ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REINGENIERÍA DE LA INFRAESTRUCTURA DE RED DEL DATA CENTER DE LA EMPRESA CONECTIVIDAD GLOBAL CÍA. LTDA. QUE PROVEE SERVICIOS DE INTRANET A LAS INSTITUCIONES DEL PROYECTO QUITOEDUCA.NET

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE LA INFORMACIÓN

DENNYS ROBERTO CHÁVEZ BECERRA
dennisrob_5@hotmail.com

CHRISTIAM MAURICIO MENA VÁSQUEZ
christiam_mena@hotmail.com

DIRECTOR: MSc. Xavier Calderón.
CODIRECTOR: Ing. Rodrigo Chancusig.

Quito, febrero 2009

DECLARACIÓN

Nosotros, Dennys Roberto Chávez Becerra, Christiam Mauricio Mena Vásquez, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____	_____
Dennys Roberto Chávez Becerra	Christiam Mauricio Mena Vásquez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Dennys Roberto Chávez Becerra y Christiam Mauricio Mena Vásquez, bajo mi supervisión.

MSc. XAVIER CALDERÓN

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Nuestro agradecimiento especial al MSc. Xavier Calderon e Ing. Rodrigo Chacusig por su colaboración durante la realización de de este Proyecto de Titulación.

Al personal de Conectivdad Global Cia. Ltda. por su ayuda y contribución al permitirnos realizar y culminar este Proyecto de Titulación.

DEDICATORIA

A mi Patria por haberme brindado la oportunidad de realizar estos estudios de pregrado. A Dios y a mi familia por haberme brindado su ayuda y comprensión para culminar esta etapa de mi vida.

A mis amigos y amigas por haberme brindado su amistad incondicional.

A todas las personas que de una u otra forma influyeron en la culminación de mis objetivos.

Dennys Roberto

DEDICATORIA

A Dios por brindarme la oportunidad de estudiar y permitirme superar todas las adversidades. A mi padre y madre por su apoyo incondicional durante toda mi vida.

A mi familia por ser el estímulo para alcanzar cualquier meta. A mis amigos por su confianza y aliento.

Christiam Mauricio

CONTENIDO

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

ÍNDICE DE ECUACIONES

CAPÍTULO 2

RESUMEN

El presente proyecto de titulación provee una solución de arquitectura segura de red para el Data Center de la empresa Conectividad Global Cía. Ltda. proveedora del espacio físico, mantenimiento y operación de la red de servicios del Proyecto QuitoEduca.Net del Distrito Metropolitano de Quito.

Además plantea los procedimientos y políticas de seguridad necesarias para mantener disponibilidad en los servicios ofrecidos.

En el primer capítulo se analiza la situación actual del Data Center determinando los servicios y aplicaciones de red que se proveen, los elementos activos y pasivos como equipos de conectividad, servidores, cableado estructurado, etc. que forman parte de la infraestructura de red. Se determina el direccionamiento IP utilizado y se realiza un análisis de tráfico interno y externo.

Conjuntamente, se analiza la seguridad de la información en la red tomando como referencia los procedimientos de la norma ISO 17799 que ayudan a gestionarla. Se elabora un diagnóstico de la seguridad de la información y el análisis de riesgos sobre ésta. Para finalizar éste capítulo se plantean los requerimientos para el diseño.

En el segundo capítulo se establecen las políticas y procedimientos necesarios para mantener seguridad de la información partiendo de la mitigación de riesgos basada en las recomendaciones NIST (National Institute of Standards and Technology) para minimizar el impacto sobre la misión de la empresa.

Basado en la arquitectura de seguridad Cisco SAFE, el diseño de la red se lo realiza por módulos. Se crea un nuevo direccionamiento IP y se estima la capaciad necesaria de los enlaces en la red. Se proponen equipos de conectividad y se dimensionan las características básicas de los equipos servidores.

En el último capítulo se presentan las conclusiones obtenidas del proyecto desarrollado y las recomendaciones para la implementación y gestión de la seguridad de la información.

Al final se presentan los anexos que dan soporte al proyecto de titulación.

PRESENTACIÓN

La información es quizás, para la mayoría de empresas el activo más importante que poseen y puede presentarse en distintas formas, impresa o a través de medios electrónicos. El saber qué y de qué protegerla es el primer paso para minimizar el impacto que pueda generar la pérdida o manipulación indebida de estos activos.

La seguridad de la información no es únicamente un problema tecnológico, sino mas bien un problema organizacional. La tecnología sirve para poner en marcha los requerimientos de seguridad que nacen justamente de un análisis de riesgos y su valoración. Si se puede proveer confidencialidad, integridad y disponibilidad de la información, se proveerá seguridad.

Los modelos de gestión de seguridad de la información involucran a todo el personal de una organización y no sólo al área tecnológica, es por esto, que se debe concienciar la participación de todos los empleados.

Tecnológicamente, para proveer seguridad de la información existen mecanismos y procedimientos que se pueden configurar sobre equipos electrónicos. Es necesaria además, una arquitectura definida, sobre la cual se puedan gestionar las necesidades de seguridad y responder en el menor tiempo posible ante cualquier eventualidad.

La información presentada en este documento constituye el primer paso para proporcionar seguridad de la información, el siguiente paso será la participación de todos los involucrados.

CAPÍTULO 1. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED Y SUS REQUERIMIENTOS

En este capítulo se describirá la infraestructura actual de la red del Data Center de la empresa Conectividad Global Cía. Ltda. Los datos obtenidos son el resultado de la información recogida en colaboración del administrador de la red de la empresa y el personal técnico.

Esta información nos permite realizar el análisis de la red informática para determinar requerimientos y detectar falencias en el esquema que brinda servicios a los clientes; lo cual establece el punto de partida para el proceso de reingeniería del Data Center.

1.1. ANTECEDENTES

El Municipio del Distrito Metropolitano de Quito empezó el Proyecto QuitoEduca.Net en el año 2002 con el fin de mejorar la calidad de la educación en las diferentes instituciones educativas del distrito promoviendo el uso de tecnología, y de medios de comprensión y aprendizaje acordes al desarrollo y a la evolución de las herramientas informáticas.

Para cumplir con tal objetivo se vieron en la necesidad de utilizar un Data Center, el cual debía concentrar los servicios y aplicaciones necesarias, que serían provistas a las instituciones que forman parte del Proyecto.

La empresa Conectividad Global Cía. Ltda. es la actual proveedora del espacio físico y de la administración de los servicios, aplicaciones y medios de transmisión de datos al usuario final, es decir a los establecimientos educativos fiscales, fiscomisionales y municipales del Distrito Metropolitano de Quito.

Conectividad Global Cía. Ltda., es una institución de carácter privado, que se dedica a la compra, venta, generación, producción e implementación de software; instalación y configuración de equipos de cómputo y de conectividad. Estas funciones las realiza para entidades académicas y comerciales, tanto del sector público como privado. Proporciona servicios de intranet a sus clientes y realiza el mantenimiento y monitorización de enlaces de telecomunicaciones necesarios para el desarrollo de sus funciones.

