban pues la mejora de los servicios mediante la aplicación de una nueva plataforma que, como ya fue mencionada, debía optimizar el recurso de ancho de banda digital.

1.4 Alcance del trabajo

El proyecto de proveer una solución de seguridad y administración de tráfico de Internet para un campus universitario es desarrollado teniendo en consideración tres aspectos esenciales, especificados en los términos de referencia provistos por la universidad:

- Los requerimientos técnicos que parten de las necesidades de la Universidad.- La universidad presenta especificaciones técnicas que el proveedor debe asegurar cumplir.
- Los requerimientos de Tiempo.- Estos fueron fijados a 180 días.
- Los requerimientos económicos.- Fijados en el monto del contrato y el plazo de servicio.

Estos tres aspectos sirven para el dimensionamiento de la solución, no solo para el cumplimiento de los requerimientos técnicos o para la adquisición y configuración de los equipos, sino también en el enfoque de rentabilidad del proveedor, el cual será detallado en el presente informe.

Como fue mencionado, el objetivo del diseño presentado en este informe, se enfoca en la ingeniería de networking, es decir, en la reestructuración de la plataforma de acceso a Internet lo cual involucra la definición de la topología, el análisis de costos y desempeño

de los equipos de administración de tráfico y de seguridad, con el propósito de optimizar los recursos del proyecto, el diseño incluye la configuración de los equipos con los respectivos protocolos de enlaces de comunicación.

El informe solo incluirá una descripción resumida de los enlaces de fibra óptica de última milla, desde los nodos del Proveedor hasta el Centro de Datos de la Universidad, dado que el objetivo del informe no es el diseño de planta externa.

1.5 Síntesis del trabajo

Para la solución serán analizados previamente todos los requerimientos del cliente, tanto en el aspecto técnico, de tiempo y económico. De este análisis se determinará la plataforma necesaria y su configuración (alta disponibilidad, protocolos, etc.).

La selección del equipamiento de la plataforma será la conclusión de un análisis comparativo de las tecnologías, capacidades funcionales, experiencia de implementación, costos y tiempo de entrega en almacén local, provisto por los principales fabricantes que abastecen el mercado mundial.

Se explicará la nueva topología; en cuanto a la administración del tráfico de Internet se precisará la asignación de cuotas y prioridades; respecto a la seguridad, se explicará los filtros aplicados (restricción de navegación, eliminación de vulnerabilidades, etc.), y finalmente se hará una descripción técnica del equipamiento utilizado.

En un capítulo final, se explican los aspectos relacionados a la gestión de tiempo, a los costos del proyecto, también se presentan las pruebas realizadas a la solución implementada y el análisis de disponibilidad de la solución.

Previo al diseño de la solución, se desarrollarán los aspectos conceptuales relacionados directamente (Marco Teórico), el cual está conformado de la siguiente manera:

1. Internet.- Tipo de tráfico (http, ftp, video streaming, etc.), priorización y administración de tráfico.
2. Seguridad.- Amenazas, técnicas de seguridad (Firewall, UTM.)
3. Dispositivos de Red.- Router, Switches.
4. Protocolos de red: HSRP, BGP, STP, etc.
5. Disponibilidad.
6. Nodos de Acceso y Última Milla.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del trabajo desarrollado en el presente informe. Los temas a tratar son:

- Internet.- Tipo de tráfico (http, ftp, video streaming, etc.), priorización y administración de tráfico.
- Seguridad.- Amenazas, técnicas de seguridad (Firewall, UTM.)
- Dispositivos de Red.- Router, Switches.
- Protocolos de enlaces.- HSRP, BGP, STP, etc.
- Disponibilidad.
- Nodos de acceso y última milla.

2.1 Internet

Internet es una red de computadoras que interconecta cientos de millones de dispositivos informáticos a lo largo de todo el mundo [1]. Las computadoras y el resto de dispositivos conectados a Internet a menudo se designan como sistemas terminales porque se sitúan en la frontera de Internet.

2.1.1 Generalidades

Entre los sistemas terminales de Internet se incluyen las computadoras de escritorio (por ejemplo, PC de escritorio, computadoras Mac y equipos Linux), servidores (por ejemplo, servidores web y de correo electrónico) y equipos móviles (por ejemplo, computadoras portátiles, dispositivos PDA y teléfonos con conexiones a Internet). Además una cantidad creciente de dispositivos alternativos están conectándose a Internet como sistemas terminales (por ejemplo, consolas de juegos, cámaras web, electrodomésticos y dispositivos de seguridad).

Los sistemas terminales se conectan entre sí mediante una red de enlaces de comunicaciones y dispositivos de conmutación de paquetes. Existen muchos tipos de enlaces de comunicaciones, los cuales están compuestos por diferentes tipos de medios físicos, entre los que se incluyen el cable coaxial, el hilo de cobre, la fibra óptica y el espectro radioeléctrico (comúnmente conocido como inalámbrico).

Los distintos enlaces pueden transmitir los datos a distintas velocidades; la velocidad de transmisión de un enlace se mide en bits/segundo. Cuando un sistema terminal tiene que enviar datos a otro sistema terminal, el emisor segmenta los datos y añade bits de

cabecera a cada segmento. Los paquetes de información resultantes se envían a través de la red hasta el sistema terminal receptor, donde vuelven a ser ensamblados para obtener los datos originales.

2.1.2 Dispositivos de conmutación

Los dispositivos de conmutación de paquetes se suministran en muchas formas y modelos, pero los dos tipos más utilizados actualmente en Internet son los routers de la capa de red y los switches de la capa de enlace. Ambos tipos reenvían los paquetes hacia sus destinos finales.

Los switches de capa de enlace normalmente se emplean en las redes de acceso, mientras que los routers suelen utilizarse en el núcleo de la red; este última determina la ruta que tomará el paquete para llegar al siguiente destino. La "ruta" es definida como la secuencia de enlaces de comunicaciones y conmutadores que atraviesa un paquete desde el sistema terminal emisor hasta el sistema terminal receptor.

Los sistemas terminales acceden a Internet a través de los ISP (Internet Service Provider, Proveedor de Servicios de Internet). Cada ISP es en sí mismo una red de conmutadores de paquetes y enlaces de comunicaciones. Los ISP también proporcionan acceso a Internet a los proveedores de contenido, conectando sitios web directamente a Internet. Dado que Internet es todo lo que conecta a los sistemas terminales entre sí, es que los ISP que proporcionan el acceso a los sistemas terminales también tienen que estar interconectados entre ellos.

2.1.3 Definición de protocolo de comunicación

La Internet tiene por finalidad crear comunicación estandarizada entre equipos. Los equipos se comunican al intercambiar mensajes. El intercambio de mensajes de Internet se apoya en un mecanismo llamado protocolo.

Los protocolos son reglas muy detalladas que explican exactamente cómo intercambiar un conjunto particular de mensajes [2]. El formato del protocolo limita la información que el protocolo puede expresar. Los protocolos a usar en la solución son desarrollados en una sección aparte (2.4).

Los sistemas terminales, los conmutadores de paquetes y otros dispositivos de Internet ejecutan protocolos que controlan el envío y la recepción de la información dentro de Internet. El protocolo TCP (Transmission Control Protocol, Protocolo de control de transmisión) y el protocolo IP (Internet Protocol, Protocolo de Internet) son dos de los protocolos más importantes de Internet.

El protocolo IP especifica el formato de los paquetes que se envían y reciben entre los routers y los sistemas terminales. Los principales protocolos de Internet se conocen colectivamente como protocolos TCP/IP.

2.1.4 Aplicaciones de red

La Web, el correo electrónico, la transferencia de archivos, las sesiones remotas, los grupos de noticias y muchas otras aplicaciones populares adoptan el modelo Cliente-Servidor [3].

Un programa cliente es un programa que se ejecuta en un sistema terminal que solicita y recibe un servicio de un programa servidor que se ejecuta en otro sistema terminal. El servidor recibe las peticiones de muchos clientes y les da el servicio respectivo. Los servidores suelen ser equipos más potentes que almacenan y distribuyen páginas web, flujos de videos, correo electrónico, etc. La Figura 2.1 ilustra el modelo cliente-servidor.

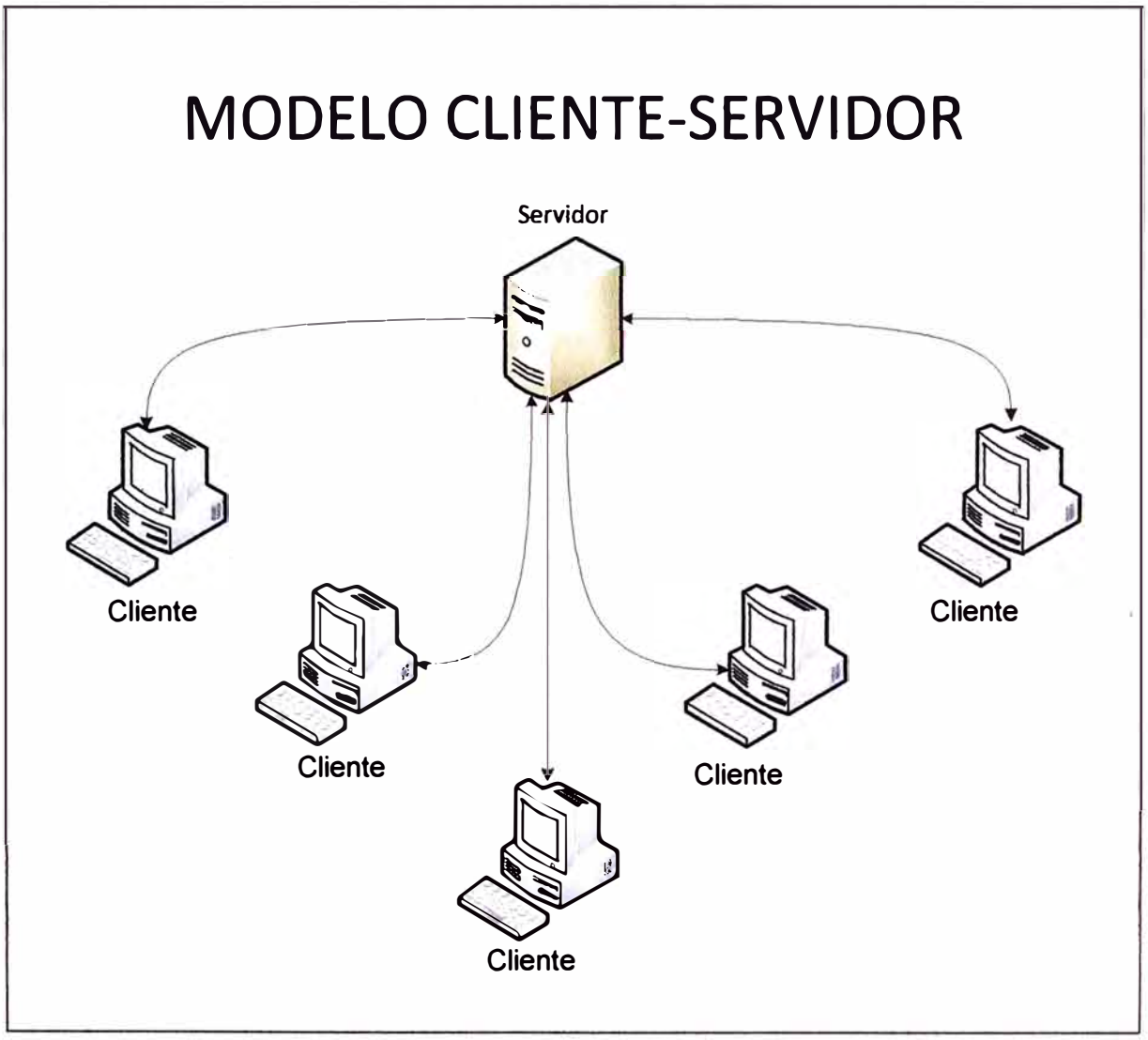

Figura 2.1 Modelo Cliente-Servidor

Internet es una infraestructura que proporciona servicios a las aplicaciones. Entre las aplicaciones se incluyen el correo electrónico, la navegación web, la mensajería instantánea, Voz sobre IP (VoIP), la radio por internet, los flujos de video, los juegos distribuidos, P2P o compartición de archivos en redes entre pares (Peer-to-peer), la

televisión a través de Internet, las sesiones remotas y otras muchas.

No todas las aplicaciones de Internet actuales están constituidas por programas cliente puros que interactúan con programas servidor puros. Cada vez más aplicaciones son entre iguales o entre pares (P2P), en las que los sistemas terminales interactúan y ejecutan programas que realizan tanto funciones de cliente como de servidor. Por ejemplo, en las aplicaciones P2P (como BitTorrent y Emule), y la telefonía por Internet.

A continuación se describirá las aplicaciones de red más comunes que son las que constituyen la mayor parte del tráfico de datos.

a. La Web y HTTP

La Web opera bajo demanda. Los usuarios reciben lo que desean y cuando lo desean. Los hipervínculos y motores de búsqueda ayudan a navegar a través de la inmensa cantidad de sitios web. Los formularios, los programas incrustados en una página web (applets de Java) y muchos otros permiten interactuar con las páginas y sitios.

Nota: Applet es un componente de una aplicación que se ejecuta en el contexto de otro programa.

El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo de la capa de aplicación de la Web y se encuentra en el corazón de la Web. HTTP se implementa en dos programas: un programa cliente y un programa servidor.

HTTP define como los clientes web solicitan páginas web a los servidores web y como estos servidores transfieren esas páginas web a los clientes.

b. Transferencia de archivos

FTP (File Transfer Protocol) es el protocolo de transferencia de archivos. En una sesión FTP típica, el usuario está sentado frente a un host (el host local) y desea transferir archivos a o desde un host remoto. Para que el usuario pueda acceder a la cuenta remota, debe proporcionar una identificación de usuario y una contraseña. Una vez proporcionada esta información de autorización, el usuario puede transferir archivos desde el sistema de archivos local al sistema de archivos remoto, y viceversa.

FTP utiliza dos conexiones TCP paralelas para transferir un archivo, una conexión de control y una conexión de datos. La conexión de control se emplea para enviar información de control entre los dos host, como la identificación del usuario, la contraseña, comandos para modificar el directorio remoto y comandos para "introducir" (PUT) y "extraer" (GET) archivos. La conexión de datos se utiliza para enviar un archivo.

c. Flujos de audio y video almacenado

En los últimos años, la transmisión de flujo de audio y de video se ha convertido en una aplicación popular, además de ser un consumidor importante de ancho de banda de red. En estas aplicaciones, el cliente solicita archivos comprimidos de audio/video que

residen en servidores.

Una vez recibida la solicitud del cliente, el servidor envía un archivo de audio/video al cliente pasando el archivo a un socket. El socket es una representación abstracta del extremo o endpoint en un proceso de comunicación; sirve como punto de acceso que una aplicación puede crear para acceder a los servicios de comunicación que ofrecen las pilas de protocolos.

Hoy día la mayor parte del tráfico de flujos de audio/video es transportado por TCP por tener un servicio de entrega fiable (se comprueba la entrega de los paquetes).

Como ejemplo de este tipo de flujo se puede mencionar a YouTube, CNN, Microsoft Video, y otros servidores de audio/video que emulan estos servicios. Las diversas páginas web complementan su información con este recurso multimedia, es decir, le añaden audio y video a la información textual.

d. Flujos de audio y video en vivo

A diferencia del flujo anterior que se encuentra almacenado y pregrabado en un servidor y al que se accede por demanda, incluso a cualquier parte del archivo que se encuentra reproduciendo, el flujo de audio y video en vivo es reproducido tan pronto como es generado [4].

Este tipo de aplicaciones es similar a la difusión tradicional de radio y televisión, excepto porque la transmisión tiene lugar a través de Internet. Estas aplicaciones se conocen como IPTV y radio por Internet.

Ejemplos de estas aplicaciones se están dando actualmente en Perú, las radios locales transmiten su programación sin restricciones, mientras que algunas televisoras lo realizan mediante un pago. Sin embargo varias instituciones vienen implementando esta aplicación para la transmisión en vivo de sus eventos, por ejemplo el Colegio de Ingenieros (Figura 2.2)

Figura 2.2 Canal de IPTV del CIP Lima

e. Audio y video interactivo en tiempo real

Este tipo de aplicaciones permite a los usuarios emplear el audio y el video para comunicarse entre si en tiempo real.

El audio interactivo en tiempo real a través de Internet suele referirse como telefonía por Internet ya que, desde la perspectiva del usuario, es similar al servicio de telefonía de conmutación de servicios tradicional, con la diferencia mucho menor en el precio de la llamada e incluso sin costo alguno. Como ejemplo se puede mencionar a Skype donde un usuario puede realizar llamadas de voz PC a teléfono así como de PC a PC.

Con el video interactivo en tiempo real, también denominado video conferencia, los individuos pueden comunicarse de forma visual y oral. Como ejemplo de estas aplicaciones se puede mencionar a NetMeeting de Microsoft, Video Skype, etc.

2.1.5 Administración y priorización de tráfico

En esta sección se analiza la administración y priorización de tráfico de manera separada.

a. Administración de tráfico

La administración de tráfico es un conjunto de técnicas que tiene por finalidad asegurar la protección a servicios críticos a través de políticas de control de QoS (calidad de servicio) definidas por el usuario y soportada tecnológicamente por la inspección profunda de paquetes (Deep Packet Inspection: DPI).

Las técnicas más comunes son la priorización del tráfico crítico, la limitación del número de conexiones y la asignación de cuotas de ancho de banda mínimo y máximo por aplicación o por usuario.

Dentro de las organizaciones, la gran mayoría de su ancho de banda está ocupado por tráfico que no está directamente relacionado con la operación del negocio, por lo tanto las aplicaciones críticas tienen que sobrevivir en un ambiente de red caótico. Estas circunstancias conducen a un uso inadecuado del ancho de banda que a su vez implican un desperdicio de recursos muy valiosos. Por lo tanto la administración de este recurso es un factor crucial para reducir costos y aumentar la productividad.

b. Priorización del tráfico de aplicaciones

Los dispositivos de administración inteligente del tráfico de red, utilizan la tecnología DPI para intervenir en el tráfico a nivel de aplicaciones (Capa 7) reconociendo en forma automática las aplicaciones de capa 7 e iniciando una categorización automática del tráfico.

Esto permite al administrador de red poder verificar el uso de los recursos por cada aplicación y priorizar los diferentes tipos de tráficos: recreacional, críticos, trafico de aplicaciones de clientes, etc.

2.2 Amenazas y técnicas de seguridad

Internet es inherentemente inseguro debido a que es una red abierta. Las amenazas a la seguridad de red son devastadoras para cualquier empresa. La Internet está plagada de amenazas. Los hackers, crackers, saboteadores y otros personajes atacan a la red y sus usuarios en cada oportunidad. Las amenazas incluyen la intrusión en el sistema, el acceso no autorizado a datos, sabotaje del sistema, la siembra de virus, robo de datos, el robo de números de tarjetas de crédito y robo de contraseñas [5].

En la actualidad existen una serie de opciones para mitigar estas amenazas, que incluyen el cifrado o encriptación de mensajes, la autenticación y la autorización.

Los Firewalls o Cortafuegos, incorporan gran parte de lo anterior, y recientemente han ganado el centro de atención en términos de un mecanismo de defensa.

2.2.1 Encriptación o cifrado

El cifrado consiste en codificar y comprimir los datos antes de la transmisión, en el dispositivo de recepción se proporciona la lógica necesaria en forma de una clave para descifrar la información transmitida. La lógica de cifrado en general reside en el firmware incluido en los dispositivos stand-alone (autónomos), aunque puede ser integrado virtualmente en cualquier dispositivo. Esa lógica ahora se incorpora en los routers, que puede cifrar/descifrar los datos, paquete por paquete.

El cifrado viene en dos formas básicas:

- Privada.- cifrado de clave, también conocido como cifrado de clave única o clave secreta, se utiliza la misma clave para encriptación (codificación) y para el descifrado (decodificación). Este enfoque requiere que la clave se mantenga en secreto a través de algún tipo de transmisión segura de claves antes de la transferencia de datos.
- Público.- cifrado de clave, consiste en la clave de cifrado RSA que puede ser utilizado por todos los usuarios autorizados de la red. La clave de descifrado se mantiene en secreto. El cifrado de clave público es mucho más lento que el de clave privada, pero la difusión de la llave se lleva a cabo mucho más rápidamente. El cifrado de clave público está disponible libremente en Internet.

2.2.2 Autenticación

La autenticación proporciona un medio por el cual los administradores de red pueden confirmar la identidad de las personas tratando de acceder a los recursos informáticos y los datos de la casa de ellos. La autenticación consiste en la protección por contraseña y tokens (fichas) inteligentes.

- La protección por contraseña se impone para restricciones individuales dentro de un sitio, host, aplicación, pantalla y a nivel de campo. Es recomendable que las contraseñas sean de larga longitud, alfanuméricos en naturaleza, y que se cambien periódicamente.

Existe una tendencia actual hacia el uso de servidores dedicados de contraseñas para la administración de ellas.

- El Protocolo de autenticación de contraseña (PAP) es un mecanismo de uso general para la protección de contraseña en apoyo de los usuarios remotos. Mientras PAP es fácil de usar, las contraseñas normalmente se envían al servidor de acceso remoto (RAS) en texto plano (es decir, sin cifrar).
- Los tokens ó fichas inteligentes son dispositivos de hardware que generan, cada vez que es usado, una contraseña para ser verificada por un servidor seguro. A menudo trabajan de forma engorrosa con un mecanismo de desafío-respuesta. El Protocolo de autenticación por desafío mutuo (CHAP) es un ejemplo de este enfoque mejorado. CHAP implica los servidores de acceso remoto (RAS) desafiando al usuario remoto con un número aleatorio. El usuario responde con un *digest*, que es una contraseña de cifrado basado en el desafío de números aleatorios. El servidor de acceso remoto (RAS) entonces descifra la contraseña con la misma clave de números aleatorios para verificar la identidad del usuario remoto.

2.2.3 Autorización

La autorización proporciona un medio para controlar cuales de los usuarios legítimos tienen acceso a ciertos recursos. Autorización implica un software complejo que se encuentra en todos los equipos asegurados en la red; idealmente, este ofrece la capacidad de un único inicio de sesión. Los sistemas de autorización comúnmente usados en apoyo a la seguridad de Internet incluyen Kerberos, Sesame, y Access Manager.

2.2.4 Firewalls o cortafuegos

Los Firewalls o cortafuegos (Figura 2.3) son dispositivos físicos y/o lógicos que permiten bloquear el acceso a entidades no autorizadas mediante el uso de políticas previamente configuradas vía web o mediante una interfaz de comandos.

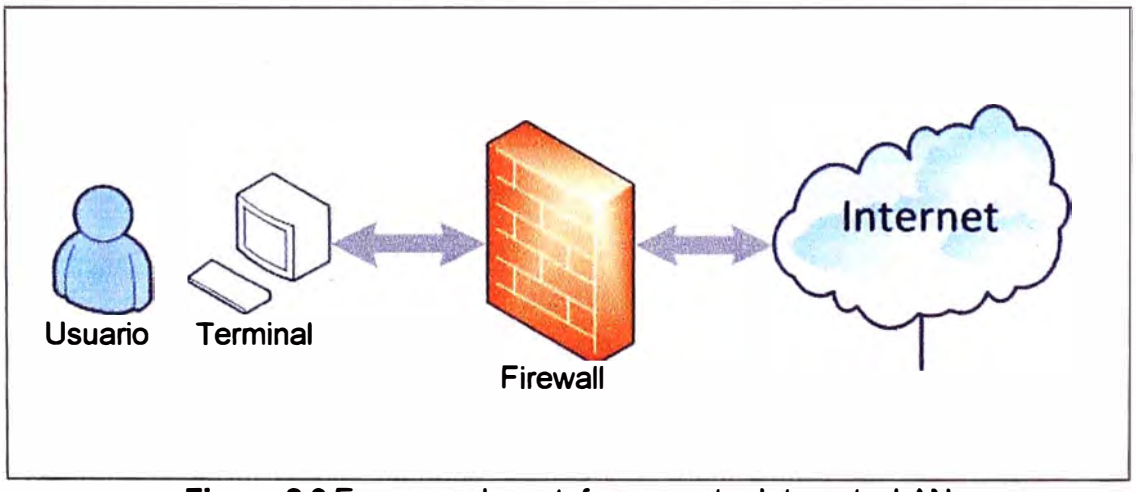

Figura 2.3 Esquema de cortafuegos entre Internet y LAN

Los cortafuegos funcionan principalmente mediante tres métodos fundamentales:

- Paquet Filtering ó Filtrado de Paquetes.- Rechaza los paquetes TCP / IP de los hosts no autorizados y rechazar los intentos de conexión a servicios no autorizados.
- Network Translation (NAT).- Traduce las direcciones IP de los hosts internos para esconderlos del monitoreo externo. También es denominado "enmascaramiento IP".
- Proxy Services Address ó servicios de proxy.- Hace las conexiones de aplicaciones de alto nivel en nombre de los host internos con el fin de romper por completo con las conexiones en capa de red entre los hosts internos y externos.

La mayoría de firewalls también llevan a cabo otros dos servicios de seguridad importantes:

- **Cifrado de autenticación**.- Permite a los usuarios de la red pública probar su identidad con el firewall, con el fin de obtener acceso a la red privada desde distintos puntos del exterior.
- **Red privada virtual (VPN)**.- Establece una conexión segura entre dos redes privadas en un medio público como Internet. Esto permite separar físicamente las redes y utilizar el Internet en lugar de arrendar líneas dedicadas para comunicarse. Las VPNs son también llamadas encrypted tunnels ó túneles cifrados.

Algunos firewall también ofrecen servicios adicionales de suscripción que no están estrictamente relacionados con la seguridad, pero que muchos usuarios encontrarán útil:

- **Virus Scanning**.- Búsquedas en los flujos de datos entrantes por las firmas de virus. Mantenerse al día con las firmas de virus actuales requiere una suscripción al servicio de actualización de virus proporcionadas por el proveedor del firewall.
- **Content Filtering ó Filtrado de contenidos**.- permite bloquear que los usuarios internos accedan a ciertos tipos de contenido por categorías, tales como la pornografía, información de hacking, ocio, etc. Mantenerse al día con la lista actualizada de sitios bloqueados para una categoría específica también requiere una suscripción.

2.2.5 Dispositivos de seguridad UTM

Los productos que brindan soluciones de seguridad para fines específicos están limitados debido a que:

- La nueva generación de ataques y amenazas combinadas utiliza una multiplicidad de vectores de ataque,
- Contar con una configuración de productos de función única es costoso y requiere de mucha experiencia para implementarla, mantenerla y administrarla.

Debido a estos motivos, recientemente ha aparecido una nueva gama de dispositivos denominados Unified Threat Management (Gestión Unificada de Amenazas) que integran múltiples capacidades de seguridad en un único producto, incluidas las de firewall,

detección y prevención de intrusiones (IDP), antivirus, anti-spam, filtro de URLs, VPN y SSLVPN, entre otros (Figura 2.4)

La consultora IDC define a los appliances de seguridad de Gestión Unificada de Amenazas como productos que unifican e integran múltiples características de seguridad integradas en una sola plataforma de hardware. Para que un dispositivo sea incluido dentro de esta categoría requiere contar con capacidades de firewall de red, detección y prevención de intrusiones de red (IDS/IPS) y gateway anti-virus (AV). Todas las capacidades no necesariamente tienen que ser utilizadas, pero estas funciones deben existir intrínsecamente en el dispositivo. En estos productos, los componentes individuales no pueden ser separados.

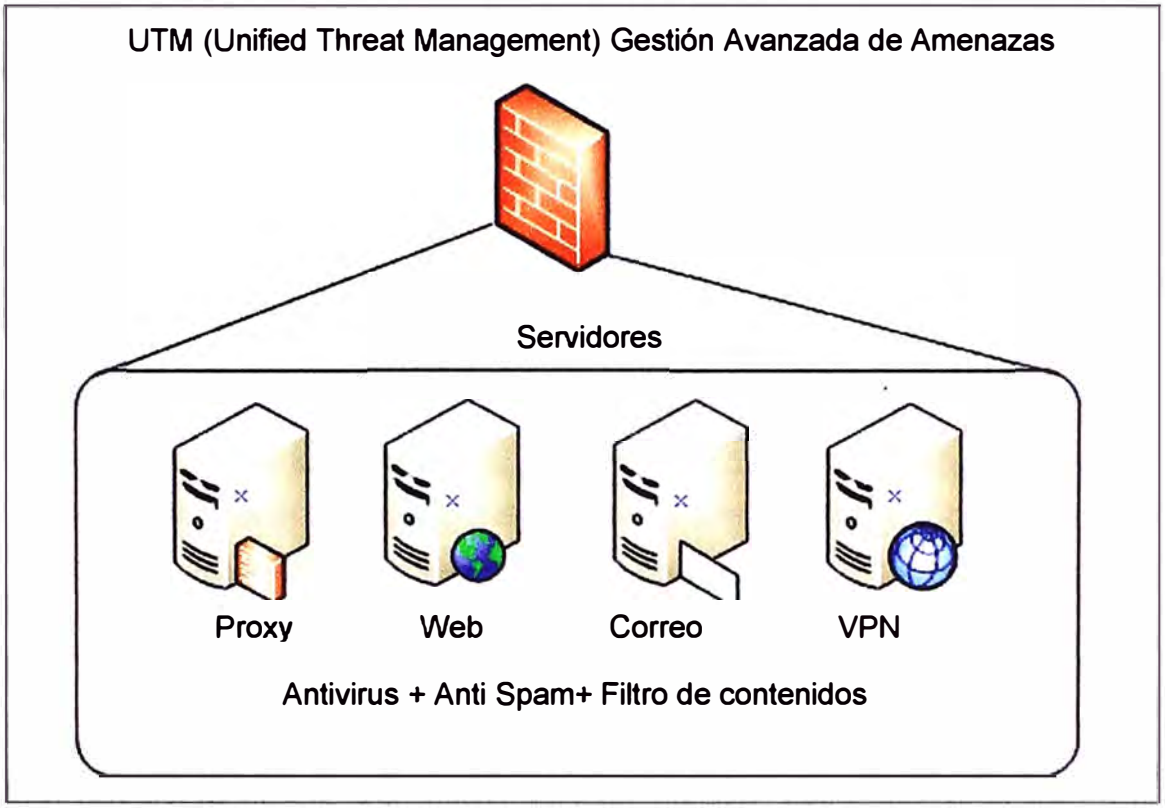

Figura 2.4 Gestión avanzada de amenazas

2.3 Dispositivos de red

En esta sección se describen los aspectos más relevantes de los dispositivos más importantes relacionados a la solución desarrollada en el informe de suficiencia

2.3.1 Switches

Los switches o conmutadores LAN son dispositivos con capacidades básicas de almacenamiento y envío de paquetes que puede soportar múltiples transmisiones simultáneas. Los switches tienen la capacidad de leer las direcciones de destino de los paquetes con la finalidad de remitirlos única y directamente al puerto correspondiente asociado con el dispositivo de destino.

