ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESTUDIO DE LA INFRAESTRUCTURA DE COMUNICACIONES Y SEGURIDAD DE RED PARA EMPRESA ADMINISTRADORA DE UN PARQUE URBANO DE LA CIUDAD DE GUAYAQUIL"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

Jenny Elizabeth Arízaga Gamboa

Guayaquil-Ecuador

2015

AGRADECIMIENTO

A mi familia mi esposo Eduardo, mis hijos Xavier, Eduardo y Jenny por darme todo su apoyo, comprensión y motivación para seguir adelante con este sueño.

A mis padres por darme su apoyo, amor y fortaleza en todo momento.

DEDICATORIA

A mis padres por su ejemplo y apoyo incondicional en todo momento.

A mi esposo e hijos.

A mis hermanos.

TRIBUNAL DE SUSTENTACIÓN

MGS. Albert Espinal S.
Director de Tesis de Grado

MGS. Robert Andrade
Miembro Principal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado me corresponde exclusivamente; y el patrimonio intelectual de la misma a la **ESCUELA SUPERIOR POLITECNICA DE LITORAL"**

(Reglamento de Graduación de la ESPOL)

Jenny Elizabeth Arízaga Gamboa

RESUMEN

En los actuales momentos el internet se ha convertido en un medio que permite a las personas y compañías estar comunicadas y disponer el acceso a la información en cualquier momento y desde cualquier lugar. Así mismo los usuarios ya no solo desean acceder al internet a través de computadores de escritorio o portátiles sino también desde sus dispositivos móviles (teléfonos inteligentes, tabletas etc.).

Esta demanda de conectividad al internet para mantenerse comunicado e informado, da lugar a que ciertas instituciones de gobierno como los municipios o ministerios brinden internet en espacios públicos o en sitios determinados, como un beneficio para los habitantes de un determinado sector de su ciudad.

En la presente tesis se aborda el estudio de la infraestructura de comunicaciones y seguridades de red para una empresa que administra un parque público y que desea brindar el servicio de internet para los visitantes al parque, manteniendo el control al acceso de información censurada.

Dado que el brindar el servicio de internet, conlleva a una serie de riesgos de seguridad, como por ejemplo personas mal intencionadas que haciendo mal uso de herramientas informáticas y podrían acceder o colectar información de la empresa vulnerando la red, es necesario diseñar e implementar redes seguras que permitan mitigar este tipo de ataques informáticos; complementando a este requerimiento de seguridad también se requieren diseños escalables que permitan dar alta disponibilidad a los servicios de internet que brinda el parque.

El presente trabajo de tesis tiene como tema "Estudio de la Infraestructura de Comunicaciones y Seguridad de Red para Empresa Administradora de un Parque Urbano de la Ciudad de Guayaquil".

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AP: Access Point – Puntos de Acceso Inalámbrica.

DMZ: Zona Desmilitarizada.

Help Desk: Centro de Ayuda de Usuarios.

LAN: Local Area Network – Red de Área Local.

Mpps: Megapaquetes por segundo

RF: Radio Frecuencia

SSID: Service Set Identifier – Identificador de Servicios de Redes Inalámbricas.

SUPERTEL: Superintendencia de Telecomunicaciones.

QoS: Quality of Service – Calidad de Servicio.

VLAN: Virtual Area Network – Red de Área Virtual

WAN: Wide Area Network – Red de Area Amplia.

WiFi: Wireless Fidelity – Fidelidad Inalámbrica.

WLC: Wireless Lan Controller – Controladora LAN Inalámbrica.

ÍNDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

El progreso de las tecnologías de comunicaciones facilita significativamente el estar siempre conectados al internet, cubriendo la necesidad de las personas de estar informados y comunicados. Esto ha generado que las compañías que administran aeropuertos, universidades, cafeterías, hoteles, restaurantes y parques brinden el acceso a internet ya sea de manera gratuita como pagada.

Por lo que la empresa que administra el parque, plantea la necesidad que el parque brinde acceso de internet de manera inalámbrica y así brindar un servicio adicional a los visitantes. Para brindar este servicio de acceso a Internet de manera continua se requiere que las redes de comunicaciones dispongan de elementos que sean escalables y redundantes.

El brindar el acceso a internet a los visitantes del parque y a los usuarios de la red de la empresa administradora también conlleva a brindar seguridades en las redes de comunicaciones y proteger a los usuarios de dichas redes como a los equipos de computación de ataques informáticos.

El presente trabajo de tesis consta de cinco capítulos. El CAPITULO 1, CONSIDERACIONES GENERALES DE LA RED ADMINISTRATIVA Y DE SEGURIDAD DEL PARQUE, se describe la identificación del problema y se analiza la infraestructura de la red LAN del parque; se culmina con la solución propuesta.

El CAPITULO 2, comprende la VALORACIÓN DE LOS DISPOSITIVOS DE RED Y ANÁLISIS DE RIESGOS, se describen todo el levantamiento de información de los dispositivos de red y dispositivos de seguridad, se realiza un análisis de riesgos,

acciones de contingencias ante fallos de dispositivos de la red y seguridades, complementando con el análisis de costo/beneficio de la implementación de la red.

El CAPITULO 3, hace relación al DISEÑO DE LA RED, en donde se realiza el diseño de la nueva arquitectura de red, seguridades y se complementa con la simulación del diseño LAN, en el diseño se contempla alta disponibilidad con funcionalidades que deberán estar soportados por los dispositivos de red, todo esto fundamentado en protocolos y estándares aplicables a este diseño.

EL CAPITULO 4, corresponde a las PRUEBAS CON SOFTWARE DE SIMULACIÓN DE LA NUEVA RED, se realizan las pruebas de simulación para evidenciar las características de alta disponibilidad, seguridad y cobertura inalámbrica. Las herramientas utilizadas para la simulación son Packet Tracert, GNS3 y Cisco Wireless Control System.

EL CAPITULO 5, en este último capítulo se indican las Conclusiones y Recomendaciones pertinentes productos de este trabajo de investigación

CAPÍTULO 1

CONSIDERACIONES GENERALES DE LA RED ADMINISTRATIVA Y DE SEGURIDAD DEL PARQUE.

1.1 Antecedentes

Una red es un conjunto de dispositivos informáticos conectados entre sí en forma lógica y física, con la finalidad de optimizar sus recursos y emular el proceso de un sistema de cómputo único.

Las redes alámbricas proporcionan a los usuarios de la misma, seguridad y la capacidad de mover datos a altas velocidades. Así mismo las redes inalámbricas han revolucionado el modelo de conexiones tanto de las personas

como de las empresas. En las empresas este tipo de conexiones evitan tener que colocar cables y elementos de conexión en todas las áreas necesarias, abaratando costos al no tener que perforar paredes o colocar techos y suelos falsos; en las personas facilitan la movilidad ya que podrán estar siempre comunicados sin importar el lugar donde se encuentren.

Además, las comunicaciones inalámbricas permiten llevar conexiones a Internet a zonas donde puede ser muy complicado tender cables, lo que amplía las zonas accesibles a Internet en todas partes.

El conectarse a Internet desde cualquier punto de nuestra ciudad es uno de los objetivo del WiFi en zonas públicas. Independientemente de dónde nos conectemos a la red WiFi pública, ya sea desde un bar, hotel, parques, se debe estar consciente de los riesgos que este tipo de conexión conlleva.

Al tratarse de redes públicas, son muy susceptibles a sufrir ataques informáticos, pues resulta relativamente sencillo, para un 'hacker' experimentado, romper los sistemas de seguridad de tales redes y analizar todas las conexiones que se realizan.

El cortafuego es una solución de seguridad informática perimetral, pero su dimensionamiento, arquitectura y alcances dependerá de las necesidades de la empresa administradora. De esta manera se eleva el nivel confianza sobre la navegación en internet, al implementar filtros de seguridad.

Entre los principales objetivos de una solución de seguridad perimetral podemos mencionar:

- Controlar el acceso al internet, para que el mismo sea una herramienta productiva.
- Controlar el uso de ancho de banda para que sea utilizado de una manera óptima de acuerdo a las necesidades de cada una de las herramientas / aplicaciones.
- Implementar esquemas de alta disponibilidad para contingencia.
- Proteger la información para que sea accesible solo desde aquellas personas que deban tener acceso desde el internet.
- Estandarizar la plataforma de seguridad informática.

1.2 Identificación del Problema

La Empresa administradora que brindara el servicio de internet para el parque urbano de la ciudad de Guayaquil, cuenta con una infraestructura de conectividad para el internet el cual es utilizado por los usuarios del edificio de administración donde se encuentran los sistemas informáticos administrativos con información sensible.

A continuación se detalla ventajas y desventajas de la infraestructura de la red actual.

Ventajas

- El Cortafuego maneja un esquema de alta disponibilidad en la conexión a Internet.

- Dado que existen poca cantidad de usuarios, la arquitectura cumple con los requerimientos de conectividad, con un bajo costo de equipos.

- Los equipos permiten la creación de redes virtuales (Vlan´s) lo que permite brindar esquemas de seguridad a la red interna de la empresa.

- Una infraestructura de red lista para soporte de Telefonía IP (Soporte de puertos PoE y Calidad de Servicio (QoS)).

Desventajas

- No es una red con esquemas de alta disponibilidad en sus componentes principales (núcleo /acceso a internet).

- Cortafuego decrece su rendimiento al habilitar funcionalidades, a pesar de que es una red con pocos usuarios.

- Cortafuego aplica filtros mediante direccionamiento IP, por lo que los usuarios cambiando su dirección IP vulneran las reglas de filtrado.

- Cortafuego no bloquea las peticiones https.

- Los componentes individuales no soportan elementos redundantes como fuentes de poder (conmutadores de núcleo, acceso, corta fuegos).

- Los puntos de acceso trabajan de una manera independiente, por lo que los usuarios al estar asociados a un punto de acceso y movilizarse a otra ubicación el otro punto de acceso les pide nuevamente autenticarse.

- No hay una correcta distribución de los usuarios en los puntos de acceso.

- En el corta fuego las reglas de filtrado no permiten ser customizadas, por lo que no son flexibles en el momento de publicar aplicaciones que no usan los puertos estándares y la solución es abrir todos los puertos a un servidor especifico.

Esta infraestructura no es la más adecuada para cumplir con los nuevos requerimientos de servicios, como lo es el brindar el servicio de internet a los visitantes del parque urbano de forma ininterrumpida, por lo que es imperativo plantear un nuevo esquema de la red de comunicaciones y seguridad perimetral.

Se adjunta el diagrama de alto nivel de la red de comunicaciones y conectividad de internet de la empresa administradora del parque.

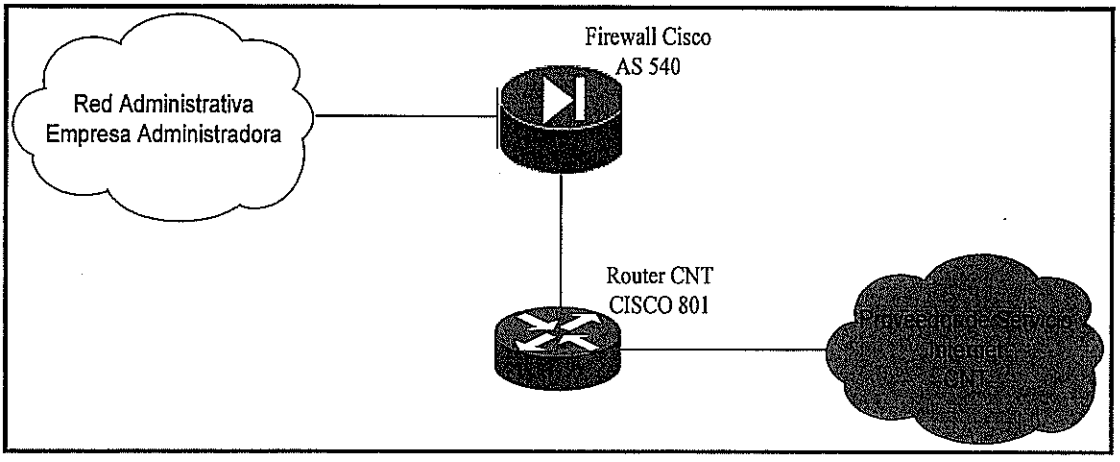

Figura N° 1.1: Diagrama de alto nivel de Conectividad de Internet.
Elaboración : Jenny Arízaga Gamboa.

A continuación se detallan los problemas más comunes que se podrían presentar en la red al compartir el acceso a internet con los visitantes al parque urbano.

1. Posibles ataques de DoS a los servidores WEB de la empresa administradora.

2. Posibles ataques a la red de gestión de los Access Point del parque.

3. Posibles ataques a los equipos de infraestructura de la red.

4. Posibles abusos en el uso del internet como lo es utilizarlo para el acceso a información pornográfica, de drogas, etc.

1.3 Infraestructura de la Red LAN del Parque.

La infraestructura actual de la empresa administradora del parque urbano presenta una topología física estrella, los equipos que la componen son un Cisco Catalyst WS-C3560X-48P-S-V04, cumpliendo las funciones de conmutador de núcleo y agregación, mientras que como conmutadores de acceso están los Cisco Catalyst WS-C2960S-48FPS-L-V03.

A continuación se adjunta el Diagrama de la red LAN actual de la Empresa Administradora. En el capítulo 3 se realizará el análisis y rediseño de la red fundamentadas en arquitecturas y protocolos estándares.

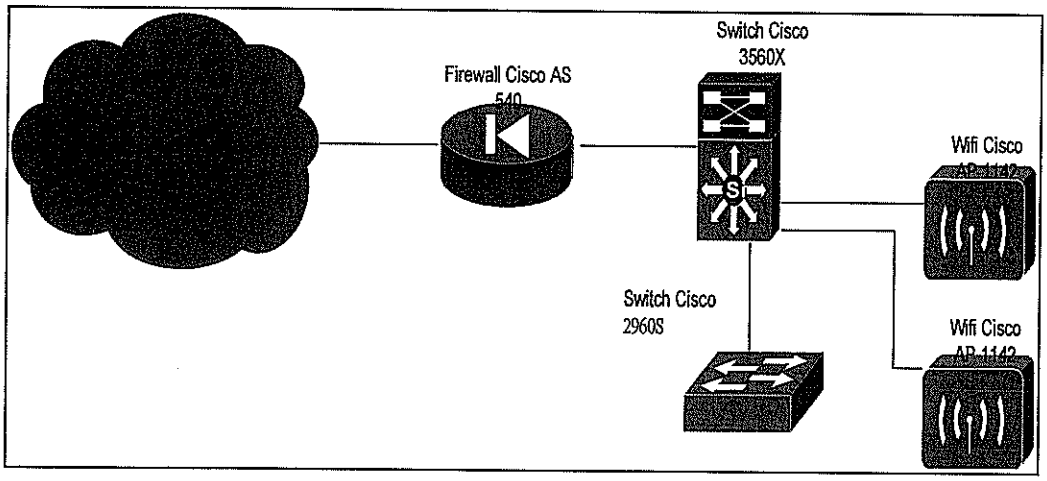

Figura N° 1.2: Diagrama de Red LAN de la Empresa Administradora
Elaboración : Jenny Arízaga Gamboa

1.4 Sistemas de Información Actuales de la Empresa Administradora del Parque.

Los sistemas de información actuales de la Empresa Administradora son:

1. Una aplicación de gestión documental que permite realizar memorandos u oficios que se maneja a través de recursos de todas las entidades de gobierno.

2. Un sistema financiero y nomina que es proporcionado para todas la entidades de Gobierno.

3. Un servicio de correo electrónico que está alojado en las instalaciones de un proveedor de servicio.

Los siguientes sistemas que se mencionan a continuación se implementarán en el transcurso de los siguientes seis meses:

1. Implementar el servidor de dominio y solución de respaldo de información de los usuarios.

2. La implantación del sistema financiero y nomina adquirido por la Empresa Administradora.

3. La implementación de un sistema de monitoreo y gestión de la infraestructura de comunicaciones.

1.5 OBJETIVO

Diseñar una infraestructura de red y seguridades para la empresa que administra el parque y brindar el acceso a internet como un servicio a los usuarios del parque.

1.5.1 Objetivo General de la Tesis

Realizar un estudio, para el diseño de una infraestructura de red de comunicaciones para la empresa administradora de un parque urbano de la ciudad de Guayaquil y brindar de forma segura el acceso a internet como un servicio a los usuarios del parque.

1.5.2 Objetivos Específicos de la Tesis

- ✓ Definir los requerimientos actuales y futuros de las comunicaciones del parque.

- ✓ Diseñar la arquitectura de comunicaciones y seguridades de la empresa administradora del parque.

- ✓ Definir el sistema de monitoreo y gestión de los dispositivos de comunicaciones.
- ✓ Realizar un análisis de costo y beneficio de la solución.
- ✓ Realizar la simulación de la nueva red de comunicaciones.

CAPÍTULO 2

VALORACIÓN DE LOS DISPOSITIVOS DE RED Y ANÁLISIS DE RIESGOS.

2.1 Levantamiento de Información de los Dispositivos de Red.

Se realizó el levantamiento de información de la empresa administradora del parque, el cual se lo divide en dos secciones:

- Levantamiento de información de la red LAN.
- Levantamiento de información de la red WAN.

1.5.3 Levantamiento de Información de la Red LAN.

En el anexo 1 se adjunta las configuraciones encontradas en los conmutadores de la red, aquí se muestran las salidas de los comandos en los equipos:

La información más relevante encontrada en la red LAN se indica a continuación:

Características de Conmutador de Núcleo.

- El conmutador principal es el Cisco Catalyst 3560X de 48 puertos.
- El conmutador cuenta con 48 puertos 10/100/1000 Mbps con funcionalidades de PoE (Potencia sobre Ethernet).
- El conmutador principal cuenta con un módulo de enlaces ascendente de 4 puertos, a 1 GigaEthernet con módulos SFP (transceptor de factor de forma pequeño conectable).
- La matriz de conmutación de este conmutador es de 160 Gbps.
- Velocidad de envió de este conmutador es de 101.2 mpps.
- Este conmutador es de capa 3.
- Este conmutador es independiente y no se puede apilar.
- Está configurado con dos redes virtuales una de usuarios y otra de servidores.

- En este conmutador se realiza el enrutamiento entre redes virtuales.

Características del Conmutador de Acceso

- El conmutador de acceso es el Cisco Catalyst 2960S de 48 puertos.
- El conmutador cuenta con 48 puertos 10/100/1000 Mbps con funcionalidades de PoE (Potencia sobre Ethernet).
- El conmutador de acceso cuenta con cuatro puertos de enlaces ascendentes, a 1 GigaEthernet con módulos SFP (transceptor de factor de forma pequeño conectable).
- La matriz de conmutación de este conmutador es de 88 Gbps.
- Velocidad de envió de este conmutador es de 77.4 mpps.
- Este conmutador se puede apilar hasta 4 unidades.
- Está conmutador es de capa 2.
- Está configurado con dos redes virtuales una de usuarios y otra de servidores.

Características del Punto de Acceso.

- El punto de acceso es el Cisco Aironet 1142.
- El punto de acceso trabaja de manera independiente, no depende de una controladora inalámbrica.

- El punto de acceso trabaja con los estándares IEEE802.11 a/b/g/n.
- Está configurado un solo SSID, para crear una red LAN inalámbrica.
- El punto de acceso maneja un rendimiento de 300 Mbps.

La tabla a continuación muestra el inventario de los dispositivos de la red LAN.

TABLA N° 1 Inventario de Equipos Activos LAN

INVENTARIO DE EQUIPOS LAN DE LA EMPRESA ADMINISTRADORA		
UBICACIÓN	**DESCRIPCIÓN**	
	MARCA	**MODELO**
CENTRO DE DATOS	CISCO	Catalyst WS-C3560X-48P-S-V04
CENTRO DE DATOS	CISCO	Catalyst WS-C2960S-48FPS-L-V03
ADMINISTRACION	CISCO	Access Point 1142
GERENCIA	CISCO	Access Point 1142
CENTRO DE DATOS	CISCO	Firewall SA 540

Elaboración: Jenny Arízaga Gamboa.

Para los siguientes dispositivos, se adjuntan las salidas de los comandos indicados para cada uno de los dispositivos. En el anexo1.

Conmutador Cisco 3560X

- Show Version.
- Dir all
- Show running-config

- Show ip route
- Show Vlan
- Show VTP Status
- Show spanning-tree
- Show interfaces status
- Show cdp neighbors

Conmutador Cisco 2960S.

- Show Version.
- Show running-config
- Show interfaces status
- Show cdp neighbors

Punto de Acceso Inalámbrico Cisco 1142.

- Show Version.
- Show running-config
- Show cdp neighbor
- Dir all
- Show vlan

- Show cdp neighbors

2.1.2 Levantamiento de Información de la Red WAN.

En el anexo 2 se adjunta la configuración encontrada en el enrutador de la red, aquí también se muestran las salidas de los siguientes comandos.

Cisco Enrutador 881

- Show version
- Dir all
- Show runn
- Show ip route
- Show ip interface brief.
- Show cdp neighbors

A continuación se describe la información más relevante de este equipo.

Características del Enrutador Cisco 881.

- El enrutador Cisco 881 tiene un rendimiento de 25 Mbps.
- La velocidad para este enrutador es de 50 kpps.
- El enrutador tiene cuatro puertos 10/100 Mbps para acceso LAN y un puerto de acceso WAN 10/100 Mbps.

- El enrutador tiene una ruta por defecto para la salida a internet.