La infraestructura de red con la que se operan los servicios hoy en día, se basa en un esquema topológico físico en estrella extendida[1]. Debido a problemas de escalabilidad, disponibilidad y seguridad se ha decidido emprender un proyecto de reestructuración de la red de servicios del Data Center de la empresa antes mencionada.

ESTRUCTURA ORGANIZACIONAL DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DE CONECTIVIDAD GLOBAL CÍA. LTDA.

El departamento de Tecnologías de la Información se conforma de tres áreas: Administración de la Red, Administración de los Sistemas y Desarrollo de Software.

Las funciones del área de Administración de Sistemas son instalación, actualización, parcheo y administración diaria de los sistemas operativos de los servidores. Es responsable de las aplicaciones que corren sobre los sistemas, como “Sistema de Gestión Académica”, “Red Educativa Virtual”, “Sistema de Seguimiento de Proyectos” y “Sistema de Educación en Línea”. Además su función es dar soporte y mantenimiento a las bases de datos de las aplicaciones.

---

[1] La topología en **estrella extendida** es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella.[16]

El personal del área de Administración de Red tiene la función de administrar diariamente la red local, la red de área metropolitana inalámbrica y la red de servicios que alberga el Data Center. Además de la instalación, configuración y soporte técnico de los dispositivos como routers, firewalls y switchs; servicios como DNS (Sistema de Nombres de Dominio), Web, correo electrónico, directorio, Internet, FTP (File Transfer Protocol), video conferencia, etc.

El área de Desarrollo de Software es responsable de la implementación personalización y soporte de las aplicaciones desarrolladas en la empresa. Además se encarga de la instalación y capacitación a los operadores de los sistemas en las diferentes instituciones.

1.2. ESTRUCTURA Y ESTADO ACTUAL DE LA RED DE DATOS

Para el análisis de la infraestructura de red se han diferenciado tres redes: la red de acceso a Internet, la red del Data Center y la red de área metropolitana.

La subred pública 157.100.135.0/27 proporcionada por el proveedor de servicios de Internet (ISP) conforma la red de acceso a Internet. La última milla del ISP es una conexión punto-punto implementada a través de bridges inalámbricos. El primer bridge está instalado en el último piso del Edificio Torre del Puente en la calle Núñez de Vela E3-13 y Atahualpa donde se encuentra el tele puerto del ISP Megadatos S.A. a una distancia de cinco kilómetros de su par, ubicado en el último piso de la Unidad Educativa Martim Cereré en la calle de los Guayacanes sector E13 N5101 y los Álamos; es necesario aclarar que no se ubicó éste último en la instalaciones del Data Center debido a que no se cuenta con línea de vista, la cual es requerida por los bridges del ISP. El flujo de información del enlace se conmuta a través de un switch a otro dispositivo inalámbrico configurado en modo bridge, el cual se conecta con su par a medio kilómetro en las instalaciones del Data Center ubicado en la Calle José Félix Barreiro E10-221 y avenida Eloy Alfaro. Aquí otro switch distribuye las distintas direcciones IP públicas asignadas por el proveedor. Los diagramas que permiten visualizar la ubicación y las distancias entre bridges se encuentran en el Anexo A.

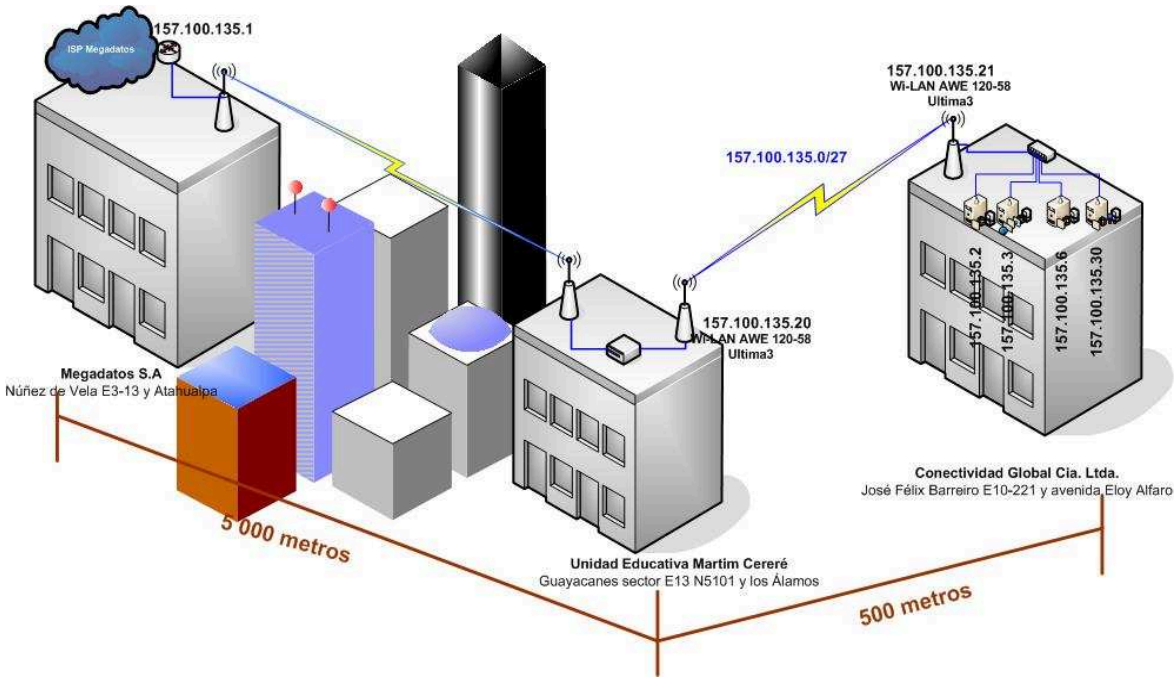


Figura 1.1 Distancia de los enlaces para el acceso a Internet

La red del Data Center está formada por tres redes independientes 172.20.0.0/24, 192.168.1.0/24 y 192.168.2.0/24, que brindan servicios de intranet mediante plataformas de software libre Linux y aplicaciones desarrolladas por la empresa manejando dominios de Internet diferentes.

Se utilizan cuatro direcciones IP públicas con fines diferentes. A cada una de ellas se ha asociado un firewall básico en el que se realizan tareas de re-direccionamiento de puertos, NAT (Traslación de Direcciones de Red) y enrutamiento; además, a estos se han añadido servicios como DNS, correo electrónico, transferencia de archivos (FTP) y controladores de ancho de banda dependiendo del servicio que provean.

La red de área Metropolitana, es la red de acceso de los clientes/usuarios y está implementada con tecnología propietaria inalámbrica Sky Pilot (802.11 modificada para redes malladas). Se proveen los servicios alojados en el Data Center a través de un Gateway principal (Sky Pilot Gateway) al que se conectan los dispositivos de distribución (Sky Pilot Extender), y a estos los equipos terminales de usuario (Sky Pilot Connector); utilizando para ello la red privada

172.20.20.0/24. Para enlazar los dispositivos inalámbricos Sky Pilot se utiliza la red privada 192.168.200.0/24, debido a que se requiere configurar en cada dispositivo Sky Pilot una dirección IP necesaria para su administración y gestión.