Los switches operan en la capa física (nivel 1) y capa de enlace (nivel 2) del modelo

de referencia OSI. Los switches leen las direcciones de destino de los paquetes, filtran y reenvían según proceda, en base a las direcciones MAC (nivel 2). La lógica del switch es relativamente simple y se presenta en forma de firmware a nivel del chip.

Por lo tanto, los switches son rápidos y relativamente barato. Algunos switches toman decisiones de enrutamiento en base a direcciones IP (nivel 3). La conmutación en nivel 3 incluye una combinación de conmutación y enrutamiento.

2.3.2 Routers

Los routers son dispositivos altamente inteligentes que puede soportar la conectividad entre dos redes de área local y puede proporcionar acceso a diversos tipos de redes WAN, como por ejemplo la IP MPLS.

Los routers son sensibles a los protocolos de las capas superiores, que suelen soportar los protocolos de múltiples capas inferiores y diferentes tamaños de paquetes, como podrían estar involucrados soportando a Ethernet.

Los routers suelen funcionar en la capa física, capa de enlace, y capa de red del modelo OSI para proporcionar conectividad, direccionamiento y conmutación. Los routers también tienen la capacidad de operar en todas las siete capas del modelo de referencia OSI, si son equipados.

2.4 Protocolos

Los protocolos son esenciales para un desempeño óptimo de la red de datos. En esta sección se hace una descripción general de la clasificación y tipos de protocolos existentes, y también se desarrollan con mayor detalle los protocolos involucrados en la solución desarrollada en el presente informe.

2.4.1 Clasificación de los protocolos

Los protocolos de comunicación de datos pueden clasificarse [6] en protocolos TCP/IP, protocolos de seguridad de red, protocolos VoIP, además de protocolos orientados a las redes WAN, LAN, MAN y SAN. Esta clasificación es desarrollada a continuación:

- **TCP/IP**.- Relacionados con el tráfico de Internet. Estos protocolos a su vez se agrupan según la capa OSI en donde se aplican, es decir: Aplicación, Presentación, Sesión, Transporte, red y capa de enlace de datos.
- **De seguridad de red**.- Orientada a brindar seguridad en el tráfico de datos, asegurando la adecuada identificación de los usuarios y de las aplicaciones que se estén ejecutando así como de los paquetes de datos. Se agrupan en : protocolos AAA (Authentication, Authorization, Accounting), protocolos tunneling, protocolos de enrutamiento seguro
- **VoIP**.- Para permitir aplicaciones de voz en la red de datos, se agrupan en: protocolos

de señalización (H.323, H.225, etc.) y los protocolos de Media/Codec (compresión, transporte, etc.)

- **WAN**.- Orientados a su uso en las redes de área extendida (amplia), se agrupan en: Protocolos ATM (Asynchronous Transfer Mode), protocolos de acceso de banda ancha (ISDN-Integrated Services Digital Network, DOCSIS-Data Over Cable Service Interface Specification, etc.) y finalmente protocolos punto a punto (PPP-Point to Point, LCP-Link Control Protocol, etc.).
- **LAN**.- Orientados a las redes de area local; se agrupan en protocolos Ethernet, protocolos de LAN Virtuales (VLAN), protocolos de LAN inalámbrica.
- **MAN**.- Una clasificación especial para las redes de área metropolitana; en esta clase existen los siguientes protocolos: DQDB (Distributed Queue Dual Bus) la cual es definida en el estándar IEEE 802.6, SMASH (Switched Multimegabit Data Service), y finalmente WiMAX (Worldwide Interoperability for Microwave Access) o IEEE 802.16.
- **SAN**.- son los protocolos utilizados en las redes de almacenamiento. Entre estas se pude mencionar a: FCIP (Fibre Channel over TCP/IP), NDMP (Network Data Management Protocol), entre otros protocolos.

También existen los protocolos propietarios, los cuales podrían caer dentro de las clasificaciones antes mencionadas. Entre los protocolos propietarios se encuentran los siguientes:

- **CISCO**.- entre los cuales se puede mencionar al EIGRP (Enhanced Interior Gateway Routing Protocol), al HSRP (Hot Standby Router Protocol), al VTP (Cisco VLAN Trunking Protocol).
- **Novell NetWare**.- Por ejemplo el IPX (Internetwork Packet Exchange Protocol) y el NCP (NetWare Core Protocol,), entre otros.
- **IBM Systems Network Architecture (SNA)**.- Se tiene al NetBIOS (Network Basic Input Output System), y al SDLC (Synchronous Data Link Control), como ejemplos de protocolos IBM.;
- **SS7/C7 (Signalling System #7 para telefonía)**.- entre los cuales destacan el TCAP (Transaction Capabilities Application Part), el MAP (Mobile Application Part), etc.
- **Apple Talk (Apple Computer Protocols Suite)**.- Estos protocolos se distribuyen en las capas OSI,, por ejemplo en la capa de enlace está el LLAP (LocalTalk Link Access Protocol), en la de red está el DDP (Datagram Delivery Protocol), en la de transporte el ATP (AppleTalk Transaction Protocol); en sesión el ASP (AppleTalk Session Protocol), y en presentación el AFP (AppleTalk Filing Protocol)
- **DECnet**.- Del mismo modo que en Apple se tienen diversos protocolos según las capas del modelo OSI: enlace de datos al MOP(Maintenance Operation Protocol), en red a DRP

(DECnet Routing Protocol), en transporte a NSP (Network Service Protocol); en sesión a SCP (Session Control Protocol), en presentación DAP (Data Access Protocol).

2.4.2 Protocolo BGP

El protocolo BGP/BGP4 (Border Gateway Protocol) es un protocolo de enrutamiento entre sistemas autónomos (AS) [7]. La principal función de un sistema BGP es el intercambio de información de accesibilidad de la red entre sistemas BGP.

Esta información de accesibilidad de la red incluye información sobre la lista de Sistemas Autónomos (AS) que intercambian información de accesibilidad. Esta información es suficiente para construir un gráfico de conectividad de los sistemas autónomos con el cual los bucles de enrutamiento pueden ser eliminados y algunas políticas a nivel sistemas autónomos pueden ser aplicadas.

Un sistema autónomo es un conjunto de redes administradas por una misma organización que tiene definida una única política de enrutamiento. Esta política de enrutamiento decide las rutas admitidas desde los sistemas autónomos vecinos y las rutas que se envían hacia estos sistemas autónomos. En su interior, el AS utiliza un protocolo interno de enrutamiento como, por ejemplo, OSPF. El protocolo BGP un protocolo de enrutamiento entre sistemas autónomos.

Cada sistema autónomo en Internet tiene un identificador (ASN) formado por 16 bits, lo que permitiría hasta 65536 sistemas autónomos teóricos diferentes, si bien el rango de 64512 a 65535 se encuentra reservado para uso privado [8].

Existen dos tipos de protocolos BGP, según la "relación" que mantengan con otros routers que ejecutan BGP, estos son: Internal BGP (iBGP) y External BGP (eBGP).

- iBGP es cuando un router que ejecuta BGP es vecino de otro router BGP en el mismo sistema autónomo.
- eBGP es cuando un router BGP es un vecino BGP en otro sistema autónomo.

2.4.3 Protocolo VTP

VLAN Trunking Protocol (VTP) de Cisco [9] es un protocolo de Capa 2 que gestiona la incorporación, eliminación y cambio de nombre de VLAN en la red.

El protocolo VTP reduce la administración en una red conmutada. Al configurar una nueva VLAN en un servidor VTP, la VLAN se distribuye a través de todos los switches en el dominio. Esto reduce la necesidad de configurar el mismo VLAN en todas partes.

VTP es un protocolo propietario de Cisco que se encuentra disponible en la mayoría de los productos Cisco de la familia Catalyst.

2.4.4 Protocolo STP

Spanning-Tree Protocol (STP) tal como se define en el estándar IEEE 802.1D [10], es un protocolo de gestión de enlace que garantiza que la topología de una red esté libre de

bucles indeseables. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones).

2.5 Disponibilidad

En esta sección se desarrolla el concepto de disponibilidad y como este es evaluado

2.5.1 Definición

La disponibilidad es el porcentaje de tiempo que un sistema o servicio (por ejemplo red, componente de red o una aplicación) se encuentran disponibles para un usuario [11].

Para medir la disponibilidad se deben definir antes los siguientes parámetros:

TBF: Tiempo entre fallos (Time Before Failure)

TTR: Tiempo de reparación. (Time to Restore)

MTBF: Tiempo medio entre fallos. (Mean Time Before Failure)

MTTR: Tiempo medio de reparación (Mean Time to Restore).

La disponibilidad D se define con la fórmula (2.1)

$$D = \frac{MTBF}{MTBF + MTTR} \tag{2.1}$$

Los valores de MTBF que son proporcionados en las hojas técnicas de los dispositivos no son valores prácticos (25,000 a 35,000 horas). Para el cálculo de disponibilidad se recurre a la estadística de su comportamiento.

En el cálculo de disponibilidad no solamente se debe tener en cuenta las fallas sino también las paradas por mantenimiento MTBO (Mean Time Before Outage) y TSR (Time to Service Restoration).

$$D = \frac{MTBO}{MTBO + MTSR} \tag{2.2}$$

En la práctica es considerada la Disponibilidad Operacional, es decir la que incluye todas las fuentes experimentadas del tiempo muerto (MTSR y MTTR). Esto se ilustra con el siguiente ejemplo.

Respecto a la cantidad de eventos de parada se puede asumir:

- Un plan de mantenimiento cada seis meses. Esto implica que habrá cuatro (4) suspensiones de servicio por mantenimiento programados en dos años.
- El MTBF (Tiempo medio entre fallas) es de dos años. Esto es una (1) falla cada dos años.

De lo anterior se resumen que habrá cinco interrupciones del servicio sobre el periodo de dos años. Por lo tanto el tiempo medio entre interrupciones es de 2 años divididos entre 5 (MTBO aproximado de 3500 horas).

Respecto a la duración de los eventos de parada se puede asumir:

- Que el tiempo promedio fuera de servicio por mantenimiento programado es de seis horas (esto es en dos años un total de 24 horas). De manera similar, si el periodo de mantenimiento no programado es de 12 horas, entonces se tendría un tiempo total fuera de servicio de 36 horas durante los dos años. Esto cubre cinco eventos de mantenimiento y por lo tanto, el tiempo medio para la restauración del servicio es de 36 horas divididas entre 5 (MTSR aproximadamente igual a 7 horas).

De los datos calculados se obtiene una disponibilidad (sobre un periodo de dos años) igual a 3500/(3500+7) = 99.8%.

2.5.2 Disponibilidad de un sistema

Depende de la disponibilidad de los componentes y de la disposición de los mismos. Para los sistemas en serie y sistemas en paralelo existe una forma de calcular la disponibilidad total del sistema, en base a la disponibilidad de cada uno de los componentes.

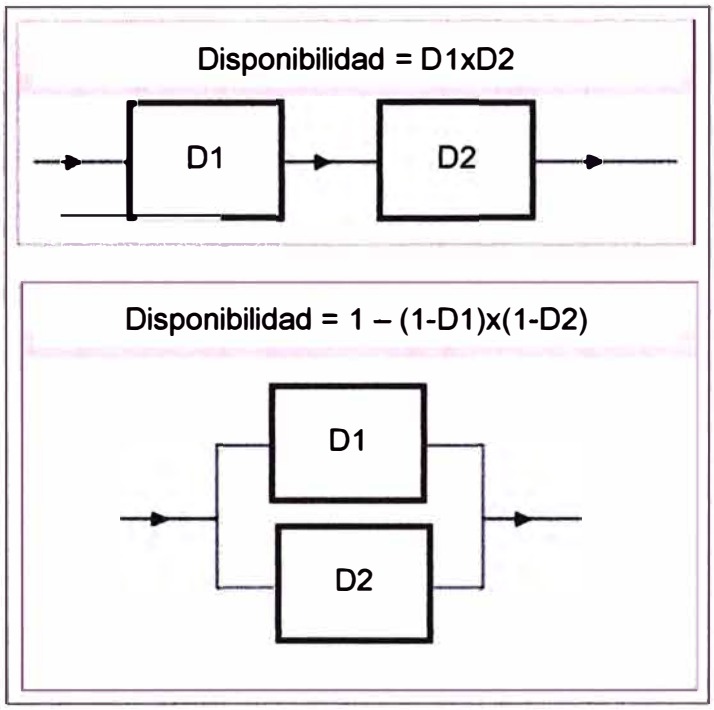

Figura 2.5 Disponibilidad del sistema (A es disponibilidad individual)

Estas configuraciones se resumen con las fórmulas (2.3) y (2.4) respectivamente, para más elementos en línea o más elementos en serie:

$$Ds = \prod_{i=1}^{n} D_i \tag{2.3}$$

$$Ds = 1 - \prod_{i=1}^{n} (1 - D_i) \tag{2.4}$$

Para el caso de estructuras tipo puente (Figura 2.6) se consideran las opciones de ruta de disponibilidad en serie y luego se considera a cada una que se encuentran en paralelo. De ese modo se obtiene una topología que es más sencilla de evaluar.

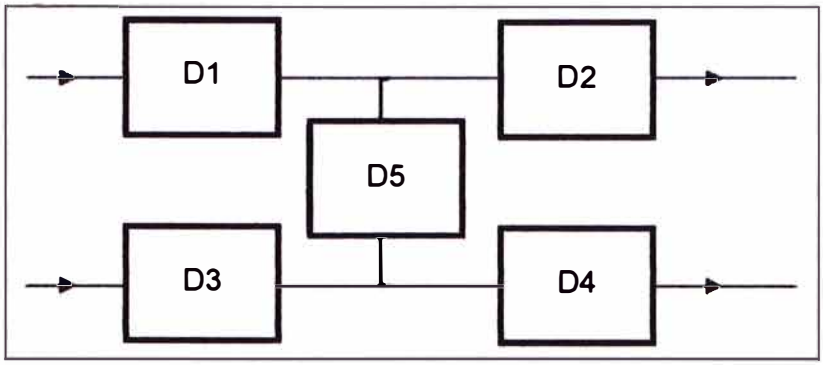

Figura 2.6 Topología tipo puente

Para el caso mostrado en la Figura 2.6, los circuitos serie a considerar son:

- Dserie1=D1 x D2
- Dserie2=D3 x D4
- Dserie3=D1 x D5 x D4
- Dserie4= D3 x D5 x D2

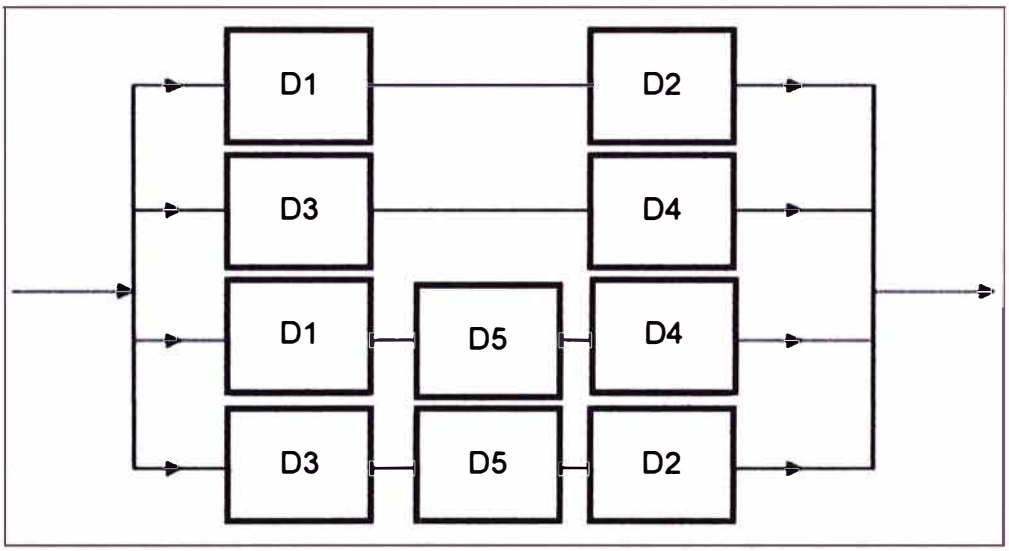

Figura 2.7 Topología equivalente

Aplicando la formula (2.4) la disponibilidad es dada por (2.5):

$$1 - (1\text{-Dserie1}) \times (1\text{-Dserie2}) \times (1\text{-Dserie3}) \times (1\text{-Dserie4}) \qquad (2.5)$$

Reemplazando:

Disponibilidad = 1 - (1-D1 x D2) x (1-D3 x D4) x (1-D1 x D5 x D4) x (1-D3 x D5 x D4)

2.5.3 Redundancia

La redundancia es la existencia de dos o más elementos similares que trabajan en paralelo de manera alternativa. Es decir que si uno falla el otro entra a reemplazarlo. Sin embargo para el análisis de disponibilidad es siempre necesario verificar cuanto mejora la disponibilidad individual al colocar un elemento redundante en paralelo.

Por ejemplo, la disponibilidad de un elemento es D, si se colocará un elemento redúndate (en paralelo), entonces la disponibilidad sería calculada por = 1-(1-D)x(1-D) = Dx(2-D). La Tabla 2.1 ilustra la mejora para un sistema redundante.

Tabla 2.1 Disponibilidad individual y disponibilidad redundante (dos en paralelo)

Disponibilidad individual	Disponibilidad con redundancia
0.9	0.990
0.8	0.960
0.7	0.910
0.6	0.840

La Tabla 2.2 presenta los valores que se obtienen al colocar a la anterior topología un elemento similar adicional (es decir tres en paralelo).

Tabla 2.2 Disponibilidad individual y disponibilidad redundante (tres en paralelo)

Disponibilidad individual	Disponibilidad con redundancia
0.9	0.999
0.8	0.992
0.7	0.973
0.6	0.936

Los valores de disponibilidad colocados no son los que se espera que tenga un elemento del sistema ya que son muy bajos, sin embargo ayudan a visualizar las mejoras al colocar elementos similares de manera redundante.

2.5.4 Conclusiones

De lo explicado, se puede concluir lo siguiente:

- La disponibilidad es el resultado práctico (real) en el que interviene el promedio de paradas en un tiempo determinado y el promedio de tiempo de las paradas (ver ejemplo sección 2.5.1).
- Las hojas técnicas no entregan valores de disponibilidad. Proporcionan valores comerciales (ideales) de MTBF (20,000 a 75,000 horas).
- No existen valores típicos de MTTR (no son proporcionados por ninguna hoja técnica) ya que el tiempo de restauración del servicio (luego de una falla, o de una parada por mantenimiento) dependen de diversos factores, en especial de la capacidad de cada organización para solucionar los problemas presentados (material, experiencia, personal, etc.)
- El modelamiento topológico de la disponibilidad del sistema (ver 2.5.2) es una herramienta que permite comparar alternativas a una solución.
- La introducción de un elemento redundante (ver 2.5.3) mejora notoriamente la disponibilidad.

2.6 Nodos de acceso y última milla

Los Nodos de Acceso son los puntos de acceso a la red del proveedor, permitiendo distribuir los datos por la red del proveedor. Básicamente los nodos de acceso están diseñados y cuentan con la infraestructura necesaria para permitir tres tipos de acceso a la red, ya sea a través de enlaces inalámbricos, por enlaces de cobre o enlaces de fibra

óptica y en algunos de los nodos dos tipos de acceso (cobre y fibra óptica).

El siguiente diagrama (Figura 2.8) describe la infraestructura y equipos existentes en los nodos, que interviene en la creación de accesos de fibra óptica:

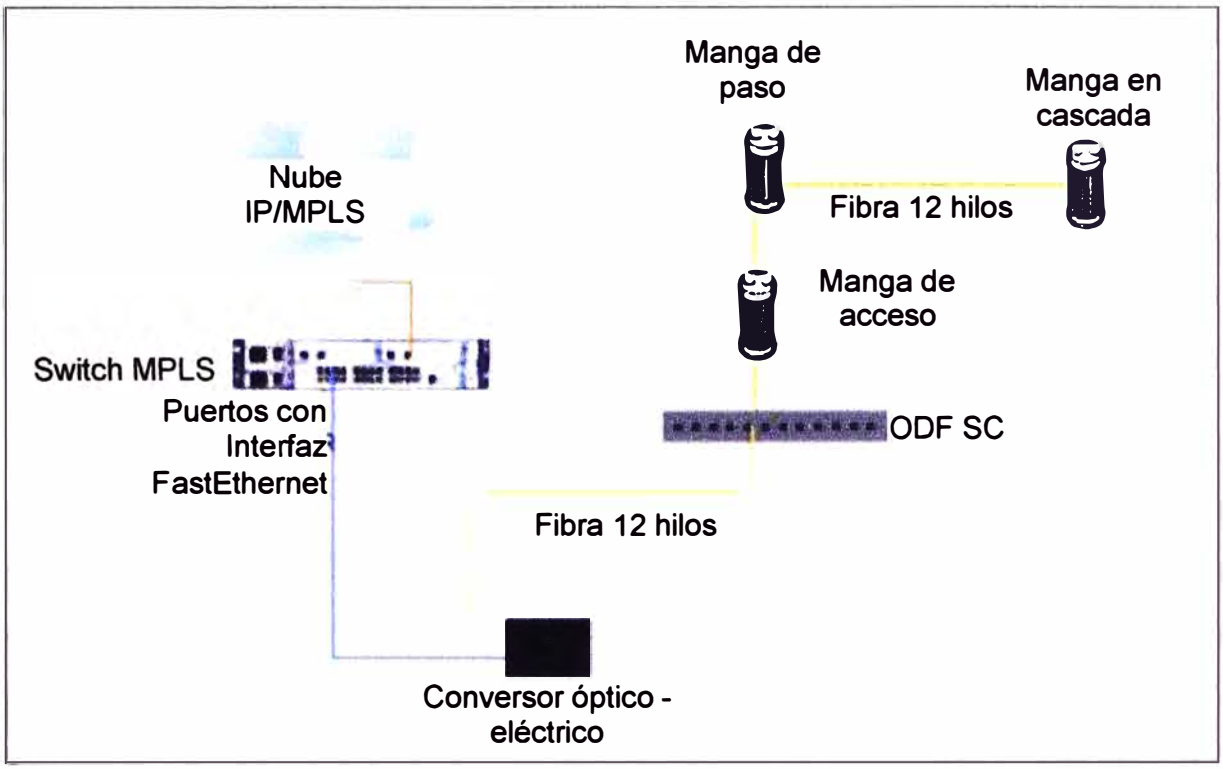

Figura 2.8 Infraestructura de un nodo para acceso por fibra óptica

Un cable de fibra óptica monomodo de doce hilos está fusionado a un ODF (Optical Distribution Frame) con conectores SC en un rack del cuarto de equipos del nodo.

El otro extremo del cable de fibra óptica está fusionado a una manga de acceso, ubicada en lugares específicos de concentración de tráfico o posibles clientes potenciales. Todo el recorrido del cable de fibra hasta la manga de acceso es a través de ductos subterráneos.

En el caso de ser necesario, la fibra recorre a través de mangas de paso, o se crean mangas en cascada fusionando un hilo de esta fibra con otro hilo de una fibra igual de doce hilos para facilitar el acceso de nuevos clientes.

En el cuarto de equipos existen racks tipo gabinetes para la ubicación de los equipos de última milla de los proveedores de este servicio, con escalerillas horizontales para el recorrido de cables y placas de tierra. Un switch MPLS (Multiprotocol Label Switching) con puertos 10/100/1000 Ethernet permite el acceso de los clientes a la red IP/MPLS.

Los equipos existentes en el nodo y los de última milla de los proveedores de servicio son energizados a través de tableros de distribución DC de -48 V o tableros de distribución AC de 220 V.

En los nodos se cuenta con sistemas de respaldo de energía, por medio de generadores y/o UPS con banco de baterías, en caso de falla de la energía comercial.

La última milla es el tramo final que une al usuario final con el nodo de acceso a la red de telecomunicaciones del proveedor y puede estar compuesta por medios alámbricos o hilos (par de cobre, coaxial, fibra óptica) o inalámbricos (microondas, infrarrojos, ondas de radio).

La fibra óptica es el mejor medio de transporte de información ya que está libre de interferencias.

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se describe la ingeniería del proyecto. Preliminarmente se hace el análisis de la solución considerando la situación inicial y los requerimientos de la universidad, luego se describe el sistema implementado.

3.1 Análisis de la solución

En esta sección se expone la situación previa a la solución y los nuevos requerimientos, se evalúan las alternativas de solución y finalmente se hace el dimensionamiento de la solución propuesta.

3.1.1 Descripción situacional y nuevos requerimientos del sistema

En esta subsección se describe la situación que tenía el campus universitario en lo que respecta a su acceso a Internet. Así mismo se exponen los requerimientos planteados por el cliente para la nueva solución a diseñar e implementar.

a. Situación previa a la solución implementada

La Figura 3.1 muestra la topología previa a la solución.

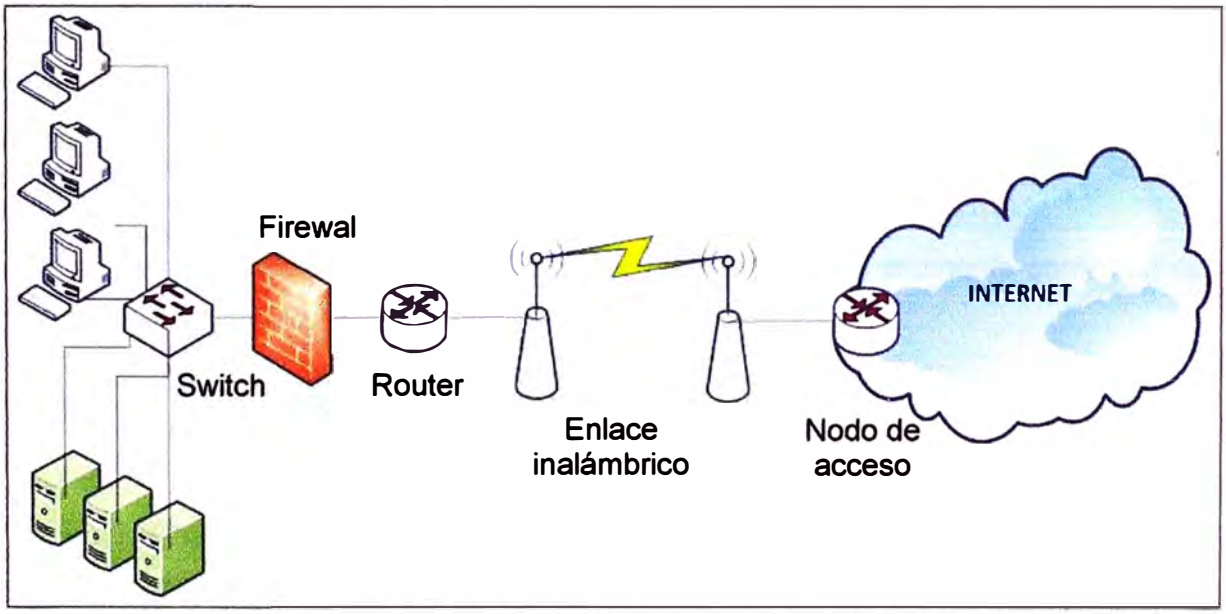

Figura 3.1 Topología previa a la solución

La universidad contaba con un acceso a Internet con capacidad de tráfico de 50 Mbps para abastecer a 3369 usuarios ó terminales (PC's) con salida a la nube de internet. Este tráfico no era administrado, es decir, cualquier usuario o terminal tenía la misma prioridad de acceso lo que producía que las aplicaciones críticas no tuvieran un desempeño

óptimo, además, cualquier usuario tenía capacidad de acceder a cualquier tipo de tráfico, incluso al ajeno a sus funciones específicas.

Este tipo de configuración podría definirse como "anárquico", y en el cual los usuarios apreciaran la lentitud del acceso a Internet.

Dada esta situación, se vio necesario aumentar la capacidad de tráfico de Internet, así como también asignar cuotas y prioridades de acuerdo a la función de cada usuario. También se debía establecer una reserva de capacidad de tráfico suficiente para situaciones especiales:

- Permitir que durante ciertos periodos se asigne recursos a eventos especiales, por ejemplo video conferencias, sin afectar la capacidad de los usuarios existentes
- Crecimiento futuro.- para la implementación de una red inalámbrica y el aumento de usuarios.

b. Requerimientos

Los requerimientos sirven para evaluar y plantear las alternativas de solución, tanto en cuanto a topología como a equipamiento y aplicaciones.

La Universidad planteó ciertos requerimientos que debía cumplir la nueva solución. Estos requerimientos nacen de un análisis que realiza el cliente tomando en cuenta las necesidades y características de su LAN.