2.2 Levantamiento de información de los Dispositivos de Seguridad.

En el anexo 3 se adjunta las configuraciones encontradas en el cortafuego para conexión a internet, se adjunta las pantallas más representativas de la configuración del dispositivo

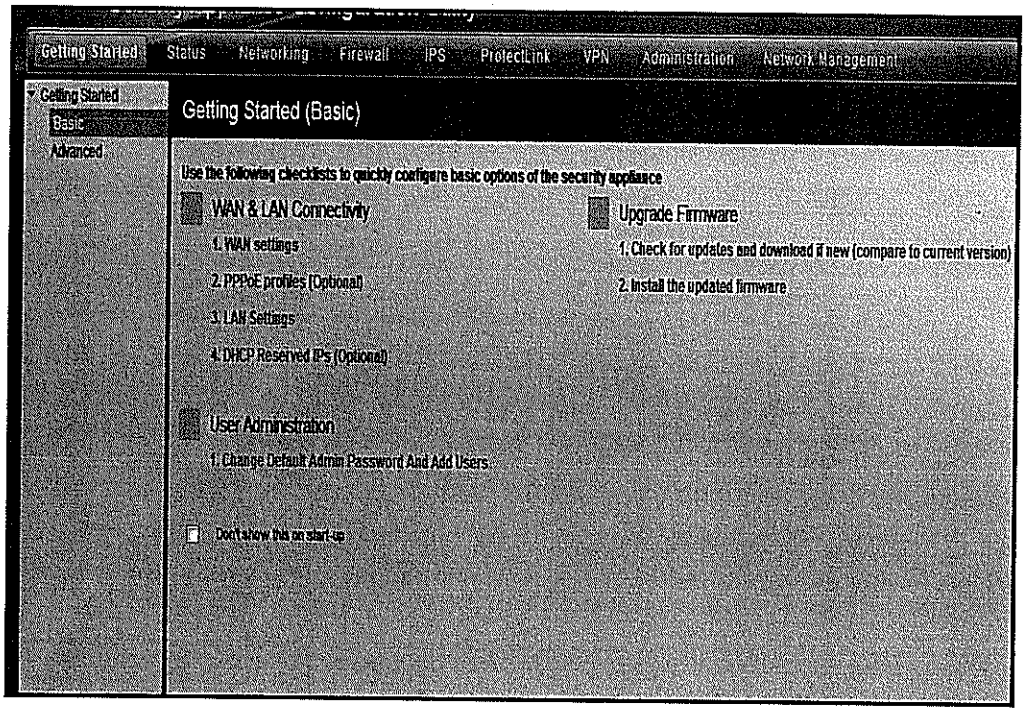

Figura N° 2.1: Pantalla Principal del cortafuego SA540
Elaboración : Jenny Arízaga Gamboa

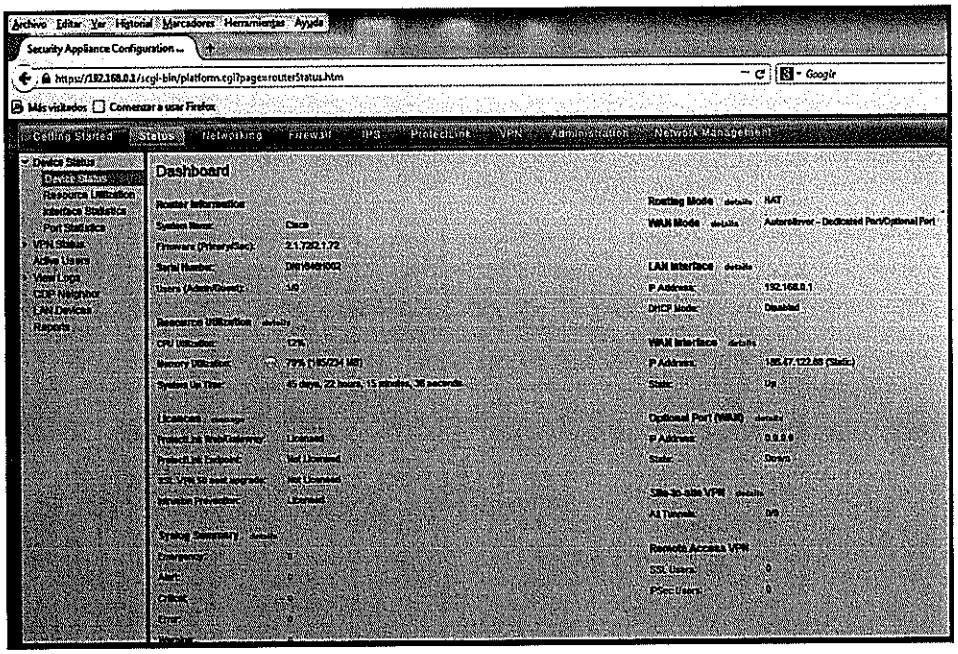

Figura N° 2.2: Vista de la configuración general del cortafuego SA540
Elaboración : Jenny Arízaga Gamboa

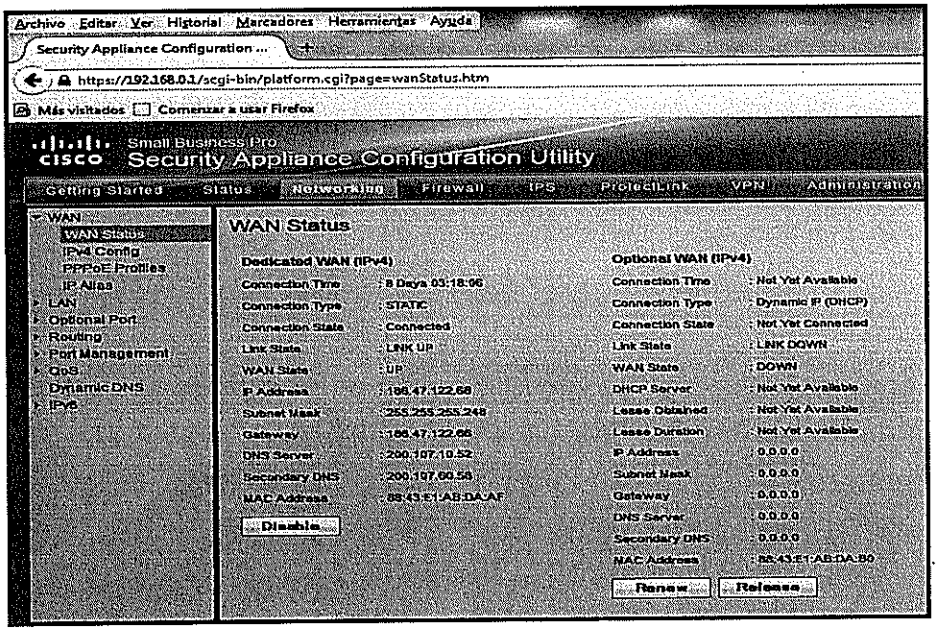

Figura N° 2.3: Vista de la configuración de la interface WAN cortafuego SA540
Elaboración : Jenny Arízaga Gamboa

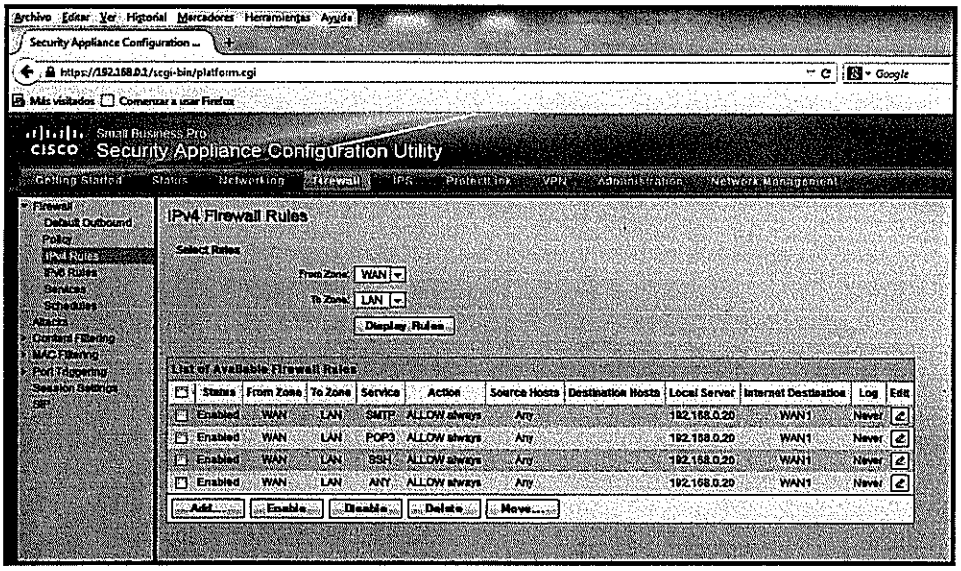

Figura N° 2.4: Vista de la configuración de reglas de acceso cortafuego SA540
Elaboración : Jenny Arízaga Gamboa

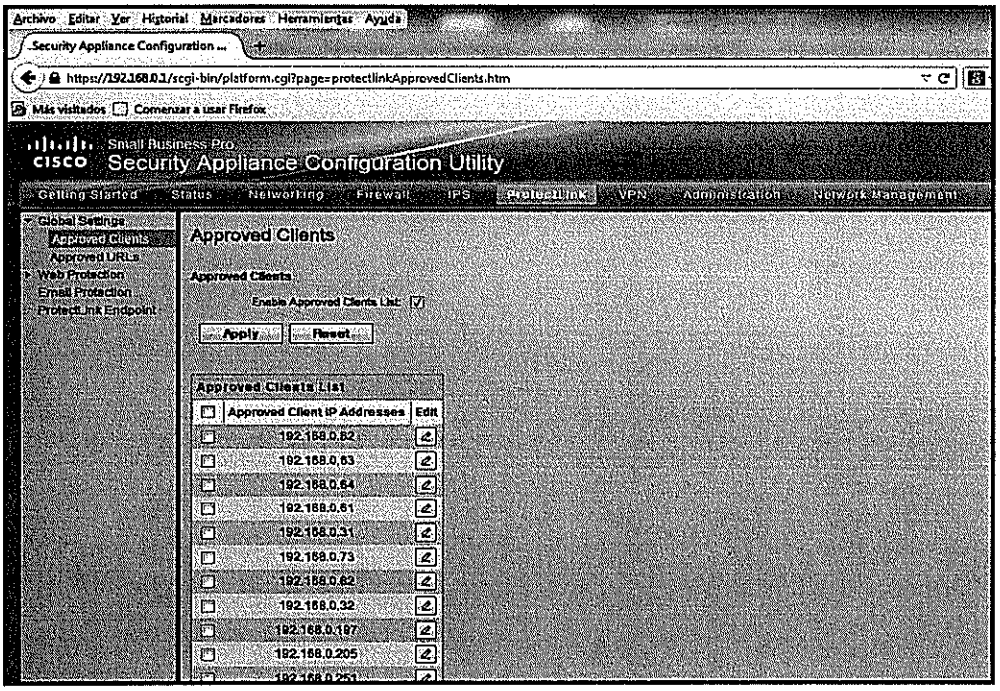

Figura N° 2.5: Vista de los usuarios permitidos de navegar en Internet cortafuego SA540.
Elaboración : Jenny Arízaga Gamboa

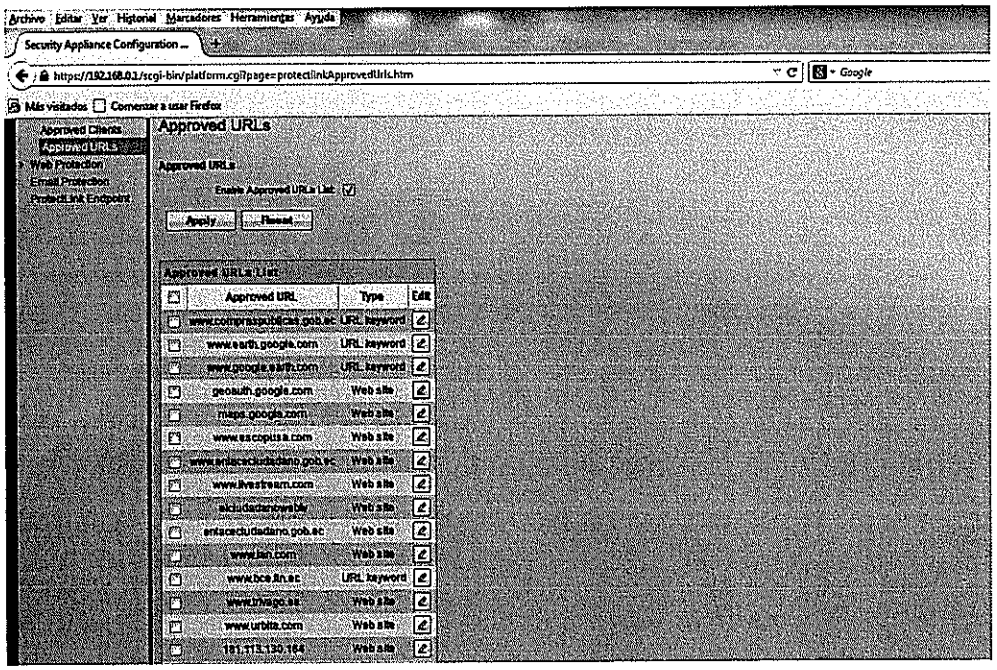

Figura N° 2.6: Vista de los URLS permitidos cortafuego SA540
Elaboración : Jenny Arízaga Gamboa

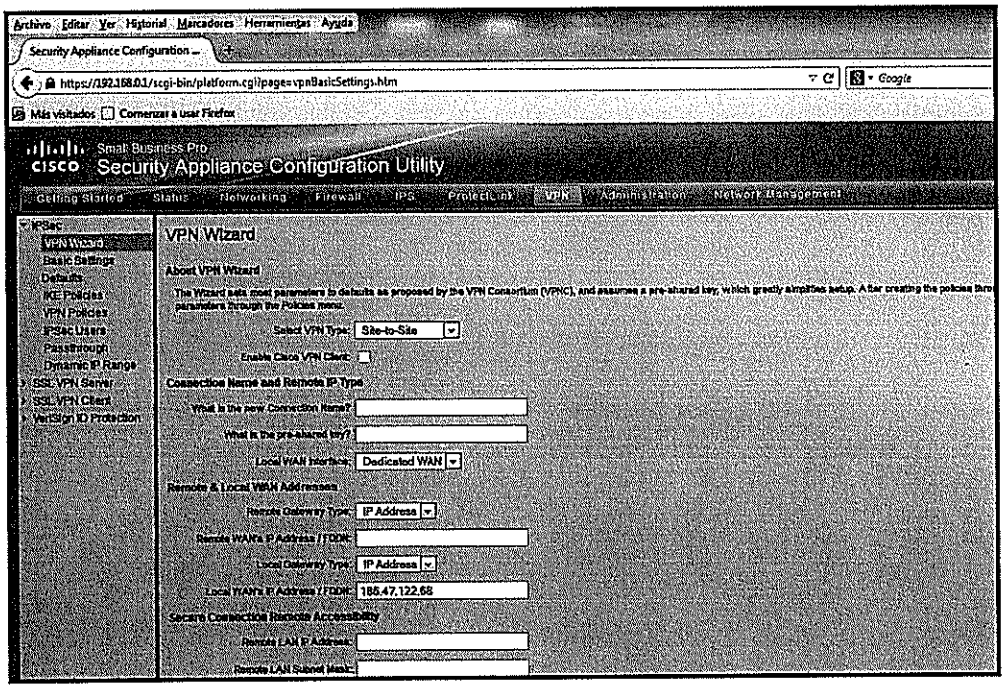

Figura N° 2.7: Vista de la guía de configuración VPN cortafuego SA540
Elaboración : Jenny Arízaga Gamboa

A continuación se detalla las características principales de la configuración del Cortafuego SA540.

Cortafuego SA540

- El Cortafuego tiene un rendimiento de 300 Mbps funcionando como cortafuego.
- El Cortafuego tiene configurado 10 reglas y soporta máximo la implementación de hasta 100 reglas.
- El Cortafuego tiene configurado el filtrado de URL.
- El Cortafuego tiene conectado actualmente 10 Mbps para acceso a Internet.
- El Cortafuego no soporta el filtrado de Https, por lo que se dificulta el control o bloqueo de estas páginas.
- El Cortafuego está realizando las funciones de Traslación de Direcciones de Red (NAT).
- El Cortafuego tiene activado el filtrado para el acceso a Internet por direccionamiento IPv4 de los usuarios.
- El Cortafuego no se integra con el directorio (AD) o con LDAP, lo que genera más carga administrativa para crear reglas de filtrado.
- El Cortafuego tiene configurado el bloqueo de mensajería instantánea.

- La activación de funcionalidades adicionales al Cortafuego genera un procesamiento adicional lo que conlleva que el rendimiento del equipo decrezca.

2.3 Análisis de Riesgo.

La siguiente tabla indica el análisis de riesgo de las posibles fallas que se puedan presentar en la infraestructura de red.

A continuación se define los parámetros y escalas para la evaluación de riesgo:

Tabla N° 2 Parámetros y Escalas para la Evaluación de Riesgo

IMPACTO

Valor	Descripción	Explicación
1	Insignificante	Impacto no significativo o con limitadas consecuencias.
2	Menor	Impacto sobre pequeñas partes del negocio solamente.
3	Importante	Impacto en la marca de la organización.
4	Material	Impacto mayor y fallas para cumplir con los reportes externos requeridos.
5	Catastrófico	Falla o reducción significativa de la capacidad de operación de la organización.

PROBABILIDAD

Valor	Descripción	Explicación
1	Raro	No se tiene registro de su ocurrencia.
2	Improbable	No ha ocurrido en los últimos 5 años.
3	Moderado	Ocurrió en los últimos 5 años, pero no el año anterior.
4	Probable	Ocurrió el año anterior.
5	Frecuente	Ocurre con regularidad.

Elaboración: Jenny Arízaga Gamboa

La calificación de riesgo = Impacto * Probabilidad

Tabla N° 3 Evaluación de riesgo

CONMUTADORES 3560 X - 2960 S									
Descripción del riesgo	**Categoría de Riesgo**	**Impacto**	**Probabilidad**	**Calificación del riesgo**	**Controles implementados**	**Impacto**	**Probabilidad**	**Riesgo Residual**	**Plan de acción**
Falta de una fuente de poder redundante. En caso de falla de la fuente de poder del equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Tener activo un contrato de reemplazo de partes. 24/7/4
No tiene Lazos en la red **(Bajo)**	Riesgo tecnológico	2	1	2	Ninguno	2	1	2	Se configurara esta protección con spanning tree.
IOS :En caso de falla del IOS en el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Se realizara copia de la imagen del IOS
Tarjeta principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Tener activo un contrato de reemplazo de partes. 24/7/4
Configuración : En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Se realizara copia de la configuraciòn y tambièn cuando se realice algùn cambio en el equipo.
Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. **(Bajo)**	Riesgo de ambiente operativo y las instalaciones	2	1	2	Esta implementado un generador y ups para el cuarto de comunicaciones.	2	1	2	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento .
ENRUTADOR 881									
Tarjeta Principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar (Critico).	Riesgo de Proveedor	5	3	15	Se reporta el problema al proveedor.	5	1	5	De acuerdo SSLA del proveedor ,debe de cambiar el equipo en 2 horas.
IOS: En caso de falla del IOS en el	Riesgo de Proveedor	5	3	15	Se reporta el problema al proveedor.	5	1	5	De acuerdo SSLA del proveedor ,debe de

equipo se quedaría sin funcionar (Critico).									cambiar el equipo en 2 horas.
Configuración :En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar (Critico).	Riesgo de Proveedor	5	2	10	Se reporta el problema al proveedor.	5	1	5	De acuerdo SSLA del proveedor ,debe de cambiar el equipo en 2 horas.
Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. (Bajo).	Riesgo de ambiente operativo y las instalaciones	2	1	2	Esta implementado un generador y ups para el cuarto de comunicaciones.	2	1	2	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.
PUNTOS DE ACCESO INALAMBRICO 1142									
IOS :En caso de falla del IOS en el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Se realizara copia de la imagen del IOS
Tarjeta principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Tener activo un contrato de reemplazo de partes. 24/7/4
Configuración : En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Se realizara copia de la configuràn y tambièn cuando se realice algùn cambio en el equipo.
Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. **(Bajo)**	Riesgo de ambiente operativo y las instalaciones	2	1	2	Esta implementado un generador y ups para el cuarto de comunicaciones.	2	1	2	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.
EQUIPO DE SEGURIDAD PERIMETRAL									
IOS :En caso de falla del IOS en el equipo se quedaría sin funcionar **(Critico)**	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Se realizara copia de la Imagen del IOS
Tarjeta principal: En caso de falla de la tarjeta principal el	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Tener activo un contrato de reemplazo de partes. 24/7/4

equipo se quedaría sin funcionar (Critico)									
Configuración : En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar (Critico)	Riesgo tecnológico	5	2	10	Ninguno	5	1	5	Se realizara copia de la configuración y también cuando se realice algùn cambio en el equipo.
Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. (Bajo)	Riesgo de ambiente operativo y las instalaciones	2	1	2	Esta implementado un generador y ups para el cuarto de comunicaciones.	2	1	2	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.

Elaboración: Jenny Arízaga Gamboa

2.4 Acciones de Contingencias ante Fallos de Dispositivos de Red y Seguridades.

La siguiente tabla indica las acciones de contingencias ante las posibles fallas que se puedan presentar en la infraestructura de red.

Tabla N° 4 Acciones de Contingencia

DISPOSITIVO	FALLO	ACCIÓN DE CONTINGENCIA
CONMUTADORES	Falta de una fuente de poder redundante. En caso de falla de la fuente de poder del equipo se quedaría sin funcionar (Critico)	Tener activo un contrato de reemplazo de partes. 24/7/4
	No tiene Lazos en la red (Bajo)	Se configurara esta protección con spanning tree.
	IOS :En caso de falla del IOS en el equipo se quedaría sin funcionar (Critico)	Se realizara copia de la imagen del IOS
	Tarjeta principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar (Critico)	Tener activo un contrato de reemplazo de partes. 24/7/4
	Configuración : En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar (Critico)	Se realizara copia de la configuración y también cuando se realice algún cambio en el equipo.
	Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. (Bajo)	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.
ADOR ENRUT	Tarjeta Principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar (Critico).	De acuerdo SLA del proveedor, debe de cambiar el equipo en 2 horas.

	IOS: En caso de falla del IOS en el equipo se quedaría sin funcionar (Critico).	De acuerdo SLA del proveedor, debe de cambiar el equipo en 2 horas.
	Configuración :En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar (Critico).	De acuerdo SLA del proveedor, debe de cambiar el equipo en 2 horas.
	Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. (Bajo).	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.
ACCESO INALAMBRICO	IOS :En caso de falla del IOS en el equipo se quedaría sin funcionar **(Critico)**	Se realizara copia de la imagen del IOS
	Tarjeta principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar **(Critico)**	Tener activo un contrato de reemplazo de partes. 24/7/4
	Configuración : En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Critico)**	Se realizara copia de la configuración y también cuando se realice algún cambio en el equipo.
	Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. **(Bajo)**	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.
SEGURIDAD PERIMETRAL	IOS :En caso de falla del IOS en el equipo se quedaría sin funcionar **(Critico)**	Se realizara copia de la imagen del IOS
	Tarjeta principal: En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar **(Critico)**	Tener activo un contrato de reemplazo de partes. 24/7/4
	Configuración : En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Critico)**	Se realizara copia de la configuración y también cuando se realice algún cambio en el equipo.
	Energía Eléctrica: En caso de falla las instalaciones posee un UPS y Generador eléctrico. **(Bajo)**	Se realizara mantenimiento preventivo y correctivo para que siempre este en buen funcionamiento.