1.2.1. SERVICIOS DE RED

Los servicios que provee Conectividad Global Cía. Ltda. están basados en la arquitectura TCP/IP (Transfer Control Protocol / Internet Protocol) implementados principalmente bajo plataforma Linux.

En adelante se expondrá la implementación de servicios sobre plataforma Linux con el fin de recabar la información necesaria para su análisis.

1.2.1.1. Routing

Un router es un dispositivo, el cual tiene múltiples interfaces y que a través de estas es conectado a múltiples redes para redirigir datos entre ellas sin alterarlos. Pueden ser implementados en software (Sistema Operativo) y hardware (equipos dedicados a esta función). Sobre Linux lo único que se debe hacer es habilitar el reenvío IP en el Kernel[2]. Las tablas de enrutamiento se almacenan en la memoria, no en el disco. [2]

En el Data Center se consideran como routers, los equipos con hostname **fw.ree.edu.ec**, **gw.conectividadglobal.net**, **fw.remq.edu.ec**, **fw.ree.com.ec** y **router**. Todos estos mantienen rutas estáticas configuradas de manera manual. Realizan funciones de traslación de direcciones de red, reenvío de información y firewall.

---

[2] **Kernel:** software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.[1]

Estos equipos realizan otro tipo de funciones y proporcionan otros servicios. Debido a esto un router basado en software puede reducir su desempeño.

1.2.1.2. Resolución de Nombres

Debido a la dificultad para recordar las direcciones IP, fue inventado el concepto de "hostname", que son nombres simbólicos que son mapeados[3] a una dirección IP y a través de un proceso llamado "Resolución de Nombres", la dirección IP que pertenece a un hostname puede ser recuperada y viceversa.

En Linux hay dos maneras básicas de almacenar el mapeado.[2]

El primer método es llamado flat network, en el que todos los hosts son palabras únicas. El mapeo de los hostnames y de las direcciones IP son almacenados en un archivo (generalmente llamado /etc/hosts) el cual es distribuido sobre la red manualmente o utilizando un sistema llamado NIS (Network Information System).

El segundo método denominado *Sistema de Nombres de Dominio* es una base de datos global y distribuida. Cada administrador de red mantiene su propia tabla, la cual describe su propia red, y es almacenada sobre su propio servidor. Todas estas tablas son enlazadas a otras usando una estructura jerárquica. Para facilitar las búsquedas, se utilizan ***registros de los recursos*** (RRs) donde cada uno de estos se asocia a un nodo y almacena información de éste. Los diferentes tipos de registros de recursos que sirven para caracterizar a un equipo son A (Address), PTR (Pointer), CNAME (Common Name), HINFO (Host Information), y para los dominios son NS (Name Server), MX (Mail Exchanger), SOA (Start of Authority). Existen servidores Maestro, Esclavo y de Caché. Los Maestros son autoritativos para múltiples dominios, pueden iniciar la transferencia de zonas a los Esclavos y dan servicio a todas las solicitudes de los clientes. Los Esclavos solamente difieren de los anteriores en que recuperan los datos de las llamadas

---

[3] **Mapear**.- Acción que permite que una aplicación pueda acceder a un determinado elemento de manera dinámica.

zonas de transferencia de los servidores maestros. Y los de Caché no son autoritativos y no contienen datos para un dominio, solo realizan consultas iterativas para clientes.

En la Tabla 1.1 se puede apreciar que en el Data Center existen cuatro servidores DNS maestros basados en plataformas Linux, uno para cada red de servicios de la empresa, implementados en los equipos ***fw.ree.edu.ec*** (157.100.135.2/27), ***fw.remq.edu.ec*** (157.100.135.3/27), ***fw.ree.com.ec*** (157.100.135.6/27) y ***gw.conectividadglobal.net*** (157.100.135.30/27), que se hallan entre la red pública del ISP y la red interna de la empresa. Estos servidores están configurados para encargarse directamente de la resolución de nombres del Internet de solicitudes hechas por usuarios internos de la Dirección de Educación del Ilustre Municipio de Quito y de los establecimientos educativos que tengan acceso a los servicios de intranet en el Data Center.

Estos servidores DNS se hallan configurados de una manera incompleta puesto que no se ha establecido los ***registros DNS de búsqueda reversa***[4] para cada uno de los dominios que mantienen en cada servidor. Además se encuentran expuestos directamente al Internet.

Servidor Maestro	Dominio	Registro de Recursos (RR)		
		FQDN	Tipo	Dirección IP
fw.ree.edu.ec	ree.edu.ec	ree.edu.ec.	NS	192.168.2.1
		ree.edu.ec.	A	192.168.2.2
		www.ree.edu.ec.	A	192.168.2.2
		ftp.ree.edu.ec.	A	192.168.2.2
		mail.ree.edu.ec.	A	192.168.2.2
		ree.edu.ec.	A	mail.ree.edu.ec.
	mcerere.ree.edu.ec	mcerere.ree.edu.ec.	A	192.168.2.2
		www.mcerere.ree.edu.ec.	A	192.168.2.2
	ctpfcevallos.ree.edu.ec	ctpfcevallos.ree.edu.ec.	A	192.168.2.2
		www.ctpfcevallos.ree.edu.ec.	A	192.168.2.2
	pensionadoolivo.ree.edu.ec	pensionadoolivo.ree.edu.ec.	A	192.168.2.2
		www.pensionadoolivo.ree.edu.ec.	MX 5	mail.ree.edu.ec.

Tabla 1.1 Registros de los recursos en los servidores DNS

[4] **Registro DNS de búsqueda reversa**: es el registro que permite, mediante un procedimiento determinar el nombre del host, dada la dirección IP.

fw.remq.edu.ec	remq.edu.ec	remq.edu.ec.	NS	192.168.1.1
		remq.edu.ec.	A	192.168.1.1
		www.remq.edu.ec.	A	192.168.1.1
		ftp.remq.edu.ec.	A	192.168.1.1
		video.remq.edu.ec.	A	192.168.1.2
		voip.remq.edu.ec.	A	192.168.1.3
		remq.edu.ec.	MX 5	mail.remq.edu.ec.
		mail.remq.edu.ec.	A	192.168.1.1
	cptquito.org.ec	cptquito.org.ec.	NS	192.168.1.1
		cptquito.org.ec.	A	192.168.1.1
		www.cptquito.org.ec.	A	192.168.1.1
		cptquito.org.ec.	MX 5	mail.cptquito.org.ec.
		mail.cptquito.org.ec.	A	192.168.1.1
fw.ree.com.ec	ree.com.ec	ree.com.ec.	NS	172.20.0.2
		ree.com.ec.	A	172.20.0.4
		www.ree.com.ec.	A	172.20.0.4
		mail.ree.com.ec.	A	172.20.0.4
		ree.com.ec.	MX 10	172.20.0.4
	quitoambiente.com.ec	quitoambiente.com.ec.	NS	172.20.0.2
		quitoambiente.com.ec.	A	172.20.0.4
		www.quitoambiente.com.ec.	A	172.20.0.4
	conectividadglobal.net	conectividadglobal.net.	NS	172.20.0.4
		conectividadglobal.net.	A	172.20.0.4
		www.conectividadglobal.net.	A	172.20.0.4
		mail.conectividadglobal.net.	A	172.20.0.4
		conectividadglobal.net.	MX 5	mail.conectividadglobal.net.
	colegiobrasil.edu.ec	colegiobrasil.edu.ec	NS	172.20.0.2
		colegiobrasil.edu.ec.	MX 10	mail.colegiobrasil.edu.ec.
		colegiobrasil.edu.ec.	A	172.20.0.4
		www.colegiobrasil.edu.ec.	A	172.20.0.4
		mail.colegiobrasil.edu.ec.	A	172.20.0.4
gw.conectividadglobal.net	Todos los dominios antes mencionados	--	--	--