La infraestructura a implementarse no es de la propiedad de la Universidad, por lo que la solución, de seguridad y administración de tráfico WAN del enlace de Internet dedicado con alta disponibilidad para un campus universitario, es considerada un servicio de responsabilidad del proveedor.

En conclusión los requerimientos para la nueva solución son los siguientes:

1. Periodo de contratación del servicio: 3 años.
2. Tipo de Servicio: Internet dedicado, carrier class (sistema altamente confiable) con protocolo BGP.
3. Ancho de banda: 200 Mbps garantizado.
4. Direcciones IP públicas: mínimo ciento veintiocho (128).
5. Redundancia: Diversidad de ruta por dos nodos distintos e independientes y llegada a Centro de Datos de la universidad.
6. Disponibilidad: 99.95 % mínima. Equivalente a máximo 4.38 horas/año sin servicio.
7. Firewall en campus que incluya antispam, antivirus, filtro WEB con su respectivo sistema de gestión y reportes.

- Número estimado conexiones concurrentes a Internet: Mínimo de 200,000
- Número estimado de buzones de correo: Mínimo de 15,000
- Número estimado de usuarios que accedan a Internet Mínimo de 3,000

- Throughput (volumen de trabajo) mínimo del firewall: mínimo 2 Gbps
- Número de Interfaces mínimas del firewall: 10 puertos Gigabit
- Manejo de políticas de acceso

8. Políticas de priorización de tráfico saliente y entrante de manera independiente de 7 ò más prioridades.
9. Capacidad de administración de ancho de banda por protocolos, contenidos y evolución de comportamiento de protocolos en el campus.
10. Plataforma de seguridad y administración de tráfico WAN en configuración redundante.
11. Equipos de enrutamiento deben ser de última tecnología, con características superiores a las que van a requerir inicialmente para operación, con la opción de contar con dos equipos, uno activo y otro en reserva o para la operación en HSRP. En tanto garanticen la operación del HSRP para el mejor cumplimiento del SLA, no es excluyente, que dichos equipos (02) de enrutamiento (router) tanto para el enlace principal y backup deban ser de características idénticas y con las mismas funcionalidades.
12. Tiempo de implementación máximo de 180 días calendario.

La Universidad (el cliente) a fin de asegurar el cumplimiento del servicio, añade ciertas condiciones de parte del proveedor, la cual se resume en lo siguiente:

- Ser miembro del NAP (Network Access Point) Perú y con conexión de capacidad mínima de 100 Mbps
- Brindar herramientas de monitoreo, gestión y reporte de tráfico para el servicio considerado, con acceso seguro para observar desde Internet el comportamiento de la calidad del servicio.
- Proveer protocolos de enrutamiento IPv4/IPv6 simultáneo.
- Contar con un servicio de soporte técnico (NOC) proactivo, con centro de atención de averías en 24x7x365, como ventanilla única para creación de tickets de avería, por cada incidencia.
- Tener redundancia de servidores DNS en arreglos de alta disponibilidad.

c. Penalidades sobre el nivel de servicio

El diseño de la solución se considera tres aspectos principales:

- Acceso a Internet.
- Seguridad.
- Administración de tráfico.

Esto se debe a que el cliente establece penalidades económicas sobre el incumplimiento de los acuerdos de niveles de servicio (SLA) por cada aspecto.

La Tabla 3.1 lista las penalidades para el incumplimiento del servicio de Internet. Por

cada falla técnica del servicio de Gestión de Ancho de Banda y/o del servicio de Seguridad, el proveedor se compromete a solucionar el problema en un plazo no mayor de cuatro horas de reportado la incidencia.

Tabla 3.1 Penalidades sobre el servicio de Internet

Rango continuidad servicio (%)	Penalidad
Menos de 99.95 a 99.90	05 % Renta Mensual
Menos de 99.90 a 99.85	10% Renta Mensual
Menos de 99.85 a 99.70	20% Renta Mensual
Menos de 99.70 a 99.50	30% Renta Mensual
Menos de 99.50	40% Renta Mensual

En los casos que la solución de la incidencia exceda el plazo antes mencionado, el proveedor se compromete a asumir las penalidades listadas en la Tabla 3.2. Estas se aplican tanto al servicio de administración de tráfico (ancho de banda) como al de seguridad:

Tabla 3.2 Penalidades sobre administración de tráfico y seguridad

Rango continuidad servicio (%)	Penalidad
De más de 4 horas a menos de menos de 8 horas	03 % Renta Mensual
De 8 horas a menos de 24 horas	06% Renta Mensual
De 24 horas a menos de 48 horas	10% Renta Mensual
De 48 horas a menos de 72 horas	20% Renta Mensual
Entre 72 horas y 96 horas	40% Renta Mensual

Cabe mencionar que pasado el tiempo de 96 horas sin que el servicio interrumpido haya sido repuesto, se considera que proveedor ha incumplido en brindar el servicio de Gestión de Ancho de Banda (administración de tráfico) y/o del Servicio de Seguridad, atribuyéndose a tomar las acciones legales correspondientes.

De lo expresado líneas arriba queda claro que el proveedor debe asegurar la calidad de los servicios a fin de hacer más rentable los servicios que se brindan a la universidad

3.1.2 Planteamiento de la solución

Con lo descrito en la sección 3.1.1, en esta sección se presentan las alternativas para los servicios a brindar.

a. Solución de acceso a Internet

La universidad solicita una solución de acceso a Internet que debe cumplir ciertos requisitos enmarcados en los términos de referencia:

1. Medio de Acceso: se requiere que sea con diversidad de ruta por dos nodos distintos e independientes y llegada a su Centro de Datos.

2. Equipos de enrutamiento: Se exigen que sean de última tecnología, y que posean características superiores a las que van a requerir inicialmente para operación, con la opción de contar con dos equipos, uno activo y otro en reserva de características idénticas y con las mismas funcionalidades.

Para el diseño se considera que el ancho de banda a brindar debe ser 200 Mbps de ancho de banda garantizado y que la disponibilidad sea de 99.95% como mínimo.

a.1 Medio de acceso

Para el medio de acceso se requiere contar con dos enlaces (principal y respaldo) con diversidad de rutas hacia dos nodos de acceso en la red del proveedor. La Tabla 3.3 muestra las características de las tecnologías existentes.

Tabla 3.3 Comparación de características de diferentes tecnologías

Características	Fibra Óptica	Cobre	Microondas
Distancia entre repetidores	40	1.5	30
Atenuación (dB / km) para un Sistema de 56 Mbps	0.4	40	Mas de 80
Delay máximo (mseg)	30	30	100
Inmunidad a la interferencia estática y fuentes de ruido	Alta	Media	Baja
Resistencia a extremos ambientales. Son menos afectadas por líquidos corrosivos, gases y variaciones de temperatura	Alta	Media	Baja
Inmunidad a la inducción magnética	Alta	Media	Baja
La seguridad en cuanto a instalación y mantenimiento	Alta	Alta	Baja
Confiabilidad y Privacidad	Alta	Alta	Baja

- **Medio de acceso de fibra óptica.-** El medio de acceso de fibra óptica en términos de confiabilidad es mejor que otras tecnologías existentes. En la Tabla 3.2 se aprecia que la fibra óptica es un mejor medio por el cual el tipo de información que la universidad está solicitando se transporta libre de interferencias y se garantiza la seguridad y escalabilidad necesarias para la implementación de una red confiable y de alta capacidad, sin restricciones ni factores externos que puedan afectar su desempeño.

- **Medio de Acceso Inalámbrico.-** El medio de acceso inalámbrico en ventajoso en el aspecto económico porque, en comparación de un medio de fibra óptica, para su implementación no requieren de licencias municipales y se requieren menos trabajos de obras civiles.

Sin embargo, en este caso el proveedor cuenta con fibra óptica instalada en la universidad, por tanto el impacto económico se reduce drásticamente, ya que parte de la inversión en infraestructura ya se ha hecho anteriormente, quedando solo la instalación de una ruta redundante..

Por otro lado, este medio presenta desventajas en el aspecto técnico en comparación

del medio de fibra óptica, como puede observarse en la Tabla 3.2.

Conclusión: Por tanto se concluye que la mejor alternativa en este caso es hacer uso de la fibra cómo el medio de acceso de última milla.

a.2 Equipos de enrutamiento

Los equipos de enrutamiento podrían ser de cualquier marca siempre y cuando cumplan con los requerimientos especificados.

El cliente sólo ha precisado que deben ser de última tecnología, y que sus características deben ser superiores a las que van a requerir inicialmente para operación, además menciona que se debe contar con dos equipos, uno activo y otro en reserva o para la operación en HSRP (redundancia en paralelo 1:1).

El cliente también indica que, en tanto garanticen la operación del HSRP para el mejor cumplimiento del SLA, no es excluyente, que dichos equipos (02) de enrutamiento (router) tanto para el enlace principal y backup deban ser de características idénticas y con las mismas funcionalidades.

Para la selección de la marca de estos equipos se ha tomado en cuenta lo siguiente:

- El cliente no ha solicitado una marca ni modelo de equipo especifico. Ya que la infraestructura no será de su propiedad, no existe el requerimiento de uniformización de tecnología con alguna marca específica.
- Los switches de acceso, de distribución y Core de la red LAN del cliente son equipos de la marca CISCO.
- El proveedor tiene una alianza estratégica con CISCO, la cual incluye descuentos especiales aprobados mediante contratos marco, lo cual facilita el proceso de compra de los equipos haciéndolo muy ágil, y así mejorando directamente en los plazos de implementación.

Según lo expresado líneas arriba, tanto técnica y económicamente se escoge la marca CISCO para esta implementación. Por lo tanto, para el dimensionamiento respectivo del equipamiento a utilizar, se tomará en cuenta solo los aspectos técnicos.

b. Solución de administración de tráfico WAN

Esta debe ser redundante y cumplir con los siguientes:

- Redundancia (1:1) en serie o paralelo.
- Políticas de priorización de tráfico saliente y entrante: de manera independiente de 7 ò más prioridades.
- Capacidad de administración de ancho de banda: por protocolos, contenidos y evolución de comportamiento de protocolos en el campus.
- Ancho de banda: debe ser 200 Mbps de ancho de banda garantizado.
- Disponibilidad: debe ser de 99.95% como mínimo.

Según lo indicado se pueden utilizar para esta solución los equipos que manejen de manera independiente 7 prioridades, y equipos con 8 prioridades.

c. Solución de Seguridad

Debe ser redundante (en paralelo 1:1), la cual debe cumplir ciertos requisitos enmarcados en los términos de referencia:

- Ancho de banda: debe ser 200 Mbps de ancho de banda garantizado.
- Disponibilidad: debe ser de 99.95% como mínimo.
- Características: Firewall en campus que incluya antispam, antivirus, filtro WEB con sistema de gestión y reportes, así como el manejo de políticas de acceso (Tabla 3.4).

Tabla 3.4 Características

Número estimado conexiones concurrentes a Internet	Mínimo de 200,000
Número estimado de buzones de correo	Mínimo de 15,000
Número estimado de usuarios que accedan a Internet	Mínimo de 3,000
Throughput (volumen de trabajo) mínimo del firewall	mínimo 2 Gbps
Número de Interfaces mínimas del firewall	10 puertos Gigabit

Según lo expuesto, se determina se determina el uso de dos equipos UTM en configuración redundante, por que estos dispositivos integran múltiples capacidades de seguridad en un único producto, incluidas las de firewall, detección y prevención de intrusiones (IDP), antivirus, anti-spam, filtro de URLs, VPN ,etc. Esto resulta más económico que contar con una configuración de productos de función única, además de la dificultad para el diagnóstico de fallas y la administración de los equipos.

Para la gestión y reportes se determina el uso de una consola de administración centralizada y un hardware dedicado para la gestión de reportes.

d. Topología

Para elaborar la topología de la solución se debe definir, en primer lugar, la ubicación de cada una de las soluciones: Acceso a Internet, Administración de Tráfico, Seguridad.

- La solución de Seguridad.- Debido a sus capacidades de firewall, webfiltering y otros, deberá ser configurada como puerta de enlace para los usuarios de la red de la universidad. Por ella pasará tanto el tráfico interno como el tráfico de Internet, por tanto dentro de la topología estará delante de la Red LAN.
- La solución de administración de tráfico WAN.- Debido a que esta dimensionado para administrar el tráfico de Internet, deberá estar delante de la solución de seguridad y antes de la solución de acceso a Internet.
- La solución de acceso a Internet.- Con sus equipos de enrutamiento, deberán estar delante de los equipos de administración de tráfico WAN, e ir conectados a la última milla (fibra óptica).

Para la selección de la topología de la solución se analizan dos opciones.

d.1 Modelo de Solución Tipo 1

En el esquema de la Figura 2.3 se muestran los equipos de enrutamiento configurados en redundancia (en paralelo 1:1), equipos de administración de tráfico en configuración redundante (en serie 1:1), y los equipos de seguridad configurados en redundancia (en paralelo 1:1).

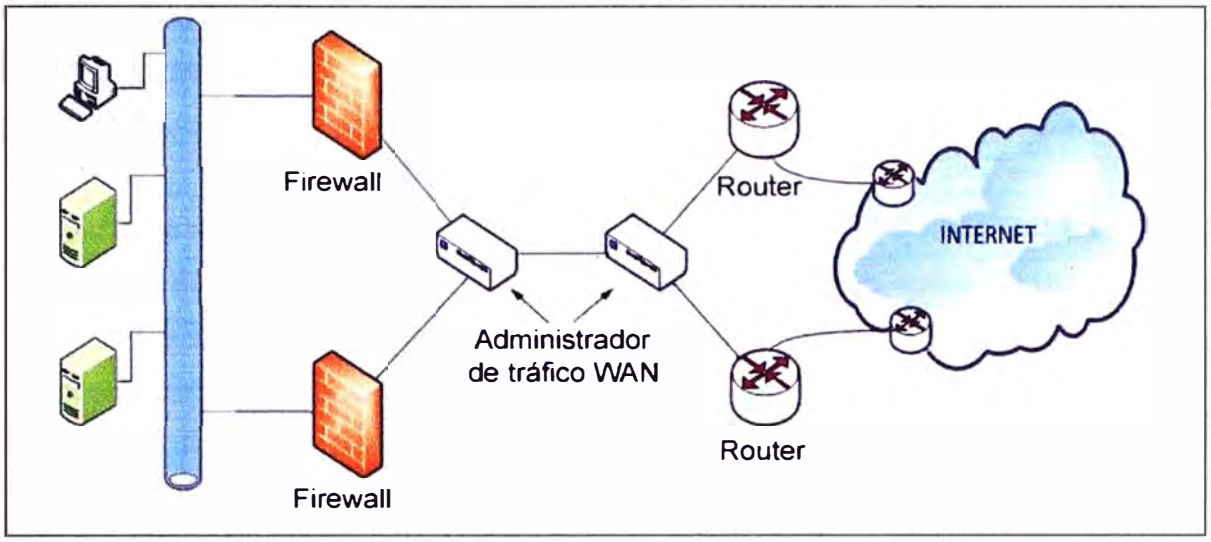

Figura 3.2 Solución tipo 1

d.2 Modelo de Solución Tipo 2

En el esquema de la Figura 2.3, se muestran los equipos de enrutamiento configurados en redundancia (en paralelo 1:1), los equipos de administración de tráfico en configuración redundante (en paralelo 1:1), y los equipos de seguridad configurados en redundancia (en paralelo 1:1).

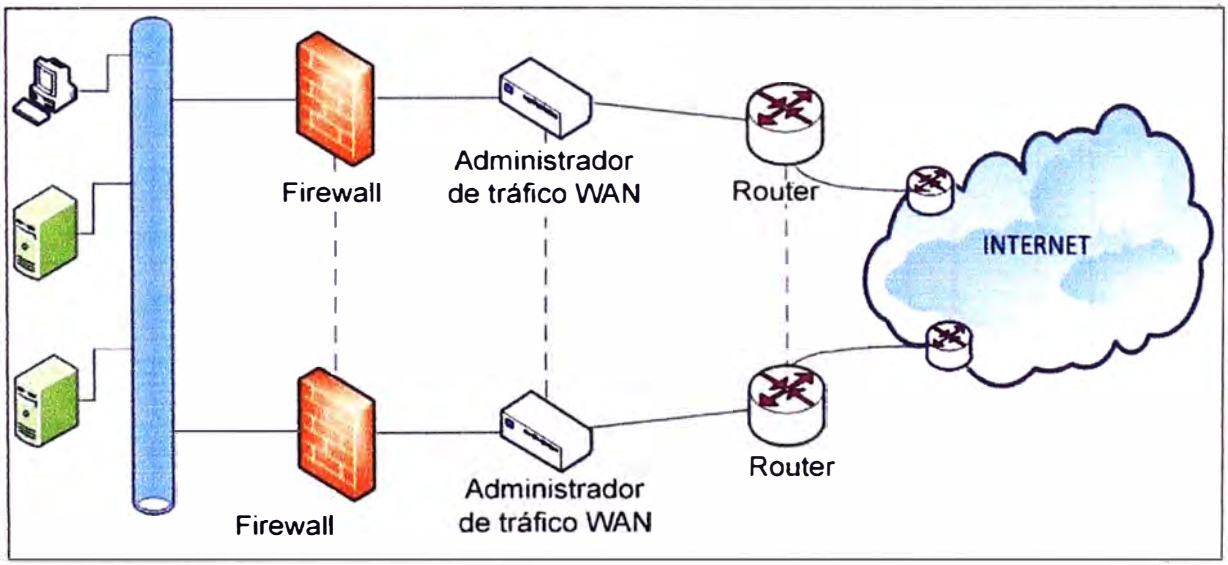

Figura 3.3 Solución tipo 2

d.3 Selección de topología

Como se podrá mostrar en el presente capitulo, se determina mediante un análisis

tecnológico, así como desde la perspectiva costo-beneficio del proveedor, escoger la topología Tipo 1. Para la selección de la topología de la solución, se toma en cuenta que el equipamiento y configuración deba cumplir los requerimientos mínimos del sistema y evitar penalidades, pero optimizando la inversión por parte del proveedor, es decir, aumentar el margen de ganancia.

3.1.3 Dimensionamiento y análisis

En esta sección se desarrollan los aspectos planteados en la anterior sección.

a. Acceso a Internet

El acceso a internet está definido en los requerimientos del cliente (ancho de banda de 200Mbps).

a.1 Medio de acceso

El medio de acceso es de fibra óptica, con dos cables de fibra óptica por diferente ruta (canalizada y subterránea) a nodos distintos de acceso a la red del proveedor. Los nodos de acceso cercanos al local del cliente son: Nodo Rímac y Nodo Los Olivos.

Para la ruta principal se emplea la ruta desde el Nodo Rimac hacia el local de la Universidad, este enlace se encuentra instalado en la Sala de Datos de la Universidad.

Para la ruta de contingencia es la que va desde el Nodo Los Olivos hacia la Sala de Datos de la Universidad.

Tomando en consideración que la capacidad solicitada de ancho de banda para cada enlace de fibra óptica es de 200Mbps, por cada cable de fibra se habilitará un par de hilos de fibra en cada extremo, configurándose y activándose un puerto Giga Ethernet óptico.

Los perfiles de la fibra óptica elaborados por el postor son mostrados en la Figura 3.4 y 3.5. La Figura 3.6 y 3.7 muestra el recorrido de la fibra de última milla para cada uno de los nodos.

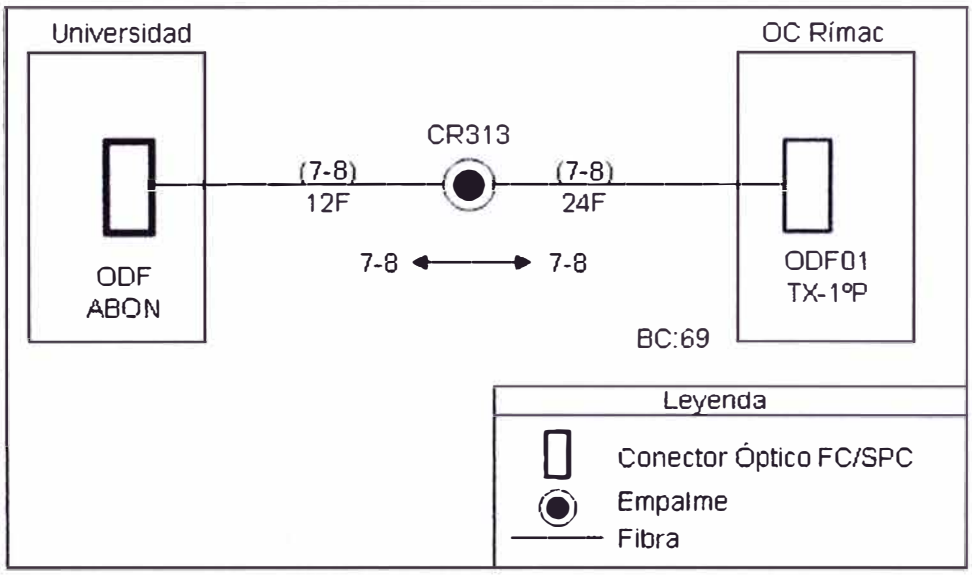

Figura 3.4 Perfil y asignación de FO para Universidad desde Nodo Rímac

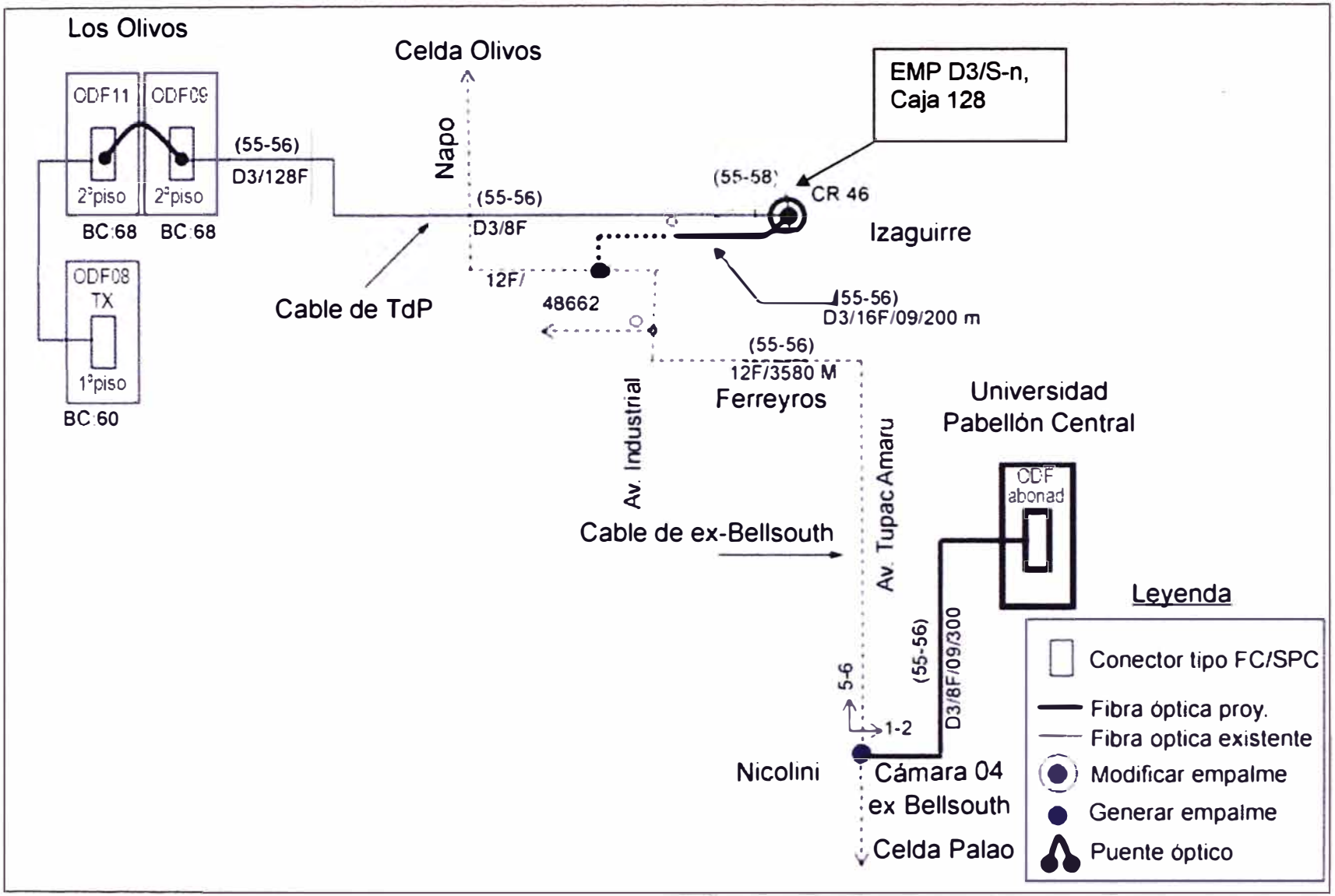

Figura 3.5 Perfil y asignación de FO para Universidad desde Nodo Los Olivos

Figura 3.6 Recorrido para Universidad desde Nodo Los Olivos

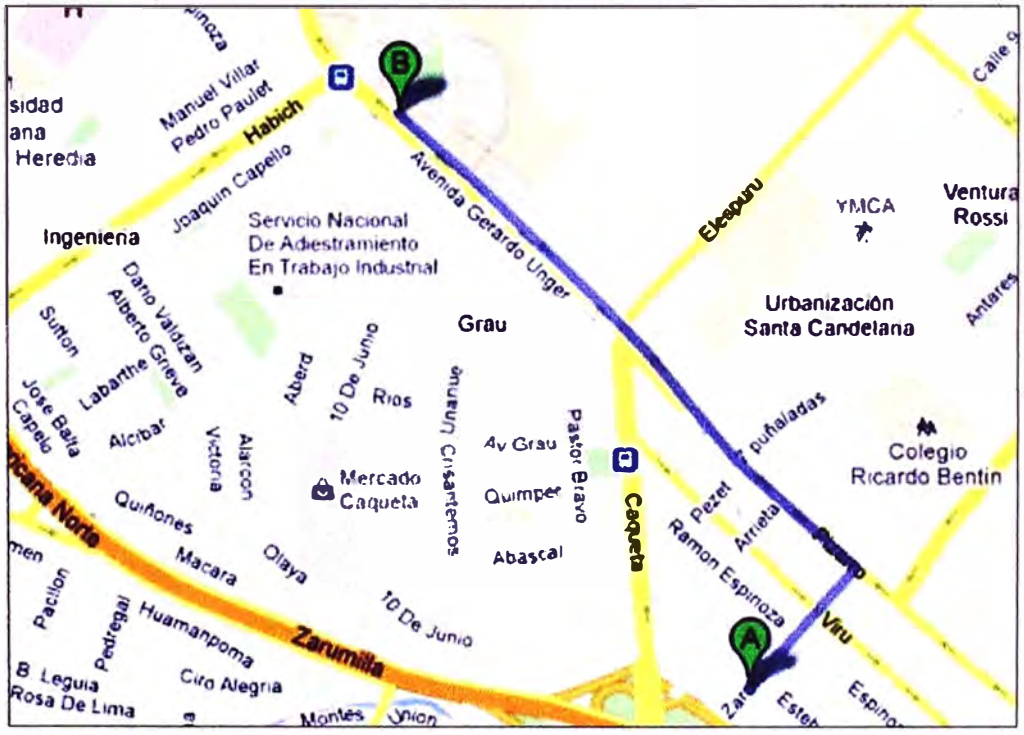

Figura 3.7 Recorrido para Universidad desde Rímac

a.2 Equipamiento de Internet

Dentro de las características que debe tener el equipo, se puede acotar que este debe soportar los 200 Mbps de ancho de banda, debe funcionar como bridge ya que el NAT, las funcionalidades de seguridad y traffic shapping (catalogación de paquetes) se configurarán en los equipos de seguridad y equipos de administración de tráfico respectivamente. Además el equipo debe contar como mínimo con dos interfaces GIGAETHERNET, una que soporte modulo SFP (small form-factor pluggable ó transceptor de fibra óptica) para la conexión de la fibra óptica y otra interfaz de cobre 10/100/1000 para la conexión con el administrador de ancho de banda.

Nota:
El "traffic shapping" optimiza y/o garantiza el rendimiento, baja latencia, y/o un ancho de banda determinado (se procura brindar a los usuarios los servicios que utilizan en la red dando mayor prioridad a aquellos que necesitan mayor velocidad como la telefonía y menos prioridad a la descargas de archivos) retrasando paquetes catalogación de paquetes.

Para dimensionar un router CISCO se debe tener en cuenta la cantidad de paquetes por segundo (PPS) que puede procesar el router y la funcionalidad que se quiera habilitar (QoS, NAT, FW, IPSec, etc).

Por ejemplo, si es solo IP (Datos) el 3945 puede procesar un aproximado de 982,000 paquetes por segundo al 100% de capacidad, si se hace el cálculo con paquetes de 64 Bytes, se podría decir que puede trabajar hasta con 502.78 Mbps de ancho de banda. Esto con la simple formula: Mbps = [(packet size) * 8 * PPS] / 1,000,000.

Para un correcto análisis es necesario comprender el escenario de implementación y hacer una recomendación del equipo que se ajuste a las necesidades.

El escenario de implementación es de un router de borde para salida a internet, que no realiza QoS, ACL, funcionalidades de seguridad (VPN, IPSEC), ni NAT ya que estos últimos se realizarán en el Firewall.

Para medir el rendimiento del equipo, debemos conocer cuál es el tamaño usual del paquete de tráfico de Internet, para ello en la industria es usado un término denominado "Internet Mix" o IMIX para describir el tráfico de Internet típico que pasa un poco de equipo de red tales como routers, switches o servidores de seguridad. Cuando se mide el rendimiento del router utilizando equipos de medición con IMIX se supone que el rendimiento que se asemejan a lo que se ve en la vida real.

El perfil de tráfico IMIX se utiliza en la industria para simular los patrones de tráfico del mundo real y la distribución de paquetes. El perfil de trafico IMIX se basa en un muestreo estadístico realizado en los routers de Internet, y aparecen en los distintos niveles de granularidad, como "simple " y "completo".