Elaboración: Jenny Arízaga Gamboa.

2.5 Análisis Costo Beneficio.

A continuación en la siguiente tabla se muestra el análisis costo beneficio para este proyecto.

Se indican las consideraciones para nuestro análisis, en el parque la administradora brindara el servicio de internet a los usuarios del mismo, el costo por hora del servicio de internet tendrá un valor mínimo de $ 0.48.

Dado que la empresa administradora del parque es una empresa estatal sin fines de lucro pero deber ser autosustentable en el tiempo, el análisis de costos de la infraestructura y el servicio de internet es pertinente. Pero es potestad de

las autoridades y funcionarios del parque si el servicio de Internet se cobra o no a los usuarios del mismo.

A continuación se detalla el análisis del valor mínimo a cobrar por el servicio de Internet.

Tabla N° 5 Análisis del Valor Costo del Internet para Usuarios

DETERMINACIÓN DE COSTO MÍNIMO DEL SERVICIO DE INTERNET POR HORA	
CONSUMO PROMEDIO DE UN USUARIO DE INTERNET MOVIL [1]	384 KBPS
CONSUMO MÁXIMO DE INTERNET CONSIDERANDO 208 VISITANTES POR HORA (384*208)	79,872.00
COSTO DE UN ENLACE DE 80 MBPS	4,300.00
COSTO PROMEDIO POR HORA (4,300/(30*24)	5.97
VISITANTES PROMEDIO POR MES	150,000.00
VISITANTES PROMEDIO POR HORA (150,000/(30*24)	208
ASUMIENDO QUE SOLO UN 30% DE USUARIOS UTILICEN EL SERVICIO DE INTERNET POR UNA HORA 208*0.03	63
VALOR QUE TENDRIAN QUE PAGAR LOS USUARIOS DE INTERNET POR HORA (5.97/63)	0.1
VALOR DE INFRAESTRUCTURA DE COMUNICACIONES=	**1,043,053.72**
CONSIDERANDO QUE LOS ACTIVOS TECNOLÓGICOS SE DEPRECIAN EN 5 AÑOS EL COSTO DE LOS EQUIPOS SE PRORRATEA POR HORA POR LOS 5 AÑOS (1.043.053,72)/(5*365*24)	$ 23.81
ASUMIENDO QUE SOLO UN 30% DE USUARIOS UTILICEN EL SERVICIO DE INTERNET POR HORA=	63
VALOR QUE TENDRIAN QUE PAGAR LOS USUARIOS DE INTERNET POR UTILIZAR INFRAESTRUCTURA(23.81/63)	0.38
VALOR A PAGAR MÍNIMO PARA CUBRIR LOS COSTOS DE INFRAESTRUCTURA Y ENLACE POR HORA(0.38+0.10)	0.48

Elaboración: Jenny Arízaga Gamboa

Si se elige cobrar a los usuarios del parque el servicio de internet, se detalla en la siguiente tabla los rubros a facturar, esto es sin considerar ninguna ganancia para la empresa solo para cubrir costos.

Tabla N° 6 Análisis Costo Beneficio del Servicio

Número promedio de Persona por día	Número Estimado de Persona Que se conectan a Internet por Hora (30%)	Costo Hora Internet	Ingresos Totales por 1 Hora	Ingresos Totales por 2 Horas	Ingresos Totales por 3 horas	Ingresos Totales por 4 horas
5,000	63	$ 0.48	$30.24	$ 60.48	$ 90.72	$ 120,96

Elaboración: Jenny Arízaga Gamboa

La creación de una infraestructura de red redundante y escalable permitirá dar a los usuarios del parque un servicio continuo y asegurar que la infraestructura de red sea costeada al cabo de los cinco años.

A continuación se realiza el análisis de afectación de los ingresos del parque debido a los SLA del proveedor de Internet.

Tabla N° 7 Análisis de Afectación de Ingresos por SLA del Proveedor de Servicios

Servicio de SLA del Proveedor de servicios	Días sin conectividad anualmente	Horas sin conectividad del parque	Personas promedio por total de horas sin internet *	Pérdida anual por falla en Conectividad 1 año	Pérdida anual por falla en Conectividad 2 años	Pérdida anual por falla en Conectividad 3 años	Pérdida anual por falla en Conectividad 4 años	Pérdida anual por falla en Conectividad 5 años
99.60	1.46	35	2205.00	$ 948.15	$ 1896,3	$ 2844.4	$ 3792.6	$ 4740.7

Elaboración: Jenny Arízaga Gamboa
Nota* se considera para efectos de cálculo un promedio de 5000 personas que visitan el parque por día, visitantes promedio por hora 208 y solo utiliza el servicio de Internet un 30% (63) por una hora.

Por lo que se justifica plenamente este proyecto de rediseño de la red, al cual el impacto del SLA del proveedor de servicio no afecta mucho. El análisis realizado es muy conservador ya que considera que solo los usuarios estarán conectados una hora.

Así este diseño permitirá:

- Mitigar los efectos de los problemas de red por puntos de falla en la misma.
- Reducir las pérdidas de desconexión de la red a 1 hora máximo, por daño o fallo e uno de los dispositivos.
- Realizar una gestión proactiva en los dispositivos de red.
- Tener un esquema de red que le permita crecer de manera escalable.
- Permitir a futuro implementar su nuevo sistema.
- Permitir a futuro implementar sistemas de Voz sobre Ip, Calidad de Servicio y Multidifusión.

CAPITULO 3

3.1 DISEÑO DE LA RED

Con la complejidad de las redes, es necesario usar arquitecturas y metodologías en el diseño de las mismas empresas requieren que las redes soporten las necesidades del negocio y las fuerzas comerciales que afectan al diseño de la red de la empresa son los siguientes:

- ✓ Retorno de la inversión: las empresas buscan obtener un retorno (ya sea ahorro de costos o aumentar la productividad) en sus inversiones de infraestructura de red. Las soluciones tienen que utilizar tecnología para trabajar dentro de una solución de negocios.

- ✓ Regulación: Las empresas en ocasiones tienen que cumplir con las regulaciones de la industria; por ejemplo: La Salud, Seguros Ley de Portabilidad y Responsabilidad (HIPAA) para la industria de seguros de salud y Payment Card Industry Data Security Standard (PCI DSS) para las empresas de tarjeta de crédito.

- ✓ Competitividad: Para mantener una ventaja competitiva, las empresas deben utilizar la tecnología para que sean más competitivos que otros negocios.

Las fuerzas tecnológicas que afectan a las decisiones de la red en una empresa son:

- ✓ La eliminación de las fronteras: Las fronteras tradicionales de red se han eliminado. El acceso a los recursos de la red debe estar activado en sucursales, tele trabajadores, oficinas en casa, dispositivos móviles, clientes y redes asociadas.

- ✓ Virtualización: Permite la maximización de la eficiencia a través de la reducción de hardware, el consumo de energía, los costos de calefacción y refrigeración, espacio las instalaciones. La Virtualización y sus beneficios son un objetivo clave para casi todas las organizaciones.

- ✓ El crecimiento de las solicitudes: Los clientes siguen pidiendo nuevos productos, ofertas de servicios, mejor servicio al cliente, una mayor seguridad, flexibilidad y personalización todo a un costo menor.

Con la complejidad en el diseño de una red, se necesita entender los modelos de red utilizado para simplificar el proceso de diseño. El modelo de red jerárquica de Cisco divide la red en las capas núcleo, distribución y acceso.[1]

Modelo de Red Jerárquica

Los modelos jerárquicos permiten diseñar redes que utilizan funciones especiales combinados con una organización jerárquica. Tal diseño simplifica las tareas requeridas para construir una red que cumple con los requisitos actuales y puede crecer para satisfacer las necesidades futuras.

Los modelos jerárquicos usan capas para simplificar las tareas de interconexión. Cada capa puede centrarse en las funciones específicas, que le permite elegir los sistemas y características adecuadas para cada capa. Los modelos jerárquicos se aplican tanto a LAN y diseño WAN.

3.1.1 Beneficios del Modelo Jerárquico.

Los beneficios del uso de los modelos jerárquicos para su diseño de la red son los siguientes:

- Ahorro de costo.
- Facilidad de entendimiento.
- Crecimiento modular de la red.
- Mejora el aislamiento de fallos.

Las arquitecturas de redes planas, los cambios tienden a afectar a un gran número de sistemas. Topologías de malla limitadas dentro de una capa o componente, tales como el núcleo del campus o backbone Después de la adopción de modelos de diseño jerárquico, muchas organizaciones reportan ahorros de costo, porque que ya no están tratando de hacer todo en un enrutamiento o plataforma de conmutación. El modelo modular permite el uso apropiado de ancho de banda dentro de cada capa, mantener cada elemento de diseño simple y funcional facilita la facilidad de comprensión, lo que ayuda al control de gastos en la formación de personal. Puede distribuir el monitoreo de la red y sistemas de gestión a las diferentes capas de red modular, lo que también ayuda al control de los gastos de gestión.

El diseño jerárquico facilita los cambios. En un diseño de red, la modularidad le permite crear diseños que se pueden reproducir cuando la red crece. Como cada elemento de la red diseñada requiere cambios, el costo y la complejidad de hacer la actualización están contenidos en un pequeño subconjunto de la red. En general, que conecta los sitios centrales. [2]

3.1.2 Capas del Modelo Jerárquico.

La arquitectura jerárquica tendrá muchos beneficios, ya que determina funciones dentro de cada capa que separara las redes en 3 niveles, que en el tiempo será menos compleja en diseñar, implementar, mantener y escalar, además que es más confiable, cada capa tendría funciones específicas.

Al realizar estas capas, puede trabajar a través de varios beneficios como alto rendimiento, eficiente gestión de la red, se puede crear políticas y filtros, el modelo de capas permite escalabilidad haciendo funcional la red.

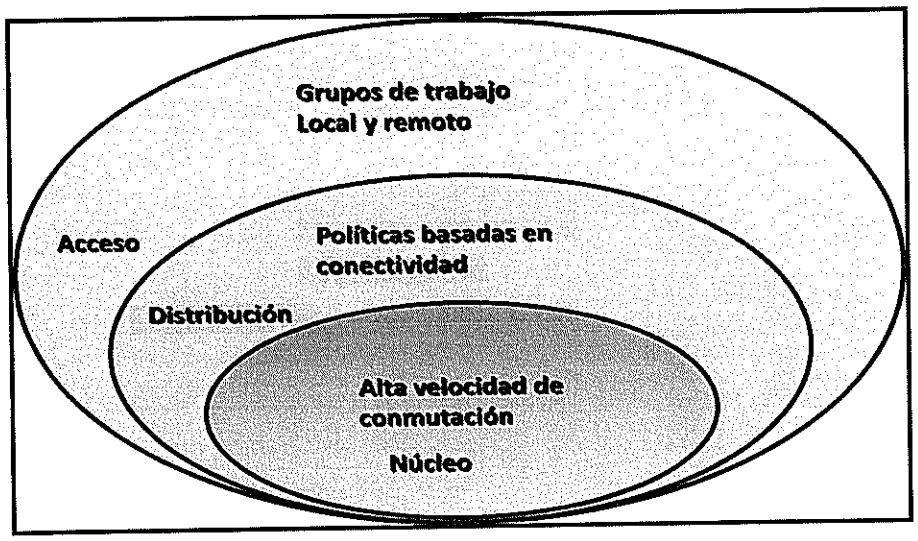

Figura N°3.1 : Modelo Jerárquico en Capas [3]

Capa de Acceso: Controla a los usuarios o grupo de trabajo, es donde se maneja el tráfico de los usuarios y de los recursos asignados de los controles de accesos lógicos. Es donde los dispositivos finales se conectan como: Ordenadores, impresoras, cámaras, servicio telefónico, dispositivos móviles etc. La capa de acceso está asignada para gestionar las funciones de conectividad de dispositivo final.

Capa de Distribución: Es el medio para controlar la comunicación entre la capa de acceso y el Núcleo. Esta capa permite realizar filtrado, ruteo interVLAN, acceso a la red WAN y también es el que responde a los

requerimientos de la red, o peticiones que realicen los usuarios finales. Brinda servicios de conectividad y de políticas de control del flujo del tráfico.

Tiene variadas funciones como:

- Servir como punto de agrupación para permitir a los dispositivos de capa de acceso, procesar el tráfico que generen los grupos de usuarios.
- Segmentar la red.
- Brindar servicios de seguridad y filtrado.

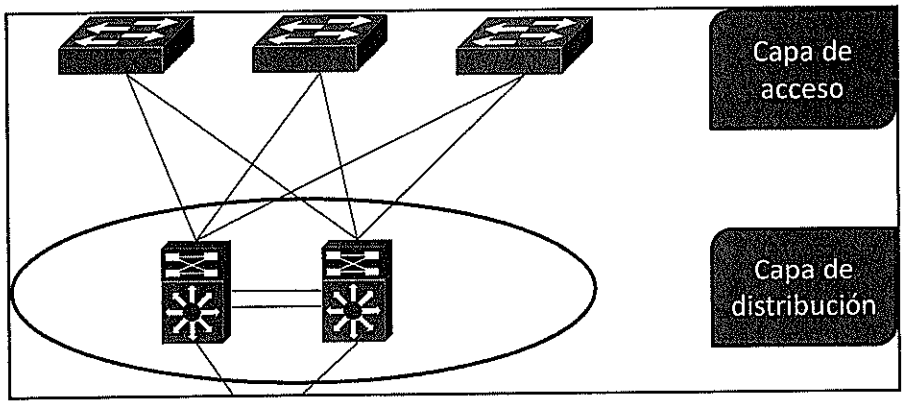

Figura N°3.2 : Capa de Distribución [3]

Capa de Núcleo: La función es gestionar a alta velocidad y certificar la entrega fiable de paquetes en la red, el núcleo debe tener una alta confiabilidad y que tengan redundancia. La capa de núcleo es la columna vertebral de la red, es el que brinda conectividad en los dispositivos finales de la red.

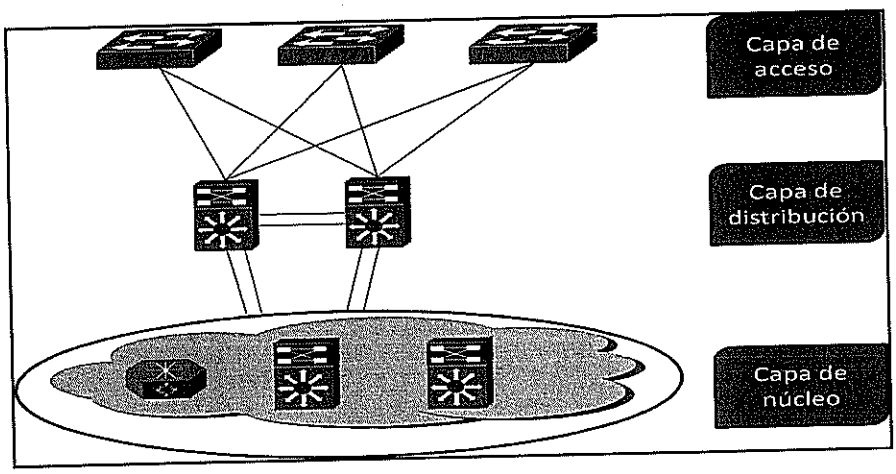

Figura N°3.3 : Capa de Núcleo [3]

3.1.3 Modelo Colapsado.

Es factible también implementar arquitecturas de red donde un solo elemento realiza las funciones de Núcleo y Distribución. Este modelo se denomina Colapsado. El sistema colapsado distribución / núcleo puede proporcionar servicios de red a un pequeño número de conmutadores de armario de cableado y conectar directamente a la red sistemas WAN.

La Implementación de un modelo de red de dos niveles para un solo bloque de distribución y núcleo no rompe los principios de tres niveles del diseño de redes de campus que se requieren en campus grandes y medianos.

Esta solución es de coste mediano siempre y cuando cumpla con las necesidades de los usuarios de la red y el número de puntos finales no es tan grande.

La red de distribución/núcleo colapsado puede activarse con dos sistemas redundantes como se recomienda en Capa de distribución Diseño o alternativamente en modo solitario como se describe a continuación.

La construcción de una sistema solitario con alta disponibilidad colapsado distribución/Núcleo para garantizar el rendimiento de la red y la disponibilidad, necesaria para ejecutar servicios con diversos componentes de hardware redundantes, esta solución puede proporcionar protección 1 + 1 en el chasis contra diversos tipos de hardware y software, pero este diseño tiene como único punto de falla el chasis.

3.1.4 Diseño de la Infraestructura de Red.

Para la infraestructura de red se utilizará el modelo jerárquico, para el diseño se tiene la siguiente información.

Tabla N° 8 Requerimientos de la Red

Descripción	Actuales	40% Crecimiento en 3 Años
Usuarios de red	145	203
Velocidad de Conexión de los usuarios	10/100/1000 Mbps	
Alta Disponibilidad	Si	
Aplicativos utilizados por los usuarios	Ofimática	
Aplicativos institucionales	Si	
Telefonía (VoIP)	Si	
Enlaces Redundantes	Si	
Acceso a Internet redundantes	Si	
Usuarios de Parque accediendo a internet	63 usuarios por hora	
Promedio de ancho de banda por usuario	384 Kbps [4]	
Conexión de otras instituciones a futuro		

Elaboración : Jenny Arizaga

Basados en esta información se utilizará como arquitectura de red el modelo colapsado, en configuración redundante dual, considerando dos conmutadores. Cumpliendo con los requisitos de una completa alta disponibilidad.

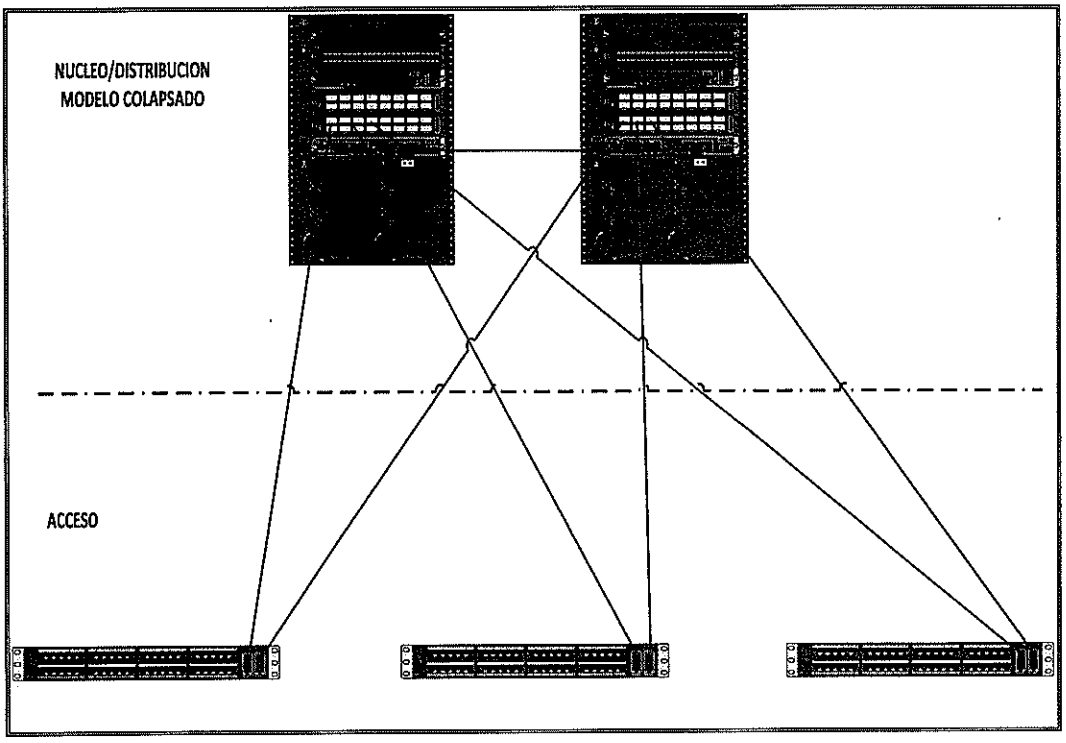

Figura N°3.4 : Modelo Colapsado
Elaboración : Jenny Arízaga

TABLA N° 9 Conectividad por Usuario

Conectividad por usuario	
USR=1000 Mbps	
Numero de Conmutadores de 48 puertos	
Num-Conmutadores=	Total usuarios / 48 puertos
Num-Conmutadores=	203 / 48
Num-Conmutadores=	5
Calculo de Tráfico de Enlaces de Subida	
Tráfico Total de usuarios por conmutador =	48x1000 Mbps
Tráfico Total de usuarios por conmutador =	48000 Mbps
Considerando como regla de diseño una relación 20:1 para la conexión Acceso a Distribución	
Numero de Enlaces=	48000 Mbps / 20
Numero de Enlaces=	2400 Mbps
Numero de Enlaces=	2x 1 Gbps

Elaboración : Jenny Arízaga

Por cada conmutador se requiere 2 enlaces de subida a 1 Gbps.

3.2 Redes Inalámbricas

Los usuarios hoy en la actualidad requieren movilidad y se debe brindar la misma accesibilidad, seguridad, calidad de servicio (QoS) y la alta disponibilidad que actualmente gozan los usuarios conectados por cable. Ya sea que usted esté en el trabajo, en casa, en la carretera, a nivel local o internacional, hay una necesidad de conectar.

Los retos tecnológicos son evidentes, pero para ello, la movilidad juega un papel para todo el mundo. Las empresas están obteniendo valor en el negocio

en las soluciones móviles e inalámbricas. Lo que antes era una tecnología de mercado vertical es ahora la corriente principal, y es una herramienta esencial para conseguir el acceso a voz, información en tiempo real, y las aplicaciones críticas, como el correo electrónico y calendario, bases de datos empresariales, gestión de la cadena de suministro, automatización de fuerza de ventas, y gestión de relaciones con los clientes.

3.2.1 Beneficios de la soluciones de Redes Inalámbricas (WLAN).

Los beneficios obtenidos por las WLAN incluyen:

- La movilidad dentro de edificios o campus.
- Simplifica la creación de grandes redes en espacios abiertos, flexibles permitiendo que el trabajo se realice en el lugar más apropiado o conveniente y no donde termina un cable.
- Más fácil de configurar espacios temporales, permite el despliegue de redes rápidamente en habitaciones, salas de reuniones.
- Menor costo que las redes cableadas, reduciendo la necesidad de instalación de la red de cable debido a la WLAN puede emplearse en sitios donde no es factible colocar redes cableadas.
- Mejora de la eficiencia.
- Más fácil para herramientas de colaboración, facilita el acceso a herramientas de colaboración desde cualquier lugar, tales como salas de

reuniones; archivos pueden ser compartidos en el acto y las solicitudes de información manejados inmediatamente.