Tabla 1.1 Registros de los recursos en los servidores DNS (continuación)

El servidor ***dc.conectividadglobal.net*** de la red de área local de la empresa implementado con el sistema operativo Windows Server 2003 Enterprise Edition, sirve a los usuarios internos de Conectividad Global. Este servidor tiene configurado de forma básica el servicio de Directorio Activo bajo el dominio conectividadglobal.net, del cual se puede utilizar el servicio DNS y DHCP. Este servidor permite que al momento de añadir un nuevo computador que utilice plataforma Microsoft Windows al dominio, crea los registros de la zona de transferencia y registros de zona inversa para el dominio conectividadglobal.net,

de forma automática. Este servidor debería ser configurado con un subdominio del dominio conectividadglobal.net, para que se mantenga una configuración estándar para los computadores de la red interna de la empresa.

Además, en el servidor **gw.conectividadglobal.net**, se repiten todos los registros de recursos para los dominios que administra la empresa, puesto que la idea es utilizar este servidor DNS exclusivamente para los equipos que accedan a los servicios del Data Center a través de la red inalámbrica Sky Pilot.

Para acceder a los servicios del Data Center a través del Internet se requiere del registro de los recursos de cada dominio, los cuales están alojados en los servidores **every-dns.net** de forma gratuita. Dichos registros apuntan a los firewalls respectivos y estos deben redireccionar los puertos de acuerdo a las solicitudes de los servicios que los clientes realicen.

Se puede concluir, que, existen varios servidores DNS en el Data Center implementados de forma individual, sin considerar ningún tipo de respaldo. Esto es un problema de organización debido a que podría optimizarse el uso de los recursos computacionales, manteniendo todas las zonas de transferencia de los dominios desde un solo servidor Maestro que sea autoritativo para todos los dominios y si se requiere uno o más Esclavos como respaldo.

1.2.1.3. Web

La red mundial de comunicaciones sobre la que se presenta información de manera interactiva y distribuida es conocida como World Wide Web (WWW)[4], la cual basa su funcionamiento en la definición TCP/IP del modelo cliente/servidor[5]. Un servidor Web almacena documentos y hace que éstos estén disponibles para su recuperación por otras computadoras. El software usado para interactuar con el usuario y múltiples solicitudes de documentos almacenados en un servidor Web

---

[5] En el modelo **cliente/servidor**, el cliente es una máquina solicitando un servicio y el servidor es una máquina que provee un servicio.[5]

es llamado navegador de Internet o cliente, el cual es responsable de dar formato y mostrar el contenido de los documentos recuperados.

HTTP (Hyper Text Transfer Protocol) es el protocolo utilizado para la transferencia de información desde el servidor hacia el navegador Web. Cada vez que el servidor entrega información, se crea una conexión, luego de que la transferencia de información es completada, la conexión se cierra.

El servicio Web ofrecido por la empresa se provee utilizando el servidor Apache versión 2.0.52-9, el cual está incluido por defecto sobre las distribuciones estándares de Linux ***Red Hat Enterprise 4 AS***; cabe aclarar que todos los servidores Web se han instalado manteniendo la misma configuración de Apache y utilizando los paquetes de software relacionados a los módulos del servicio Web Apache establecidos en esta distribución de linux, para la publicación de páginas Web de contenido estático con lenguaje HTML y para páginas Web de contenido dinámico utilizando php4. A continuación se describirá el estado actual de este servicio obtenido de las directivas del archivo de configuración de los servidores Web Apache */etc/httpd/conf/httpd.conf* descrito en el Anexo B.

Conexiones: no se permiten conexiones persistentes.

Bitácoras de eventos: solo se registran en la bitácora los errores de nivel de advertencia (warn).

Seguridad en los Directorios: no se tiene establecido un esquema de acceso y privilegios por directorio para los diferentes usuarios y clientes.

Información de estado del servidor: los módulos usados en Apache para proveer información detallada sobre la configuración del servidor y estado de los procesos, no se encuentran asegurados correctamente para permitir sólo a ciertos hosts ver esta información.

Daemons[6] httpd: al momento de iniciar Apache se mantienen cinco procesos de servidor, además se mantienen veinte procesos idles[7] en memoria, se permite cuatro mil solicitudes por proceso hijo antes que éste sea removido del servicio y un máximo de 256 clientes simultáneos conectados.

Este servicio es proporcionado en el Data Center a través de los servidores ***fw.ree.edu.ec***, ***correo.conectividadglobal.net***, ***fw.remq.edu.ec*** y ***web.conectividadglobal.net.*** En la Tabla 1.2 se muestran los sitios Web en los diferentes servidores.

Servidor Web	Sitio Web
fw.ree.edu.ec	www.ree.edu.ec
fw.remq.edu.ec	www.remq.edu.ec
	www.cptquito.org.ec
correo.conectividadglobal.net	www.conectividadglobal.net
web.conectividadglobal.net	www.quitoambiente.com.ec
	www.colegiobrasil.edu.ec
	www.pensionadoolivo.ree.edu.ec
	www.cptfcevallos.ree.edu.ec
	www.ree.com.ec
	www.mheidegger.edu.ec
	www.sb.remq.edu.ec
	www.ajsucre.remq.edu.ec
	www.fm.remq.edu.ec
	www.cemepp_apguerrero.remq.edu.ec
	www.ue_jmoreno.remq.edu.ec
	www.espejo.remq.edu.ec
	www.cemepp_9octubre.remq.edu.ec
	www.cemepp_zambiza.remq.edu.ec
	www.cemei_uyjusticia.remq.edu.ec
	www.ueN8.remq.edu.ec
	www.cemepp_vaaguirre.remq.edu.ec
	www.cemei_sroque.remq.edu.ec
	www.ueN7.remq.edu.ec
	www.cemei_sclara.remq.edu.ec
	www.ueN6.remq.edu.ec

Tabla 1.2 Sitios Web

[6] **Daemon:** Proceso que corre en segundo plano y controla un recurso del sistema o algún servicio de red. Inicia cuando el sistema arranca y deja de ejecutarse cuando se detiene. Se lo conoce también como demonio.