- 1518 bytes x 15 paquetes (15%).

- 594 bytes x 24 paquetes (24%).
- 64 bytes x 61 paquetes (61%).

El promedio de tamaño de los paquetes es: 409 bytes.

Se debe considerar también la utilización del CPU, ya que la mayoría de los proveedores de servicios (ISP) fijan las alarmas de la CPU a 60 o 65 por ciento.

Para la colocación de rendimiento de los routers Cisco ISR G2, el umbral de la CPU se establece en el uso de 75 por ciento. Esta configuración proporciona un indicador válido para la forma en que el router se comporta en un entorno de producción.

Bajo estos parámetros, el fabricante CISCO ha realizado una medición del rendimiento de los equipos CISCO de la serie 3900, donde se muestra el efecto en la performance del equipo cuando se utilizan los múltiples servicios que se incluyen en el IOS del equipo.

Por ejemplo, en el escenario donde el router 3945 utilice los servicios de ACLs, NAT, HQoS, al 75% de utilización del CPU, el equipo soportaría 200 Mbps de ancho de banda, esto se puede validar en el documento: Cisco Integrated Services Routers—Performance Overview publicado por CISCO.

En el escenario de implementación de este proyecto, ninguna de estas características será usada inicialmente, ya que en el caso de las ACLs, NAT serán habilitadas en el Firewall.

Conclusión:

Del análisis realizado se considera en el diseño al equipo CISCO modelo 3945/K9. Por tanto la solución quedaría según lo mostrado en la Figura 3.8.

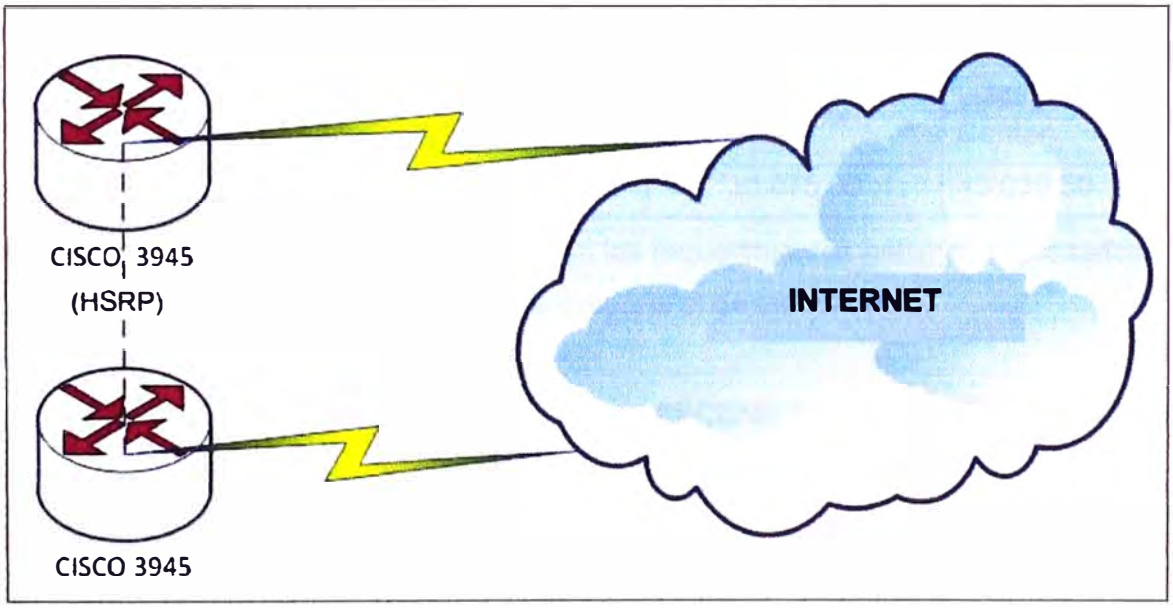

Figura 3.8 Equipos Cisco para solución de acceso a Internet

b. Administración de tráfico

Para definir el modelo y marca del equipo Administrador de Trafico WAN, se toma en

cuenta lo siguiente:

- Análisis de los parámetros indicados en los términos de referencia.
- El cliente no ha solicitado una marca ni modelo de equipo especifico.

La Tabla 3.5 muestra marcas y modelos de equipos que cumplen estas especificaciones:

Tabla 3.5 Equipos y características

	Marca/Modelo del equipo		
Característica	NetEnforcer 804	Ascenflow M1000i	PacketShapper 7500
Ancho de Banda (máx.)	310 Mbps	200 Mbps	200 Mbps
Número Máximo de Conexiones	256,000	1,000,000	100,000
Clases	3072	1024	1024
Alta disponibilidad (HA)	Si Serial, paralelo y activo (1:1, 1+1)	Si Serial (1:1)	No especifica.
Monitoreo de aplicaciones a nivel 7	Si	Si	Si
Múltiples niveles de prioridad (X niveles)	8	7	7
Interfaz de Red	4x10/100/1000 BaseT o 4x1000 BaseSX o 4x1000 BaseLX (5KM)	5x10/100/1000 Base–TX	No especifica
Herramienta para gestión de reportes en línea	Si NetExplorer	Si NetFlow	Si Intelligence Center
Precio (US$)	56,848.00	30,075.00	43,030.50

Dado que todos los equipos cumplen con los requerimientos mínimos expresados por el cliente en los términos de referencia, se propone el de menor costo.

Conclusión:

Por tanto se considerará para el diseño el equipo ASCENFLOW modelo M1001i.

c. Dimensionamiento Seguridad

Para definir el modelo y marca del equipo UTM, se toma en cuenta lo siguiente:

1. Análisis de los parámetros indicados en los términos de referencia.
2. El cliente no ha solicitado una marca ni modelo de equipo especifico.
3. En el pasado, la solución de seguridad del cliente ha sido soportada por equipos de las siguientes marcas: FORTINET y JUNIPER.

4. Estudios realizados por consultoras independientes sobre el mercado de UTM. Los estudios realizados por la consultora Gartner, coloca a FORTINET como el líder indiscutido en el mercado de los equipos de tecnología UTM.

5. El proveedor tiene una alianza estratégica con un distribuidor de equipos UTM de la marca FORTINET, la cual incluye descuentos especiales aprobados mediante Contrato Marco, lo cual facilita el proceso de compra de los equipos haciéndolo muy ágil, y así mejorando directamente en los plazos de implementación.

6. Experiencia del postor implementando soluciones con esta marca.

A continuación mostraremos una tabla con marcas y modelos de equipos que cumplen las especificaciones técnicas:

Tabla 3.6 Equipos y características

	Marca/Modelo del equipo				
Característica	FortiGate 1240B	Cisco ASA 5580-20	Juniper SRX 3400	Sonicwall NSA E5500	Astaro ASG525
Firewall Throughput (512 Byte)	40 Gbps	10/5 Gbps	20 Gbps	3.9 Gbps	5.5 Gbps
Número Máximo de Conexiones Concurrentes	2,000,000	1,000,000	2,250,000	700,000	1,700,000
Usuarios Soportados por el Firewall	Ilimitado	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Alta disponibilidad (HA)	Si	Si	Si	Si	Si
Antivirus Throughput	450 Mbps	No	Si (TBA)	750 Mbps	Si (TBA)
AntiSpam	Si	No	No	Si	Si (TBA)
Filtro WEB	Si	No	No	Si	Si
IPS Throughput	1.5 Gbps	No	No especifica.	550 Mbps	800 Mbps
Interfaz de Red	16x10/100/1000 + 24xSFP	4x10/100/1000	8x10/100/1000 + 4xSFP	8x10/100/1000	10x10/100/1000 + 4xSFP
Manejo de políticas de acceso	Si	No	Si	Si	Si
Sistema de Gestion	Si (FortiManager)			Si (GMS)	Si (ACC1000)
Sistema de Reportes	Si (FortiAnalyzer)			Si (ViewPoint)	Si (Report Manager)
Cumple técnicamente	Si	No	No	No	Si
Precio (US$)	77,529.72				135,768.00

Las Tablas 3.7 y 3.8 son usadas para elegir la mejor alternativa técnica económica.

Tabla 3.7 FORTIGATE 1240B

Parámetro de Diseño	Cumple	Puntaje
Cumple especificaciones técnicas mínimas.	SI	40 puntos
Líder en el mercado de UTM según consultoras internacionales.	SI	03 puntos
Postor tiene Contrato Marco con Distribuidor.	SI	03 puntos
Experiencia del Postor implementando soluciones con esta marca.	SI	04 puntos
Propuesta económica (máx. 50 puntos).	SI	50 puntos
TOTAL		100 puntos

Tabla 3.8 ASTARO ASG525

Parámetro de Diseño	Cumple	Puntaje
Cumple especificaciones técnicas mínimas	SI	40 puntos
Líder en el mercado de UTM según consultoras internacionales	NO	00 puntos
Postor tiene Contrato Marco con Distribuidor	NO	00 puntos
Experiencia del Postor implementando soluciones con esta marca	NO	00 puntos
Propuesta económica (máx. 50 puntos)	SI	28.55 ptos
TOTAL		78.55 ptos

De acuerdo al análisis realizado, se escogió el modelo FORTIGATE 1240B.

3.2 Descripción de la solución

La solución consta de dos enlaces de fibra óptica, canalizada y subterránea con diferentes rutas a distintos nodos de presencia del proveedor con llegada al Centro de Datos de la Universidad; dos (02) equipos de enrutamiento marca CISCO modelo 3925/K9 configurados en redundancia (en paralelo 1:1), dos (02) equipos de administración de tráfico marca XTERA modelo ASCENFLOW M1000i en configuración redundante (en serie 1:1), y dos (02) equipos de seguridad marca FORTINET modelo FORTIGATE 1240B configurados en redundancia (en paralelo 1:1).

Los equipos FORTIGATE 1240B operan en alta disponibilidad, formando un cluster master-slave mediante un cable de alta disponibilidad (HA). Ambos equipos se mantienen configurados idénticamente, teniendo uno de ellos el rol de master (maestro) y el otro el rol de slave (esclavo). El equipo con el rol de master (maestro) es la puerta de enlace para los usuarios de la red de la Universidad, por ella pasa tanto el tráfico interno como el tráfico hacia/desde Internet, por tanto dentro de la topología esta delante de la red LAN de la Universidad. El equipo con el rol de slave (esclavo) tiene la función de continuamente verificar la salud del equipo master (maestro) y solo en caso que detecte que el equipo master está inactivo, asumirá el rol de maestro.

Con la finalidad de un mejor orden de las políticas de seguridad se usan dominios virtuales (VDOMS) que agrupan a las distintas dependencias de la universidad en función a los recursos a los que estos acceden. Los equipos ASCENFLOW 1001i están configurados en alta disponibilidad y en serie, de manera similar forman un cluster

master-slave mediante un cable de alta disponibilidad (HA) con el cual el equipo que tiene el rol de slave (esclavo) está continuamente verificando el estado del equipo master (maestro). Estos equipos se comportarán como un cable en caso de falla permitiendo que el tráfico pueda pasar sin interrupciones. La administración puede realizarse localmente y remotamente, y los reportes se realizan mediante un software instalado en la PC del Administrador de Red de la Universidad.

Los equipos CISCO 3945/K9 están configurados en alta disponibilidad, usando el protocolo BGP, funcionando en modo brigde (puente) recibiendo y enviado el tráfico WAN desde/hacia Internet, dichos equipos irán conectados a la ultima milla (fibra óptica) y al equipo ASCENFLOW 1001i que esté configurado como maestro por defecto (ver topología).

Para interconectar, física y lógicamente, a los equipos que forman parte de la solución con la red LAN de la Universidad, se consideran dos (02) equipos de conmutación marca CISCO modelo 2960G. En la Figura 3.9 se muestra la topología de la infraestructura de la solución. Se ha delimitado en el diagrama esquemático la zona correspondiente a la solución desarrollada en el presente informe. En gris se muestra a la zona de la planta externa.

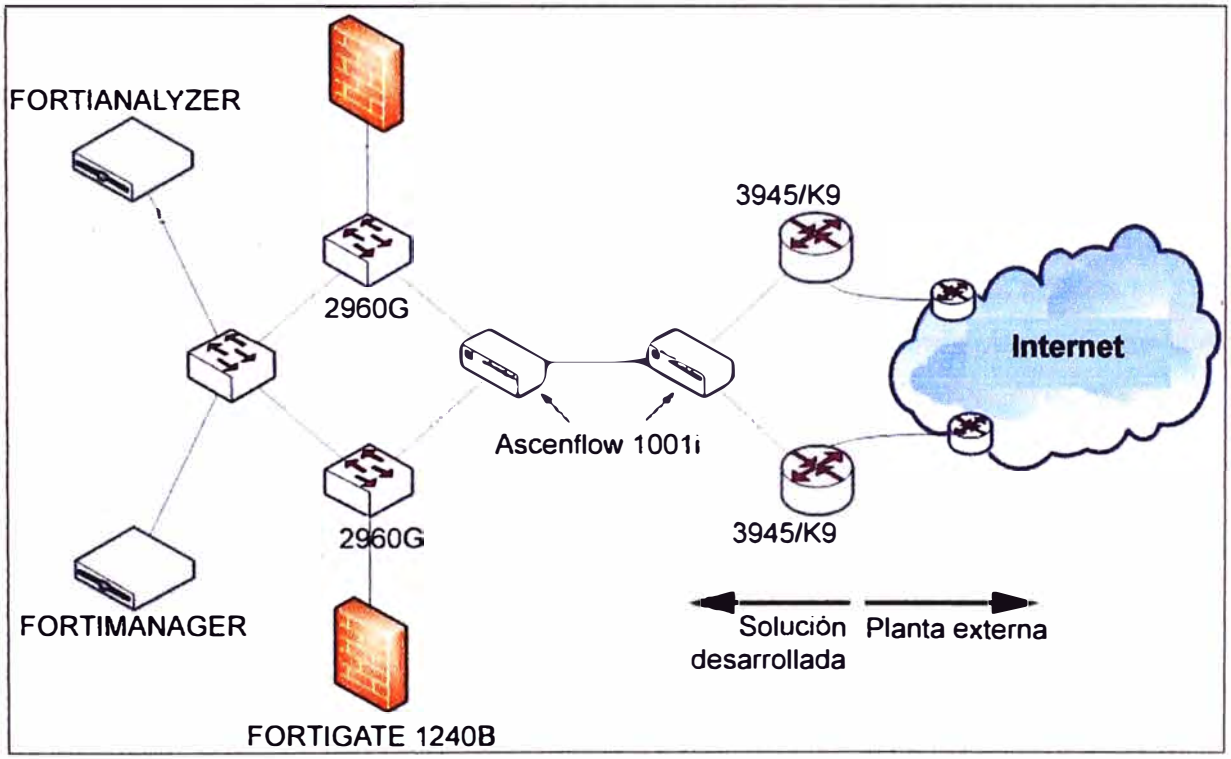

Figura 3.9 Topología de la solución

A continuación se describe los componentes de la solución, su funcionalidad y finalmente su configuración.

3.2.1 Componentes

Son analizados para las tres soluciones que incluye la solución general: Solución de

acceso a Internet, solución de administración de tráfico, solución de seguridad

a. Solución de acceso a Internet

Está compuesta por los equipos de enrutamiento en casa de cliente. Complementariamente, con el propósito de ilustrar su operatividad, se describe también a la planta externa, es decir a la última milla, y a los equipos en el nodo del proveedor.

a.1. Equipos de enrutamiento en casa de cliente

Son los equipos marca CISCO modelo 3945/K9 (Figura 3.10), a continuación se menciona sus características más resaltantes [12]:

- Tres (03) puertos integrados Ethernet 10/100/1000 con dos (02) puertos con capacidad de soportar conectores RJ-45 o SFP.
- Cuatro (04) ranuras para módulos de servicio (SM, Service Module).
- Cuatro (04) ranuras para tarjetas de interfaz WAN de alta velocidad mejorada (HWIC).
- Doble fuente de alimentación integrada.

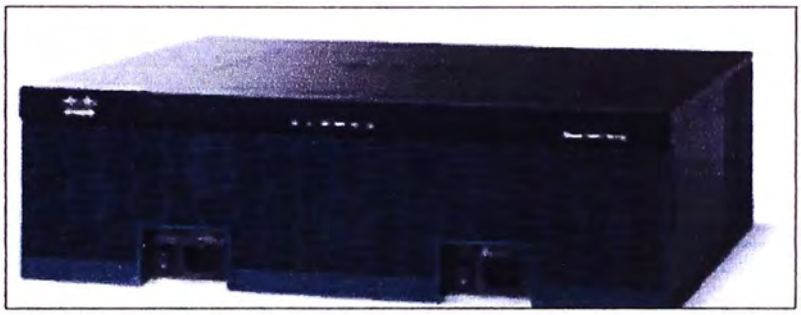

Figura 3.10 Cisco 3945/K9

Los equipos CISCO 3945/K9 instalados en la universidad incluyen para la conexión del enlace WAN dos tarjetas HWIC con puerto GigaEthernet SFP (número de parte: HWIC-1GE-SFP), esto con la finalidad de tener redundancia física ante la falla de uno de las tarjetas. Se incluyen también los respectivos transceptores (o módulos SFP) de fibra óptica que se instalarán en cada tarjeta HWIC-1GE-SFP (Figura 3.11).

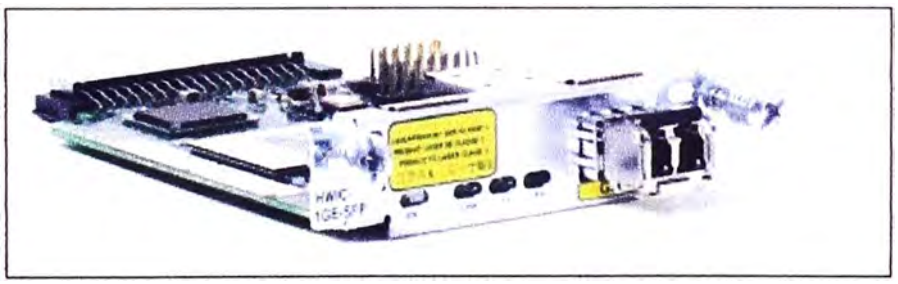

Figura 3.11 Cisco Gigabit Ethernet HWIC con modulo SFP

Los módulos SFP (Small Form-Factor Pluggable ó Dispositivo de forma pequeña para insertar) son dispositivos de entrada-salida (transceptores) que se insertan en el puerto de la tarjeta HWIC-1GE-SFP. Los módulos SFP considerados son del tipo GLC-LH-SM (Figura 3.12), que soportan fibra óptica monomodo y el tipo de conector LC que es utilizado por el proveedor en la última milla.

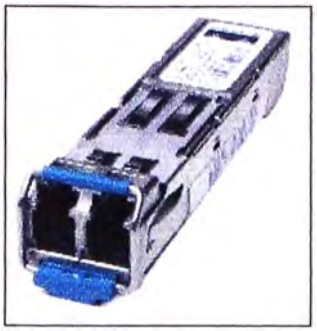

Figura 3.12 Modulo SFP (Conector LC)

a.2. Última milla

Está compuesta por el cable de fibra óptica de planta externa, el ODF de abonado y patchcord de fibra óptica.

El cable de fibra óptica de planta externa utilizado por el proveedor es del tipo monomodo G.655, diseñado para ambientes de instalación externo-subterráneo en ductos.

El repartidor óptico (ODF), es una caja metálica que posee uno o varios puertos de ingreso de cables, y un área de conectorización con adaptadores o transiciones, en la cual se conecta la terminación del cable de fibra por un extremo y el patchcord hacia el equipo activo por el otro extremo.

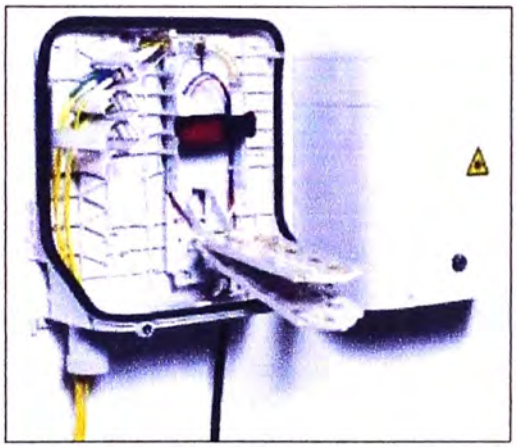

Figura 3.13 ODF de abonado

El patchcord de fibra óptica utilizado es de presentación dúplex y tipo LC/LC, un extremo del cordón va conectado al ODF y el otro extremo se conecta al módulo SFP insertado en el equipo router Cisco 3945/K9.

a.3. Equipos en nodo del proveedor:

El nodo del proveedor es el punto de llegada del cable de fibra de alta capacidad conteniendo los dos hilos de fibra con continuidad hasta el ODF del cliente.

Estos hilos de fibra son terminados en un ODF de gran capacidad dentro del nodo del proveedor, este ODF a su vez es reflejado en el área donde se encuentran los equipos de borde de la red IP/MPLS que proveen el transporte de Datos e Internet según el tipo de

acceso contratado por el cliente.

Los equipos de borde del proveedor son:

- Huawei S8512 (para el enlace Principal).
- Huawei NE80E (enlace de contingencia).

Figura 3.14 Huawei S8512 [13]

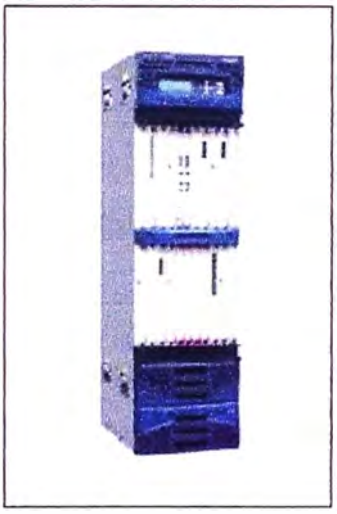

Figura 3.15 Huawei NE80E [14]

b. Solución de administración de tráfico

Está compuesta por los equipos de administración de tráfico instalados en casa de cliente y el software de gestión de reportes.

b.1. Equipos de Administración de Tráfico

Son los equipos de la marca XTERA NETWORKS modelo AscenFlow M1000i (Figura 3.16). Los equipos AscenFlow [15] utilizan una tecnología denominada *inspección profunda de paquetes* o *Deep Packet Inspection (DPI)* que le permite observar el trafico de entrada y de salida clasificándolo de acuerdo a prioridades según el tipo de aplicación, y asignando una determinada cuota de ancho de banda por sesión, segmento de red y

tipo de aplicación. De esta manera se optimiza el uso del ancho de banda del enlace de internet, se evitan congestiones en horas pico y se provee de una herramienta de análisis que permite optimizar y ahorrar este valioso recurso a nivel institucional.

Los equipos cuentan con las siguientes características:

- Cinco (05) puertos 10/100/1000 Base-TX.
- By Pass por falla Hardware/Software.
- Siete (07) niveles de prioridades
- Alta Disponibilidad (HA).

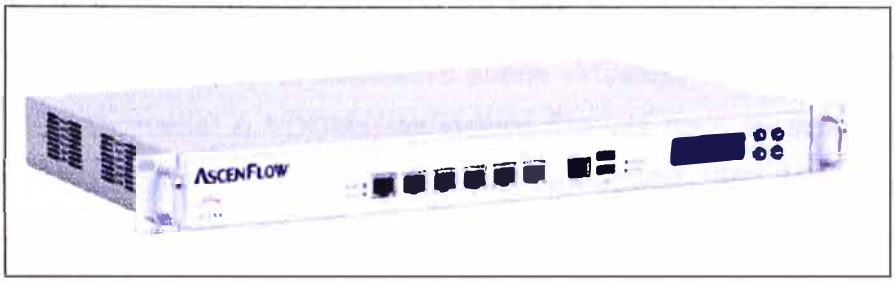

Figura 3.16 Ascenflow

b.2. Software de gestión de reportes:

El software de gestión de reportes "FlowReport" forma parte de la solución de administración de tráfico, siendo una herramienta muy importante dado que provee reportes detallados en tiempo real del comportamiento del tráfico del enlace de Internet; permitiendo luego de analizar la data, determinar nuevas políticas que permitan una mejor utilización del recurso.

Este software se encuentra instalado en una computadora personal del Centro de Datos de la Universidad.

c. Solución de Seguridad

Está compuesta por los equipos de seguridad perimetral instalados en casa de cliente, su consola de administración centralizada y el hardware dedicado para la gestión de reportes.

c.1. Equipos de Seguridad Perimetral

Son los equipos de la marca FORTINET, modelo FORTIGATE 1240B (Firewall UTM) [16]. Los equipos FortiGate (Figura 3.17) son un sistema de seguridad informática del tipo "Administración Unificada de Amenazas" ó UTM (por sus siglas en inglés), donde se ofrecen ya incluidas y listas para ser utilizadas las funcionalidades de Firewall, VPN, Traffic Shapping, Antivirus, Antispam, Filtrado de URL, Protección contra Intrusos (IPS), Prevención de Fuga de Información (DLP), Control de Aplicaciones, entre otros. Estos equipos cuentan con las siguientes características:

Throughput (volumen de trabajo o de información que fluye a través del sistema)

- Firewall: 40/44 Gbps

- VPN (3DES): 16 / 18.5 Gbps
- Antivirus: 900 Mbps
- IPS: 1.5 Gbps

Conexiones concurrentes totales: 2'000,000

Nuevas conexiones por segundo: 100,000

Interfaces de Red

- Interfaces 10/100/1000 Mbps basadas en cobre.
- 24 Interfaces Gigabit SFP

Alta Disponibilidad (HA): activo-pasivo, activo-activo.

Dominios Virtuales (VDOMs): El dispositivo puede virtualizar los servicios de seguridad mediante "Virtual Domains" ó VDOMs, se incluye licencia para 10 instancias virtuales. Cada instancia virtual soporta las funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus; puede tener un administrador independiente y su configuración puede estar aislada de manera lógica del resto de las instancias virtuales.

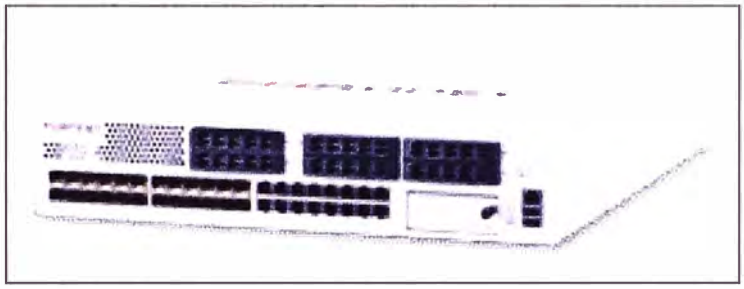

Figura 3.17 FortiGate 1240B

c.2. Consola de Administración Centralizada:

Es el equipo FortiManager 400B [17] (Figura 3.18), es un sistema de gestión (consola de administración) centralizado, en formato de hardware de propósito especifico ó "appliance", desde donde se puede realizar la configuración de dispositivos, gestión de actualizaciones, monitoreo y control de dispositivos de seguridad que sean del tipo UTM. Entre sus principales funcionalidades, se incluyen:

- Centralización de Configuración y monitoreo de todos los dispositivos de seguridad UTM. Así como todas sus funciones de protección de red
- Administración de dispositivos "virtuales" que residen en una misma unidad física.
- Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos.
- Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los dispositivos UTM.
- Administra el firmware de los dispositivos de seguridad, permitiendo programar y aplicar actualizaciones de sistema operativo de forma desatendida a un equipo o grupo de equipos administrados por la consola, reduciendo tiempos de operación y administración

del personal que administra los equipos de seguridad.

Figura 3.18 FortiManager 400B

Este equipo se encuentra instalado en el Centro de Datos de la Universidad.

c.3. Hardware dedicado para la gestión de Reportes:

Es el equipo FortiAnalyzer 1000B [18] (Figura 3.19), es un sistema de reporte, análisis y almacenamiento de bitácoras, que incluye capacidades de correlación y análisis de vulnerabilidades en la red para dispositivos de Administración Unificada de Amenazas (UTM).

Entre sus principales características, se incluyen:

- Formato tipo "appliance" con sistema operativo propietario.
- Interfaz de administración gráfica (GUI) vía Web (http y HTTPS).
- Interfaz de administración vía CLI (Línea de comando) vía telnet, ssh y consola serial.
- Capacidad mínima de almacenamiento incluida: 1 TB total.
- Conectividad con interfaces Ethernet 10/100/1000: 4.
- Dispositivos UTM que pueden enviar bitácoras: 250

Entre sus principales funcionalidades, se incluyen:

- Capacidad de poder integrar dispositivos tipo UTM para que le reporten, y establecer comunicaciones seguras con dichos dispositivos.
- Capacidad de asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución.
- Capacidad de hacer correlación de la información almacenada. Esto es, identificar patrones y/o tendencias en la información almacenada.
- Capacidad de hacer búsquedas por nombre de usuario (username) o dirección IP, para que toda la información almacenada de dicho nombre de usuario o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.
- Capacidad de hacer análisis de vulnerabilidades en la red, mediante complementos (plug-ins) de ataques actualizables, y generar un reporte de cuáles vulnerabilidades fueron encontradas en la red.
- Capacidad de recibir bitácoras de los protocolos http, SMTP y messengers (Yahoo, MSN) para poder almacenar los mensajes que han fluido en la red a través de dichos protocolos, para su posterior visualización.

- Capacidad de hacer búsquedas sobre los mensajes almacenados.