Los Sistemas WLAN funcionan ya sea como complemento a la red de la empresa por cable existente o como una red de independiente dentro de un campus. La WLAN también puede estar vinculada a las aplicaciones, como los servicios basados en la localización, en las industrias de ventas al por menor, manufactura, o el cuidado de la salud.

Las WLAN deben permitir cifrado, para una comunicación segura para acceso a los datos, la comunicación y servicios de la oficina como si estuvieran conectados a los recursos por una red cableada.

3.2.2 Componentes de las Redes Inalámbricas (WLAN).

Los componentes principales de las redes inalámbricas son:

- Puntos de Acceso (access points - APs).
- Controladora Inalambrica (Wireless LAN controller -WLC).
- Sistema de Gestión y Monitoreo.

Puntos de Acceso (APs): Un punto de acceso inalámbrico es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un AP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red por cable y los dispositivos inalámbricos.

Existen dos modos de operación de los puntos de acceso:

- Punto de acceso autónomo.
- Punto de acceso ligero.

Los **puntos de acceso autónomos** funcionan como una unidad independiente, sin tener interacción con otros puntos de acceso. Inicialmente el modo autónomo estaba bien cuando las redes inalámbricas a menudo solo se limitaban a proporcionar acceso a la red en las zonas comunes o zonas donde no existían redes cableadas.

Cuando la cantidad de puntos de acceso es pequeño es factible la administración, ya que se debe configurar uno a uno, aunque estos puntos de acceso están conectados a la misma red, y pueden utilizar el mismo SSID, todos ellos están configurados de forma individual y separada.

Los **puntos de acceso ligeros**, son controlados y supervisados por una Controladora de Red Inalámbrica. Estos puntos de acceso se comunican utilizando un protocolo especial llamado el Protocolo de Punto de Acceso Ligero (LWAPP) para transmitir información a la Controladora de Red Inalámbrica acerca de la cobertura, la interferencia que el punto de acceso está experimentando y datos de los clientes acerca de las asociaciones, entre otra información, esta comunicación a través de LWAPP está encriptado. Los datos del cliente se envían dentro estas cabeceras de trama LWAPP, adicionalmente se envía la información acerca del Indicador de Fortaleza de la Señal Recibida (RSSI) y la relación señal-ruido (SNR). La Controladora Lan

Inalámbrica utiliza esta información para tomar decisiones que pueden mejorar las áreas de cobertura inalámbrica.

Si se está planeando instalar una red nueva, se debe considerar las ventajas de los puntos de acceso de modo ligero dado las ventajas en administración a través de la Controladora de LAN Inalámbrica.

Controladora LAN Inalámbrica (WLC): Es un dispositivo que permite administrar centralizadamente un grupo de Puntos de Acceso, los cuales solo pueden ser administradas a través de la WLC [9], este dispositivo adicionalmente permite:

- Auto detectar y auto configurar puntos de acceso que sean agregados a la red.
- Control total de los puntos de acceso.
- Los puntos de acceso logran conectividad con la controladora inalámbrica a través de la red.

Sistema de Gestión y Monitoreo: Se requiere un sistema de gestión y monitoreo que permita:

Diseño: La fase de diseño se centra en el diseño general de las características de los dispositivos con patrones o plantillas. El área de diseño es donde se crean los patrones de diseño reutilizables tales como plantillas de configuración.

- **Implementar:** La fase de despliegue se centra en la implementación de diseños o plantillas previamente definidas en su red, haciendo uso de las plantillas creadas en la fase de diseño. La fase de despliegue le permite empujar configuraciones definidas en sus plantillas a uno o varios dispositivos.
- **Reportes:** También se debe proporciona informes que se puedan utilizar para supervisar el sistema y estado de la red, así como los problemas y la solución de los problemas.

3.2.3 Diseño de Red Inalámbrica.

Para el diseño de una red inalámbrica se tiene dos maneras de ser desplegadas:

- Utilizando puntos de acceso autónomos
- Utilizando un elemento de control y gestión centralizada como una Controladora Lan inalámbrica y puntos de acceso ligeros.

Utilizando Punto de acceso autónomo: Inicialmente los sistemas Wi-Fi utilizaban puntos de acceso autónomos. Cada punto de acceso tenía toda la capacidad para crear la celda y gestionar los clientes que se asocian a ella y las comunicaciones entre estos, adicionalmente las comunicaciones entre ellos y la red cableada.

Cuando las redes Wi-Fi pasaron de ser una solución puntual para solucionar problemas específicos siempre de tamaño reducido, a dar solución a grandes

instalaciones complejas que soportan gran parte de las comunicaciones de una empresa, o incluso en algunos casos se utilizan como una fuente de ingresos (como puede ser el caso de los hoteles que brindan a sus usuarios por el pago de valor adicional el servicio de internet), entonces se vio la necesidad de disponer de sistemas de gestión centralizados.

Con el tiempo, las redes Wi-Fi están soportando más servicios, teniendo que aportar más opciones de configuración y funcionalidades que las hicieran aptas para que las aplicaciones y servicios puedan hacer uso de ellas. En una instalación con un gran número de puntos de acceso, la configuración manual de cada uno de ellos y su mantenimiento, de igual manera la detección y corrección de errores se torna compleja y el coste en tiempo y personal demasiado elevado.

Utilizando un elemento de control y gestión centralizados se puede mitigar estos problemas y ofrecer funcionalidades adicionales.

Los Access point utilizados en estas redes son los ligeros, lo que permiten que una vez añadido el punto de acceso al controlador se le cargara automáticamente una configuración base, lo cual reduce los tiempos de instalación y minimiza los errores de configuración.

Algunas de las funcionalidades ofrecidas por las redes inalámbricas que utilizan un elemento de control y gestión centralizada son:

- Gestión centralizada: Una sola consola para gestionar los distintos puntos de acceso.

- Centralización de eventos: En instalaciones amplias, con un gran número de puntos de acceso, resulta no muy práctico y eficiente acceder a cada uno de ellos para tener conocimiento de los eventos acontecidos y posteriormente relacionar los datos obtenidos de cada uno de ellos. La controladora permite automatizar este proceso con un ahorro en costes y un aumento en la fiabilidad de la red.

- Seguridad avanzada y centralizada: Permite gestionar la admisión de clientes Wi-Fi, definir perfiles, permitir el acceso de los clientes a distintas partes de la red o servicios dependiendo de su identidad y perfil, filtrados y detección de accesos, etc.

- Servicios de localización de clientes Wi-Fi: Dado que el sistema de gestión centralizada controla a todos los puntos de acceso, este sistema es capaz de obtener los datos de potencia de recepción que cada uno de los puntos de acceso obtiene de cada uno de los clientes. Con estos datos y relacionando los que distintos puntos de acceso obtienen de un mismo cliente, por triangulación, y conociendo previamente la localización de los puntos de acceso el gestor tendrá la capacidad de obtener la localización de los clientes.

- Tunelización: Es posible ofrecer el servicio de tunelización de los datos de la red Wi-Fi para que sean enviados a la red cableada a través de un túnel entre el punto de acceso y el gestor centralizado, de esta manera se permite que el gestor pueda controlar los datos del cliente realizando sobre ellos funciones como priorización, filtrado y monitorización.

Para este diseño su utilizará el diseño utilizando un elemento de control y gestión centralizado, para el diseño de la red inalámbrica se utilizará los elementos básicos:

- Puntos de acceso
- Controladora Inalámbrica.
- Sistema de gestión y monitoreo.

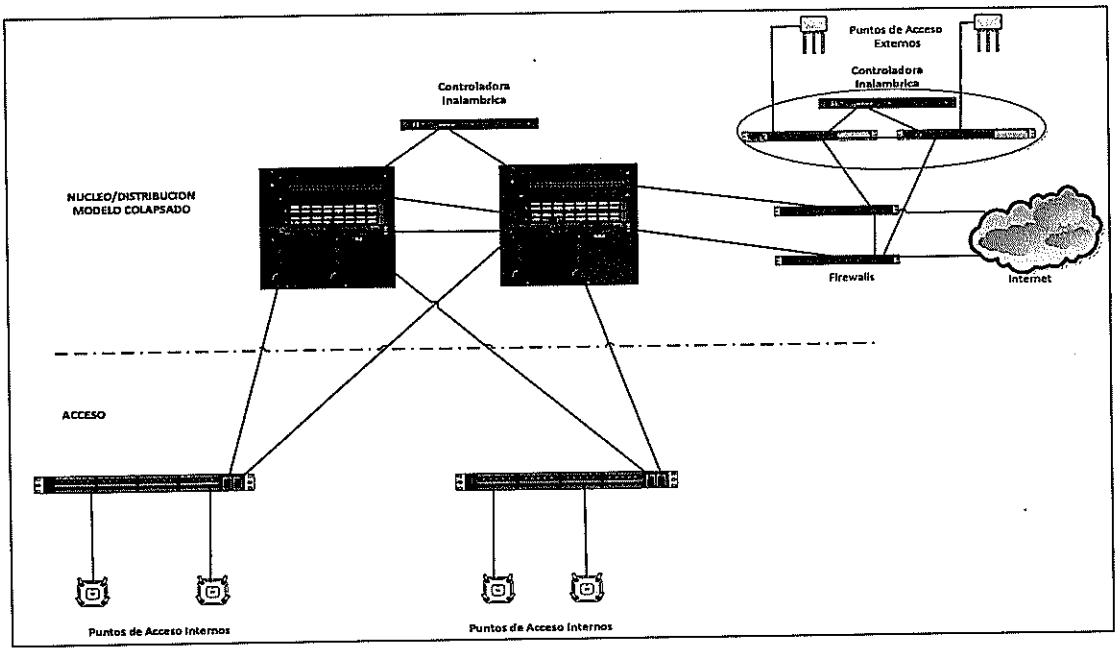

Figura N°3.5 : Esquema Centralizado de Controladora Inalámbrica
Elaboración : Jenny Arízaga

Se utilizará dos equipos controladores inalámbricas, una para los puntos de acceso de la red interna y otra controladora para los puntos de acceso que estarán ubicados en el parque.

Dado que los puntos de acceso de la red del parque son vulnerables a ataques ya que se utilizaran para dar internet al público visitante, se los ubico en una zona desmilitarizada junto con su respectiva controladora.

Los puntos de acceso de la red interna, son para los usuarios propios de la empresa.

La cantidad de equipos y la zona de cobertura de los puntos de acceso serán determinadas de manera teórica mediante un software de planificación y diseño de redes Wireless.

3.2.3.1 Software Sistema de Control Inalámbrica de Cisco.

El software de Cisco Sistema de Control Inalámbrico (WCS) es una plataforma completa escalable para satisfacer las necesidades de redes inalámbricas de las pequeñas, medianas y grandes empresas que requieren redes inalámbricas a gran escala a través de distintas ubicaciones locales, remotas, nacionales e internacionales. Esta solución proporciona a los administradores un acceso inmediato a las herramientas que necesitan y cuando los necesitan, para implementar de manera más eficiente y mantener las redes LAN inalámbricas seguras, todo desde una ubicación centralizada.

El WCS tiene una interfaz gráfica intuitiva que simplifica su uso, cuenta con herramientas integradas que proporcionan una mayor eficiencia y minimizan las necesidades de personal de TI que hacen uso de esta herramienta.

El WCS es una aplicación de software basada en navegador web que ofrece la capacidad de gestionar implementaciones de múltiples controladoras a través de una interfaz única.

Los beneficios de WCS incluyen lo siguiente:

- Planificación de redes inalámbricas.
- Diseño de redes inalámbricas.
- Gestión de redes inalámbricas.

El WCS se basa en un sistema de licencias. El licenciamiento permite despliegues en un único servidor desde 500 hasta 2.500 puntos de acceso, con el WCS se puede proporcionar mucha información a los administradores de red, incluyendo los siguientes:

- Seguimiento en tiempo real de hasta 2.500 clientes.
- Información histórica.
- Mapas de RF.
- Un punto de gestión único.

La herramienta de planificación y diseño de WCS simplifican el proceso de definición de la colocación del punto de acceso y la determinación de las áreas de cobertura del punto de acceso para edificios y campus. Esta herramienta permite a los administradores de TI una visibilidad clara en el entorno RF. Hacen que sea más fácil de visualizar el entorno ideal de RF, anticiparse a las necesidades futuras de cobertura, y evaluar los eventos de LAN inalámbrica. Ellos ayudan a los administradores de TI a reducir y en muchos casos eliminar, diseños RF indebidos y con problemas de cobertura que pueden conducir a problemas de conectividad de los usuarios finales.

La herramienta de planificación especializada WCS permite una evaluación inmediata de la disposición de la red inalámbrica para soportar voz sobre una red inalámbrica servicios sensibles al contexto (ubicación). Los servicios de voz sobre redes inalámbricas permiten la utilización de los teléfonos con capacidad Wi-Fi de modo dual. Para este proyecto se utilizó la herramienta de planificación.

3.3 Seguridad Perimetral (Cortafuego)

El borde Internet es la infraestructura de red que ofrece conectividad a Internet y que actúa como puerta de enlace para la empresa al resto del ciberespacio. El borde Internet sirve a otros bloques para conectarse al internet. Este enfoque de bloques de construcción modular permite flexibilidad y personalización en el diseño de la red para satisfacer las necesidades de los clientes y los modelos de negocio de diferentes tamaños y necesidades [6].

La figura 3.6 muestra la infraestructura de borde Internet como parte de una red empresarial. La infraestructura de borde Internet sirve la mayoría de las áreas de la red de la empresa, incluyendo el centro de datos, campus y sucursales remotas. El adecuado diseño e implementación de la infraestructura de borde Internet es crucial para asegurar la disponibilidad de servicios de Internet a todos los usuarios de la empresa.

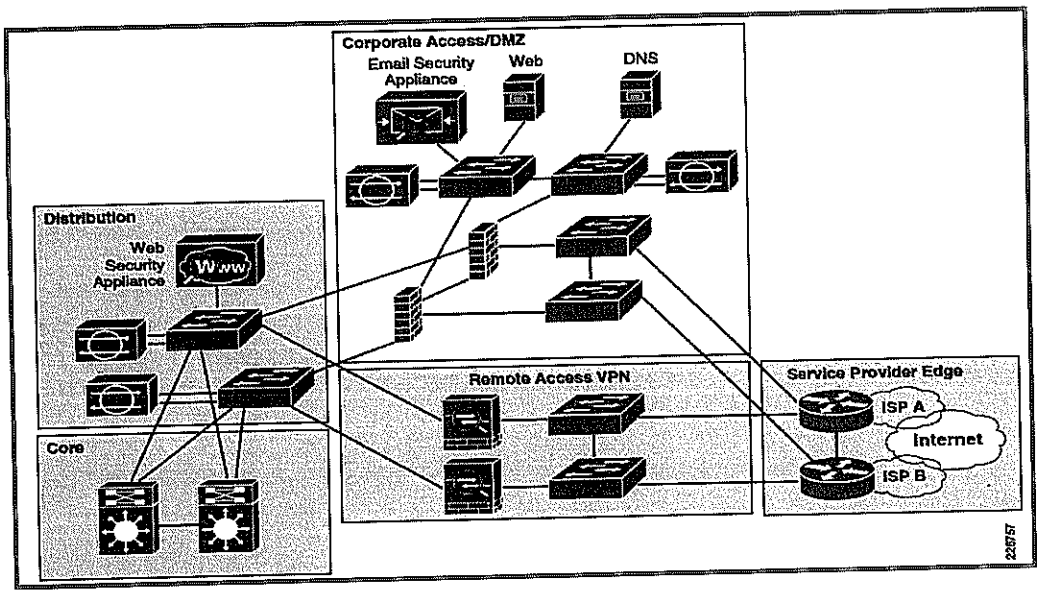

Figura N°3.6 : Seguridad Perimetral [3]

La infraestructura de borde Internet incluye los siguientes elementos funcionales:

Servicios del Proveedor (SP) de Borde: Esta parte frontera de la infraestructura de borde Internet consiste en enrutadores que interconectan directamente a Internet. Los enrutadores fronterizos orientados a Internet se conectan directamente al Internet del proveedor de servicio. Se debe tener una consideración cuidadosa al trabajar con el diseño de enrutamiento, la redundancia y la seguridad de estos enrutadores fronterizos.

Acceso Corporativo y DMZ: Una de las principales funciones de la ventaja de Internet es para permitir el acceso seguro a Internet de los usuarios corporativos, mientras que la prestación de servicios al público en general. Los cortafuegos de este módulo aseguran estas funciones a través de la aplicación de la aplicación de reglas de corta fuegos stateful e inspección de nivel de

aplicación. Los usuarios en los campus pueden acceder al correo electrónico, mensajería instantánea, navegación web y otros servicios comunes a través de los servidores de seguridad de borde Internet. Opcionalmente, la misma infraestructura puede servir a los usuarios en las sucursales que tienen permisos para acceder a Internet mediante una conexión centralizada. Los servicios públicos-que enfrentan, tales como el Protocolo de transferencia de archivos (FTP) servidores y sitios web, se pueden proporcionar mediante la implementación de una zona desmilitarizada (DMZ) dentro de este dominio de la red. El cortafuego de aplicaciones web es otro aparato que protege los servidores web de los ataques a nivel de aplicaciones (como XML). El cortafuego de aplicaciones web también reside en la infraestructura de DMZ y proporciona seguridad principal para el protocolo de transferencia de hipertexto (HTTP) y aplicaciones basadas en comercio electrónico.

Acceso remoto: La infraestructura de acceso remoto que proporciona acceso corporativo a los usuarios remotos a través de protocolos como Capa de Socket Seguro (SSL), red privada virtual (VPN) y Easy VPN.

3.3.1 Amenazas en el Borde del Internet.

El borde Internet es una infraestructura de red orientada hacia el público y está particularmente expuesta a gran variedad de amenazas externas. Algunas de las amenazas esperadas son los siguientes:

- Denegación de servicio (DoS), denegación de servicios distribuidos (DDoS).

- El spyware, malware, adware.
- Intrusiones en la red, toma de posesión, y el acceso no autorizado a la red.
- E-mail de spam y virus.
- Phishing basado en la Web, los virus y spyware.
- Ataques capa de aplicación (ataques XML, secuencias de comandos entre, y así sucesivamente).
- El robo de identidad, el fraude y la fuga de datos.

3.3.2 Diseño para internet en el Borde.

La red de borde Internet se puede dividir en varios bloques funcionales. Cada bloque funcional tiene sus propias consideraciones de diseño y de seguridad:

Acceso Corporativo y DMZ: Un par de Corta fuegos (Firewall) de seguridad proporcionan control de acceso con estado y la inspección profunda de paquetes [8]. Estos Corta Fuegos de seguridad están desplegados para proteger los recursos y los datos de las amenazas internas y externas de la organización al impedir el acceso entrante de Internet; para proteger los recursos públicos atendidos por la DMZ al restringir el acceso de entrada a los servicios públicos y al limitar el acceso de salida de recursos de la DMZ a la Internet; y para controlar el tráfico de Internet determinada de usuario. A tal fin, los cortafuegos están configurados para hacer cumplir las políticas de acceso, realizar un seguimiento de estado de la conexión, e inspeccionar las cargas

útiles de los paquetes. Los Corta Fuegos están configurados en modo activo / en espera, para fines de redundancia.

Los servicios de hosts en la Zona Desmilitarizada (DMZ), como el servidor de Seguridad de Correo, el servidor Web (HTTP), el servidor del Sistema de Nombre de Dominio (DNS), y el servidor de Transferencia de Archivo (FTP). El corta fuegos de aplicaciones web también reside en la zona desmilitarizada. El cortafuego de aplicación web proporciona seguridad perimetral para los ataques basados en aplicaciones que el corta fuegos no puede proteger y puede proporcionar salvaguardias para aplicaciones clave, como las transacciones de empresa a empresa. En la mayoría de los casos, el centro de datos implementa su propio servidor de seguridad de aplicaciones web. El cortafuego de aplicaciones web en la DMZ puede proporcionar la primera línea de defensa para aplicaciones de comercio y proteger los servidores web en la zona desmilitarizada contra ataques a nivel de aplicaciones.

Acceso remoto: Una función esencial del módulo de Internet es el de proporcionar un acceso seguro a los trabajadores remotos. Muchos enfoques diferentes se pueden tomar, dependiendo de los requerimientos y políticas particulares dentro de la empresa. Acceso para clientes remotos se puede implementar utilizando SSL VPN con clientes ligeros. Los clientes en este caso sólo se les permiten el acceso a los servicios HTTP específicas dentro de la empresa. Esto está en contraste con el acceso remoto de cliente completo en el que los clientes tienen acceso completo a todos los servicios dentro de la empresa y experimentan el mismo nivel de servicio como a los usuarios

corporativos internos. Se recomienda que dos corta fuegos de seguridad separadas se utilizan para proporcionar funcionalidad de acceso remoto. Aunque un solo par de corta fuegos de seguridad podría ser aprovechado tanto para el acceso remoto y acceso corporativo. El acceso remoto se puede asegurar aún más al exigir la autenticación y autorización de usuarios, y hacer cumplir políticas granular por usuario o controles de acceso por grupo.

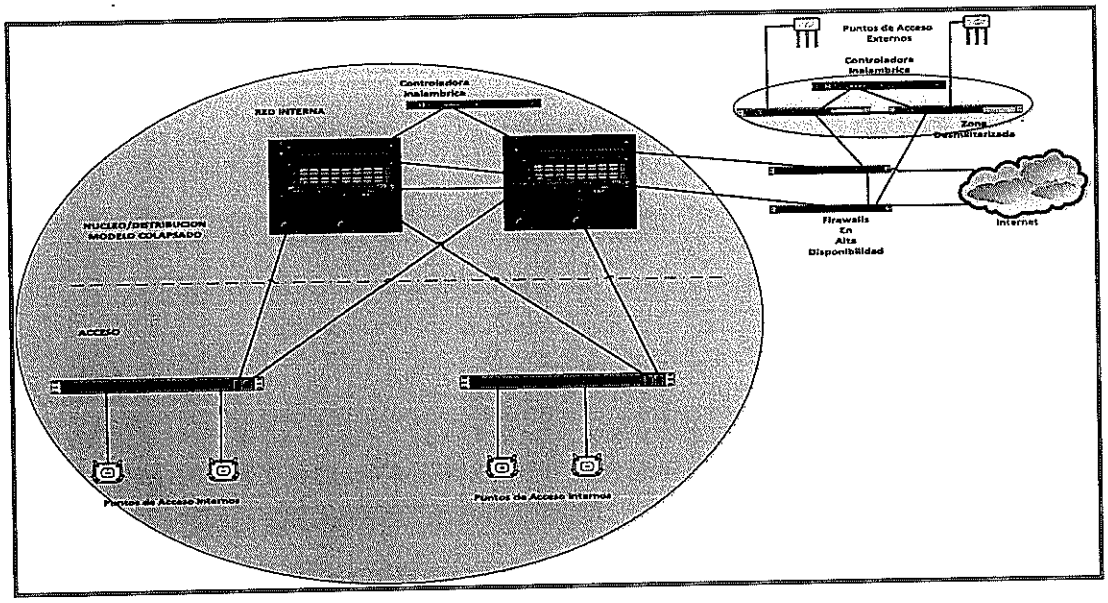

Figura N°3.7 : Acceso Remoto
Elaboración : Jenny Arízaga

3.4 Funcionalidades a ser Soportados por los Dispositivos de Red.

A continuación se detalla las funcionalidades a ser soportados por los distintos elementos de red.