[7] **Idle**: Inactivo, fuera de uso.

	www.cemepp_ralvarado.remq.edu.ec
	www.cemei_magdalena.remq.edu.ec
	www.ueN5.remq.edu.ec
	www.cemepp_pptraversari.remq.edu.ec
	www.cemei_ipiales.remq.edu.ec
	www.ueN4.remq.edu.ec
	www.cemepp_mcdvaca.remq.edu.ec
	www.cemei_iburneo.remq.edu.ec
	www.ueN3.remq.edu.ec
	www.cemepp_itpymino.remq.edu.ec
	www.cemei_emunicipales.remq.edu.ec
	www.ueN2.remq.edu.ec
	www.cemepp_impenaherrera.remq.edu.ec
	www.ueN11.remq.edu.ec
	www.cemepp_hmmartinez.remq.edu.ec
	www.cemei_colibri.remq.edu.ec
	www.ueN10.remq.edu.ec
	www.cemepp_dwisneth.remq.edu.ec
	www.cemei_cdluz.remq.edu.ec
	www.ueN1.remq.edu.ec
	www.cemepp_dirussel.remq.edu.ec
	www.cemei_carolina.remq.edu.ec
	www.sfquito.remq.edu.ec
	www.cemepp_csespinoza.remq.edu.ec
	www.cemei_carapungo.remq.edu.ec
	www.cemepp_cotocollao.remq.edu.ec
	www.cemei_andalucia.remq.edu.ec
	www.quitumbe.remq.edu.ec
	www.cemepp_calderon.remq.edu.ec
	www.cemei_acalderon.remq.edu.ec
	www.olombeyda.remq.edu.ec
	www.cemepp_bellavista.remq.edu.ec
	www.cemepp_rchiriboga.remq.edu.ec

Tabla 1.2 Sitios Web (continuación)

Todos los sitios Web en la empresa han sido desarrollados utilizando HTML y/o a través de un WCMS (Web Content Management System) denominado Joomla, el cual se deriva de Mambo. Joomla es un administrador de contenidos Web el cual funciona bajo LAMP (Linux, Apache, MySQL y PHP), es decir tiene contenido dinámico con soporte de base de datos en Internet y que permite además administración de usuarios, puesto que se puede asignar una cuenta de usuario y una contraseña para que cada cliente pueda manipular la información en su sitio Web.

Estos servidores utilizan la capacidad de Virtual Hosting[8] que provee el servidor Web Apache, basado en IP o basado en nombres. Los servidores Web del Data Center están configurados con virtual hosts basados en Nombres, razón por la cual los Web browsers requieren soportar al menos http versión 1.1. La capacidad de espacio en disco para cada sitio no está determinada. No existe redundancia del servicio, lo que implica problemas de disponibilidad.

1.2.1.4. Correo Electrónico

El servicio de correo electrónico [2] permite intercambiar mensajes entre usuarios de un sistema (servidor) o de sistemas diferentes. El modelo básico ***Internet e-mail*** mostrado en la Figura 1.2 basa su funcionamiento en la utilización de dos agentes denominados "Agente de Usuario" (***UA***) y "Agente de Transferencia de Mensajes" (***MTA***).

Cuando un usuario requiere enviar correo electrónico, usa un programa computacional conocido como UA para componer un mensaje e iniciar la transferencia para su destino. Los ejemplos de agentes de usuario populares en UNIX son el comando básico *mail*, así como también programas más poderosos, como *mails, elm y pine*. También pueden ser usadas herramientas más avanzadas como *Netscape Mail o Eudora* y para plataformas Windows se pueden usar Microsoft Outlook, Windows Live Mail.

Una vez que el usuario ha compuesto el mensaje de correo, su UA lo pasa a un MTA de origen para llevar a cabo la transmisión; esto lo hace utilizando el protocolo SMTP (Simple Mail Transfer Protocol). Luego este MTA transmitirá también el mensaje, estableciendo una conexión TCP con el MTA de destino en los recipientes del sistema. Los MTAs normalmente escuchan las solicitudes en el puerto 25. Una vez que el MTA de destino ha recibido el mensaje, se lo entrega al

---

[8] **Virtual Hosting**.- Es la capacidad de alojar múltiples y separados sitios Web sobre un solo equipo, con diferentes DocumentRoot, logs, permisos, etc.[4]

UA de destino, el cual recibe el mensaje a través de los protocolos POP3 (Post Office Protocol) o IMAP (Internet Message Access Protocol).

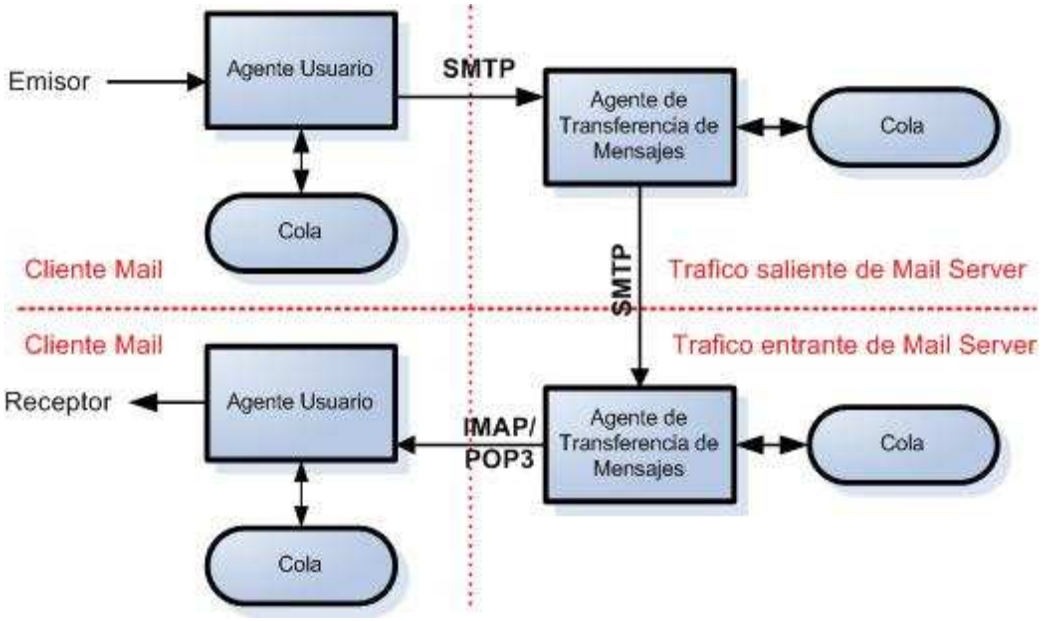


Figura 1.2 Diagrama del Modelo Internet e-mail

El servicio de correo electrónico se provee a través de tres servidores **correo.conectividadglobal.net**, **fw.remq.edu.ec** y **correo.ree.edu.ec**. El primero soporta el servicio para los dominios: conectividadglobal.net, mcerere.ree.edu.ec, colegiobrasil.edu.ec y ree.com.ec; el segundo mantiene el servicio para los dominios: remq.edu.ec y cptquito.org.ec; y el último proporciona el servicio al dominio ree.edu.ec. En la Tabla 1.3 se detalla el número de usuarios por dominio que mantienen actualmente los servidores.