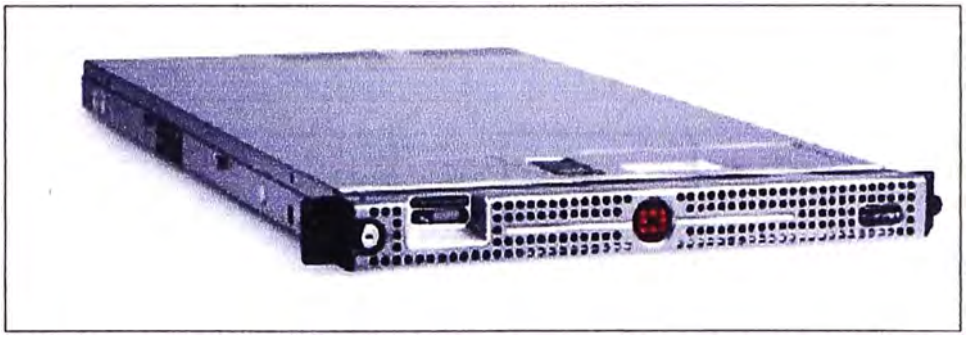

Figura 3.19 FortiAnalyzer 1000B

c.4. Equipos Switch:

Son los equipos de la marca Cisco modelo 2960G-24TC-L, conmutadores de capa 3, a continuación sus características más resaltantes:

- 24 puertos Ethernet 10/100/1000, cuatro de los cuales son de doble propósito.
- 16 Gbps de switching fabric.
- Tasa de reenvío (calculada con paquetes de 64 bytes): 35.7 Mpps.
- 64 MB DRAM
- 32 MB flash memory

3.2.2 Descripción funcional

En esta subsección se describe la funcionalidad, tanto a nivel de cada tipo así como para el sistema.

a. Funcionalidad a nivel de componente

Para su descripción se toma como referencia al esquema de la Figura 3.20.

a.1 Equipos de Enrutamiento (R)

Su función es de dirigir al tráfico de entrada y de salida (inbound y outbound) desde/hacia la red del proveedor, basándose para ello en su tabla de enrutamiento dinámica.

Dentro de la solución también cumplen la función establecer la sesión eBGP con los equipos de borde de la red del Proveedor (PE, Provider Edge) y la sesión iBGP con los equipos FortiGate 1240B (puerta de enlace de la red del cliente), lo cual permite brindar alta disponibilidad en caso de falla de alguno de estos equipos, estableciendo una ruta alternativa para el tráfico.

a.2 Equipos AscenFlow (AF)

Su función es administrar el ancho de banda a través de políticas definidas por la Universidad, su configuración es basada en objetos.

Se crearon objetos por cada área en la Universidad, identificándosela por la IP publica asignada mediante el NAT que realiza el FGT, a cada objeto se le aplicó políticas para garantizar un ancho de banda mínimo y máximo garantizado.

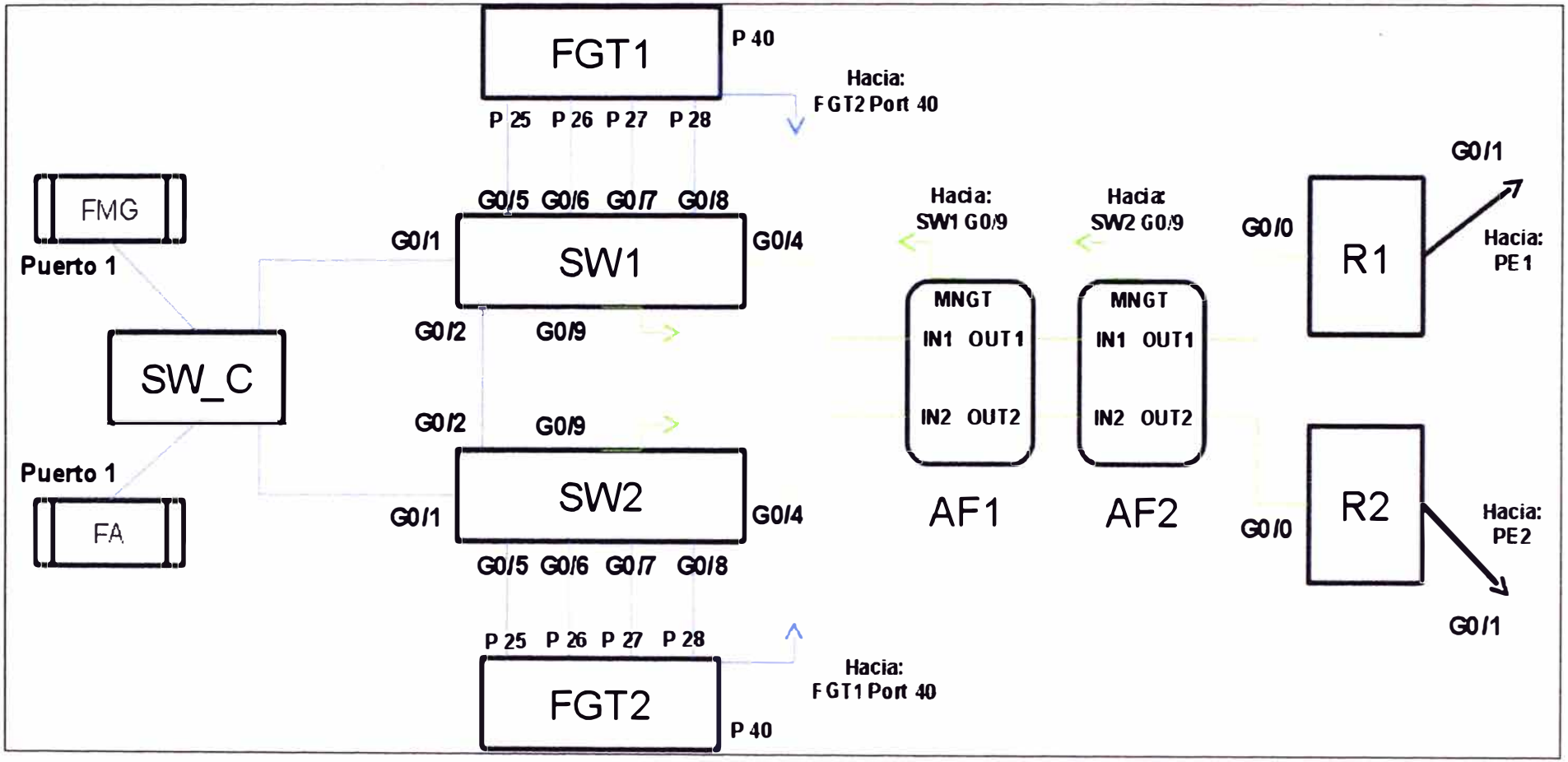

Figura 3.20 Diagrama de conexiones de la solución

Asimismo se aplicaron políticas en la capa aplicaciones para garantizar el acceso a páginas web de vital importancia para la Universidad, por ejemplo la página de acceso al correo web institucional alojado en Edu@Live, páginas de acceso a bibliotecas digitales, páginas de gobierno (SENAMHI, INEI, MEF, ProInversión, FITEL, etc.), es decir, con carácter administrativo y de investigación..

Dentro de la solución, uno de los equipos está configurado como maestro ("master") y el otro como esclavo ("slave"), ésta sincronización se mantiene por medio de un cable HA, lo cual permite que cualquier cambio de políticas en el equipo master sea automáticamente replicado en el equipo slave.

Ésta configuración también permite brindar alta disponibilidad ante la caída de uno de los equipos, ya que el equipo esclavo está continuamente verificando el estado del equipo maestro por medio del cable HA, asumiendo el rol de maestro automáticamente en caso detecte una caída. Cabe señalar que el equipo averiado a nivel físico se comporta como un cable, permitiendo al tráfico pasar sin interrupciones.

a.3 Equipos FortiGate (FGT)

Son la puerta de enlace para los usuarios de la red de la universidad, por ella pasa tanto el tráfico interno (entre facultades, consultas internas hacia la DMZ, etc.), como el tráfico hacia/desde Internet, por tanto dentro de la topología lógica esta delante de la red interna de la Universidad.

Con la finalidad de un mejor orden de las políticas de seguridad se usan dominios virtuales (VDOMS) que agrupan a las distintas dependencias de la universidad en función a los recursos a los que estos acceden, siendo funcionalmente una VDOM un firewall UTM independiente.

Dentro de la solución uno de los equipos está configurado como maestro y el otro como esclavo, esta configuración permite brindar alta disponibilidad ante la caída de uno de los equipos, ya que el equipo esclavo está todo el tiempo verificando el estado del equipo maestro por medio de un cable HA, asumiendo el rol de equipo maestro automáticamente apenas pierde la comunicación con él.

a.4 Equipos de Conmutación (SW)

Su función es conmutar el tráfico que cursan los equipos conectados a sus puertos, dirigiéndolo hacia el puerto por donde se llega al equipo de destino, para ello se basa en las direcciones MAC. Cumplen la función de interconectar, física y lógicamente, a los equipos que forman parte de la solución con la red LAN de la Universidad.

b. Funcionalidad a nivel de sistema

Dentro de la solución se ha modelado lógicamente las conexiones basándose en la infraestructura de la universidad mediante la utilización de dominios virtuales (VDOMs).

La utilización de dominios virtuales permite establecer una arquitectura virtual, permitiendo ordenar las múltiples redes lógicas independientes (VLANs) que conforman la red interna de la universidad, ayudando a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. También permite establecer reglas personalizadas de acuerdo a las funciones y actividades de cada área ó tipo de usuarios.

Un dominio virtual (VDOM) puede representar a una dependencia de la universidad o a una zona perimetral. Una dependencia puede a su vez contener un área o más de una, cada área está identificada por un número de VLAN. Para identificar las dependencias de la Universidad, se han creado las VDOMs: ADMINISTRATIVOS, FACULTADES, ALUMNOS, INALAMBRICO y EVENTOS.

Una zona perimetral, se ubica entre la red interna de la universidad y la red externa (Internet) permitiendo ordenar lógicamente las conexiones entre las dependencias, las conexiones hacia/desde la DMZ, y las conexiones hacia/desde Internet. Para identificar las zonas perimetrales, se ha creado las VDOM: UNIVERSIDAD, DMZ, INTERNET.

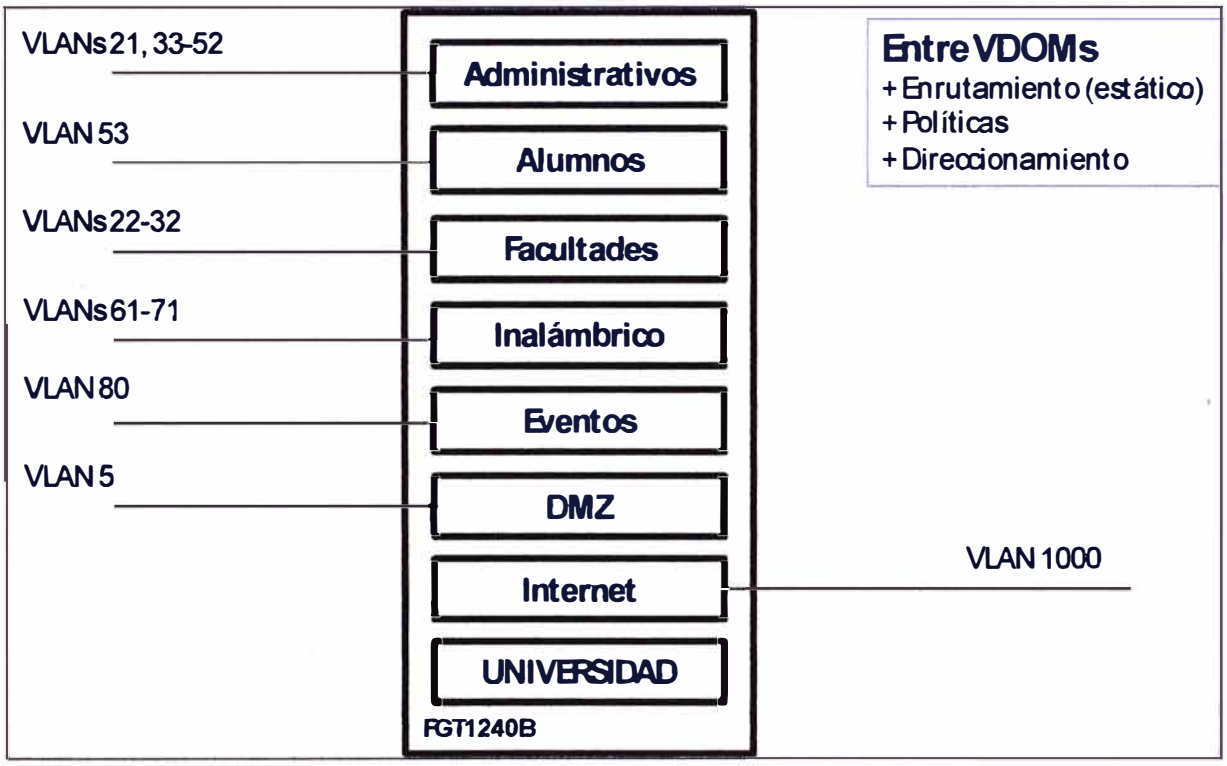

Figura 3.25 Esquema lógico de virtualización del FortiGate.

Para ordenar las conexiones entre las dependencias, se ha configurado una zona perimetral identificada con la VDOM UNIVERSIDAD. Esto permite definir políticas específicas para controlar, por ejemplo, las conexiones de los usuarios de la VDOM Facultades a los recursos de la VLAN Administración Central (Figura 3.21).

Para ordenar las conexiones entre los usuarios de las dependencias de la Universidad y los servidores de la DMZ, se ha configurado una zona perimetral

identificada con la VDOM DMZ (Zona desmilitarizada), utilizándose políticas de seguridad en el firewall (Figura 3.22).

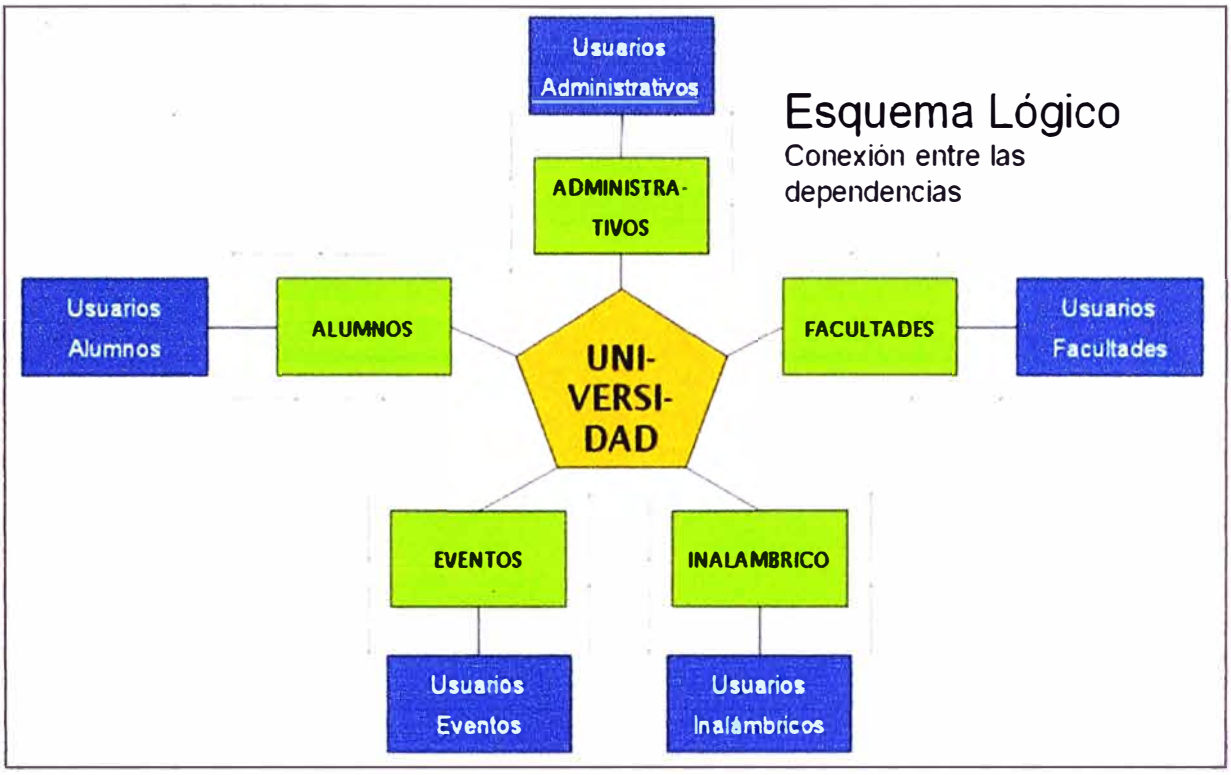

Figura 3.21 Conexiones lógicas entre las dependencias.

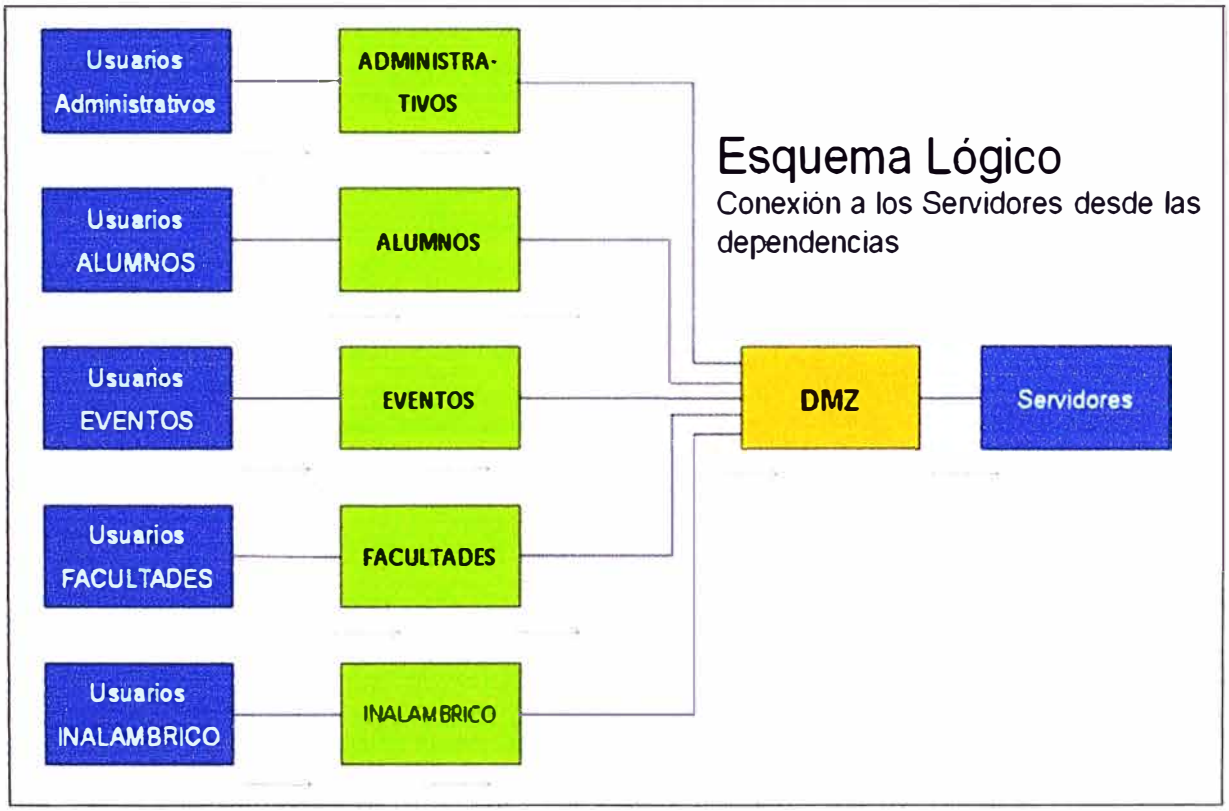

Figura 3.22 Conexiones lógicas a los Servidores desde las dependencias.

Para ordenar las conexiones entre los usuarios de las dependencias de la Universidad e Internet se ha configurado una zona perimetral identificada con la VDOM

INTERNET, donde se establecen los privilegios de los usuarios a acceder a contenidos de Internet mediante la utilización de la funcionalidad de Filtrado de URL. La función principal de la VDOM es la de realizar el NAT (Figura 3.23).

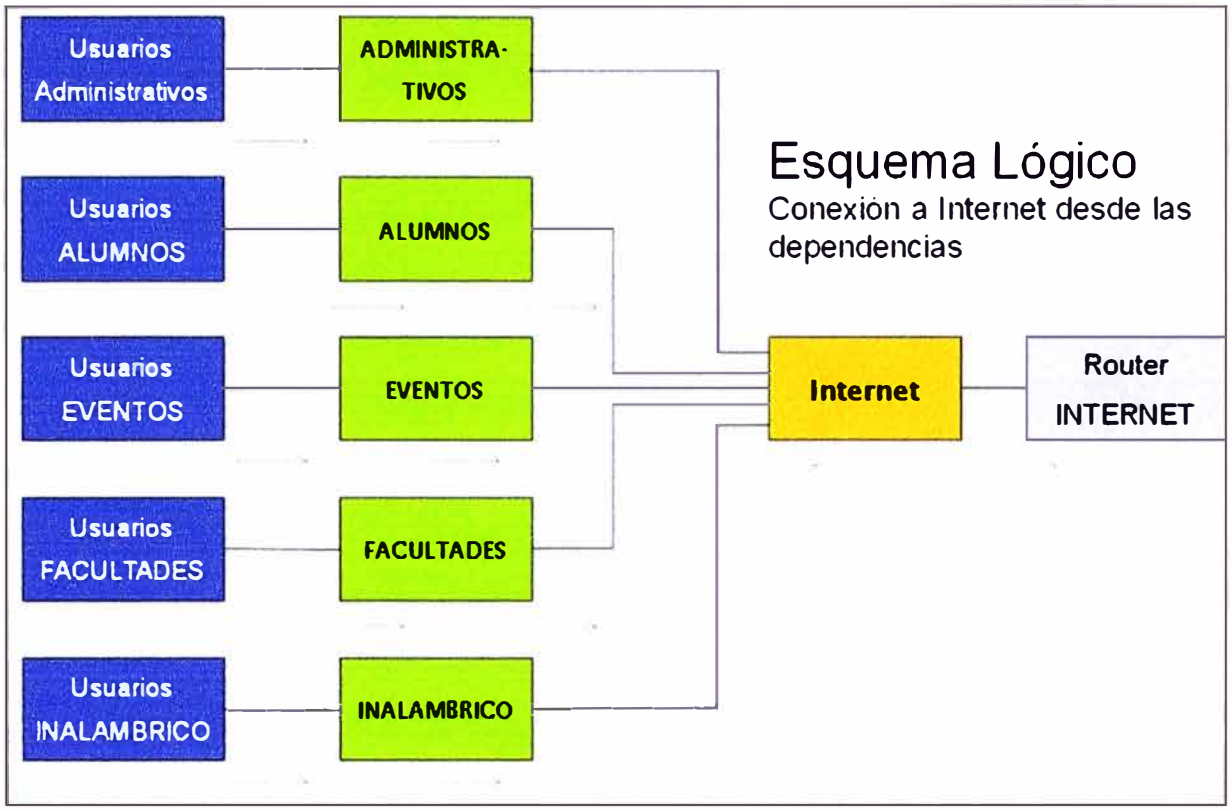

Figura 3.23 Conexiones lógicas a Internet desde las dependencias.

En la VDOM INTERNET también se establecen políticas de seguridad a las conexiones entre los servidores de la DMZ e Internet, utilizándose la funcionalidad de Prevención de Intrusos (IPS). Ver Figura 3.24.

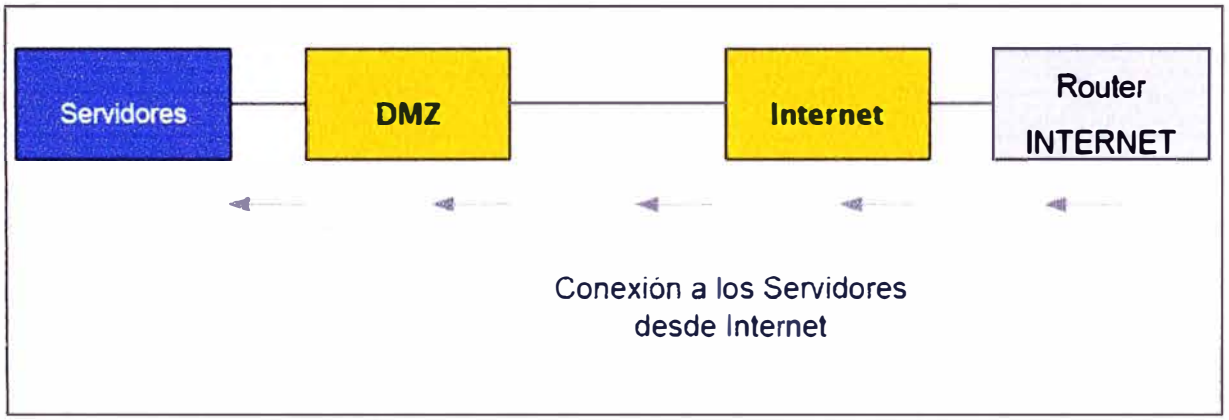

Figura 3.24 Conexiones lógicas a los Servidores desde Internet.

En total se crearon ocho VDOMs (Administrativos, Alumnos, Facultades, Universidad, Eventos, Internet, DMZ, Inalámbrica).

Se modeló el tráfico de interés por segmento, mediante el uso de redes lógicamente independientes (VLANs), asignándoles una cuota de ancho de banda y configurándose

mayor prioridad para el acceso a los protocolos de interés según su actividad, mediante el equipo de administración del tráfico. Según se muestra en la Tabla 3.9. No se incluye el direccionamiento público de la solución por un aspecto de confidencialidad.

Tabla 3.9 Cuota de ancho de banda

VDOM	Área	VLAN	Porcentaje	BW
Administrativos	Centro T.I.C.	21	6	10.8
	Investigación Sísmica	33	2.4	4.32
	Biblioteca	34	2.4	4.32
	Autoridades	35	3	5.4
	Logística y Planificación	36	3	5.4
	Escuela de Postgrado	37	9.48	17.064
	Departamento Medico	38	2	3.6
	Departamento de Finanzas	39	2	3.6
	Proyección Social	40	4	7.2
Alumnos	Residencia Universitaria	53		4
Facultades	Facultad A	31	9.48	17.064
	Facultad B	22	9.48	17.064
	Facultad C	23	4.26	7.668
	Facultad D	24	4.26	7.668
	Facultad E	25	4.26	7.668
	Facultad F	26	4.26	7.668
	Facultad G	27	4.26	7.668
	Facultad H	28	4.26	7.668
	Facultad I	29	4.26	7.668
	Facultad J	30	4.26	7.668
	Facultad K	32	4.26	7.668
Inalambrico	Facultad A	61	0	0
	Facultad B	62	0	0
	Facultad C	63	0	0
	Facultad D	64	0	0
	Facultad E	65	0	0
	Facultad F	66	0	0
	Facultad G	67	0	0
	Facultad H	68	0	0
	Facultad I	69	0	0
	Facultad J	70	0	0
	Facultad K	71	0	0
Eventos	Eventos	80	0	0
Internet	Red Publica		0	0
DMZ	Servidores Universidad	5	8	14.4
UNI	Policy InterVDOM		0	0
root	Device Manager Broup		0	0

Para establecer estas reglas personalizadas se tomo en cuenta que la Universidad tiene establecida mediante Resolución Rectoral una división del ancho de banda por porcentajes según el aporte económico de cada dependencia; así como también se tomó en cuenta la dinámica del acceso a las aplicaciones de Internet (prioridad según tipo tráfico), en base a información recopilada en un periodo de prueba de una semana en la cual el equipo administrador de tráfico estuvo monitoreando el tráfico de los usuarios hacia Internet, lo cual permitió mediante un análisis estadístico y funcional determinar las políticas a aplicar.

Las actividades de observación del tráfico diferenciado por protocolos se realizaron en un terminal (PC) del cliente, mediante el software FlowReport, propietario de la marca ASCENFLOW. Este terminal está conectado al equipo SW_C, y pertenece al dominio de la VLAN 3 para poder comunicarse con los equipos ASCENFLOW que le proveen la información para sus reportes en línea.

El sistema esta conceptualizado para funcionar en alta disponibilidad, para ello se ha establecido ciertas configuraciones en los equipos que forman parte de la solución y los equipos en la red del proveedor, mediante el uso del protocolo BGP externo e interno.