Conmutador de Acceso.

Las funcionalidades a ser soportadas por los conmutadores de acceso serán las siguientes:

- ✓ Árbol Expandido (Spanning Tree).
- ✓ Árbol Expandido Rápido (Rapid Spanning Tree).
- ✓ Protocolo de Troncal de Redes Virtuales (VTP).
- ✓ Seguridad de Puertos (Port Security).
- ✓ Calidad de Servicio (QoS).
- ✓ Redes Virtuales (Vlan´s).
- ✓ Protocolos de Autodescubrimiento de dispositivos.
- ✓ Protocolo de Control de Agregación de Enlaces (LACP).
- ✓ Soporte a IEEE 802.1x Control de acceso a la red.
- ✓ Incluir IEEE 802.3af Potencia sobre Ethernet.
- ✓ Deben soportar conexiones en pila para crecimiento futuro.
- ✓ Protocolo Sencillo de Administración de Redes. (SNMP).
- ✓ Deben contar con interfaces que soporten transceptores conectables de forma pequeña (SFP y SFP+), para los enlaces ascendentes.

- ✓ Contar con 48 Puertos que soporten velocidades de 10/100/1000 Mbps.
- ✓ Deben ser de configuración fija.

Conmutador de Distribución/Núcleo.

Los conmutadores de Distribución/Nucleo deben de soportar las siguientes funcionalidades:

- ✓ Árbol Expandido (Spanning Tree).
- ✓ Árbol Expandido Rápido (Rapid Spanning Tree).
- ✓ Protocolo de Troncal de Redes Virtuales (VTP).
- ✓ Calidad de Servicio (QoS).
- ✓ Redes Virtuales (Vlan´s).
- ✓ Protocolos de Autodescubrimiento de dispositivos.
- ✓ Protocolo de Control de Agregación de Enlaces (LACP).
- ✓ Soporte a IEEE 802.1x Control de acceso a la red.
- ✓ Deben soportar conexiones en pila para crecimiento futuro.
- ✓ Protocolo Sencillo de Administración de Redes. (SNMP).
- ✓ Deben contar con interfaces que soporten transceptores conectables de forma pequeña (SFP y SFP+), para los enlaces ascendentes.

- ✓ Contar con 48 Puertos que soporten velocidades de 10/100/1000 Mbp
- ✓ Deben ser modulares.
- ✓ Deben contar con fuentes redundantes.
- ✓ Protocolo Activo Pasivo de Enrutadores (HSRP)
- ✓ Incluir soporte de virtualización (Virtualización de Sistema de Conmutación – VSS).
- ✓ Soporte de Protocolos de Enrutamientos para conectividad con la WAN.

Controladora LAN Inalámbrica (WLC).

- ✓ Solución que pueda ser escalable en el tiempo, se escale a través de licenciamiento en la cantidad de puntos de acceso a ser soportados.
- ✓ Soporte de redes IEEE 802.11: IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac.
- ✓ Proporciona tanto en tiempo real e información histórica acerca de la interferencia de RF afectar el rendimiento de la red a través de los controladores.
- ✓ Soporte para control de video y optimizarlo.
- ✓ Soporte para un segundo controlador en alta disponibilidad.

- ✓ Soporte para conexión en redes IEEE 802.3 10BASE-T, IEEE 802.3u especificación 100BASE-TX, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q Etiquetas de Redes Virtuales, y IEEE 802.1AX Agregación de Enlaces.
- ✓ Soporte de IEEE 802.1x
- ✓ Soporte de SNMP.
- ✓ Integración con Active Directory, soporte de LDAP.
- ✓ Soporte de Fuente redundante.

Puntos de Acceso (AP) Internos.

- ✓ Soporte para trabajar con Controladora LAN Inalámbrica.
- ✓ Soporte para IEEE 802.11, IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac.
- ✓ Soporte para antenas externas.
- ✓ Soporte para IEEE 802.3af y 802.3at+
- ✓ Interface para conexión a la red cableada 10/100/1000BASE-T autosensado (RJ-45).
- ✓ Punto de acceso para interiores.
- ✓ 4x4 múltiple entrada múltiple salida (MIMO) con tres flujos espaciales.

- ✓ Tecnología proactiva para combatir los problemas de rendimiento debido a la interferencia inalámbrica.
- ✓ Tecnología para mejorar el rendimiento del enlace descendente para todos los dispositivos móviles.
- ✓ Interface para administración.

Puntos de Acceso (AP) Externos.

- ✓ Soporte para trabajar con Controladora Lan Inalámbrica.
- ✓ Soporte para IEEE 802.11, IEEE 802.11a, 802.11g, 802.11n.
- ✓ Soporte para antenas externas.
- ✓ Soporte para fuentes de poder externas.
- ✓ Interface para conexión a la red cableada 10/100/1000BASE-T autosensado (RJ-45) o interfaces que soporten transceptores conectables de forma pequeña (SFP) para fibra óptica.
- ✓ Punto de acceso para exteriores.
- ✓ 2x3 múltiple entrada múltiple salida (MIMO) con dos flujos espaciales.
- ✓ Tecnología para mejorar el rendimiento del enlace descendente para todos los dispositivos móviles.
- ✓ Interface para administración.

3.5 Funcionalidades a ser soportados por los dispositivos de seguridad.

A continuación se detalla las funcionalidades a ser soportados por los distintos elementos de red en las funciones de seguridad.

Los conmutadores de Acceso/Distribución/Núcleo deben de soportar las siguientes funcionalidades:

- ✓ Soporte de Port Security.
- ✓ Soporte de esquemas de AAA (Autorización, Autenticación y Auditorias)
- ✓ Soporte de BPDU guard.
- ✓ Soporte de Root guard.
- ✓ Cortafuegos (Firewall).
- ✓ Capacidad de envió de tráfico con inspección 3Gbps.
- ✓ Capacidad de envió de tráfico con inspección y visibilidad de aplicaciones 1 Gbps.
- ✓ Soporte para Vlan´s.
- ✓ Soporte para implementar corta fuegos virtuales.
- ✓ 8 Interfaces de 10/100/1000 (RJ45).
- ✓ Interface de Administración.
- ✓ Soporte para incluir módulo de IPS a futuro.

- ✓ Soporte para LDAP.
- ✓ Soporte para VPN (IPSEC).
- ✓ Licenciamiento de usuarios ilimitado.
- ✓ Incluir alta disponibilidad activo/pasivo.
- ✓ Incluir fuente de poder redundante.
- ✓ Soporte para encripción 3DES/AES.
- ✓ Tener por lo menos 1 slots para crecimiento de interfaces.

3.6 Descripción de las características de los equipos que formaran la nueva red.

3.6.1 Conmutadores de Distribución/Núcleo.

A continuación se describe las características de los equipos seleccionados para ser Distribución/Core.

Se seleccionó un Cisco Catalyst 6509-E para realizar las funciones de Distribución/Core, este equipo cumple con las funcionalidades solicitadas anteriormente:

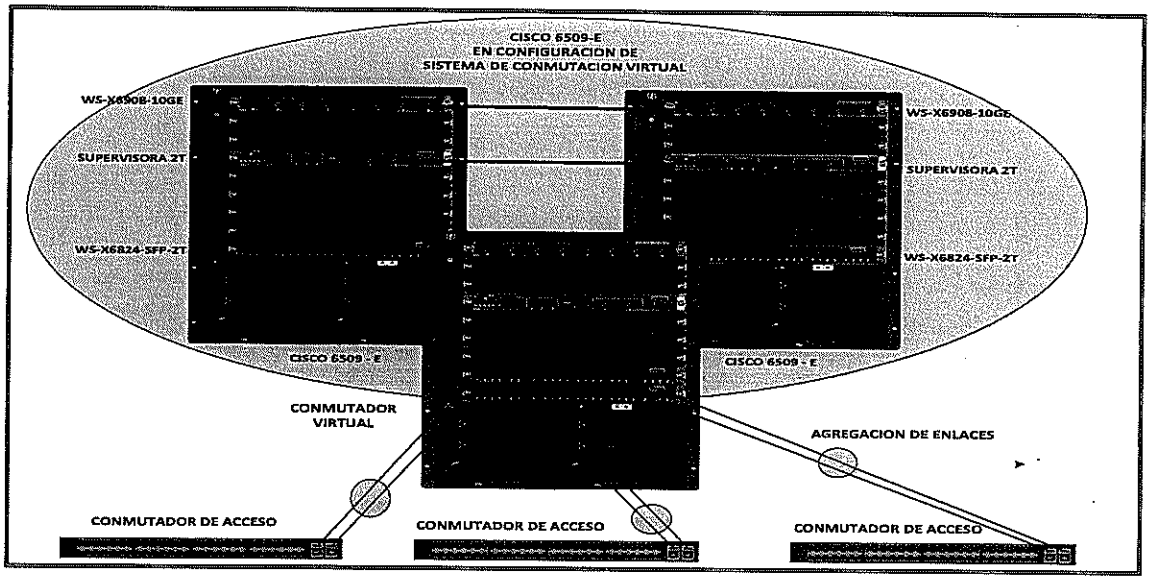

Figura N°3.8 : Conmutadores de Distribución/Núcleo
Elaboración : Jenny Arízaga.

Se consideran dos equipos Cisco 6509-E, con su configuración de Sistema de Conmutación Virtual (VSS).

La implementación de VSS, permitirá desde el punto de vista lógica a los dos equipos verse como un solo equipo, esto representa que para los equipos de acceso una conexión doble hacia a un solo equipo, y podremos agregar los dos enlaces de conexión con un Etherchanel brindando una conexión de 2 Gbps entre los conmutadores de acceso y distribución/núcleo.

Para la conexión de VSS se requiere el siguiente hardware:

La supervisora: VS-SUP2T-10G

Una tarjeta: WS-X6908-10GE

Para crear la conexión Virtual de los dos chasises.

Con la supervisora VS-SUP2T-10G, cada slots del chasis maneja una capacidad de conmutación de 80 Gbps.

Se utilizan tarjetas de línea:

WS-X6908-10GE: Para crear conexiones redundantes para la conexión virtual de los switches junto con las procesadoras.

WS-X6824-SFP-2T: Esta tarjeta de línea es de 24 puertos SFP de 1 Gbps con una conexión a la matriz de conmutación de 20 Gbps, lo cual nos da una relación efectiva aproximadamente de 1 a 1 para la conexión a los conmutadores de acceso.

El consumo de potencia de cada equipo, se presenta a continuación, el mismo fue calculada con la herramienta Power Calculator de Cisco:

Tabla N° 10 Detalle de Potencia del Conmutador Núcleo de Distribución

Configuration Details				
Slot	Line Card	Output Current(@42V) (A)	Output Power (W)	Typical Power Used (W)
FAN1	WS-C6509-E-FAN	5.00	210.00	168.00
1	WS-X6908-10G-2T	14.00	588.00	470.40
2	WS-X6824-SFP-2T	4.87	204.54	163.63
3	--EMPTY-SLOT--	0.00	0.00	0.00
4	--EMPTY-SLOT--	0.00	0.00	0.00
5	VS-S2T-10G	10.37	435.54	348.43
6	-- Reserved Power --	10.37	435.54	348.43
7	--EMPTY-SLOT--	0.00	0.00	0.00
8	--EMPTY-SLOT--	0.00	0.00	0.00
9	--EMPTY-SLOT--	0.00	0.00	0.00
		Output Current(@42V) (A)	Output Power (W)	Typical Power Used (W)
	Total	44.61	1873.62	1498.90

Elaboración : Jenny Arízaga

Dado esto se utilizará en el equipo fuentes de poder de 4000W.

TABLA N° 11 Detalle de Fuentes de Poder del Conmutador Núcleo /Distribución

Power Supply Details				
Minimum Power Supply	Percentage of Power used	Total Output Current(@42V) for This PSU(A)	Total Output Current(@42V) Used (A)	Total Output Current(@42V) Remaining (A)
Single/Redundant WS-CAC-2500W	80.38 %	55.50	44.61	10.89
Other Power Supply Options	Percentage of Power used	Total Output Current(@42V) for This PSU(A)	Total Output Current(@42V) Used (A)	Total Output Current(@42V) Remaining (A)
Single/Redundant WS-CAC-8700W-E with a Single 220V input	72.81 %	61.27	44.61	16.66
Single/Redundant WS-CAC-6000W with a Single 220V input	70.12 %	63.62	44.61	19.01
Single/Redundant WS-CAC-3000W	67.61 %	65.98	44.61	21.37
Single/Redundant WS-CAC-4000W	49.37 %	90.36	44.61	45.75

Elaboración : Jenny Arízaga

Con la configuración actual del equipo, se estaría utilizando el 49,37% de la potencia de la fuente, lo que permite holgura en crecimiento del mismo.

3.6.2 Conmutadores de Acceso.

Para los conmutadores de acceso se utilizaran los conmutadores Cisco 2960S, de 48 puertos con características PoE (IEEE 802.3 af).

Se utilizará conmutadores de capa 2 cuyas interfaces de enlaces de subida sean SFP/SFP+, ya que inicialmente se trabaja con enlaces ascendentes de 1 Gbps y a futuro estos módulos se puedan remplazar por módulos de 10 GE.

El modelo elegido es el Cisco Catalyst 2960S-48FPD-L, el cual cumple con lo solicitado.

En sus características PoE son de 48 Puertos 10/100/1000 Mbps (IEEE802.3 af) o 24 puertos IEEE 802.3at.

3.6.3 Controladora LAN Inalámbrica.

Se utilizar como controladora lan inalámbrica el modelo 5508, el cual permite el crecimiento de 500 access point mediante licenciamiento y soporta clientes con los estandares IEEE 802.11 a,b,g y n.

De acuerdo al diseño se implementan dos controladoras las cuales cumplen la siguiente función.

Controladora Interna: Dara el control de los Access Point de la red interna de la Empresa Administradora del Parque.

Controladora Externa DMZ: Dara el control de los Access Point de la red Wi-Fi del parque, dado que esta red es pública y estará expuesta a posibles ataques, por ello se la ubica en una red DMZ, al equipo se lo administrara desde la red interna.

La red Lan de la DMZ está conformada por dos conmutadores Cisco 4500X de 40 puertos en fibra óptica, estos se consideraron de esa manera ya que los puntos de acceso utilizados en el red Wi-Fi del parque poseen puertos para la conexión a la red cableada en fibra óptica, eliminando la necesidad de colocar convertidores de medio.

3.6.4 Puntos de Acceso Internos y Externos.

Para los puntos de acceso externo se eligió un modelo para exteriores y con puertos de fibra óptica, por lo que el modelo elegido es Cisco Aironet 1552E, este modelo cuenta con tres antenas externas que pueden ser omnidireccional

o direccional y cumple con el estándar IEEE 802.11b/g/ en la banda de los 2.4 GHz y 802.11a/n en la banda de los 5-GHz, este modelo es soportado por la controladora de lan inalámbrica Cisco WLC 5500.

Este modelo tiene la ventaja de que cuenta con un puerto PoE para conexión de otro dispositivo tal como una cámara de video vigilancia, y es el recomendado por el fabricante para modelos tipo campo de exteriores.

Adicionalmente este dispositivo cuenta con una tecnología del fabricante que mitiga las interferencias inalámbricas.

Para los puntos de acceso internos se eligió el modelo cisco Aironet CAP2602 con antenas externas que son omnidireccional, este modelo soporta los estándares IEEE 802.11a/g/n y es un modelo soportado por la controladora Lan inalámbrica Cisco WLC 5500.

Adicionalmente este dispositivo cuenta con una tecnología del fabricante que mitiga las interferencias inalámbricas.

Se utilizó el software de simulación Cisco Wireless Control System, para determinar la cantidad de puntos de acceso, se adjunta los diagramas de los patrones de radiación de los pisos del edificio de la EPPUEP.

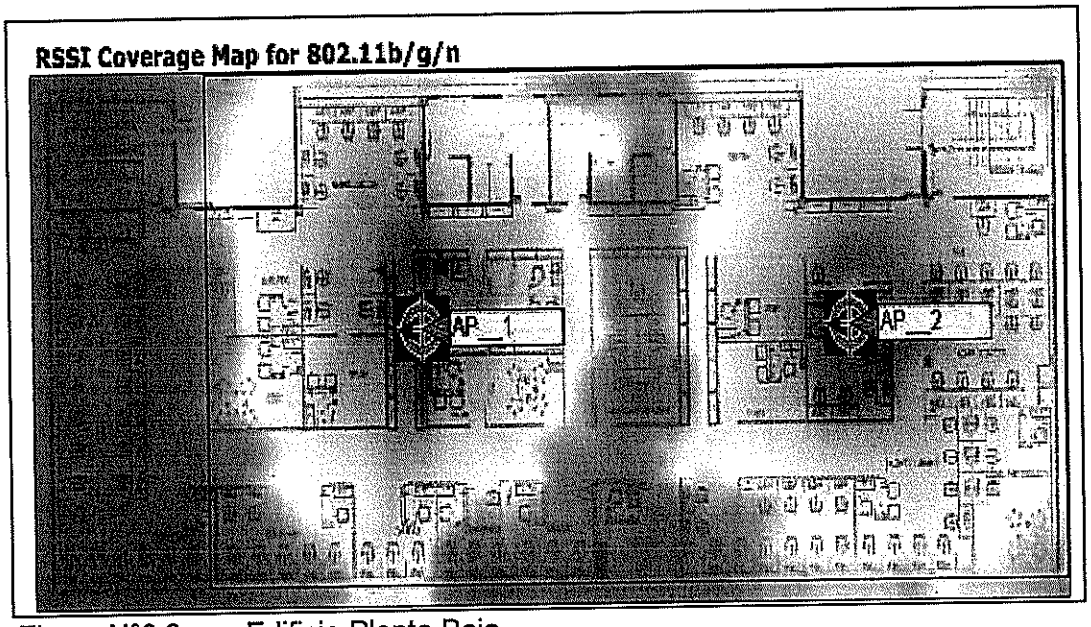

Figura N°3.9 : Edificio Planta Baja

Elaboración : Jenny Arízaga

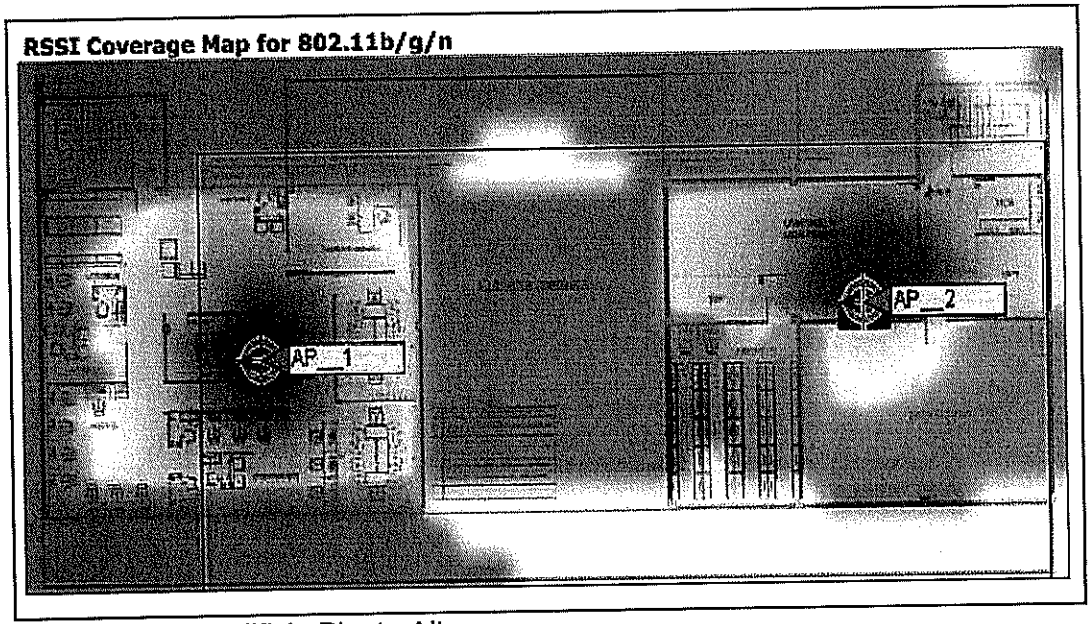

Figura N°3.10: Edificio Planta Alta

Elaboración : Jenny Arízaga

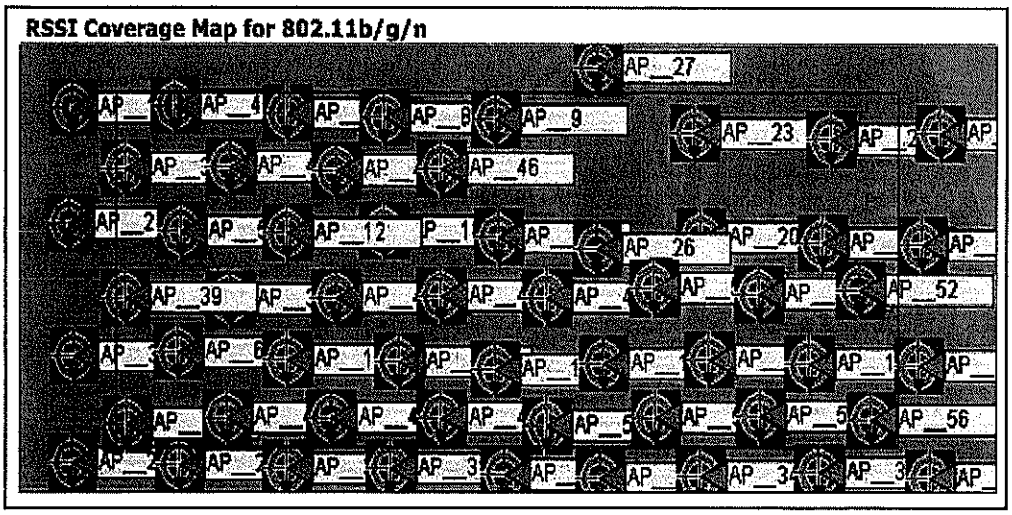

Figura N°3.11 : Simulación Cisco Wireless Control System
Elaboración : Jenny Arízaga

Figura N°3.12 : Fotografía del Parque
Elaboración : Jenny Arízaga

3.6.5 Cortafuegos.

Para el ámbito de la seguridad se utilizó la solución de Cisco ASA 5500 Cortafuego de Siguiente Generación, el dispositivo elegido incluye 8 puertos de 1 GEthernet los cuales son de uso independiente y pueden ser utilizados para definir las redes internas, externas y DMZ, dependiendo del nivel de seguridad asignado a cada una de ellas.