Equipo	Dominio	Número de Usuarios
correo.conectividadglobal.net	conectividadglobal.net	19
	mcerere.ree.edu.ec	58
	colegiobrasil.edu.ec	17
	ree.com.ec	225

Tabla 1.3 Número de cuentas de usuario del servicio de Correo Electrónico

fw.remq.edu.ec	remq.edu.ec	1244
	cptquito.org.ec	13
correo.ree.edu.ec	ree.edu.ec	15

Tabla 1.3 Número de cuentas de usuario del servicio de Correo Electrónico (continuación)

El servidor correo.conectividadglobal.net se encuentra en la red privada 172.20.0.0/24 tras un firewall que recepta las solicitudes externas (desde Internet) y las reenvía.

El servidor fw.remq.edu.ec se encuentra expuesto directamente a una interfaz ethernet configurada con una IP pública. Realiza también funciones de firewall y DNS local, la interfaz ethernet interna se encuentra configurada en la red 192.168.1.0/24.

Los dos servidores usan software propietario para la provisión del servicio, el cual utiliza un MTA denominado ***KerioMailServer*** versión 6.2.1.[19] Proporciona también la administración completa del servidor de correo de manera gráfica, es decir dominios, cuentas de usuario, cuotas de disco, filtros antispam, antivirus, etc. a través de la aplicación ***KerioAdministrationConsole.*** Además incluye una aplicación para administración de cada dominio vía web identificada con usuario "admin" y autenticada mediante contraseña, denominada ***KerioWebAdmin***. ***KerioWebMail*** proporciona el acceso de los usuarios a sus cuentas de correo.

La configuración para la entrega SMTP se lo hace de forma directa (sin uso de mail relay) utilizando los registros MX. En caso de que el MTA origen no pueda entregar el mensaje al MTA destino, por configuración se reenvía el mensaje cada 30 minutos; y si después de 5 días no se entrega el mensaje, éste es reenviado al emisor.

El servicio de correo electrónico para el dominio ree.edu.ec está implementado bajo el software Comercial ***Communigate Pro Communication Server*** versión

5.1-10 sobre plataforma Linux, el mismo que se encuentra aún en fase de pruebas.

Ninguno de los servidores de correo utilizan algún tipo de respaldo para mantener disponibilidad en caso de fallas. No existe servidores mail relay que permitan la protección de ataques, malware, spam, etc. a las cuentas de correo de los usuarios.

1.2.1.5. Dynamic Host Configuration Protocol, DHCP

Cada host en una red, para acceder a los servicios que proporciona necesita ser configurado al menos con ciertos parámetros como su dirección IP, la máscara de subred, la dirección IP del gateway por defecto y la dirección del servidor DNS. Para esto existen dos formas de proveer estos parámetros a los hosts.

La configuración manual en cada uno de los equipos se denominada ***estática*** y es recomendada en los servidores, mientras, la asignada a través de un servidor se denomina ***dinámica*** y es usada para los usuarios de la red.

La configuración dinámica se lo hace a través del protocolo “Dynamic Host Configuration Protocol” (***DHCP***). [2]

Linux puede funcionar como cliente, relay o servidor DHCP. Para el cliente el demonio integrado por defecto en las distribuciones actuales es ***dhclient*** y su configuración se almacena en /var/lib/dhcp. El relay se lo puede configurar sobre un router en hardware o en software si fuese necesario. El servidor utiliza el demonio ***dhcpd*** y se configura en /etc/dhcpd.conf.

En la red de Conectividad Global Cía. Ltda., los equipos servidores y de usuarios están configurados de manera estática de acuerdo a la red a la que pertenecen. Existe un servidor DHCP con hostname **dc.conectividadglobal.net** el cual se lo utiliza para proveer dirección IP inicial necesaria para cargar el sistema operativo en los equipos “Thin Client” que comercializa la empresa.

1.2.1.6. File Transfer Protocol, FTP

Es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente se pueda conectar a un servidor para descargar archivos desde él o para enviar archivos independientemente del sistema operativo utilizado en cada equipo. Ofrece máxima velocidad en la conexión, pero sin seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado.

La figura 1.3 muestra que el ***intérprete de protocolo*** (PI) de usuario (cliente), inicia la conexión de control en el puerto 21. El PI del servidor responde al PI de usuario por la conexión de control. El ***proceso de transferencia de datos*** (DTP) de usuario, debe esperar a que el servidor inicie la conexión al puerto de datos especificado (puerto 20 en modo activo) y transferir los datos en función de los parámetros que se hayan especificado.

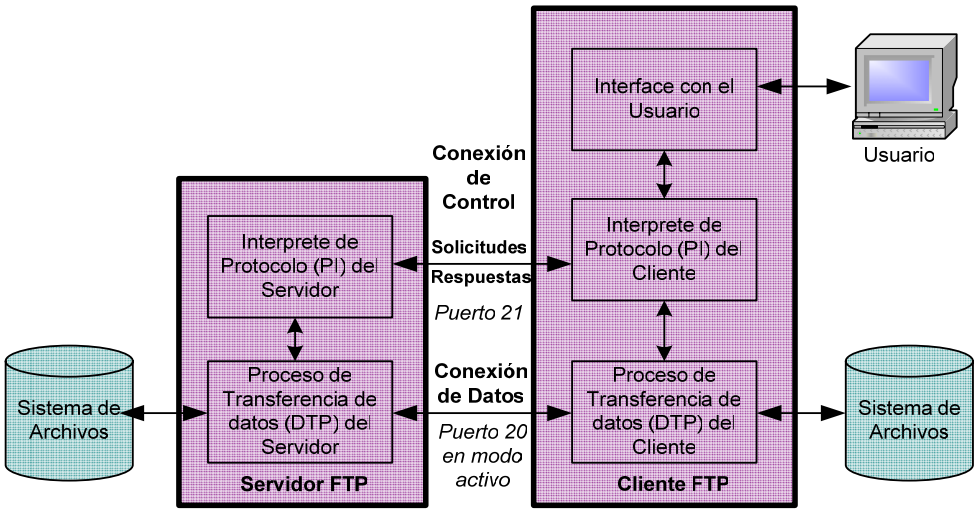


Figura 1.3 Diagrama del modelo del servicio FTP

Modo activo.- En el servicio ftp en modo activo (normal) se establecen dos conexiones distintas. En primer lugar se establece una conexión para la transmisión de comandos (puerto cliente mayor a 1024 hacia el puerto 21 del

servidor) y por esa misma conexión se indica al servidor cuál es el puerto (distinto) del cliente que está esperando los datos. Las conexiones son abiertas por el que envía los datos (el servidor si se trata de bajar archivos a la PC, o el cliente si se trata de subir archivos al servidor). La Figura 1.4 indica el esquema de funcionamiento.[20]