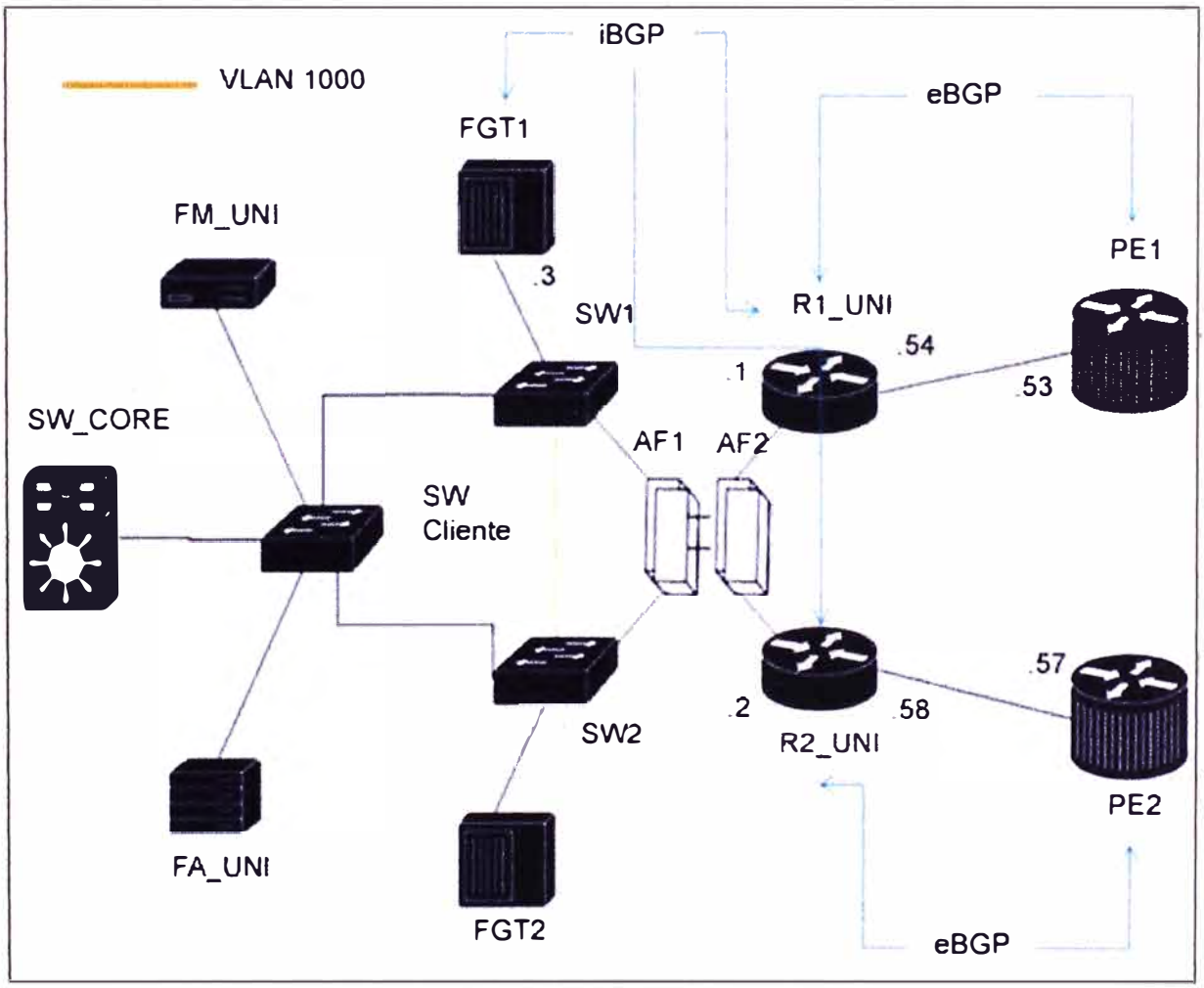

Figura 3.25 Solución a nivel de enrutamiento

Enrutamiento EBGP

R1_UNI y R2_UNI reciben la ruta cero de PE1 (WASPENG1) y PE2 (MONPENG2) respectivamente. Así también, R1_UNI y R2_UNI se encargan de redistribuir las redes LAN asignadas a la UNI tanto a PE1 como a PE2.

Así también, el equipo R1_UNI envía estas redes LAN hacia el equipo PE1 con el parámetro "local-preference" configurado en 100, y el equipo R2_UNI lo envía con el valor de 90. Por lo expuesto, desde INTERNET el cliente es conocido preferentemente a través del equipo PE1 y en caso de caída de este equipo, el cliente será conocido a través del equipo PE2.

Enrutamiento IBGP

Los equipos R1_UNI y R2_UNI establecen sesiones IBGP con el equipo FORTIGATE virtual (FGT_HA) que representa el comportamiento de alta disponibilidad establecido entre FGT1 y FGT2.

Los equipos R1_UNI y R2_UNI se encargan de redistribuir la ruta cero aprendida por EBGP hacia el equipo FGT_HA, sin embargo, R1_UNI envía a FGT_HA la ruta con el parámetro "local-preference" configurado a 100 y el equipo R2_UNI lo envía con valor de 90.

Por lo expuesto, la red LAN de la universidad se conectará de forma preferente hacia Internet a través del equipo R1_UNI y en caso de caída de este equipo, llegará a Internet a través del equipo R2_UNI.

VLANs

A nivel de VLAN, la solución se plantea bajo el esquema mostrado en la Figura 3.26 . Cada interfaz mostrada permite solamente las VLAN indicada en la leyenda adjunta de la propia figura.

Esta declaración de VLAN forma parte de la configuración de los puertos utilizados en los switches SW1, SW2 y SW_C. Así también, para todas las VLAN configuradas, el SW1 hace la función de "ROOT BRIDGE" (también conocido como switch raíz del spanning tree).

Las VLANs pertenecientes a las dependencias de la UNI están identificadas con VLAN ID del 21 al 40, la VLAN perteneciente a la DMZ con el VLAN ID: 5, la VLAN de comunicación entre los equipos de la solución está identificada con el VLAN ID: 3, y como medida de seguridad se ha establecido una VLAN de Gestión identificada con el VLAN ID: 1000; es necesario que en los switches SW1 y SW2 y en el SW_CLIENTE se configuren estas VLANs de lo contrario la solución podría no funcionar.

Finalmente, los enlaces mostrados entre SW1 y FGT1 como entre el SW2 y FGT2 son enlaces PORT-CHANNEL (CISCO) o LINK-AGGREGATE (FORTINET) conformados

cada uno por dos enlaces GIGABITETHERNET (TRUNK).

En la Figura 3.26 se muestra el diagrama de conexiones a nivel de switching.

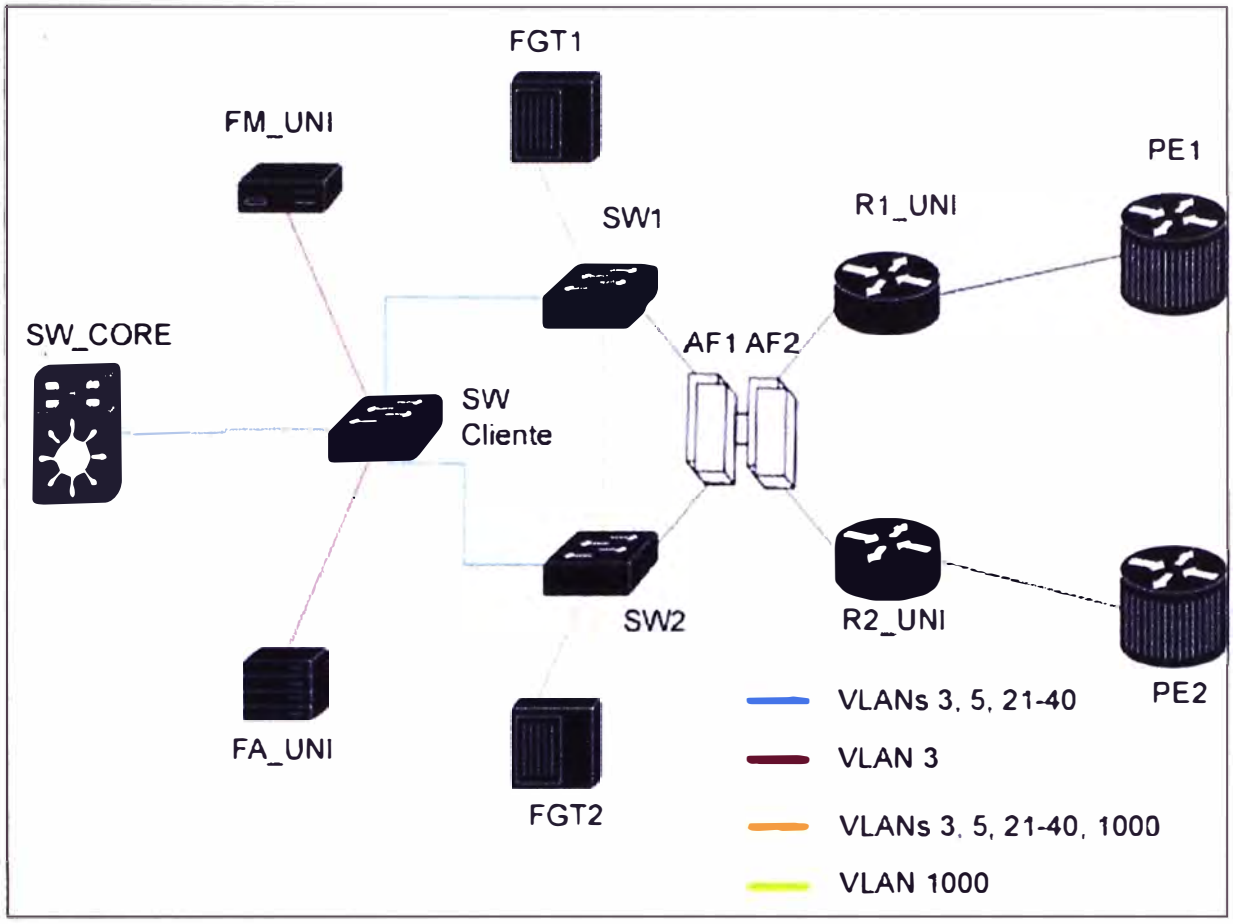

Figura 3.26 Diagrama de conexiones a nivel de switching

3.2.3 Descripción de la configuración

Las plantillas de configuración de los equipos se encuentran ubicadas en el Anexo X del presente documento.

En el presente capitulo describiremos los aspectos más importantes de la configuración de cada equipo, poniendo énfasis a aquellos comandos que permiten la alta disponibilidad de la solución.

a. Equipos de Enrutamiento (R):

Los pasos a seguir para configurar el router Cisco 3945/K9 son: configurar el nombre del equipo (hostname), crear los usuarios que podrán acceder al equipo y su nivel de privilegios, configurar las interfaces GigaEthernet (hacia PE1 y hacia SW1), configurar el protocolo de enrutamiento BGP y la comunidad BGP.

b. Equipos de Conmutación (SW):

Los pasos a seguir para configurar el switch Cisco 2960G son: configurar el nombre del equipo (hostname), crear los usuarios que podrán acceder al equipo y su nivel de privilegios, configurar el protocolo de spanning tree, configurar las interfaces GigaEthernet, y configurar las VLANs permitidas por interfaz.

c. Equipos FortiGate (FGT):

El equipo FortiGate tiene una interfaz grafica (GUI) para configurar los equipos. Primero se establecen los permisos de administración, luego se crean las VDOMs, y en una VDOM se crean las políticas de seguridad.

Luego se activan los módulos de seguridad que necesita cada VDOM (por ejemplo: IPS, Filtro Web, Antivirus/Antispam, etc).

Se crean los perfiles de administración tanto para el usuario como para el soporte del proveedor, se configura los envíos de logs hacia los equipos FortiAnalyzer y FortiManager. La Figura 3.27 muestra un detalle de la interfaz Fortigurad

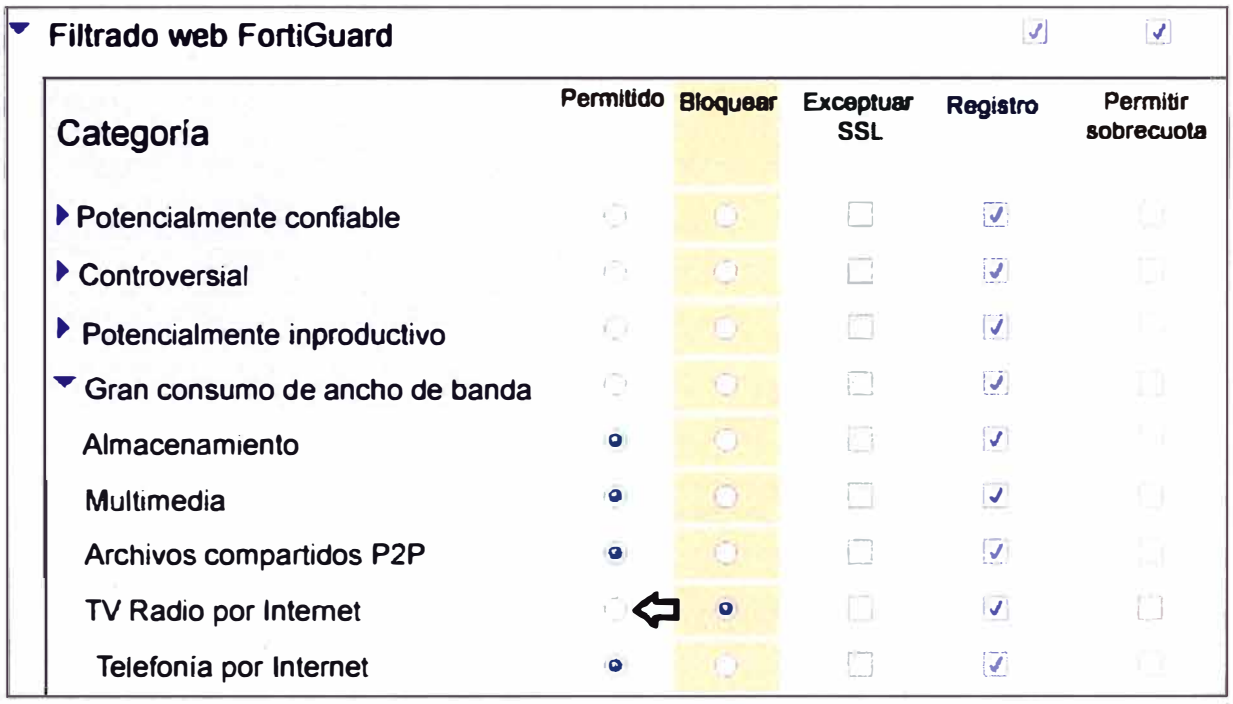

Figura 3.27 Interfaz FortiGuard

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

En el presente capítulo se tocan los temas involucrados al presupuesto, al cronograma, al análisis de la disponibilidad y a la presentación de resultados.

4.1 Relación de equipamiento

La Tabla 4.1 muestra el listado de equipos, licencias y aplicativos utilizados en el proyecto.

Tabla 4.1 Listado de equipos

Ítem	Descripción	Unidad	Cantidad
1	FortiGate-1240B 24x7 Comprehensive Support Bundle. 3 Year 24x7 Comprehensive Bundle	unidad	2
2	FortiManager-400B. FortiManager-400B, manages up to 200 FortiGate devices, recommended for all FG models	unidad	1
3	FortiManager-400B 24x7 Comprehensive FortiCare. 3 Year 24x7 Comprehensive FortiCare	unidad	1
4	FortiAnalyzer-1000B. FortiAnalyzer-1000B, One (1) removable 1TB HDD, up to 1000 logs/sec, up to 2000 devices (any FortiGate model),rack mountable	unidad	1
5	ASCENFLOW M1001I	unidad	2
6	ASCENFLOW M1001I-RPT	unidad	2
7	CISCO 2960G-24TC-L	unidad	2
8	CISCO 3945/K9	unidad	2
9	Interfaces de fibra SFP	unidad	4
10	Cable UTP categoría 6	metro	100

4.2 Estimación de costos

Los costos del proyecto fueron organizados de la siguiente manera, y se encuentran descritos en las Tablas 4.2, 4.3, 4.4 y 4.5.:

- Costos de adquisición de equipamiento.

- Costos de conectividad.
- Costos de instalación y puesta en marcha.
- Costos de capacitación, garantía y de soporte técnico.

Tabla 4.2 Costos de adquisición de equipamiento

N°	Ítem	Cant.	Descripción	Marca Modelo	Precio Unitario Dólares	Precio Total Dólares
1	Router CISCO 3945/K9 con 02 HWIC-1GE-SFP, 01 HWIC-4ESW y 02 GLC-LH-SM	2 un	Equipo de enrutamiento con tarjetas de switching y puertos GE.	CISCO 3945/K9	10,741.54	21,483.08
2	FortiGate-1240B 24x7 Comprehensive Support Bundle. 3 Year 24x7 Comprehensive Bundle	2 un	Equipo Firewall UTM con soporte 24x7 por 03 años.	FORTINET FORTIGATE 1240B	29,129.01	58,258.02
3	FortiManager-400B. FortiManager-400B, manages up to 200 FortiGate devices, recommended for all FG models	2 un	Equipo de Administración Centralizada, gestión para hasta 200 dispositivos FortiGate.	FORTINET FORTI-MANAGER 400B	5,244.09	5,244.09
4	FortiAnalyzer-1000B. FortiAnalyzer-1000B, One (1) removable 1TB HDD, up to 1000 logs/sec, up to 2000 devices (any FortiGate model), rack mountable	2 un	Equipo de Administración de Reportes, gestión para hasta 2000 dispositivos.	FORTINET FORTI-ANALYZER 1000B	6,410.09	6,410.09
5	ASCENFLOW M1001I	2 un	Equipo de Administración de Trafico WAN.	XTERA ASCENFLOW 1001I	8,500.00	17,000.00
6	M1001I-RPT FLOW REPORT	2 un	Licencia para Software de Reportes.	XTERA ASCENFLOW FLOWREPORT	2,500.00	5,000.00
7	CISCO 2960G-24TC-L	2 un	Equipo Switch de 24 puertos 10/100/100.	CISCO 2960G-24TC-L	1,975.35	3,950.71
8	PUERTO GIGAETHERNET	2 un	Adquisición de 2 Tarjetas y 2 Módulos Ópticos.	CISCO	3,000.00	6,000.00

Tabla 4.3 Costos de Conectividad

N°	Ítem	Cant.	Descripción	Precio Unitario Dólares	Precio Total Dólares
1	Acceso a Internet de 200 Mbps para Enlace Principal	200 Unidades	Servicio Internet@s a 200Mbps	45.00	9,000.00
2	Acceso a Internet de 200 Mbps para Enlace Contingencia	200 Unidades	Servicio Internet@s a 200Mbps	45.00	9,000.00

Tabla 4.4 Costos de Instalación y Capacitación

N°	Descripción	Cant.	Descripción	Precio Unitario Dólares	Precio Total Dólares
1	Instalación de Equipos de FORTINET y CISCO	1 Unidad	Servicios de Telefónica	0.00	0.00
2	Workshop CCNA de 30 horas	1 Unidad	Capacitación en Equipos CISCO	1,985.00	1,985.00
3	Workshop-Fortinet no certificado para 4 personas de 24 horas	1 Unidad	Capacitación en Equipos de Seguridad	2,600.00	2,600.00
4	Instalación de equipos ASCENFLOW y capacitación para 04 personas de 50 horas.	1 Unidad	Servicios Externos	1,000.00	1,000.00
5	Estudio Especial: Habilitación de Fibra Óptica	1 Unidad	Habilitación de fibra óptica	24,000.00	24,000.00
6	Estudio Especial: Instalación de Tarjetas Giga-Ethernet en Nodos del Rimac y Los Olivos	1 Unidad	Instalación, Cableado y Puesta en Producción de Tarjetas.	750.00	750.00
7	Estudio Especial: Configuración y Activación de Puerto Giga Ethernet	1 Unidad	Configuración y Activación de Puerto Giga Ethernet	1,050.00	1,050.00

Tabla 4.5 Garantía y Soporte técnico

N°	Descripción	Cant.	Descripción	Precio Unitario Dolares	Precio Total Dolares
17	FortiManager-400B 24x7 Comprehensive FortiCare. 3 Year 24x7 Comprehensive FortiCare	1 Unidad	Soporte 24x7 para equipos FortiManager 400B	5,017.52	5,017.52
18	Garantía Anual para equipo Ascenflow M10001l ó M1001l-RPT (Flow Report)	6 Unidad	Garantía Anual	1,250.00	7,500.00
19	CISCO Shared Support para Router CISCO 3945/K9 por año	6 Unidad	Garantía Anual	684.89	4,109.34
20	CISCO Shared Support para Switch CISCO 2960G-24TC-L por año.	6 Unidad	Garantía Anual	24.74	148.44
	Soporte Técnico				
21	Asistencia Técnica Anual para Switch CISCO 2960G-24TC-L	6 Unidad	Asistencia Técnica Anual	34.20	205.20

4.3 Tareas y cronograma

La Figura 4.1 muestra el diagrama de Gantt. Las tareas están organizadas de la siguiente manera:

- Iniciación
- Planificación
- Ejecución, seguimiento y control.
- Cierre

4.3.1 Iniciación

Corresponde a las negociaciones previas al desarrollo del proyecto: Consta de las siguientes tareas (33 días):

- Firma del Contrato. 1 días
- Apertura Proyecto. 2 días
- Gestión Logística – Compras. 30 días
- Kick Off Proyecto (Reunión técnica inicial). 1 días
- Levantamiento de Información en local de Cliente. 10 días
- Generación OOSS (Ordenes de servicios). 3 días

4.3.2 Planificación

Consta del desarrollo del cronograma de implementación (4 días), la asignación de personal técnico (1 día) y la planificación de Instalación del equipamiento (82 días)

Éste último (77 días) consta de lo siguiente:

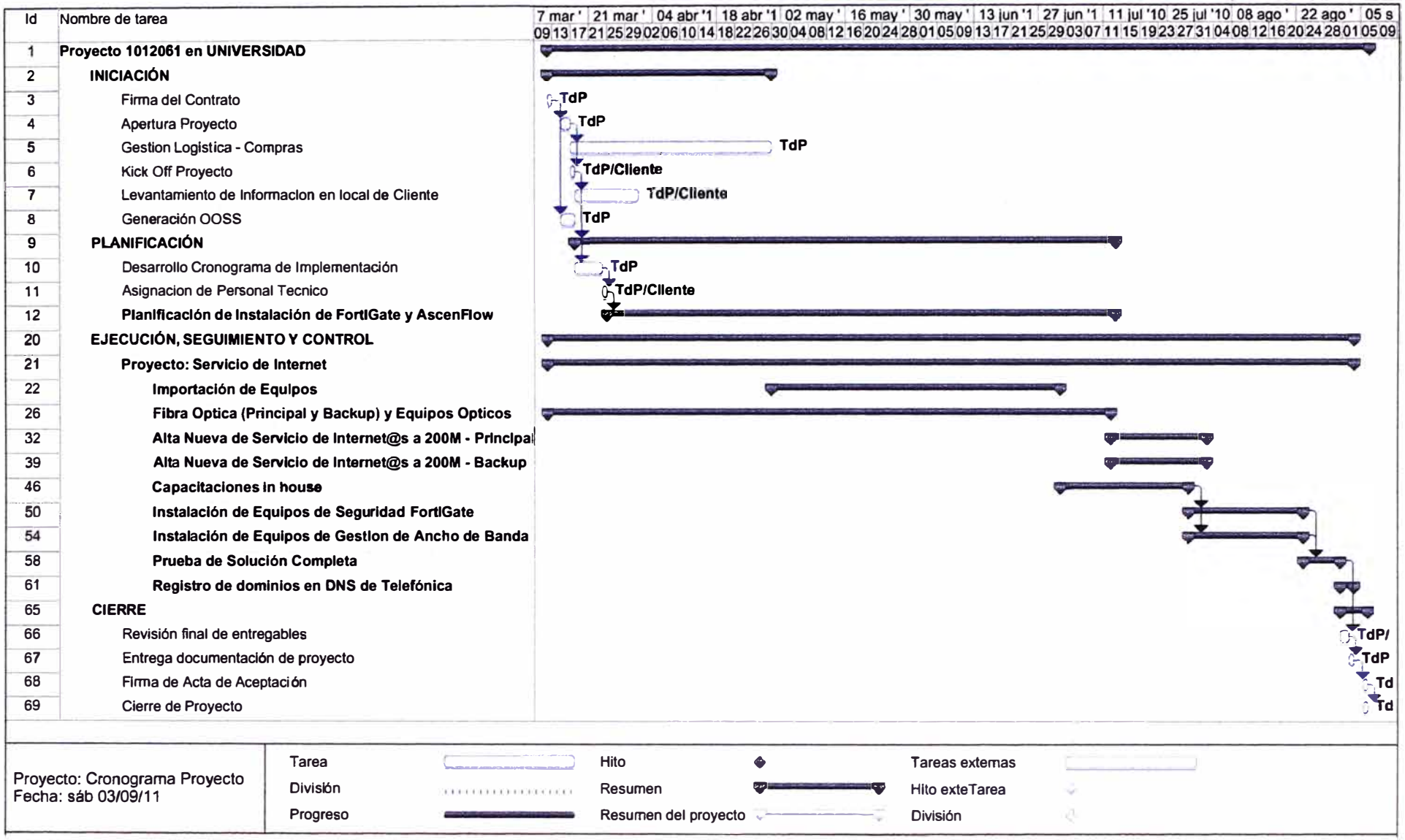

Figura 4.1 Diagrama de Gantt

Planificación de Instalación del equipamiento

- Reunión con Cliente. 1 día.
- Envío de Plantilla de Configuración de FortiGate y AscenFlow. 1 día.
- Envío de Información sobre Topología LAN. 15 días.
- Entrega de Documentación sobre Políticas de FortiGate. 30 días.
- Entrega de Documentación sobre Políticas AscenFlow.30 días.
- Revisión de Documentación entregada. 15 días
- Definición del Alcance de la Instalación. 30 días

4.3.3 Ejecución, seguimiento y control

Está dividido en las siguientes tareas (124 días):

a. Importación de Equipos

Consta de (45 días):

- Entrega de Equipamiento Cisco. 45 días
- Entrega de Equipamiento FortiGate. 45 días
- Entrega de Equipamiento Xtera. 45 días

b. Fibra Óptica (Principal y Backup) y Equipos Ópticos

Consta de (85 días):

- Permisos Municipales para Obras Civiles. 30 días.
- Obras Civiles. 30 días.
- Obras Civiles en local de cliente. 10 días.
- Tendido de FO. 15 días.
- Pruebas de Reflectometría y PMD. 1 día.

c. Alta Nueva de Servicio de Internet@s a 200M - Principal

Consta de (15 días):

- Habilitación de puerta GigaEthernet. 5 días.
- Prueba a nivel de transmisiones. 3 días.
- Configuración a nivel de Red. 3 días.
- Montaje de Equipo Router 3945. 1 día.
- Configuración del equipo. 1 día.
- Pruebas. 5 días.

d. Alta Nueva de Servicio de Internet@s a 200M - Backup

Consta de (15 días):

- Habilitación de puerta GigaEthernet. 5 días.
- Prueba a nivel de transmisiones. 3 días.
- Configuración a nivel de Red. 3 días.
- Montaje de Equipo Router 3945. 1 días.

- Configuración del equipo. 1 días.
- Pruebas. 5 días.

e. Capacitaciones in house

Consta de (20 días):

- Capacitación en Equipos Cisco. 20 días
- Capacitación en Equipos FortiGate. 20 días
- Capacitación en Equipos Xtera. 20 días

f. Instalación de Equipos de Seguridad FortiGate

Consta de (17 días):

- Montaje de Equipos FortiGate y 02 Switches 3560. 2 días.
- Configuración de equipos. 14 días.
- Pruebas. 1 día.

g. Instalación de Equipos de gestión de Ancho de Banda

Consta de (17 días):

- Montaje de Equipos. 2 días.
- Configuración de equipos. 14 días.
- Pruebas. 1 día.

h. Prueba de Solución Completa

Consta de (6 días):

- Pruebas y afinamientos en la configuración. 5 días.
- Validación de Checklist de Pruebas. 1 día.

i. Registro de dominios en DNS de Telefónica

Consta de (3 días):

- Envío de Formato por Cliente. 1 día.
- Configuración de nuevas IP publicas en servidores u otros. 1 día.
- Actualización de DNS. 1 día.

4.3.4 Cierre

Está dividido en las siguientes tareas (4 días):

- Revisión final de entregables. 2 días.
- Entrega documentación de proyecto. 1 día.
- Firma de Acta de Aceptación. 1 día
- Cierre de Proyecto. 1 día.

Nota:

Para un mayor entendimiento de la organización de actividades, en la siguiente página se proporciona un esquema desglosado de las actividades

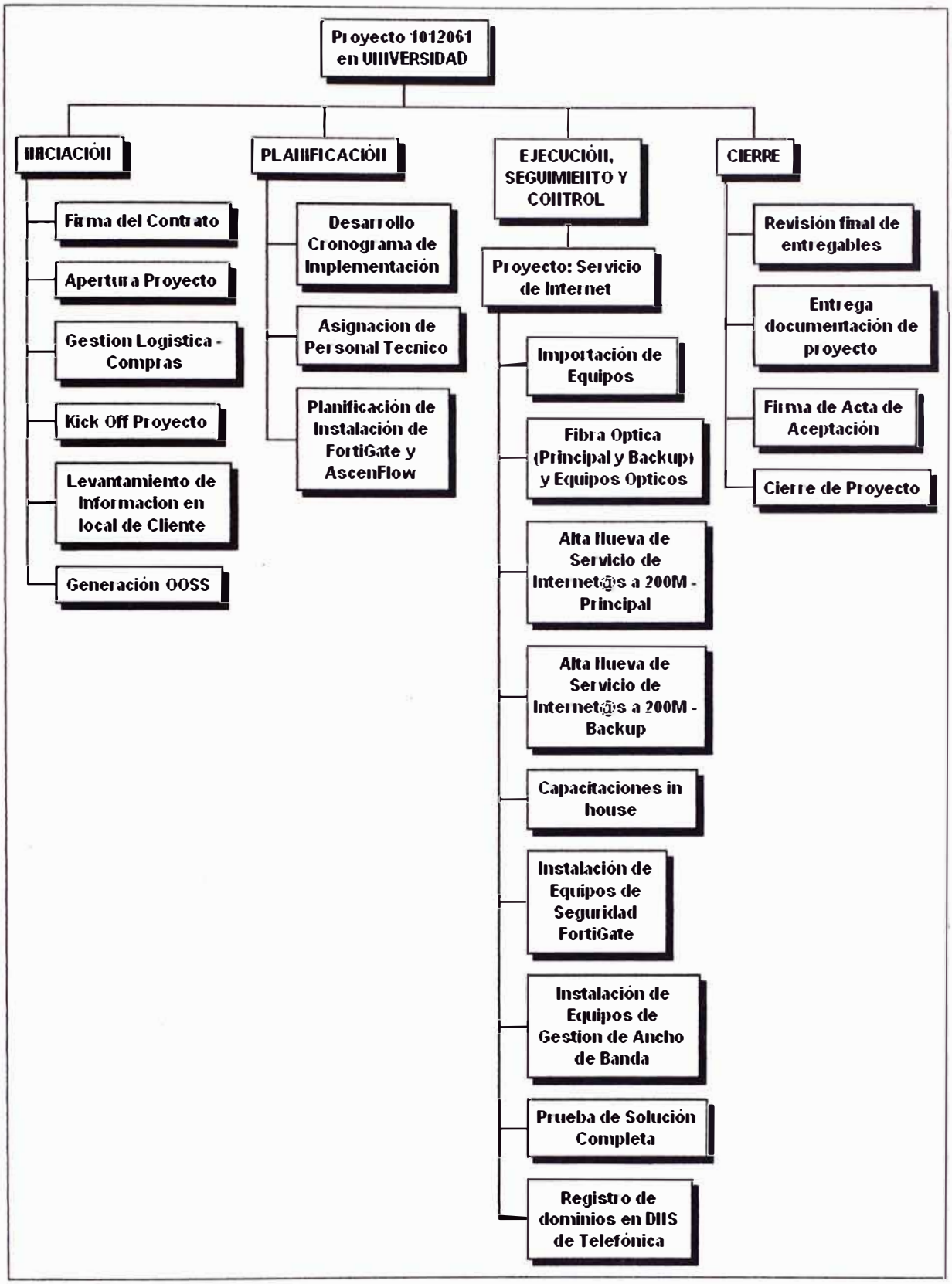

Figura 4.2 Desglose de actividades

4.4 Análisis de disponibilidad

Para el análisis de confiabilidad se ha visto la necesidad de desdoblar el diagrama de conexiones presentado en el capitulo anterior, de tal forma que permita un mejor análisis de los parámetros de disponibilidad (Figura 4.3).