El dispositivo también incluye licencias de Visibilidad y control de aplicaciones el cual permitirá el control de más de 1200 aplicaciones y 150000 micro aplicaciones, posibilitando el control de las aplicaciones utilizadas por los empleados de la Empresa Administradora de Parques.

Para la red Wi-Fi del Parque que tendrá acceso a Internet se utilizará la licencia de Seguridad Web Esencial, que permitirá realizar el filtrado de URL y bloquear las páginas y contenidos como Sexo, drogas, etc. Evitando el mal uso del internet del parque.

Se utilizan dos dispositivos para tener alta disponibilidad, independientemente se cuenta también con dos conexiones a Internet.

3.6.6 Descriptivo de los elementos de la Solución.

A continuación se detalla los elementos que constituyen la solución de Conectividad Lan y seguridad perimetral.

TABLA N° 12 Detalle del Equipamiento Nuevo

Numero de Parte	Descripción Conmutador de Núcleo	Cantidad
WS-C6509-E	Catalyst 6500 Enhanced 9-slot chassis 14RU no PS no Fan Tray	2
CON-SNT-WS-C6509	8x5xNBD ServiceCatalyst 6509	2
VS-S2T-10G	Cat 6500 Sup 2T with 2 x 10GbE and 3 x 1GbE with MSFC5 PFC4	2
S2TAIK9-15102SY	Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES FULL ENCRYPT	2
MEM-C6K-INTFL1GB	Internal 1G Compact Flash	2
VS-F6K-PFC4	Cat 6k 80G Sys Daughter Board Sup2T PFC4	2
VS-SUP2T-10G	Catalyst 6500 Supervisor Engine 2T Baseboard	2
MEM-SUP2T-2GB	Catalyst 6500 2GB memory for Sup2T and Sup2TXL	2
X2-10GB-SR	10GBASE-SR X2 Module	4
VS-S2T-10G	Cat 6500 Sup 2T with 2 x 10GbE and 3 x 1GbE with MSFC5 PFC4	2
MEM-C6K-INTFL1GB	Internal 1G Compact Flash	2
VS-F6K-PFC4	Cat 6k 80G Sys Daughter Board Sup2T PFC4	2
VS-SUP2T-10G	Catalyst 6500 Supervisor Engine 2T Baseboard	2
MEM-SUP2T-2GB	Catalyst 6500 2GB memory for Sup2T and Sup2TXL	2
X2-10GB-SR	10GBASE-SR X2 Module	4
WS-X6824-SFP-2T	Catalyst 6500 24-port GigE Mod: fabric-enabled with DFC4	2
GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM	10
WS-X6908-10G-2T	C6K 8 port 10 Gigabit Ethernet module with DFC4 (Trustsec)	2
WS-F6K-DFC4-E	Cat 6k 80G Sys Daughter Board DFC4E	2
WS-X6908-10G	Catalyst 6500 8 Port 10G SFP Baseboard	2
X2-10GB-SR	10GBASE-SR X2 Module	4
WS-CAC-4000W-INT	4000W AC PowerSupply International (cable included)	4
WS-C6509-E-FAN	Catalyst 6509-E Chassis Fan Tray	2
Numero de Parte	**Descripción Conmutador de Acceso**	**Cantidad**
WS-C2960S-48FPD-L	Catalyst 2960S 48 GigE PoE 740W 2 x 10G SFP+ LAN Base	5
CON-SNTP-2960S4FD	SMARTNET 24X7X4 Cat 2960S Stk48 GigE PoE 740W2x10G LANB	5
CAB-16AWG-AC	AC Power cord 16AWG	5
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	5
Numero de Parte	**Descripción Controladora Lan Inalámbrica**	**Cantidad**
AIR-CT5508-100-K9	Cisco 5508 Series Wireless Controller for up to 100 Aps	2
CON-SNT-CT08100	SMARTNET 8X5XNBD Cisco 5508 Series	2
SWC5500K9-74	Cisco Unified Wireless Controller SW Release 7.4	2
AIR-PWR-CORD-NA	AIR Line Cord North America	4
LIC-CT5508-100	100 AP Base license	2
LIC-CT5508-BASE	Base Software License	2
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	2
AIR-PWR-5500-AC	Cisco 5500 Series Wireless Controller Redundant Power Supply	2
Numero de Parte	**Descripción Conmutador de Zona Desmilitarizada**	**Cantidad**
WS-C4500X-32SFP+	Catalyst 4500-X 32 Port 10G IP Base Front-to-Back No P/S	2
CON-SNT-C45X32SF	SMARTNET 8X5XNBD Catalyst 4500-X 32 Port 10G IP Base Fro	2
C4500X-IPB	IP Base license for Catalyst 4500-X	2
C4KX-PWR-750AC-R	Catalyst 4500X 750W AC front to back cooling power supply	2

C4KX-PWR-750AC-R/2	Catalyst 4500X 750W AC front to back cooling 2nd PWR supply	2
CAB-US515-C15-US	NEMA 5-15 to IEC-C15 8ft US	4
S45XU-35-1521E	CAT4500-X Universal Image	2
C4KX-NM-8SFP+	Catalyst 4500X 8 Port 10G Network Module	2
GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM	40
GLC-LH-SMD	1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm DOM	38
GLC-T	1000BASE-T SFP	2
SD-X45-2GB-E	Catalyst 4500 2GB SD Memory Card	2
Número de Parte	**Descripción Puntos de Acceso Internos**	**Cantidad**
AIR-CAP2602E-A-K9	802.11n CAP w/CleanAir; 3x4:3SS; Mod; Ext Ant; A Reg Domain	4
CON-SNT-C262EA	SMARTNET 8X5XNBD 802.11n CAP w/CleanA	4
AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	4
AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	4
SWAP2600-RCOVRY-K9	Cisco 2600 Series IOS WIRELESS LAN RECOVERY	4
AIR-ANT2524DB-R	2.4 GHz 2 dBi/5 GHz 4 dBi Dipole Ant. Blk RP-TNC	16
Número de Parte	**Descripción Puntos de Acceso Externos**	**Cantidad**
AIR-CAP1552E-A-K9	802.11N Outdoor Mesh Access Point Ext. Ant. A Reg. Domain	56
CON-SNT-C1552EA	SMARTNET 8X5XNBD 802.11N External Antenna Mesh Access Poi	56
S155W7K9-15202JB	Cisco 1550 Series IOS WIRELESS LAN – Autonomous	56
AIR-ANT2547V-N	2.4 GHz 4dBi/5 GHz 7dBi Dual Band Omni Antenna N connector	168
AIR-ACCPMK1550=	1550 Series Pole-Mount Kit	56
GLC-LX-SM-RGD=	1000Mbps Single Mode Rugged SFP	56
AIR-CORD-R3P-40NA=	1520 Series AC Power Cord 40 ft. N. Amer Plug	56
Número de Parte	**Descripción Corta Fuegos**	**Cantidad**
ASA5545-2SSD120-K9	NGFW ASA 5545-X w/ SW 8GE Data 1GE Mgmt AC 3DES/AES 2 SSD120	2
CON-SNT-A45SDK9	SMARTNET 8X5XNBD ASA 5545-X with SW	2
SF-ASA-X-9.1-K8	ASA 9.1 Software image for ASA 5500-X Series5585-X & ASA-SM	2
SF-ASA-CX-9.1-K8	ASA 5500 Series CX Software v9.1	2
ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	2
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2
ASA5545-AW1Y	ASA 5545-X CX AVC and Web Security Essentials 1Year	2
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows Solaris Linux Mac)	2
ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	2
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2
ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	2
ASA5500X-SSD120INC	ASA 5512-X through 5555-X 120GB MLC SED SSD (Incl.)	4
ASA5545-MB	^ASA 5545 IPS Part Number with which PCB Serial is associated	2
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2

Elaboración : Jenny Arízaga

A continuación se detalla el costo de la solución a implementar

Tabla N° 13 Detalle Resumido del Costo de la Solución a Implementar

Numero Linea	Numero Parte	Descripción de Equipamiento	Cantidad	Precio Lista	Precio Total
1	WS-C6509-E	Catalyst 6500 Enhanced 9-slot chassis 14RU no PS no Fan Tray	2	158.526,09	317.052,18
2	WS-C2960S-48FPD-L	Catalyst 2960S 48 GigE PoE 740W 2 x 10G SFP+ LAN Base	5	8.447,60	42.238,00
3	AIR-CT5508-100-K9	Cisco 5508 Series Wireless Controller for up to 100 APs	2	45.396,12	90.792,24
4	WS-C4500X-32SFP+	Catalyst 4500-X 32 Port 10G IP Base Front-to-Back No P/S	2	72.275,00	144.550,00
5	AIR-CAP2602E-A-K9	802.11n CAP w/CleanAir; 3x4:3SS; Mod; Ext Ant; A Reg Domain	4	1.322,53	5.290,13
6	AIR-CAP1552E-A-K9	802.11N Outdoor Mesh Access Point Ext. Ant. A Reg. Domain	56	6.881,00	385.336,00
7	ASA5545-2SSD120-K9	NGFW ASA 5545-X w/ SW 8GE Data 1GE Mgmt AC 3DES/AES 2 SSD120	2	28.897,59	57.795,17
				TOTAL	1.043.053,72

Elaboración : Jenny Arízaga

3.7 Definición de políticas de seguridad y control de acceso.

Las políticas de la Empresa administradora se definen de la siguiente manera:

Políticas de Control de Acceso a Internet

Se distribuye de la siguiente manera:

Permisos de acceso a internet restringido para las siguientes áreas:

- Usuarios Administrativos.
- Usuarios Financieros.

Permisos de acceso a internet libre para las siguientes áreas:

- Usuarios de Diseño.

- Usuarios Administradores.
- Usuarios Gerenciales.

Políticas de Control de Acceso a la Red Interna

Solo el personal autorizado tendrá acceso a la red interna de la empresa, tanto inalámbrico como alámbrico, sean dispositivos alámbricos o inalámbricos. Cada funcionario tendrá un usuario y contraseña única con los estándares definidos en la empresa, donde se le otorga el acceso de los permisos establecidos por el jefe inmediato.

Se creara redes independientes dentro de la misma red, segmentada por VLAN'S de la siguiente manera:

- Cámaras de seguridad.
- Servidores
- Telefonía Ip
- Red alámbrica
- Red inalámbrica.

Los usuarios que se conecten a la red WLAN, y no tengan permiso autorizados se conectaran a una VLan´s donde no tendrán acceso a ningún servicio y quedarán aislados a algún tipo de servicio como internet, aplicaciones.

Control de Acceso al Sistema Operativo

Tipo de Usuario

Se define el tipo de usuario de la siguiente forma:

- **Usuario Normal:** No podrán realizar cambios.
- **Usuario Avanzado:** Pueden ejecutar pluggins para gestionar páginas que necesiten.
- **Usuario Help Desk:** Podrán realizar instalaciones, formatear disco duro, instalar controladores, parches de sistema operativos o programas.
- **Usuario Administrador:** Podrá crear, eliminar usuarios, permisos, instalar programas, cambios de contraseña.

Los usuarios que estén debidamente autorizados podrán llevar su portátil o equipo asignado por la empresa, fuera de la institución.

Control de Acceso mediante VPN

El funcionario tendrá que llenar una solicitud firmada por el jefe inmediato dando la autorización respectiva e indicando los motivos y a que información accedería vía remota, luego de esto el área de tecnología de seguridad informática evaluara los riesgos que implicaría estos permisos y luego emite un informe del acceso permitido o no permitido una vez revisado los riesgos para la seguridad de la información.

Políticas de Control de Acceso a Información de Archivos de Respaldo

Solo los funcionarios o usuarios dueño de la información generada podrán acceder a sus respaldos, o caso contrario el jefe inmediato autorizar quien pueda visualizar o copiar dicha información.

3.8 Selección del Software de Monitoreo y Gestión de los Dispositivos de la Red.

Las redes y los sistemas de procesamiento distribuido son de una importancia crítica y creciente en los negocios, gobierno y otras instituciones. Dentro de una institución, la tendencia es hacia redes más grandes, más complejas y dando soporte a más aplicaciones y a más usuarios.

Una red grande no se puede instalar y gestionar sólo con el esfuerzo humano. La complejidad de un sistema tal, impone el uso de herramientas automáticas de gestión de red. La urgencia de la necesidad de esas herramientas se incrementa, y también la dificultad de suministrar dichas herramientas, si la red incluye equipos de múltiples distribuidores. En respuesta, se han desarrollado normalizaciones para tratar la gestión de red, y que cubren los servicios, los protocolos y la base de información de gestión.

3.8.1 Requerimientos para la Gestión y Monitoreo de la Red.

Los requerimientos del departamento de tecnología, es un sistema de monitoreo y gestión para de forma permanentemente y proactiva monitorear y gestionar la red y no trabajar de una manera solo reactiva, el software debe tener las siguientes funcionalidades:

- Agendar el respaldo automático de las imágenes IOS de los equipos Cisco.
- Soporte de protocolo SNMP.

- Colección de eventos estadísticos.
- Actualización de imágenes IOS en forma remota.
- Envió de alarmas vía correo electrónico.
- Permita realizar el inventario de los dispositivos de red al detalle de chasis, modulo e interface.
- Monitoreo del performance de los equipos.
- Analizador de protocolo integrado en la herramienta.
- Facilidad en acceso a soporte y documentación de la herramienta.
- Auto descubrimiento de la red.
- El software de gestión de monitoreo debe ser homogéneo a los equipos de la red.

Permitiendo la recolección, almacenamiento de históricos y análisis de las principales variables de la red (Memoria, consumo de CPU, consumo de memoria RAM, tráfico de las interfaces, etc.), además de permitir monitorear permanentemente los retardos de los enlaces WAN parámetro que es de gran utilidad especialmente para las aplicaciones de voz, también nos brinda una visión de la disponibilidad de la red.

Adicionalmente resulta de gran utilidad contar con la herramienta de análisis de protocolos, y a través de la configuración de puertos espejos en los conmutadores administrables permite conocer cualitativamente el tráfico que

esta fluyendo a través de la red, de este modo se puede diagnosticar de mejor manera los problemas que pueden surgir, así como también permite identificar tráfico indeseable o utilidades de internet que no son productivas para el desarrollo del trabajo y más bien producen un consumo innecesario de ancho de banda.

3.8.2 Análisis y Selección de Software de Monitoreo y Gestión.

A continuación se describe tres software de gestión y monitoreo, dos de código abierto y una del fabricante de los equipos de la red LAN y WAN.

CACTI, es una herramienta que permite monitorizar y visualizar gráficas y estadísticas de dispositivos conectados a una red y que tengan habilitado el protocolo SNMP. En determinados momentos, necesitamos visualizar gráficas del estado de nuestra red: ancho de banda consumido, detectar congestiones o picos de tráfico o monitorizar determinados puertos de un equipo de red.

Con Cacti podremos monitorizar cualquier equipo de red que soporte el protocolo SNMP, ya sea un conmutador, un enrutador o un servidor Linux. Siempre que tengan activado el protocolo SNMP y conozcamos las MIBs con los distintos identificadores de objeto (OID), que podemos monitorizar y visualizar, podremos programar la colección de gráficas con las que queramos realizar el seguimiento. Cacti es una aplicación que funciona bajo entornos Apache + PHP + MySQL, por tanto, permite una visualización y gestión de la herramienta a través del navegador web. La herramienta utiliza

RRDtool, que captura los datos y los almacena en una base de datos circular, permitiendo visualizar de forma gráfica los datos capturados mediante MRTG.

ANALIZADOR DE RED NAGIOS, proporciona información del tráfico de red y del ancho de banda para toda su infraestructura de TI. Analizador de Red asegura que los sistemas, aplicaciones, servicios y procesos de negocio están funcionando correctamente. En caso de una amenaza a la seguridad o el ancho de banda pico inesperado, Analizador de Red proporciona a las organizaciones muchos beneficios, incluyendo:

• Análisis de Redes Amplia: Analizador de Red ofrece una mirada en profundidad a todas las fuentes de tráfico de red y posibles amenazas de seguridad que permiten a los administradores de sistemas para reunir rápidamente información de alto nivel con respecto a la salud de la red, así como datos altamente granulares para el análisis de la red completa y exhaustiva.

• Diseño intuitivo: Con una potente e intuitiva interfaz web, Analizador de Red es fácil de usar, mientras que proporciona el rendimiento y la velocidad óptima. Analizador de Red se integra perfectamente con nuestra solución de monitorización de red, Nagios XI, lo que permite la consolidación de alertas y notificaciones, así como el mantenimiento de una red segura y protegida. Fácilmente entrega alertas de configuración y añade fuentes con asistentes intuitivos en Analizador de Red con sólo unos clics.

• Claridad en la Red: Analizador de Red proporciona una visión central de su tráfico de red así como también los datos de ancho de banda, así como compromisos potenciales de la red. El tablero de instrumentos principal proporciona una vista rápida de las fuentes fundamentales de flujo de red de datos, métricas del sistema del servidor, y el comportamiento anormal de la red para la rápida evaluación de la salud de la red.

• Análisis en Profundidad: La alerta avanzada de Analizador de Red y la generación de informes proporcionan al personal de TI información de su red, altamente granular. Cuando se superan los umbrales críticos, la actividad de red anormal ocurre, o se cumplan las restricciones de ancho de banda, analizador de red puede activar alertas que permiten Administradores para iniciar la resolución de los problemas de inmediato.

• Adaptabilidad: Crear un entorno de Analizador de Red que refleje la identidad de su red a través de SNMP.

• Arquitectura extensible: Un API totalmente accesible ofrece una integración sencilla con las aplicaciones de terceros para personalizaciones avanzadas y la adaptación a su entorno.

CISCO PRIME INFRAESTRUCTURA, se ha desarrollado de una colección de productos individuales en un conjunto de funciones de gestión integrada basada en la manera que los administradores de red realizan su trabajo. Organizar el producto basado en la función de gestión, simplifica la experiencia del usuario al reducir la necesidad de cruzar los límites de una

aplicación para completar una tarea específica de gestión. Los flujos de trabajo son autónomos y toda la funcionalidad requerida se mantiene dentro de un área funcional.

Se indica las principales áreas funcionales.

- Forma rápida y proactiva para identificar y corregir problemas en la red antes de que afecten a los usuarios finales o servicios.
- Navegador centralizado de fallos y de eventos (consolidado, syslog, trampas, los eventos y alarmas).
- Integración con el Módulo de Análisis de Redes (NAM) para el análisis detallado del rendimiento y resolución de problemas (a nivel de decodificación de paquetes, análisis de protocolos).
- Copia de seguridad de configuración, gestión de imagen de software, el cumplimiento y gestión del cambio necesaria para mantener y actualizar los dispositivos de red.
- Las mejores prácticas de plantillas de configuración para desplegar configuraciones totales o parciales basadas en recomendaciones de diseño validadas.
- Los flujos de trabajo dinámicos dirigidos a reducir las probabilidades de error en las plantillas de configuración, las nuevas actualizaciones y configuraciones se puede descargar fácilmente desde Cisco.com

- Inventario completo y detallado de todos el equipamiento de Cisco chasis, módulo, interfaz.
- Ofrece un único menú del estado del dispositivo.
- Soporte para más de 560 tipos de dispositivos de Cisco.
- Todos los informes están centralizados en un solo menú, lo que simplifica la navegación y el acceso a los informes detallados y la información.
- Todas las funciones administrativas para la instalación y configuración de la aplicación están centralizadas para facilitar el acceso.

A continuación se detalla una tabla de evaluación de los tres software de gestión y monitoreo. Para ello se utilizo el cumplimiento de los aspectos más importantes para la empresa administradora.

TABLA N° 14 Cuadro de Evaluación de Funcionalidades de Software de Gestión y Monitoreo

FUNCIONALIDAD	PUNTAJE	NAGIOS NETWORK ANALIZER	CACTI	CISCO PRIME INFRAESTRUCTURA
Respaldo Archivos de Configuración	10	0	10	10
Respaldo de Imágenes IOS	10	0	0	10
Actualización de Imágenes en Forma Remota	10	0	0	10
Auto Descubrimiento de la Red	5	5	5	5
Soporte de SNMP	5	5	5	5
Colección de eventos y estadísticas de la Red	5	5	5	5
Envió de alarmas vía correo electrónico	5	5	5	5
Inventario de dispositivos al detalle	5	5	5	5
Monitoreo del Rendimiento de Dispositivos	5	5	5	5
Analizador de Protocolos	5	0	0	5
Interfaz del Usuario Intuitiva	9	9	9	7
Facilidad de acceso a Soporte	8	5	5	8
Facilidad de acceso a Documentación en Línea	8	5	5	8
Costo Licenciamiento (Sin Costo 5 - Con Costo 0)	5	0	5	0
Soporte Virtualización	5	5	5	5
TOTAL	100	54	69	93

Elaboración: Jenny Arizaga

El software elegido para esta implementación es Cisco Prime Infraestructura dado que es mejor contar con una herramienta que nativamente gestione y se integre de mejor manera con los dispositivos de red.

- Evaluación detallada de la infraestructura objeto y que se relaciona con la solución a implementar. Esto incluye verificación de la disponibilidad de los medios de transmisión con las condiciones de ancho de banda, retardos y jitter adecuados para el desarrollo del proyecto.

➢ Planeación e ingeniería de detalle, con base en las conclusiones de las actividades anteriores, incluyendo:

- Diseño detallado de red existente, provisto por el cliente
- Programación de la instalación en los ambientes de pruebas y producción si se requiere una diferenciación de los mismos.
- Creación y entrega de:
  - Evaluación de la red.
  - Plan detallado de implementación.
  - Cronograma de implementación.
  - Protocolo de pruebas.
  - Plan de proyecto.