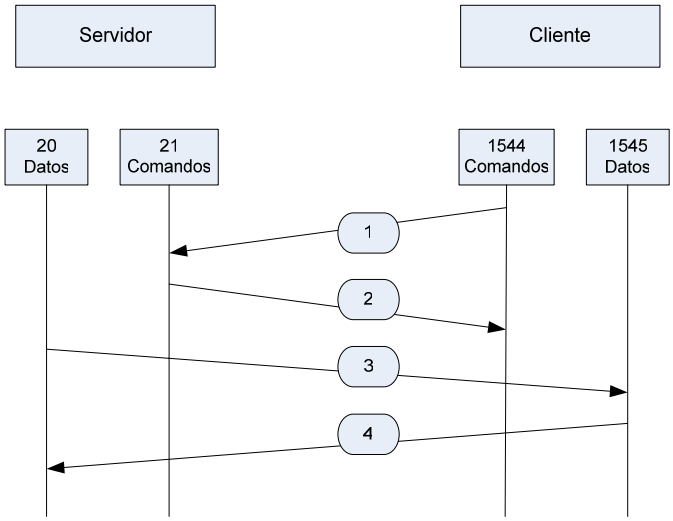


Figura 1.4 Diagrama del servicio FTP en modo activo

Modo pasivo.- En modo pasivo [20] el programa cliente siempre inicia la conexión con el servidor. Al abrir una conexión ftp el cliente abre dos puertos aleatoriamente (N>1023 y N+1). Se abre primero una conexión de control (puerto N del cliente al puerto 21 del servidor), el cliente pide un puerto aleatorio abierto al servidor (P>1023). Recibida la contestación, será el cliente el que establezca la conexión de datos al servidor a través de ese puerto P. Esto resuelve el problema del filtrado de los firewalls a la conexión entrante del puerto de datos al cliente desde el servidor. En la Figura 1.5 se indica el funcionamiento de este modo.

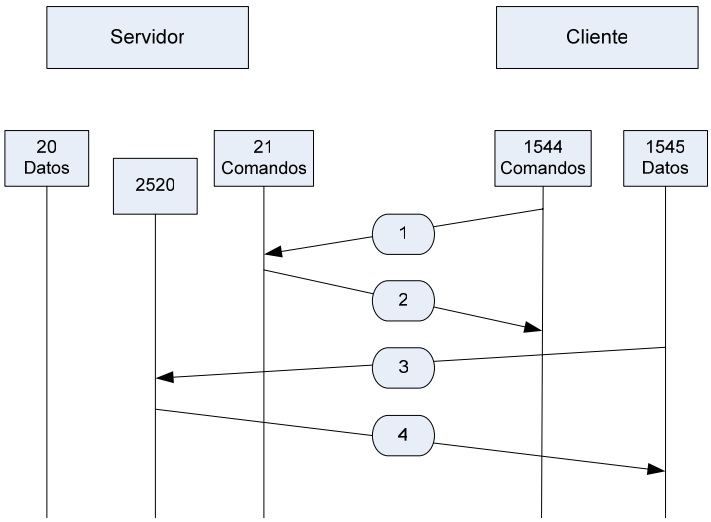


Figura 1.5 Diagrama del servicio FTP en modo pasivo

Conectividad Global Cía. Ltda. provee este servicio en modo activo en los servidores **fw.remq.edu.ec**, **fw.ree.edu.ec**, **correo.conectividadglobal.net**, **web.conectividadglobal.net** en los puertos 20-21. Es utilizado por el personal de diseño de cada institución para modificar o actualizar sus sitios Web cuando no utilizan Joomla.

Existe el problema de usar este servicio desde Internet en los servidores Web que no disponen de una IP pública, debido principalmente a que el firewall ***firestarter*** de filtrado de paquetes instalado en los equipos que forman parte de la red de acceso a Internet no considera los módulos de iptables llamados ip_conntrack_ftp e ip_nat_ftp que deberían ser cargados al momento de arrancar el sistema o al momento de iniciar el servicio iptables. Estos módulos son necesarios para el servicio FTP y permitirán un NAT reverso tan pronto como el comando PORT sea enviado en una conexión de control FTP.

El servidor **files.conectividadglobal.net** por medio de transacciones ftp pone a disposición archivos e instaladores necesarios para sus clientes y/o para el departamento técnico al momento de configurar equipos en sus visitas a las instituciones.

1.2.1.7. Network File System, NFS

Network File System (NFS)[2], es un protocolo de nivel de aplicación, según el modelo de referencia de ISO/OSI[9]. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratase de locales en un ambiente heterogéneo de máquinas, sistemas operativos y redes. Utiliza UDP como protocolo de transporte. Aunque NFS puede funcionar sobre cualquier red TCP/IP se requiere la velocidad de una red de área local para obtener un buen desempeño.

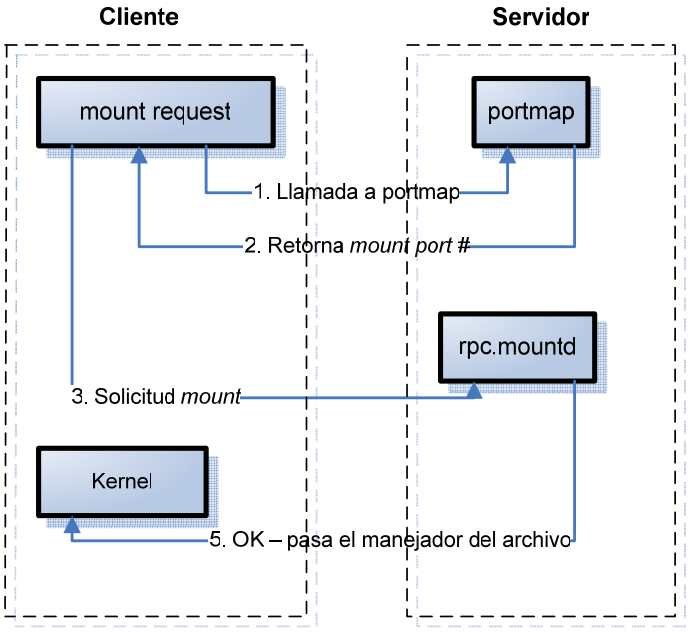


Figura 1.6 Procedimiento de montaje de un sistema de ficheros

Está incluido por defecto en los Sistemas Operativos UNIX y en las distribuciones Linux. El servidor abre dinámicamente un puerto menor al 1024 y lo registra con el portmapper, el cual corre sobre el puerto 111 y es habilitado para enviar el número de puerto usado por el demonio NFS a los clientes. Este procedimiento se muestra en la Figura 1.6.

---

[9] **ISO/OSI** (International Organization for Standardization / Open System Interconnection): modelo de referencia de interconexión de sistemas abiertos emitido por la organización internacilonal para la estandarización.[25]

Linux usa una estructura llamada ***sistema de archivos virtual*** (VFS) para definir un mecanismo independiente en hardware para direccionar diferentes tipos de sistemas de archivo. Está incorporado dentro del kernel de tal manera que las aplicaciones que usan llamadas al sistema como abrir, cerrar, leer y escribir para acceder a los archivos, no necesiten ser modificadas.

En el Data Center el servicio NFS es utilizado en: instalaciones avanzadas remotas en la red interna, de sistemas operativos Fedora Core 3, Red Hat Linux Enterprise EL 4 y OpenSuse 10.2; para compartir CD-ROMs e instaladores necesarios en los servidores. El servicio se encuentra en **files.conectividadglobal.net**.