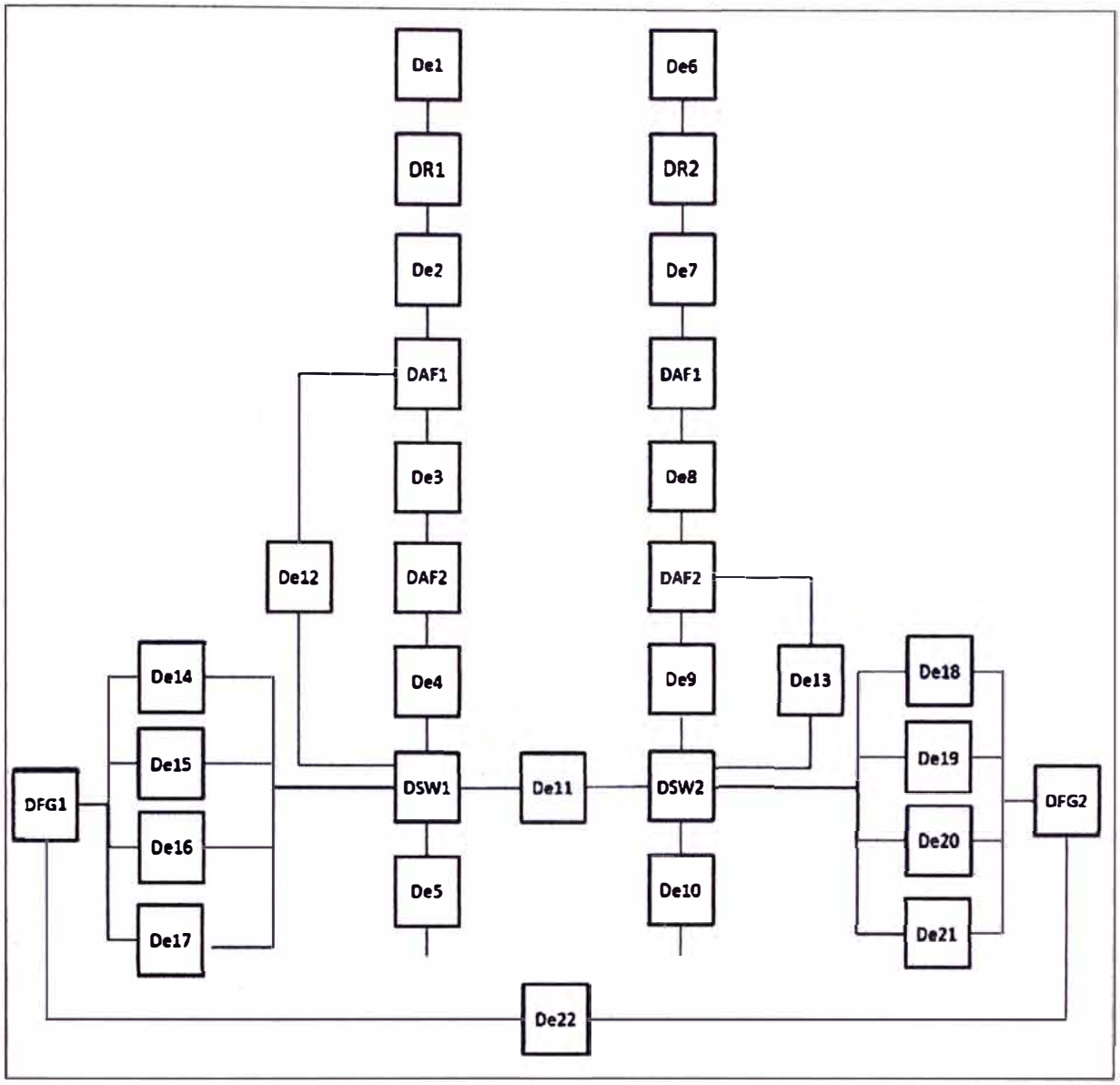

Figura 4.3 Esquema de conexiones

En la figura mostrada los componentes De11, De22, De23 son críticos ya que en caso de falla, toda la solución puede verse afectada, por tanto estos componentes irán en serie con la disponibilidad de los demás componentes de la solución.

En el caso de los componentes De12, De13 en caso de falla no se afecta la solución, por tanto no son críticos, y no serán considerados para el cálculo de la disponibilidad.

Comportamiento de la solución

Dado que la sesión eBGP establecida por R1 con PE1 tienen mayor prioridad que la sesión eBGP entre R2 y PE2, entonces el trafico de internet será enrutado por la red del proveedor hacia R1; y como la sesión iBGP establecida por R1 con FGT1 tienen mayor prioridad que la sesión iBGP entre R2 y FGT1, entonces, el trafico pasara por AF1, e3, AF2, e4, SW1, FGT1, y por medio del enlace e5 a la red LAN de la Universidad. Esto puede ser ilustrado con la Figura 4.4.

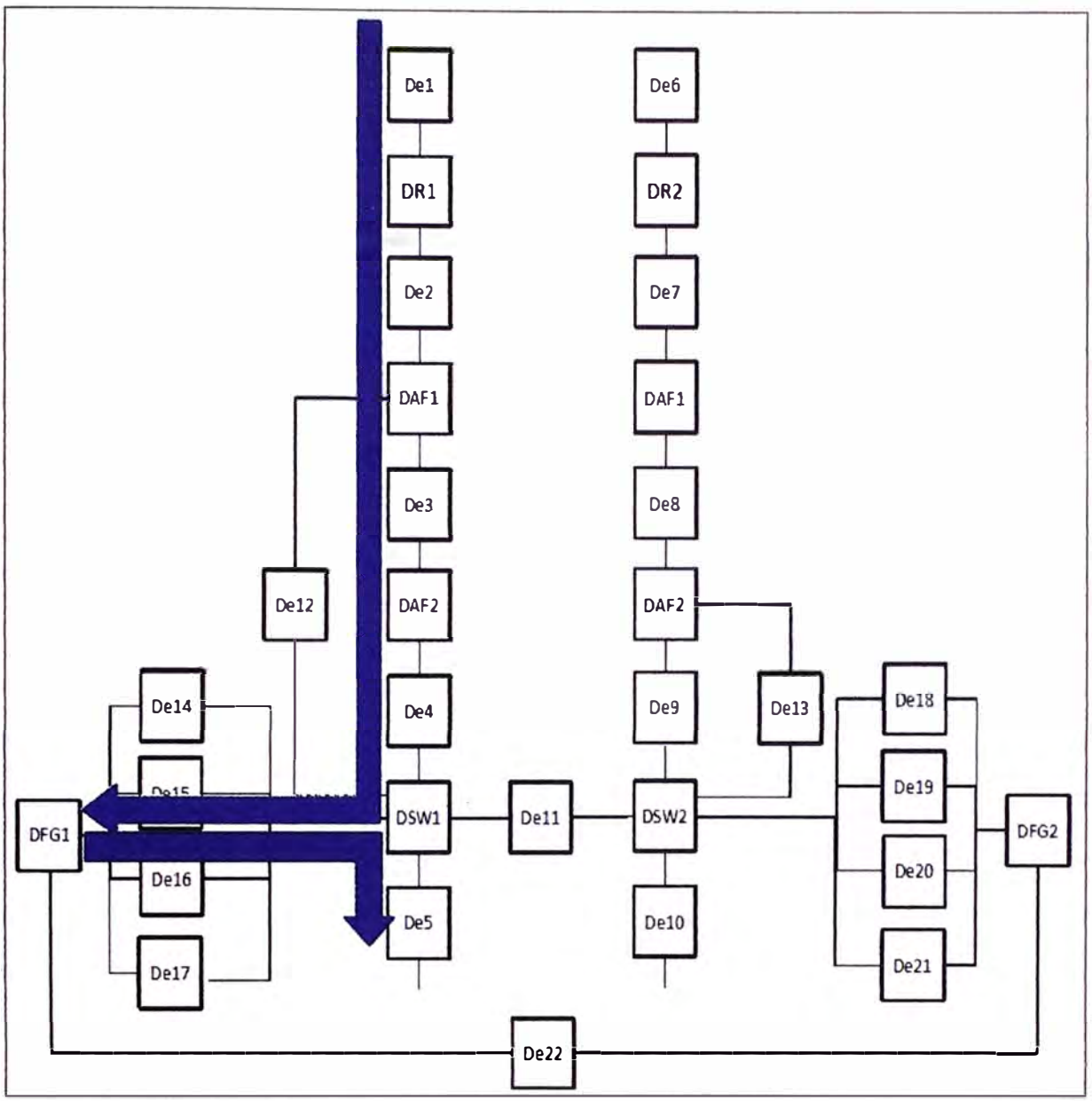

Figura 4.4 Funcionamiento normal de la solución.

4.4.1 Análisis de fallas

Antes de realizar el cálculo de la disponibilidad, se va a revisar cómo se comporta el tráfico ante la falla de uno de los componentes del sistema.

a. En caso de falla de e1, R1, e2, e3, e4

En caso de Falla de e1, R1, e2, e3, e4, automáticamente el tráfico será direccionado por la Red del Proveedor hacia R2, dado que la sesión iBGP establecida por R1 con FG1 se vería afectada, por tanto al caer la sesión con FG1 automáticamente la red del proveedor enrutará el tráfico hacia R2, pasando por SW1 y SW2 a través del enlace e11, pasando luego por el enlace e9, AF2, e8, AF1, e7 y llegando a R2. Ver Figura 4.5.

b. En caso de falla de e6, R2, e7, e8, e9

En caso de Falla de e6, R2, e7, e8, e9 dado que la sesión eBGP principal es entre la red del proveedor y R1, no ocurrirá una falla del sistema. Ver Figura 4.6.

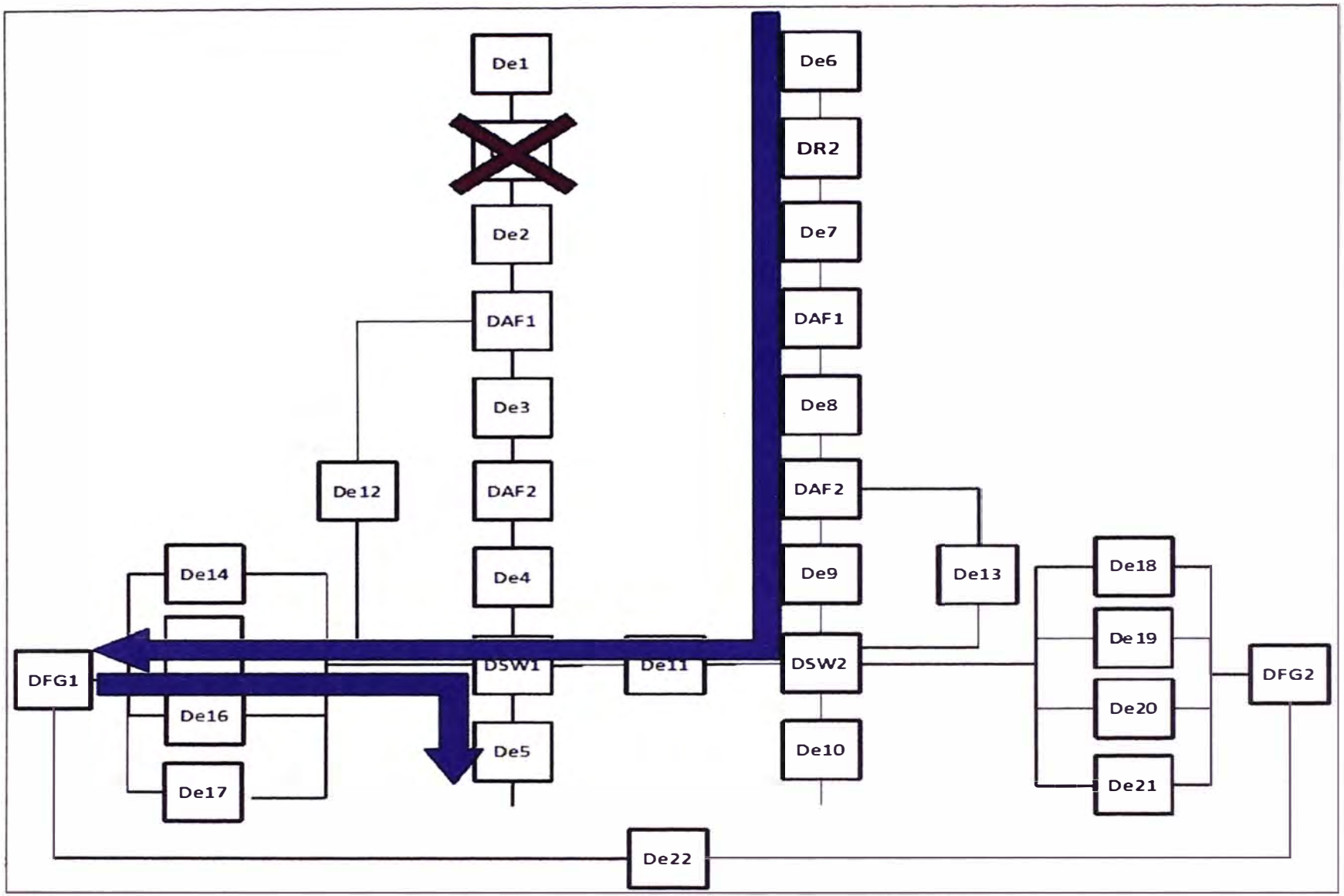

Figura 4.5 Funcionamiento en caso de caída de e1, R1, e2, e3, e4

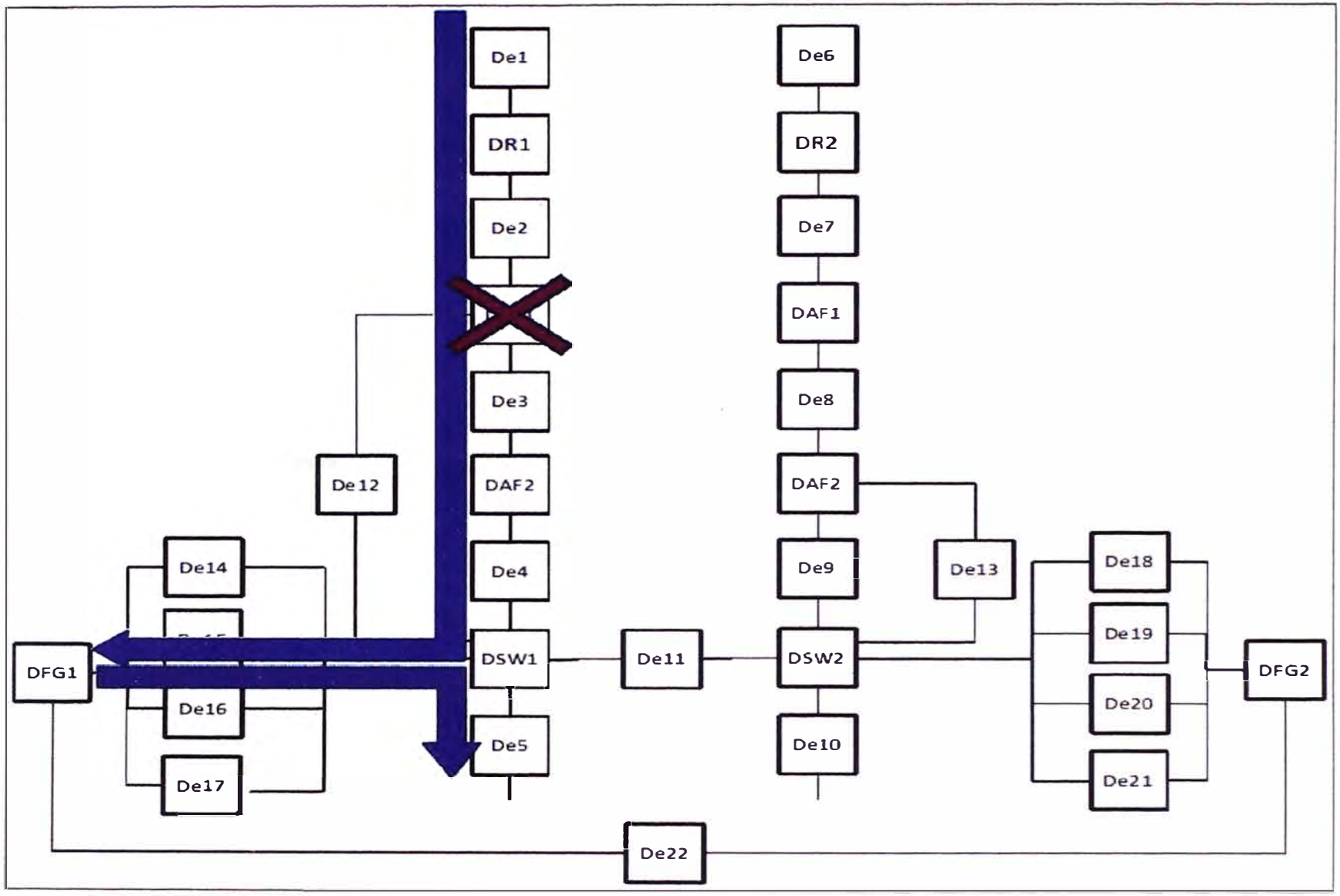

Figura 4.6 Funcionamiento en caso de caída de AF1 ó AF2

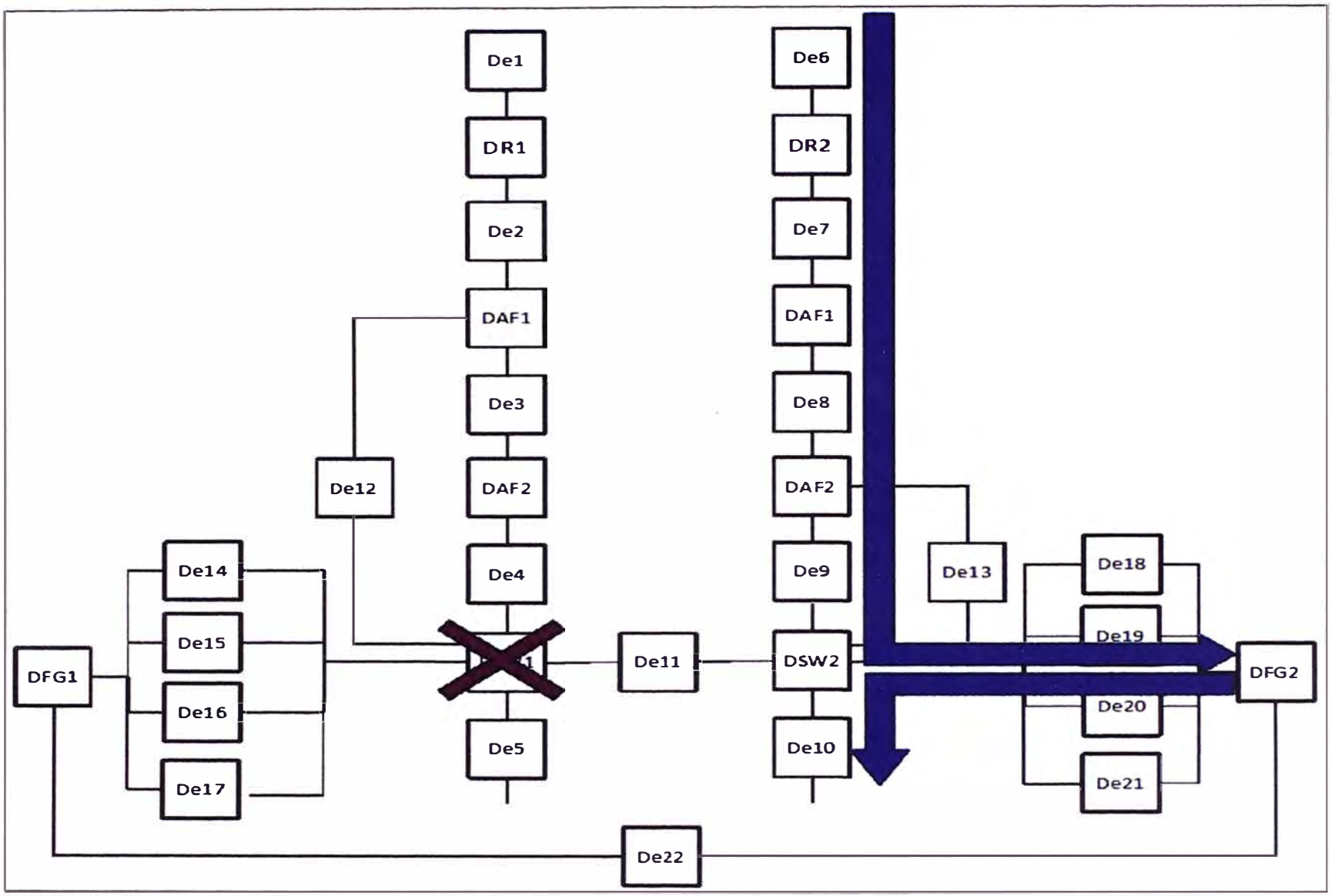

Figura 4.7 Funcionamiento en caso de caída de SW1

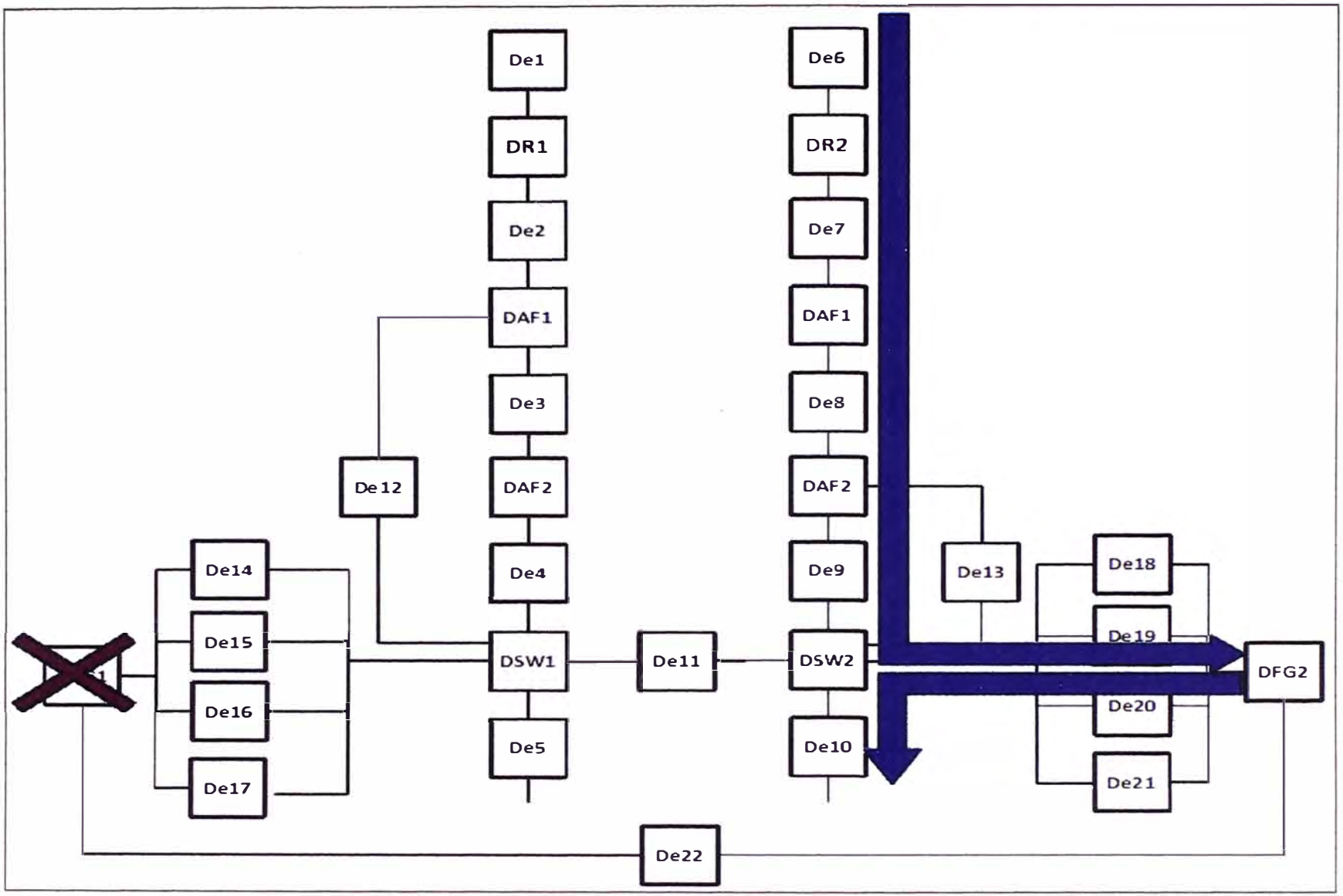

Figura 4.8 Funcionamiento en caso de caída de FG1.

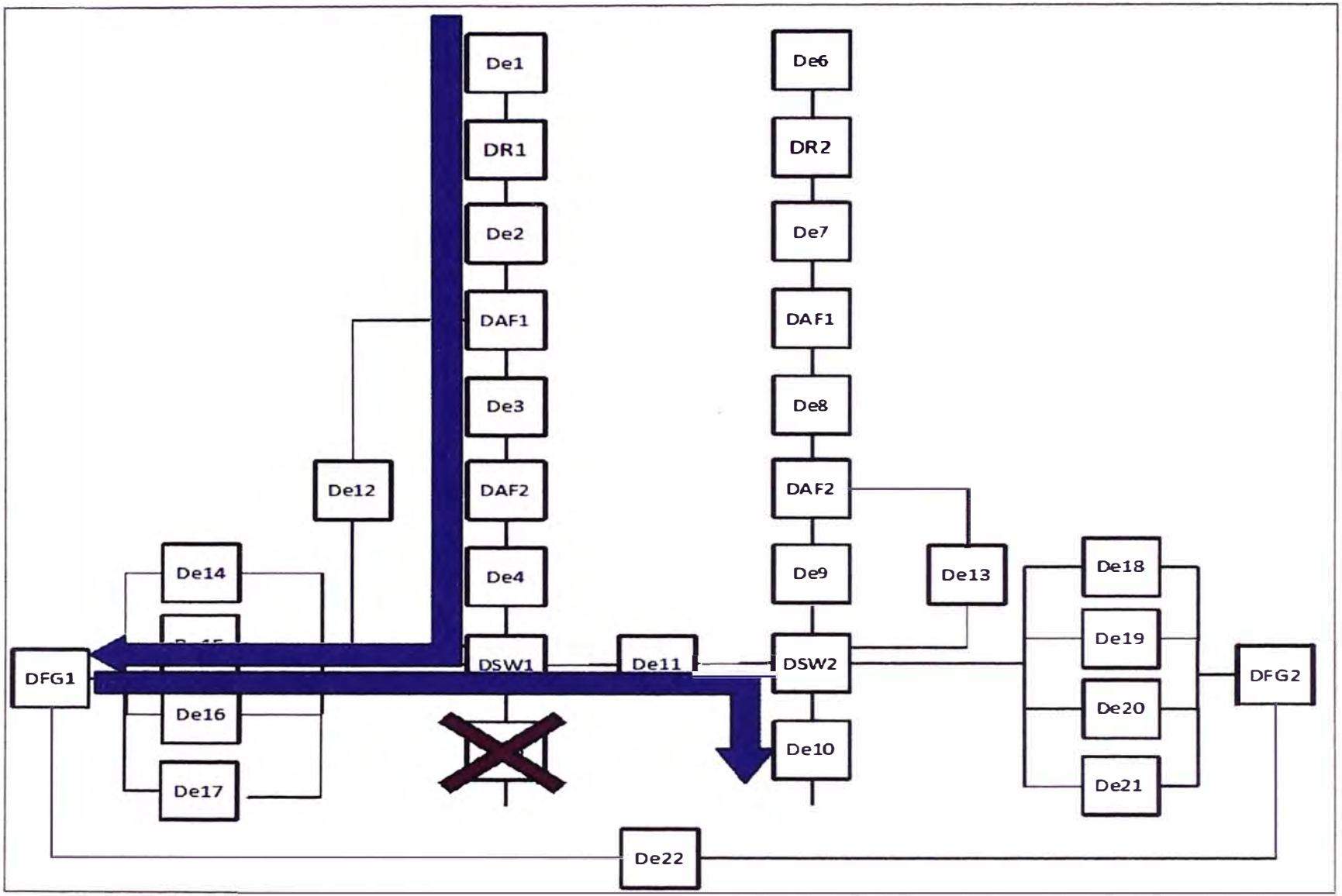

Figura 4.9 Funcionamiento en caso de caída de e5.

c. En caso de falla de AF1 ó AF2

En caso de falla de AF1 ó AF2, este equipo se comporta como un cable, asumiendo automáticamente la función de administrador de tráfico el equipo master ó esclavo que esta operativo. Ver Figura 4.7.

d. En caso de falla de SW1 ó FGT1

En caso de Falla de SW1 ó FGT1, dado que la sesión iBGP establecida por R1 con FGT1 y la sesión iBGP entre R2 y FGT1 se verían afectadas, entonces se establecería la sesión iBGP entre R2 y FGT2 lo cual mantendría la comunicación, automáticamente la red del proveedor enrutará el tráfico hacia R2, pasando por AF1, e8, AF2, SW2, FGT2, y por medio del enlace e10 a la red LAN de la Universidad. Ver Figura 4.8.

e. En caso de falla de e5

En caso de Falla de e5, el trafico seguiría la ruta de e1, R1, e2, AF1, e3, AF2, e4, SW1, FG1, SW1, e11, SW2 y por medio del enlace e10 a la red LAN de la Universidad. Ver Figura 4.9.