3.10.1 Fase de seguimiento y control.

Las actividades a realizar en esta fase son:

- Programación y ejecución de reuniones de seguimiento periódicamente, con el objetivo de mantener bajo control las siguientes áreas del proyecto:
- Verificación del cumplimiento del Alcance del proyecto.
- Cumplimiento del cronograma.
- Gestión del Tiempo de los involucrados en el proyecto.
- Gestión de los planes de comunicaciones y de riesgos, definidos en el Plan de Proyecto.

3.10.2 Ejecución.

Las actividades a realizar en esta fase son:

- Coordinación la logística de la entrega de los productos para realizar la validación y la pre-configuración.
- Coordinación de actividades con el objetivo de verificar que los productos especificados en el documento de entrega cumplan las especificaciones solicitadas en la Orden de Compra y que no se encuentren dañados o deteriorados físicamente.
- Reemplazo del producto no conforme en caso de presentarse.
- Instalación y configuración de los equipos provistos, en el ambiente definitivo, de acuerdo con lo definido en la fase de Planeación e Ingeniería de detalle.

- Verificación de funcionamiento y ajuste en caso de ser necesario.

Es importante destacar que el cumplimiento de condiciones ambientales, de seguridad, eléctricas de los sitios, especificados en las hojas de especificaciones de los equipos.

3.10.3 Fase de pruebas.

Las actividades a realizar en esta fase son:

- Verificación de funcionamiento y ajuste en caso de ser necesario.
- Una vez ejecutado el Protocolo de Pruebas de manera exitosa se firma el protocolo de pruebas en señal de aceptación por parte del cliente.

3.10.4 Documentación.

La documentación comprometida a entregarse durante la fase de ejecución del proyecto es la siguiente:

3.10.4.1 Planificación

- Actas de reuniones y de acuerdo
- Diagrama de Gantt del proyecto
- Plan de implementación: Diseño de la solución, Diagrama de Arquitectura de la Aplicación, Diagramas de contexto o funcional en la que se muestran las entradas, salidas y relaciones entre las diferentes aplicaciones de la solución.

- Plan de pruebas.

3.10.4.2 Implementación

- Actas de entrega: Documento de partes, documento de licencias entregadas.
- Planeación en el sitio.
- Verificación del sitio
- Resultados de pruebas.
- Configuraciones realizadas en la solución
- Memoria técnica de implementación
- Documentación de la instalación realizada mediante el Informe de Cierre del Proyecto el cual incluye diagrama general, configuraciones finales y resultados de las pruebas para la verificación de funcionamiento.
- Si el proyecto contempla servicios de Soporte o Mantenimiento se entrega el procedimiento para la gestión de los servicios post-implementación.
- Firma del acta de aceptación del proyecto y cierre del mismo.
- Seguridad: Roles definidos, perfiles, grupos, usuarios, claves de administración.

3.10.4.3 Operación y Mantenimiento

- Manuales de operación: Plan de contingencia, procesos de recuperación y respaldo (Indicando descripción, modo de ejecución de procesos, periodicidad de ejecución).
- Contrato de soporte: Proceso de escalamiento y apertura de llamadas, SLAs.
- Reporte de asistencias de mantenimiento correctivo realizadas (incluyendo la revisión de actividades, reporte de solución y recomendaciones).

3.10.4.4 Administración

- Manuales de Guía de administrador
- Procedimientos para Operadores.
- Procedimientos de cambios de claves usuarios de administrador, niveles de seguridad recomendados y permitidos en la solución.

CAPITULO 4

PRUEBAS DE SIMULACIÓN DE LA NUEVA RED

En el presente capitulo se detalla las pruebas de simulación realizadas, como pruebas conceptuales de dos funcionalidades críticas a aplicar en el diseño de la red.

- Pruebas de simulación de Alta Disponibilidad en Seguridad.

- Pruebas de simulación de la Red LAN de Alta Disponibilidad.

4.1 Pruebas de Simulación de Alta Disponibilidad en Seguridad.

4.1.1 Alcance de la prueba.

El alcance de esta prueba es aplicar la alta disponibilidad en los cortafuegos conocida como conmutación por error (failover), esta configuración de

conmutación por error requiere dos dispositivos de seguridad idénticos conectados entre sí a través de un enlace dedicado, la operatividad de las interfaces y de las unidades se controlan para determinar si se da lugar a la conmutación por error. Si alguna unidad falla se produce la conmutación por error.

Las pruebas de simulación se realizaran en modo Active/Pasivo, en este modo sólo una unidad pasa el tráfico mientras que la otra unidad se encuentra en un estado de espera. Ante un fallo en la unidad principal se activara la unidad en estado pasiva, por lo que la conectividad de los usuarios se mantendrá hacia el internet.

4.1.2 Descripción del escenario de prueba.

El escenario de pruebas consiste en:

Dos Cisco ASA 5520 conectados en alta disponibilidad Activo/Pasivo, los enrutadores R2 y R3 configurados con HSRP para simular alta disponibilidad en la LAN, el enrutador R1 para simular la conectividad a internet, el enrutador R6 para simular la conectividad a una zona DMZ y C2 para simular la conectividad de un usuario de la red interna.

Se utiliza la versión de GNS3 0.87, la misma que no soporta la simulación de conmutadores, es por ello que la alta disponibilidad en la LAN se la realiza con HSRP configurados en dos enrutadores.

Las siguientes imágenes se utilizaron:

Routers Cisco 7200: c7200-jk9s-mz.124-13b.bin

Cisco ASA 5520: asa842-initrd.gz

Cisco ASDM: asdm-645-204.bin

Existen tres zonas en nuestro diagrama, una zona de Internet, Desmilitarizada e Interna, también se observara una conexión directa de cortafuegos a cortafuegos que es por donde los Cisco ASA se monitorean para la alta disponibilidad, el ASA 4 (en la parte superior de la figura 4.1) es el secundario pasivo y el ASA 7 (en la parte inferior de la figura 4.1) es el primario activo.

Desde la pc C2 se puede ejecutar el ambiente gráfico de configuración ASDM de los cortafuegos, se adjuntan varias pantallas del ASDM con la que se administra a los Cisco ASA 5520.

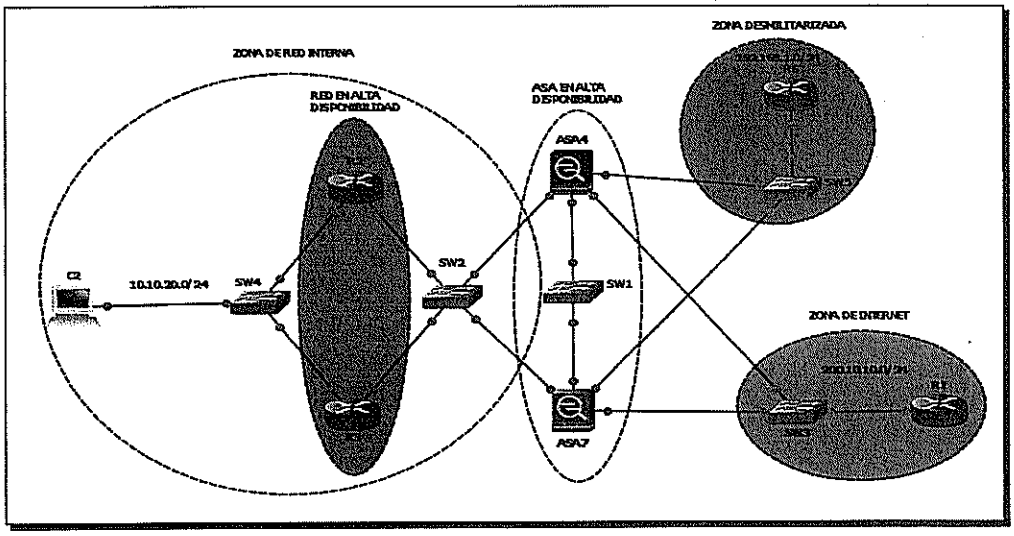

Figura N°4.1 : Diagrama de Simulación de Asa en Alta Disponibilidad
Elaboración : Jenny Arizaga

4.1.3 Detalle de la Prueba.

4.1.3.1 Objetivo

Simular la operatividad de la alta disponibilidad en los cortafuegos, mediante la simulación de falla en el enrutador R2 y cortafuegos ASA 7.

4.1.3.2 Pasos antes del fallo.

1.- Accesos a Pantallas del ASDM desde el Pc2.

A continuación se muestran las pantallas de acceso al corta fuegos ASA 7 desde el Pc2 utilizando el aplicativo de interfaz gráfica ASDM.

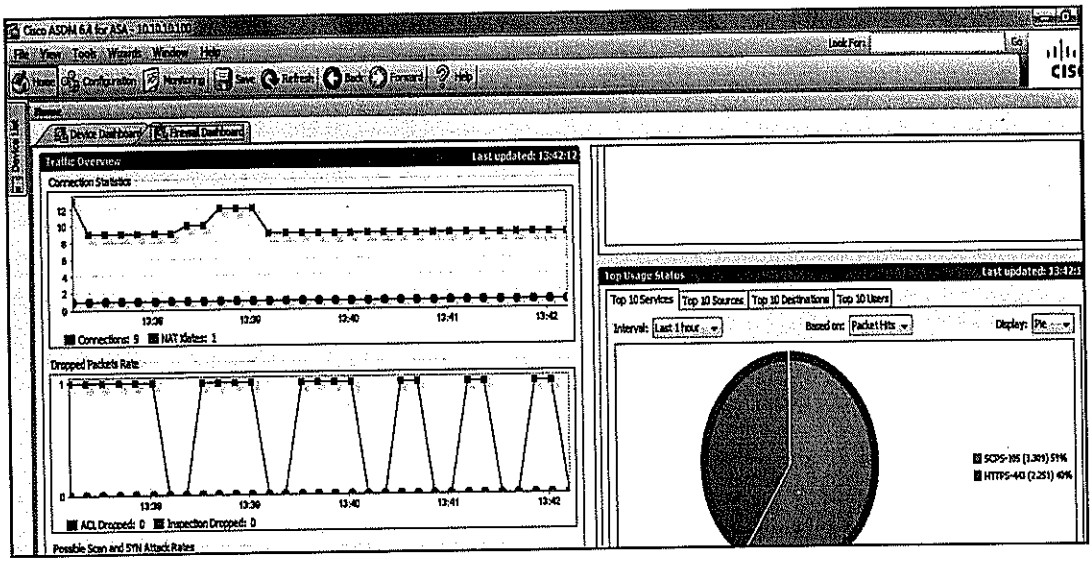

Figura N°4.2 : Vista 1 de la Interfaz de Gestión de los Cisco ASA - ASDM
Elaboración : Jenny Arízaga

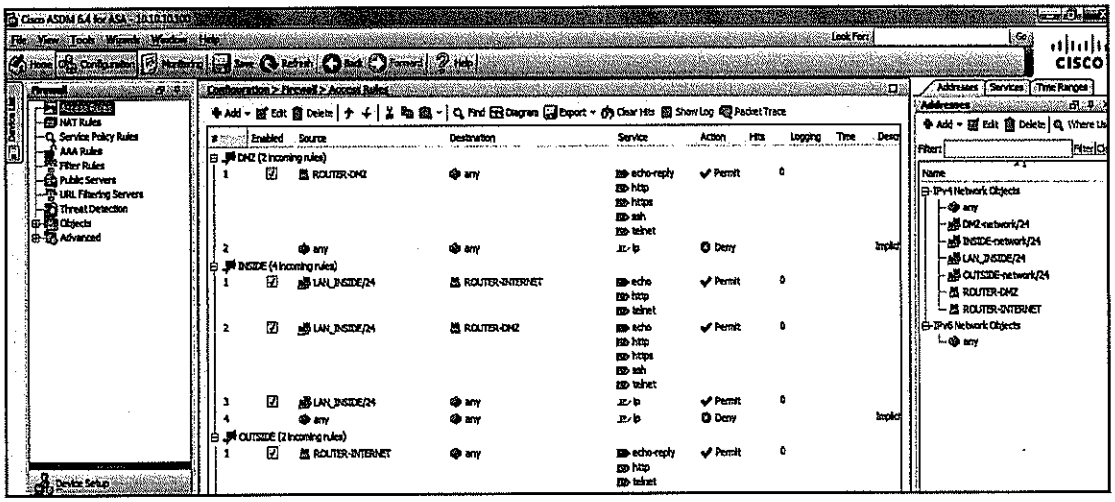

Figura N°4.3 : Vista 2 de la Interfaz de Gestión de los Cisco ASA - ASDM
Elaboración : Jenny Arízaga

2.- Acceso a enrutador R2 desde Pc2.

A continuación se muestran pantallas de acceso al enrutador R2 desde el Pc2, mediante Telnet.

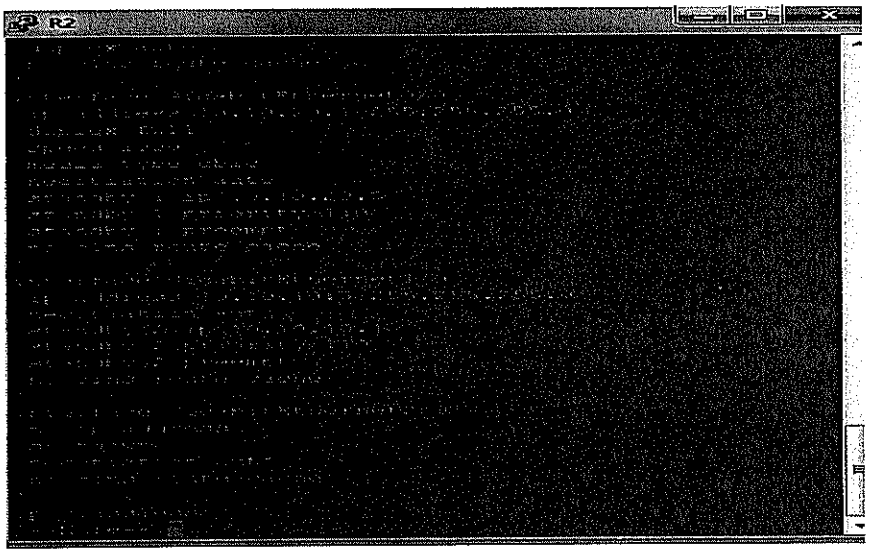

Figura N°4.4 : Vista de Configuración de HSRP en Enrutador R2
Elaboración : Jenny Arízaga

4.1.3.3 Falla en enrutador R2 y ASA 7.

A continuación se simula la falla del enrutador R2 y Cisco ASA 7, en el grafico se realiza un trazado con líneas rojas donde se indica los caminos del tráfico desde el computador C2 para realizar un telnet al enrutador R6 (tráfico desde la zona red interna hasta la zona desmilitarizada) y un telnet desde el enrutador R1 hasta el enrutador R6 (Trafico desde el internet hacia la zona desmilitarizada).

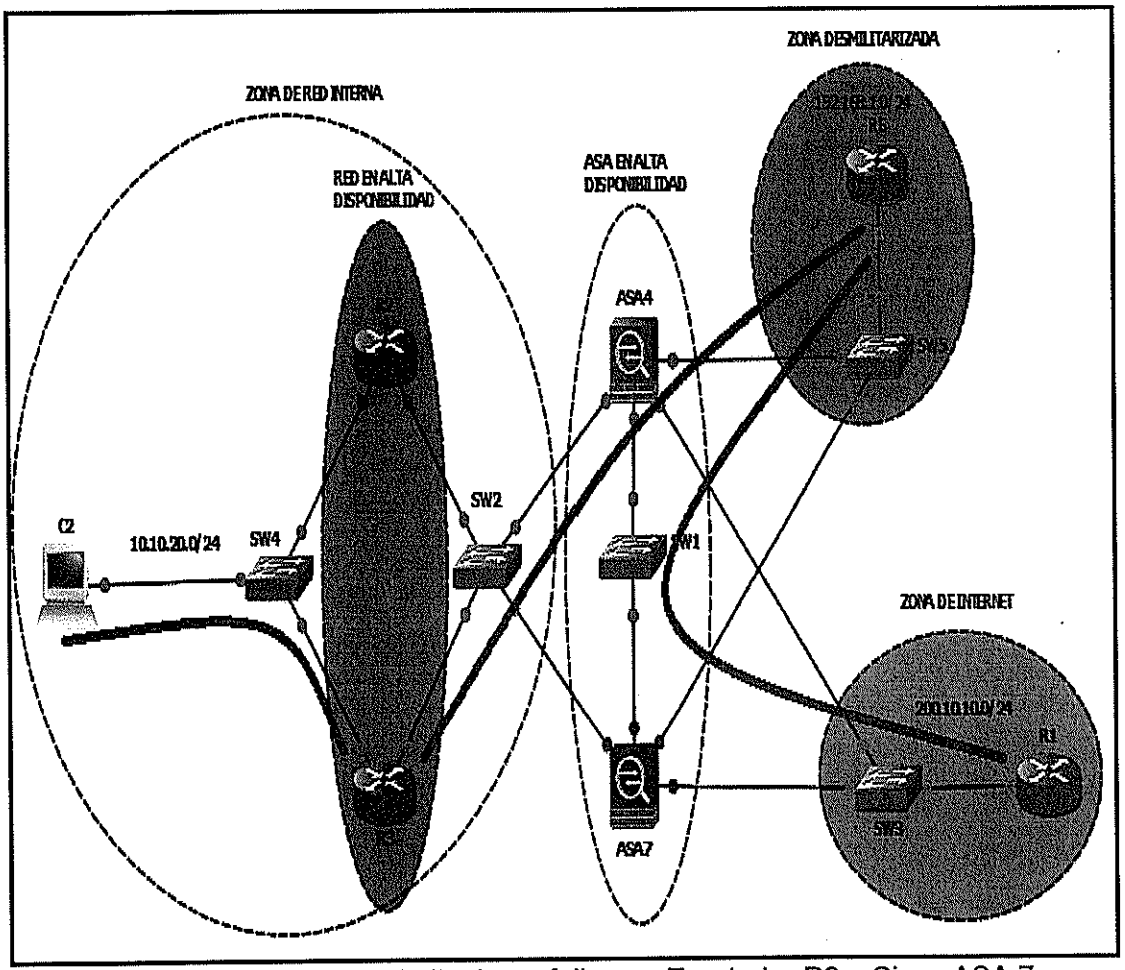

Figura N°4.5 : Diagrama de Red con fallos en Enrutador R2 y Cisco ASA 7
Elaboración : Jenny Arízaga

Como se observa en las figuras de abajo, la conexión entre los dispositivos se mantiene aun cuando uno de los enrutadores y un corta fuego están desactivados.

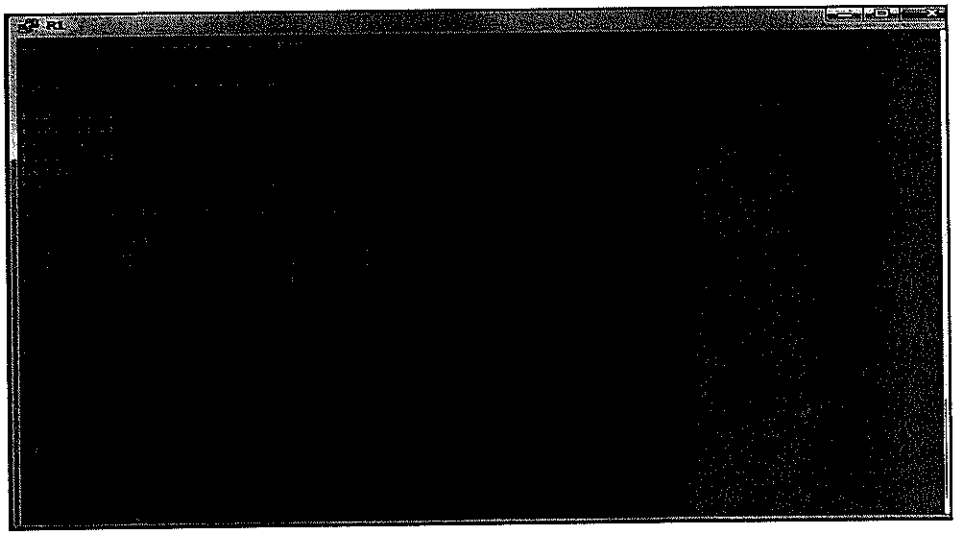

Figura N°4.6 : Vista de Acceso desde R1 a R6 Con Fallos en la Red de Enrutador R2 y ASA7
Elaboración : Jenny Arízaga

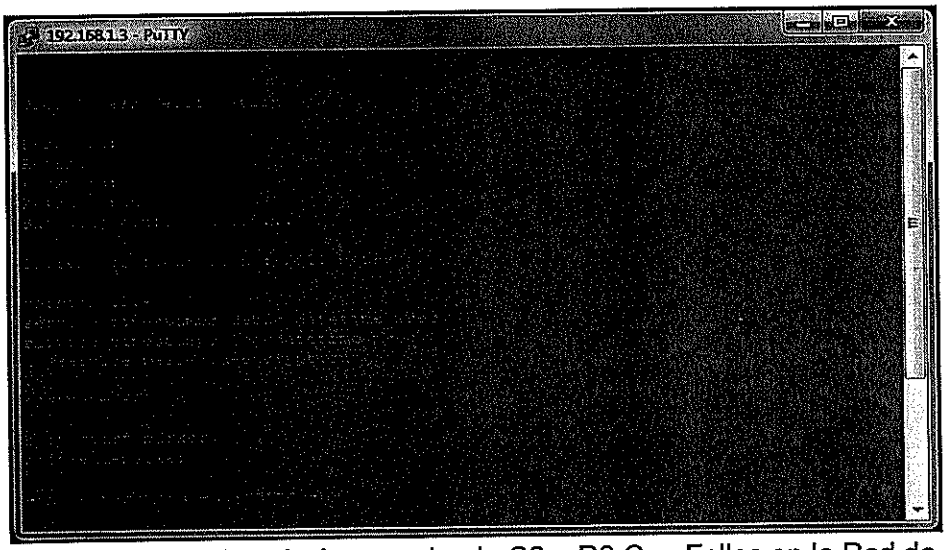

Figura N°4.7: Vista de Acceso desde C2 a R6 Con Fallos en la Red de Enrutador R2 y ASA7
Elaboración : Jenny Arízaga

Con ello se demuestra la alta disponibilidad ante un fallo crítico de los elementos de la red como lo son los cortafuegos o un conmutador principal (simulado mediante enrutadores), esta prueba permite garantizar que el diseño en alta disponibilidad es factible garantizando el acceso a internet a los usuarios internos de la empresa administradora del parque y a los visitantes del parque. Ver anexo 4, donde se indica la configuración de alta disponibilidad del Cisco ASA 7.