4.4.2 Cálculo de la disponibilidad

Para realizar el cálculo de la disponibilidad del sistema, es importante calcular la disponibilidad de cada componente (ver Tabla 4.6) a partir del valor de MTBF de las hojas técnicas y considerando el MTTR igual a 4 horas (tiempo promedio de reparación de averías para zonas urbanas del proveedor).

Tabla 4.6 MTBF, MTTR, y disponibilidad de equipos equivalentes y componentes

Componente	MTBF (horas)	MTTR (horas)	Disponibilidad
CISCO 3945/K9 (R)	61320	4	0.999935
FortiGate 1240B (FGT)	44391	4	0.999910
Administrador de Trafico (AF)	53436	4	0.999925
Switch 2960G (SW)	61320	4	0.999935
Cable UTP Cat. 6	175200	4	0.999977
Fibra Óptica	175200	8	0.999954

Para realizar el cálculo de la disponibilidad del sistema, se desdobla la solución en A y B (Figura 4.10), dado que la contingencia es del tipo activo-pasivo. Luego se calculará la disponibilidad de A y la disponibilidad de B independientemente, y finalmente se analizará el sistema en general.

Calculo de la Disponibilidad de A (Da):

DA=De1 x DR1 x De2 x DAF1 x De3 x DAF2 x De4 x DSW1 x (De15 // De16) x DFG1 x (De16 // De17) x DSW1 x De5

Del cálculo se desprende: DA=0.999427145

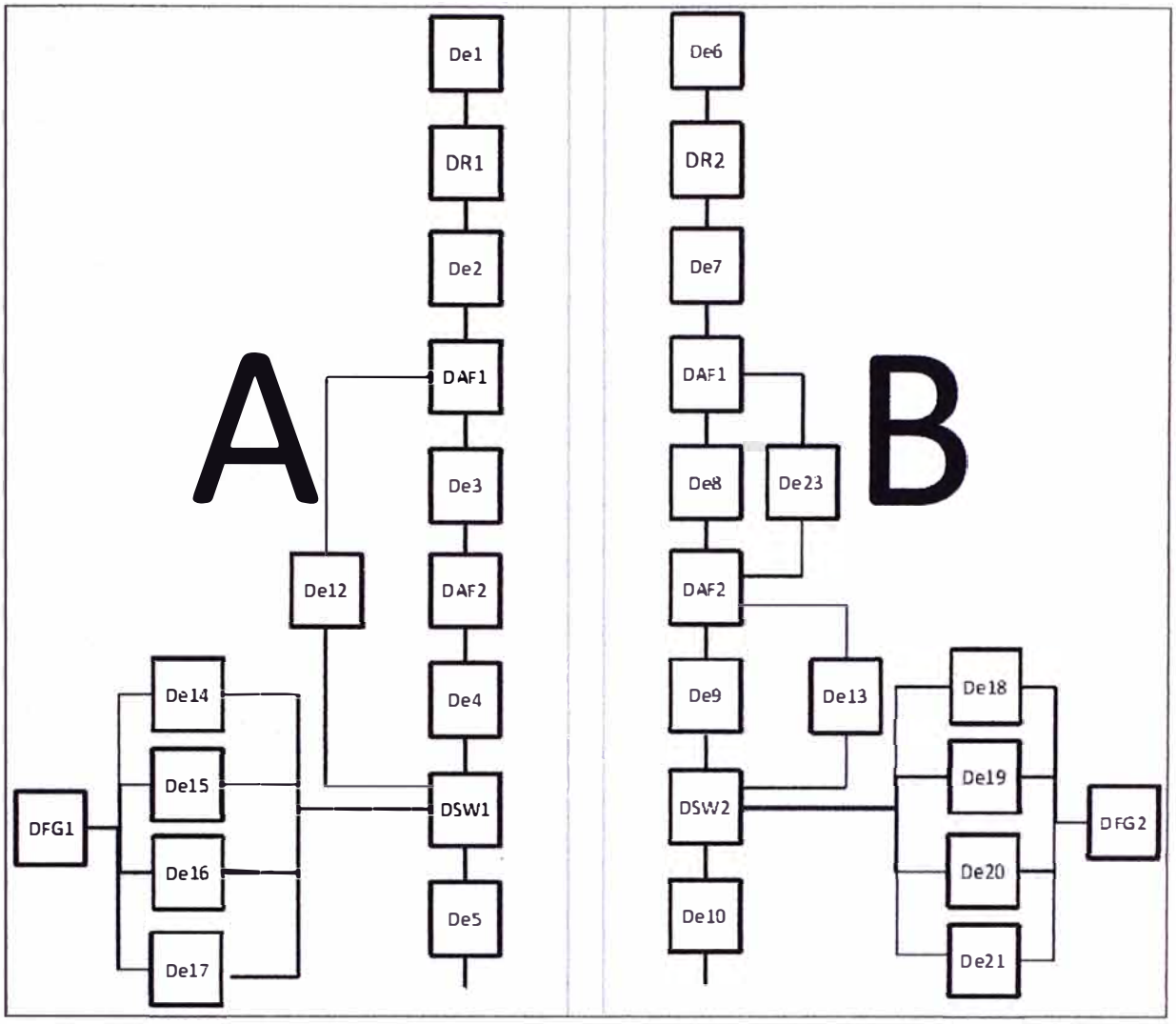

Figura 4.10 Solución desdoblada en A y B

Calculo de la Disponibilidad de B (Db):

DB=De6 x DR2 x De7 x DAF1 x De8 x DAF2 x De9 x DSW2 x (De18 // De19) x DFG2 x (De20 // De21) x DSW2 x De10

Del cálculo se desprende: DB=0.999427145

Calculo de la disponibilidad del sistema:

Para el cálculo de la disponibilidad del sistema, se consideran los componentes críticos de la solución en serie y los sistemas A y B en paralelo (Figura 4.11):

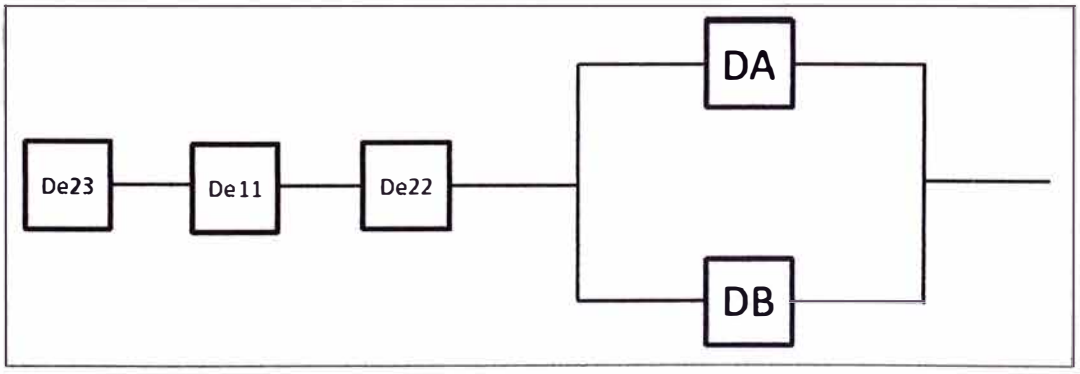

Figura 4.11 Disponibilidad del sistema

Dsistema=De23*De11*De22*(DA//DB)=0.999977*0-999977*0.999977*0.9999996718

Dsistema=0.9999306734=99.993%

4.5 Presentación de resultados

Se presentan tres aspectos:

- Disponibilidad
- Consumo de ancho de banda
- Implementación

a. Disponibilidad

En la Figura 4.12 se observa, en la herramienta web del proveedor, que la disponibilidad del servicio es del 100% en los primeros ocho meses del año posterior a la implementación, es decir, sin presentar ninguna caída durante ese periodo.

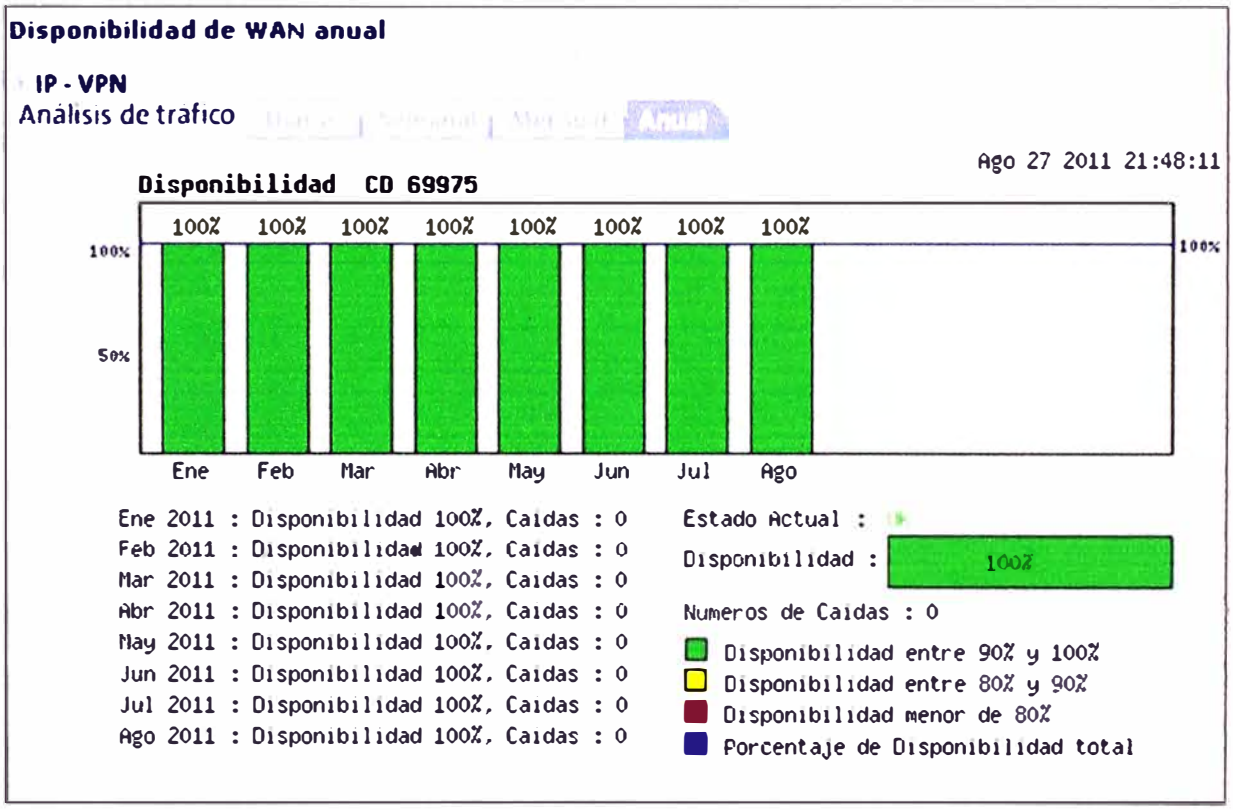

Figura 4.12 Disponibilidad WAN Anual

b. Consumo de ancho de banda

Se observa en la herramienta web del proveedor, que el consumo del ancho de banda durante la primera semana del servicio (Figura 4.13) y durante el primer año del servicio (Figura 4.14) no excedió el umbral del 80% del consumo de ancho de banda total, es decir, no presentó saturación.

c. Implementación

Las Figura 4.15 muestran la disposición de los equipos dentro de su gabinete en la sala de datos de la universidad. La Figura 4.16 muestra al grupo de trabajo en plena labor de configuración y pruebas.

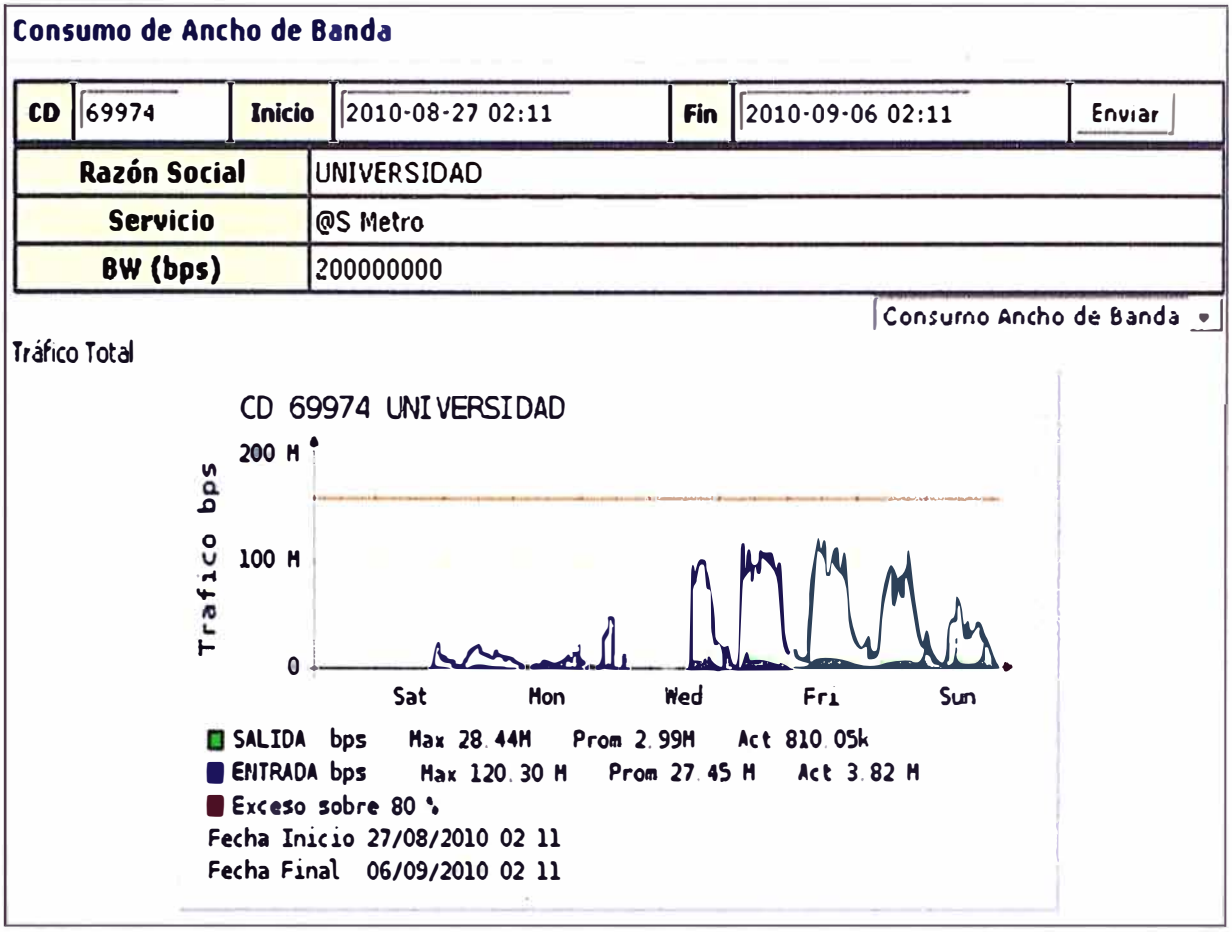

Figura 4.13 Consumo del ancho de banda durante la primera semana del servicio

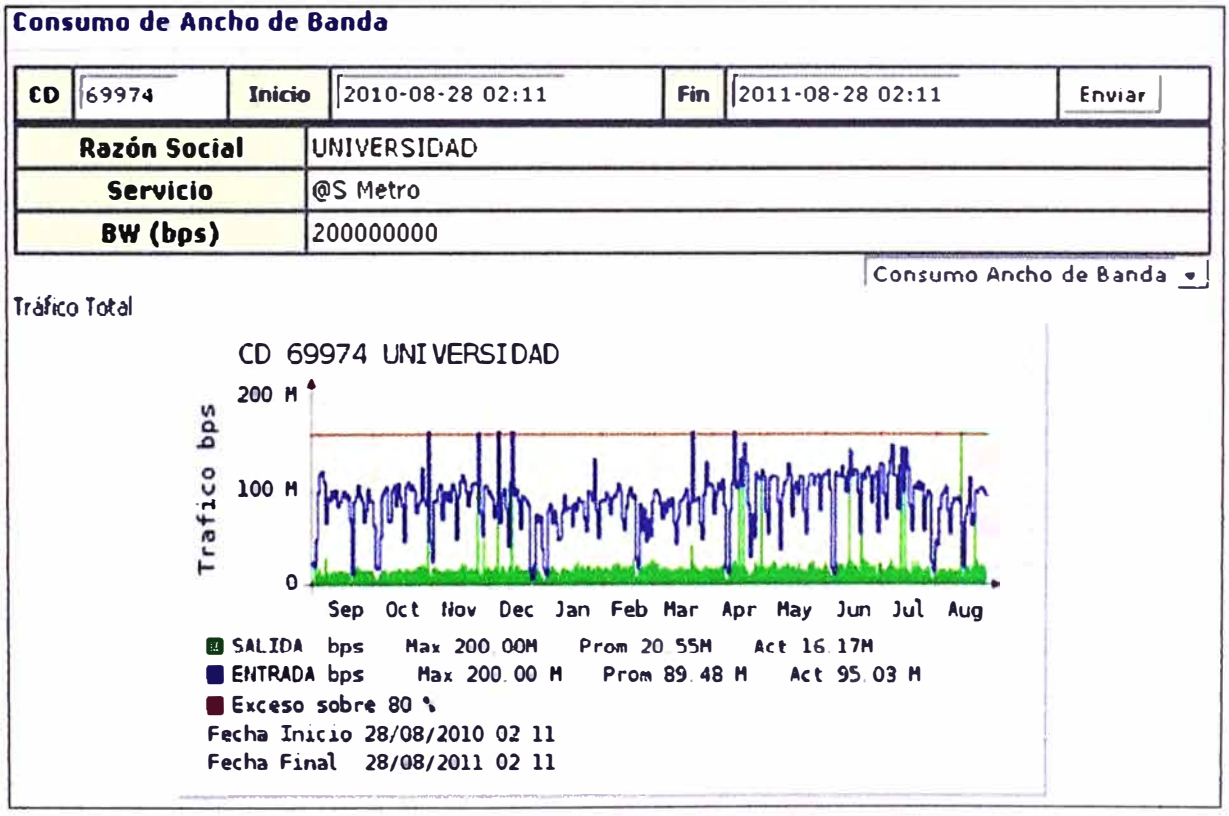

Figura 4.14 Consumo del ancho de banda durante el primer año del servicio

Figura 4.15 Disposición de los equipos dentro de su gabinete en la sala de datos

Figura 4.16 Trabajos de configuración y pruebas.

CONCLUSIONES Y RECOMENDACIONES

1. Se diseñó una solución que brinda una óptima seguridad y administración del tráfico WAN del enlace de Internet dedicado, asegurando una alta disponibilidad de la misma.
2. La solución fue lograda mediante la reestructuración de la plataforma de acceso a Internet, la cual está conformada por un equipo de administración de tráfico y un equipo de seguridad (Firewall avanzado), en una topología redundante la cual es optimizada mediante el uso de diversos protocolos de enlaces de comunicación.
3. La estrategia de virtualización por medio de VDOMs permitió ordenar la gran cantidad de políticas definidas por la Universidad según el perfil de los usuarios de cada VDOM, brindando con ello servicios diferenciados.
4. El sistema supera la disponibilidad requerida por la Universidad.
5. La solución está preparada para un escenario futuro en que la Universidad implemente un Switch Core de respaldo, el cual se conectaría directamente a los switches del proveedor, ya que se cuenta con puertos disponibles.
6. La solución brinda una redundancia a nivel 2 hacia la LAN de la Universidad, y una redundancia a nivel 3 hacia Internet.
7. La administración de tráfico ha permitido a la Universidad mejorar la productividad del recurso de acceso a internet, garantizando el buen funcionamiento del servicio a sus usuarios en horas de mayor demanda.
8. Se recomienda a la Universidad implementar un Switch Core de respaldo para mejorar la disponibilidad de su red LAN.
9. Se recomienda evaluar la adquisición de un equipo adicional que brinde una administración de tráfico por usuario, ya que para ello se requiere aplicar una gran cantidad de políticas que nos son soportadas por el equipo actual.

ANEXO A
GLOSARIO DE TÉRMINOS

3DES	Triple Data Encryption Standard. Algoritmo de encriptación
3G	3era generación. Tercera generación de transmisión de voz y datos a través de telefonía móvil
AAA	Authentication, Authorization, Accounting.
ADSL	Asymetric Digital Subscriber Line. Tecnología de transmisión digital que usa la línea telefónica para transmitir datos
ATM	Modo de transferencia asíncrona. Estándar internacional para relay de celdas en el que varios tipos de servicios se transmiten en celdas de longitud fija (53 bytes).
AS	Autonomous System. Sistema autónomo. Es un conjunto de redes y dispositivos router IP que se encuentran administrados por una sola entidad.
AV	Anti-Virus.
Backbone	Núcleo estructural que conecta todos los componentes de la red de manera que se pueda producir la comunicación.
Banda Ancha	Técnica de transmisión de alta velocidad que permite la transmisión de diferentes tipos de señales (voz, datos, imágenes, etcétera)..
BGAN	Broadband Global Area Network. Servicio satelital de banda ancha de INMARSAT que permite la transmisión de voz y acceso a Internet desde cualquier parte del mundo.
BGP	Border Gateway Protocol. Protocolo de enrutamiento WAN utilizado en redes MPLS.
BPS	Bits por segundo. Medida de velocidad de transferencia
BRI	Basic Rate Interface. Línea básica RDSI (2B+D)
BW	Bandwidth. Cantidad de información que se puede enviar a través de un medio en un período de tiempo dado
CD	Circuito Digital. Identificador de un circuito de datos
CPE	Equipo terminal del abonado. Equipo de terminación (por ejemplo: terminales, teléfonos y módems) proporcionados por la compañía telefónica.
Cracker	Individuo que intenta tener acceso a sistemas informáticos sin autorización (según RFC 1983 de IETF)
DLP	Prevención de fuga de información.
DMZ	Demilitarized Zone. Zona desmilitarizada ó red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DNS	Domain Name System. Base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.
DPI	Deep Packet Inspection. Inspección profunda de paquetes.
DTE	Equipo terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario a red que sirve como origen de datos, destino, o ambos.
Ethernet	10Mbps. Especificación de LAN de banda base.
Fast Ethernet	100Mbps. Cualquiera de varias especificaciones de Ethernet de 100-Mbps.
FO	Fibra Óptica
FTP	File Transfer Protocol. Protocolo de transferencia de archivos.
Gbps	Gigabytes por segundo. Medida de velocidad de transferencia (1Gbps = 1,000Mbps)
GPRS	General Package Radio Service. Servicio general de paquetes por radio que permite manejar datos sobre redes celulares de una manera más eficiente.
GUI	Graphical User Interface. Interfaz grafica de usuario.
HA	High Availability. Alta disponibilidad.
HSRP	Hot Standby Router Protocol. Protocolo propietario de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red.
Hacker	Persona con un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas (según RFC 1983 de IETF)
HTTP	HyperText Transfer Protocol. Protocolo de transferencia de hipertexto.
IDC	International Data Corporation. Es una compañía especializada en análisis e investigación de mercados de tecnologías de la información, telecomunicaciones y tecnologías de consumo masivo.
IDP	Intrusion Detection and Prevention. Detección y prevención de intrusiones.
IDS	Intrusion Detection System. Sistema de detección de intrusos.
IP	Internet Protocol. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión.
IP Sec	IP Security. Estándar de encriptación de datos.
IPv6	IP versión 6. Reemplazo de la versión 4 de IP.
IPS	Intrusion Prevention System. Sistema de prevención de intrusos.
ISP	Internet Service Provider, Proveedor de Servicios de Internet.
Kbps	kilobits por segundo. Medida de velocidad de transferencia (1Kbps = 1,000bps).

LAN	Red de área local. Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña.
LDN	Larga Distancia Nacional. Caudal IP entre localidades remotas geográficamente.
Mbps	Megabits Por Segundo. Medida de velocidad de transferencia (1Mbps = 1,000Kbps).
MPLS	Multi Protocol Label Switching. Mecanismo de transporte de datos para formar VPNs en redes IP.
MTBF	Mean Time Before Failure. Tiempo medio entre fallos
MTBO	Mean Time Before Outage. Tiempo medio entre parada de mantenimiento.
MTTR	Mean Time to Restore. Tiempo medio de reparación.
NAP	Network Access Point. Institución privada que agrupa a los principales operadores de telecomunicaciones y proveedores de acceso Internet del Perú.
NAT	Network Address Translation. Traducción de las direcciones IP de los hosts internos para esconderlos del monitoreo externo.
NOC	Network Operation Center. Centro de operaciones de redes.
ODF	Optical Distribution Frame. Distribuidor de fibra óptica.
P2P	Peer to Peer. Compartición de archivos en redes entre pares.
PE	Provider Edge. Equipo de borde de la red del proveedor.
POP	Point of Presence. Punto de presencia del operador
QoS	Calidad de servicio. Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.
RDSI	Red digital de servicios integrados . Protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.
Router	Ruteador. Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red.
SFP	Small Form-Factor Pluggable. Módulo transceptor de alto rendimiento enchufable.
SLA	Service Level Agreement. Documento que estipula los acuerdos de servicio comprometidos por el operador de servicios de comunicaciones o TI.
SOC	Security Operation Center. Centro de gestión de Seguridad.

STP	Spanning-Tree Protocol. Protocolo de gestión de enlace que garantiza que la topología de una red esté libre de bucles indeseables.
TBF	Time Before Failure. Tiempo entre fallos.
TCP	Transmission Control Protocol, Protocolo de control de transmisión.
Throughput	Volumen de trabajo o de información que fluye a través de un sistema.
TSR	Time to Service Restoration. Tiempo de restauración del servicio por mantenimiento.
TTR	Time to Restore. Tiempo de reparación.
URL	Uniform Resource Locator. Localizador uniforme de recursos. Secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación.
UTM	Unified Threat Management. Gestión Unificada de Amenazas. Dispositivos que integran múltiples capacidades de seguridad en un único producto.
VDOM	Virtual Domain. Dominio virtual.
VLAN	Virtual Local Area Network. Red de área local virtual. Método de crear redes lógicamente independientes dentro de una misma red física.
VoIP	Voz sobre IP.
VPN	Virtual Private Network. Red privada virtual. Conexión segura entre dos redes privadas en un medio público como Internet.
VTP	VLAN Trunking Protocol. Es un protocolo usado para configurar y administrar VLANs en equipos CISCO.
WAN	Wide Area Network. Redes de área extendida.

BIBLIOGRAFÍA

[1] Kurose, James F. "Redes de Computadoras - Un enfoque descendente"; Pearson Education Inc. 2010.

[2] John R. Vacca, "Network and System Security", Elsevier Inc., 2010.

[3] Ian J. Taylor, " From P2P to Web Services and Grids - Peers in a Client/Server World", Springer, 2005

[4] Wes Simpson, "IPTV and Internet Video: Expanding the Reach of Television Broadcasting" NAB Executive Technology Briefings, Segunda Edición, 2005.

[5] Kwok T. Fung, "Network Security Technologies", CRC Press-Auerbach Publications, 2005.

[6] Javvin Technologies Inc.," Network Protocols Handbook", 2004, Segunda Edición.

[7] Y. Rekhter, "Application of the Border Gateway Protocol in the Internet", MCI Editors, 1995. www.javvin.com/protocol/rfc1772.pdf

[8] Saulo Barajas, "Seguridad en BGP", http://www.saulo.net/pub/inv/BGP-art.htm. 2005

[9] Cisco Systems, Inc.,"Understanding VLAN Trunk Protocol (VTP)", Document ID: 10558, 2007. www.cisco.com/application/pdf/paws/10558/21.pdf

[10] IEEE Standars Association, "802.1D -Media Access Control (MAC) Bridges", standards.ieee.org/getieee802/download/802.1D-2004.pdf

[11] Dr. Primitivo Reyes Aguilar, "Curso de Confiabilidad", 2006 www.icicm.com/files/CURSO_CONFIABILIDAD.doc

[12] Cisco 3945 Integrated Services Router, "Enabling Borderless Networks at the Branch". www.cisco.com/en/US/products/ps10541/index.html

[13] Huawei "Quidway® S8500 Series 10G Core Routing Switches Product Specification" www.huawei.com/products/datacomm/pdf/view.do?f=111

[14] Huawei Quidway® NetEngine80E Core Router, www.huawei.com/en/ucmf/groups/public/documents/attachments/hw_093130.pdf

[15] XTera,"Brochure Ascenflow" www.xtera.com/download/2/140/pdf/XTERA_xtera_brochure_ascenflow_en_110324.pdf

[16] Fortinet, "FortiGate® 1240B Datasheet". www.fortinet.com/doc/FGT1240B_DS.pdf

[17] Fortinet, "FortiManager 400B" http://www.fortinet.com/doc/FM/FortiManager_Family_Datasheet.pdf

[18] Fortinet, "FortiAnalyzer 1000B", www.fortinet.com/doc/FortiAnalyzer-1000B_DS.pdf