4.2 Pruebas de simulación de la red LAN

4.2.1 Alcance de la prueba.

El alcance de esta prueba es validar la disponibilidad de los servicios de red hacia los usuarios ante fallo de uno de los conmutadores de núcleo/distribución, en la implementación real se aplicara sobre los conmutadores Cisco Catalyst 6509 la funcionalidad de VSS. Mientras que en nuestra simulación como protocolo de alta disponibilidad para los conmutadores, aplicaremos HSRP (Protocolo de enrutadores Activo y en Espera) el cual si permite ser simulador en el software Packet Tracer, mientras que VSS no puede ser simulado a la actualidad, se aclara que dado que la prueba es orientada a validar la alta disponibilidad de los servicios de red para los usuarios mas no la funcionalidad de VSS es por ello que se utiliza un protocolo alterno como HSRP.

4.2.2 Descripción del escenario de pruebas.

El escenario de pruebas consiste en:

En la simulación de la disponibilidad de los servicios de red LAN hacia los usuarios, se utilizó el software Packet Tracert Version 6.1 para instructores, el diagrama propuesto fue el siguiente:

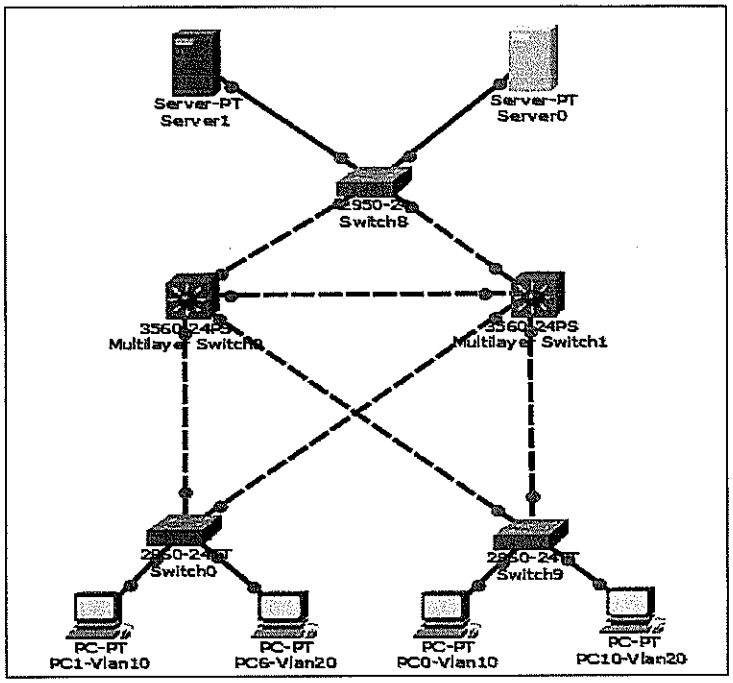

Figura N°4.8: Simulación de la Red LAN.
Elaboración : Jenny Arízaga

Dado que en el diseño se utilizó el modelo colapsado, en la simulación se utilizaron los Cisco Catalyst 3560 24PS para los conmutadores de núcleo/distribución en capa 3 y para los conmutadores de acceso se utilizaron los Cisco Catalyst 2960 24TT en capa 2.

Para la simulación de la alta disponibilidad se utilizó el Protocolo de enrutador Activo en Espera (HSRP) configurados en los Cisco Catalyst 3560. Los computadores PC0 y PC1 se encuentran en la Vlan 10 y los PC6 y PC10 en la

Vlan 20, adicionalmente en los Server 0 y 1 se configuro servidores Web para simular la conexión a una intranet.

4.2.3 Alcance de las pruebas

4.2.3.1 Objetivo

Simular la disponibilidad de los servicios de red LAN hacia los usuarios, mediante protocolos de alta disponibilidad en la LAN, ante un fallo en uno de los conmutadores de Núcleo/Distribución.

4.2.3.2 Pasos antes del fallo.

1.- Se realizara un ping para validar la conectividad y un acceso con un navegador al Server 0, a continuación se observa un ping desde el PC1 que pertenece a la Vlan 10 al PC6 que pertenece a la Vlan 20 y al Server 0, el comando ping permite validar la comunicación hasta la capa 3 del modelo OSI, y el acceso via http demuestra conectividad hasta capa 7 del modelo OSI.

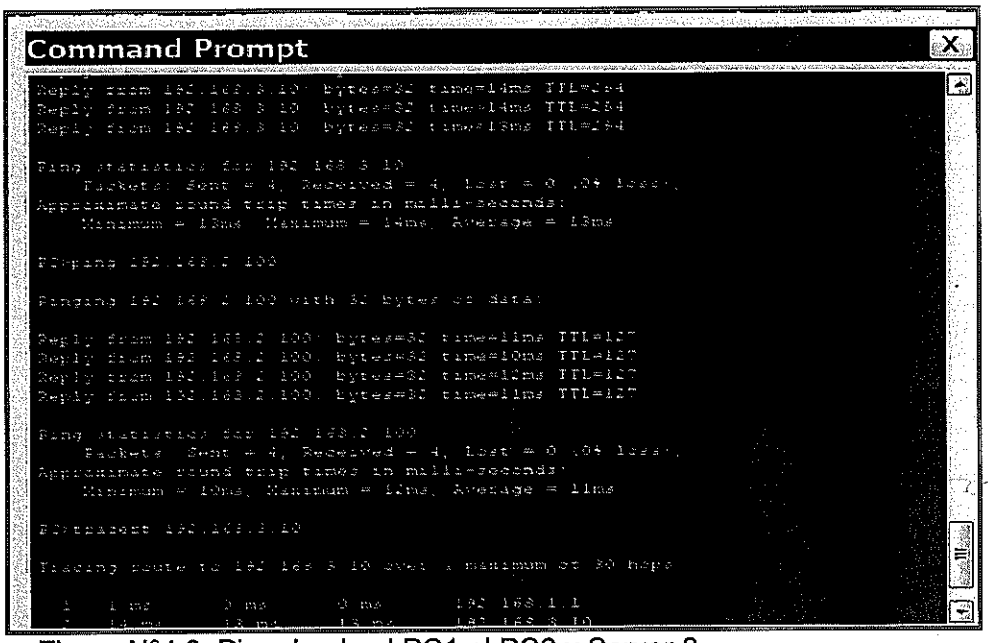

Figura N°4.9: Ping desde el PC1 al PC6 y Server 0
Elaboración : Jenny Arízaga

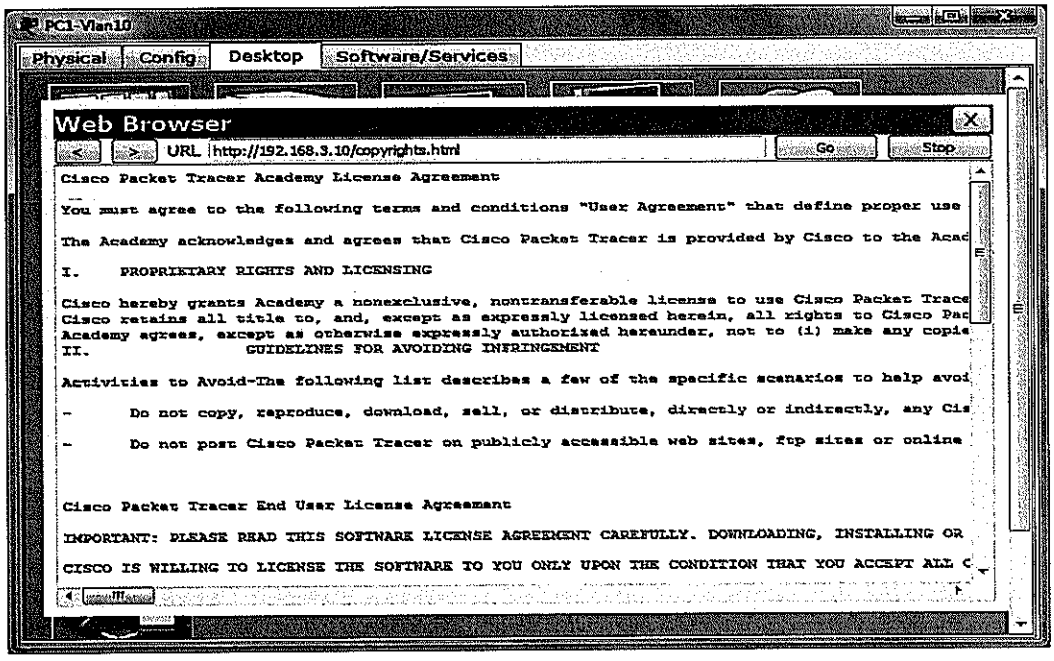

Figura N°4.10 : Acceso desde PC1 al Server 0 vía http
Elaboración : Jenny Arízaga

4.2.3.3 Fallo en un conmutador Núcleo/Distribución

Se simula una falla en uno de los conmutadores de núcleo/ distribución y se valida la conectividad en la red.

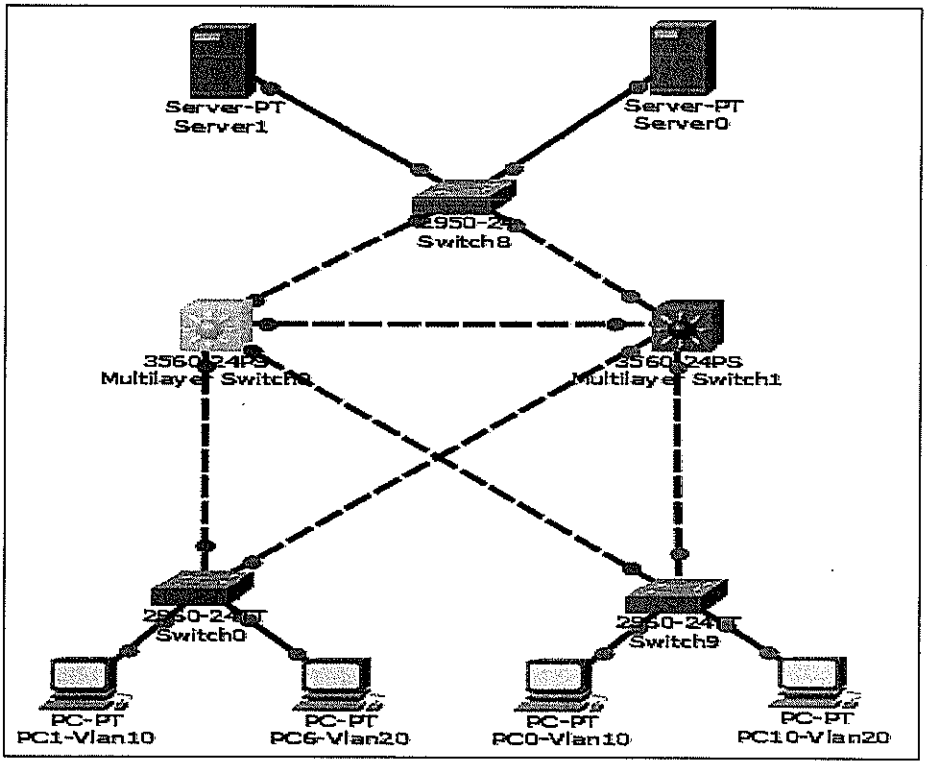

Figura N°4.11: Falla en uno de los Conmutadores de Núcleo/ distribución.
Elaboración : Jenny Arízaga

A continuación se observa un ping desde el PC1 que pertenece a la Vlan 10 al PC6 que pertenece a la Vlan 20 y un ping al Server 0, adicionalmente se presenta un acceso http al Server 0.

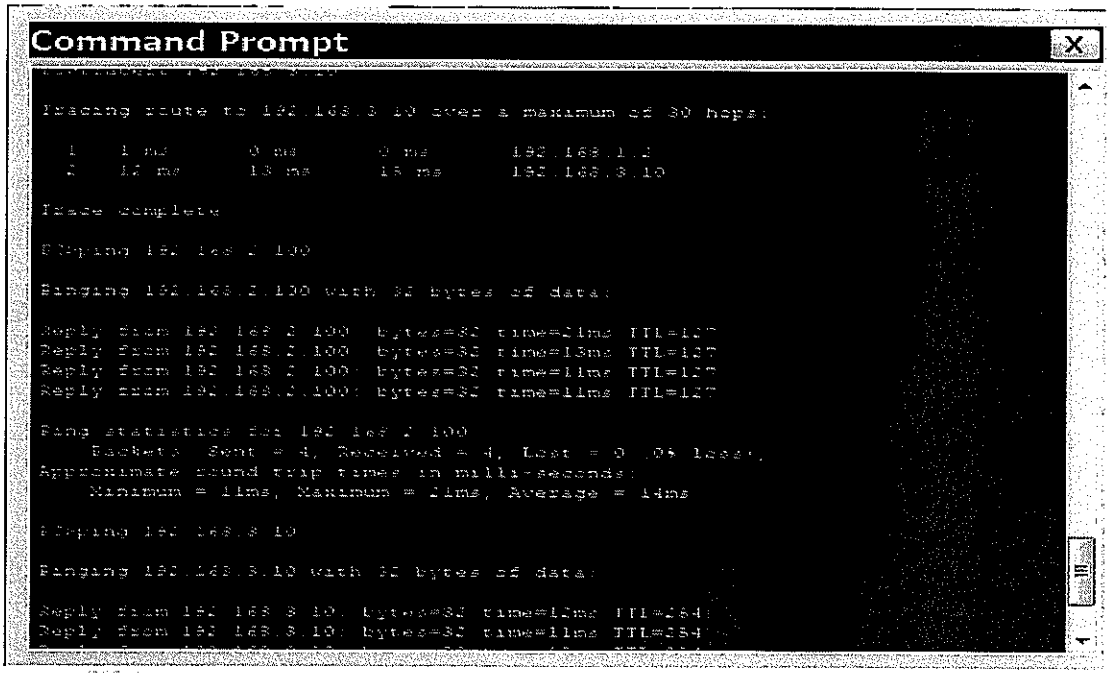

Figura N°4.12: Ping desde el PC1 al PC6 y al Server 0
Elaboración : Jenny Arízaga

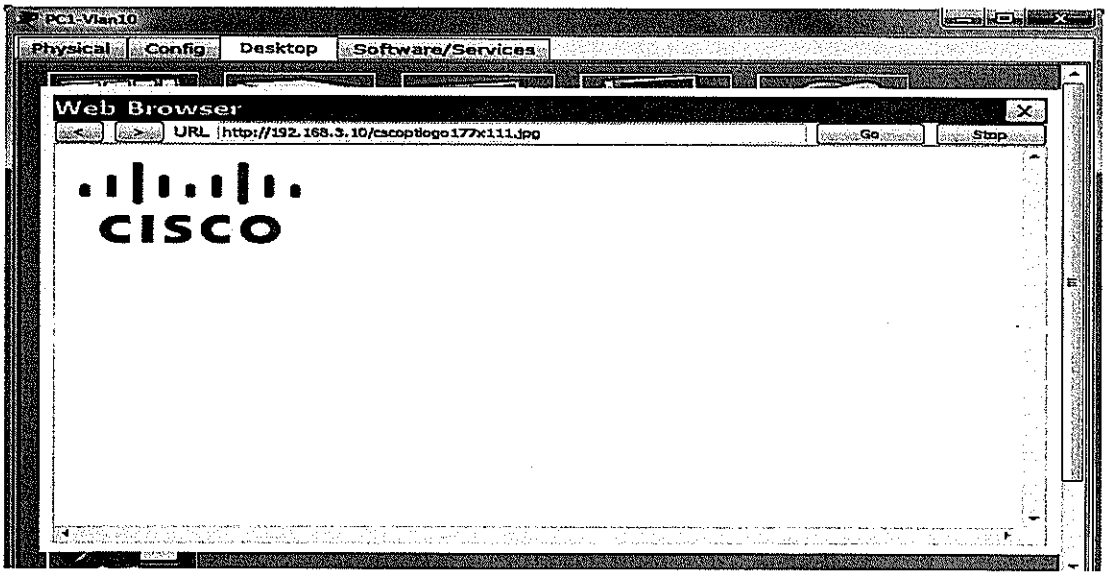

Figura N°4.13: Acceso http desde el PC1 al Server 0
Elaboración : Jenny Arízaga

Con esta prueba se demuestra que la conectividad en la red no se pierde ante un fallo en uno de los dispositivos principales, como lo son los conmutadores de Núcleo/Distribución. Ver anexo 5, donde se indica la configuración de alta disponibilidad de un conmutador de núcleo y distribución.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.

La presente tesis está basada en el estudio de la infraestructura de comunicaciones y seguridades para empresa administradora de un parque, en la cual se pueden llegar a las siguientes conclusiones.

1. La infraestructura actual del parque es un modelo muy simple en la cual se utiliza un conmutador como central y otro de acceso, los mismos no cuentan con esquemas de contingencia como alta disponibilidad en las fuentes de

2. alimentación o esquemas de redundancia de conectividad entre los dos conmutadores.

3. En su conexiona Internet están con un cortafuego muy limitado en cuanto a números de usuarios, el máximo para estos equipos es 100, considerando que

en la empresa existen alrededor de 203 empleados sin considerar los usuarios del internet del parque.

4. Su red inalámbrica cuenta con dos puntos de acceso en modo autónomo y validando los usuarios con clave compartida, lo cual es muy inseguro ya que los usuarios comparten la clave entre ellos para ganar acceso a internet en sus computadores y sus teléfonos inteligentes.

   Por lo que dada estas limitantes en los equipos se rediseño la red considerando alta disponibilidad y escalabilidad en el tiempo.

5. El modelo elegido es el modelo jerárquico Colapsado considerando dos conmutadores para alta disponibilidad, pero al mismo tiempo se pensó en un esquema virtualizado de los mismos, el cual a pesar de que son dos conmutadores físicos desde el punto de vista de los conmutadores de acceso se ven como uno solo, lo cual da muchas ventajas al no aplicar el protocolo de árbol expandido y bloquear un enlace, sino que permite que dos enlaces puedan ser agrupados en uno solo como un canal Etherchannel.

6. Estos equipos de núcleo cuentan con fuentes de poder redundantes cada uno de ellos, las tarjetas de conexión hacia los conmutadores de acceso también son redundantes. Al tener cada equipo una capacidad de 9 bahías y el estar ocupando solo 3 da escalabilidad en el tiempo.

7. Para los conmutadores de acceso se considera equipos con capacidad de QoS y PoE lo cual en el tiempo permitirá estar aptos para una solución de telefonía IP.

8. En la conexión a Internet se estará manejando dos Cortafuegos en alta disponibilidad uno activo y el otro en espera, con una capacidad total de manejo de tráfico de Internet de 1,5 Gbps. Se manejan tres zonas bien marcadas la zona de red interna, zona desmilitarizada y zona de internet.

9. En la zona desmilitarizada se ubicara a los servidores web o de correo que la empresa desee implementar y publicar. Adicionalmente aquí en esta zona se colocaran los puntos de acceso para el acceso a Internet de los usuarios del parque.

10. La red inalámbrica estará basada en una gestión centralizada, se utiliza dos controladoras de LAN inalámbrica la cual da un esquema de alta disponibilidad, las controladoras utilizadas permiten una escalabilidad de hasta 500 puntos de acceso.

    Por los puntos expuestos arriba se cumplen los objetivos de una red con alta disponibilidad, segura y escalable en el tiempo.

Recomendaciones.

Tomando en consideración los resultados alcanzados en el estudio de la infraestructura de comunicaciones y seguridad para una empresa administradora de un parque, se pueden resaltar una serie de recomendaciones.

1. Se recomienda a futuro la implementación de IPv6, pues todos sus componentes activos soportan este protocolo, que es hacia donde apuntan las nuevas aplicaciones.

2. A futuro también se recomienda implementar calidad de servicio (QoS) para soportar el transporte de voz y videos para aplicaciones de colaboración, como por ejemplo las aplicaciones de carteleras digitales los cuales serían muy útiles en el parque.
3. En la proyección a futuro se requiere implementar seguridades a nivel de LAN como Network Access Control para la red alámbrica e inalámbrica y su integración con el directorio activo, lo cual sería muy fácil de implementarlo ya que los conmutadores soportan la funcionalidad de IEEE 802.1X. Esta solución permitirá controlar a los usuarios implementando perfiles de ingreso a la red.
4. Se recomienda implementar servicios de AAA como Radius y Tacas para realizar auditorías de los cambios de configuración realizados en los dispositivos de red.
5. Es muy recomendable adquirir un sistema de Portal Cautivo, para poder controlar el acceso a internet a los usuarios del parque, ya que toda la infraestructura de red inalámbrica se encuentra lista para la implementación de este tipo de soluciones.
6. Finalmente se recomienda socializar los resultados de este estudio, con el propósito de valorarlos y crear conciencia de la importancia de contar con redes escalables y de alta disponibilidad para las empresas y en especial aquellas que permiten ofrecer servicios de internet a sus usuarios en lugares de esparcimiento.

BIBLIOGRAFÍA

[1] Cisco Learning, The three-layer hierarchical design model, http://www.cisco.com/web/learning/netacad/demos/CCNP1v30/ch1/1_1_1/index.html , fecha de consulta Octubre 2014.

[2] Cisco, Enterprise Campus 3.0 Architecture: Overview and Framework, http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html, fecha de consulta Octubre 2014.

[3] Tiso, Caswell, Designing Cisco Network Service Architectures (ARCH) Foundation Learning Guide, Cisco Press 3rd Ed, 2011.

[4] SUPERTEL, Revista Institucional 2012, http://www.supertel.gob.ec/pdf/publicaciones/revista_supertel_16_final.pdf, fecha de consulta Julio 2014.

[5) Cisco, Wireless Lan Deployment Guide, http://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_WirelessLANDeploymentGuide-Feb2013.pdf, fecha de consulta Octubre 2014

[6] Cisco, Firewall and IPS Technologhy Design Guide , http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-FirewallAndIPSDesignGuide-AUG13.pdf, fecha de consulta Octubre 2014

[7] Vacca, High Speed Cisco Network Planning Design and Implementation, Auerbach Publication, 2001

[8] Convery, Network Security Archictecture, Cisco Press, 2004

[9] Cisco, Wlan Design Guide,

http://www.cisco.com/web/strategy/docs/education/cisco_wlan_design_guide.pdf

fecha de consulta Noviembre 2014.