1.2.1.8. Lightweight Directory Access Protocol, LDAP

El servicio de directorio usa un objeto como única entrada. Un objeto consta de un número de atributos, como el nombre, la dirección o el número de teléfono.

Existen un gran número de implementaciones LDAP[2]: *OpenLDAP*, *IBM SecuryWay Directory, iPlanet Directory Server* (Netscape), *Lotus Domino*, *Novell Directory Services* y *Microsoft Active Directory*.

En el Data Center de Conectividad Global Cía. Ltda., se utiliza Active Directory para permitir el acceso del personal a sus estaciones de trabajo, brindar niveles de autorización en la red, compartir recursos y mantener las mismas configuraciones en los equipos Windows de la empresa. Estas funciones son realizadas desde el servidor **dc.conectividadglobal.net**. Este servicio es subutilizado debido a que no provee niveles de acceso a nivel de hardware, es decir no bloquea acceso a dispositivos de almacenamiento, uso de recursos, etc.

1.2.1.9. Internet

Existen muchas maneras de proveer el servicio de Internet en una red. Entre los principales mecanismos utilizados se encuentran los servidores Proxy y los ruteadores trabajando como gateways.

El protocolo Proxy es un servicio que recibe las conexiones de clientes y las reenvía a otros servidores. El cliente puede solicitar a través de un Proxy algún servicio como un archivo, una conexión, una página Web u otro recurso disponible en otro servidor. Provee el recurso al conectarse al servidor especificado y solicita el servicio en nombre del cliente. Un Proxy opcionalmente puede alterar la solicitud de respuesta del servidor, a veces puede servir la solicitud sin contactar al servidor especificado. En este caso, almacenaría en caché la primera solicitud al servidor remoto, así mantendría la información para futuras solicitudes.

De acuerdo a las funciones los servidores Proxy pueden ser: Servidor Proxy caching, Web Proxy, Web Proxy con filtrado de contenido, Proxy hostil, Proxy Transparente, Proxy Reverso, Aceleración de Encriptación SSL, Balaceo de carga, Circumventor, etc.

Para segmentar y distribuir el ancho de banda en una red se pueden utilizar algunos programas que permiten indicar cómo debe ser el uso del canal y a quién permitirlo. CBQ (Class-Based Queueing) y HTB [22](Hierarchical Token Bucket) ayudan a controlar el uso del ancho de banda de salida a un determinado vínculo y permiten utilizar un enlace físico para simular varios enlaces más lentos para enviar distintos tipos de tráfico sobre diferentes enlaces simulados. En ambos casos, se tiene que especificar cómo dividir el enlace físico dentro de enlaces simulados y como decidir el enlace simulado para un determinado paquete a ser enviado.

HTB asegura que el importe del servicio prestado a cada clase es de al menos el mínimo monto que solicita y el monto que se le ha asignado. Cuando una clase solicita menos que la cantidad asignada, el resto (exceso) de ancho de banda se distribuye a otras clases las cuales solicitan servicio.

En el Data Center no se utiliza Proxy para permitir el acceso a Internet a los empleados, tampoco hay un esquema de asignación de ancho de banda por IP o por red.

1.2.1.10. Video Conferencia

La videoconferencia es un conjunto de tecnologías de telecomunicación interactiva que permiten la comunicación simultánea bidireccional de dos o más lugares de forma que interactúen a través de video y audio.[23] Adicionalmente, existe ***presencia*** donde pueden ofrecerse facilidades telemáticas o de otro tipo como el intercambio de informaciones gráficas, imágenes fijas, transmisión de ficheros desde el PC, escritorio compartido, etc.

El núcleo tecnológico usado en un sistema de videoconferencia es la compresión digital de los flujos de audio y video en tiempo real. El hardware o software que realiza esta compresión es conocido como **codec** (codificador-decodificador).

En el Data Center el servicio de Video Conferencia se brinda a través de un servidor dedicado a este propósito con hostname **MUNICIPIO**, el cual utiliza una herramienta sobre plataforma Windows denominada e/pop. Permite utilizar codecs para compresión de video como H263, H263+ y MPEG4.[24] Es importante recalcar que las prestaciones de este software van más allá de una simple video conferencia, sino que también cuenta con elementos que permiten interacción de aplicaciones, lo que se denomina presencia. Gracias a la administración Web que presenta esta herramienta, es fácil para el administrador poder planificar sesiones de video conferencias remotamente, además realizar invitaciones vía e-mail, controlar el audio, la cancelación de eco, permisos, ancho de banda para cada sesión y configurar si se desea la comunicación en una o en dos vías.

1.2.2. APLICACIONES

Las aplicaciones que Conectividad Global Cía. Ltda., ofrece a sus clientes han sido elaboradas por el ***Área de Desarrollo de Sistemas*** bajo plataformas Windows. Mediante herramientas de desarrollo como Microsoft Visual .Net 2003 y 2005, haciendo uso del lenguaje de programación C# conjuntamente con el motor de base de datos SQL Server 2005 y además Internet Information Server se han desarrollado herramientas que aportan al continuo crecimiento de la interrelación entre la educación y la tecnología.

Por otro lado, bajo programación en php-mysql se han creado herramientas que ayudan al crecimiento operativo de una empresa. Dentro del área de Desarrollo de Sistemas se encuentra un grupo dedicado a modificar software ***open source*** con el fin de personalizar aplicaciones que han sido reconocidas por su eficacia en las labores destinadas.

Bajo el aval de la Red Educativa Ecuatoriana, que agrupa a las aplicaciones del Sistema de Gestión Académica, Sistema de Gestión Académica FLASH y a la Red Educativa Virtual desarrolladas por la empresa que son entregadas sin costo a las instituciones educativas, permiten a los padres de familia mantenerse informados de los progresos, logros y falencias de sus hijos, puesto que los padres de familia podrían tener acceso a toda la información referente a las obligaciones, anotaciones y calificaciones de los estudiantes mediante una publicación personalizada vía Web a través del Internet que permiten este conjunto de aplicaciones.

1.2.2.1. Sistema de Gestión Académica (SGA)

Este sistema es el de mayor difusión entre los clientes de la comunidad de instituciones educativas debido a que poco a poco ha ido concentrando mayores beneficios para los profesores, estudiantes y padres de familia.

Este sistema permite automatizar los procesos del centro educativo que generan la información relevante para el establecimiento como: matriculación,

calificaciones, asistencias, recorridos de buses, promociones, reportes a la Dirección Provincial. Este aplicativo va a residir en la institución educativa.

Los profesores pueden cargar información en el sistema desde cualquier computador con acceso a la red institucional. Disponen de una agenda personal, pueden programar tareas, definir periodos de clase, configurar el número de evaluaciones por periodo, cambiar los porcentajes de peso en los aportes, entre otros. Los estudiantes pueden conocer sus calificaciones realizando consultas en una interfaz Web desarrollada para ellos.

Esta herramienta se encuentra instalada en cada una de las instituciones educativas que pertenecen al proyecto QuitoEduca.Net y en algunas instituciones privadas, en un servidor planificado para albergar esta aplicación.

Los requerimientos de hardware y software para la instalación de esta aplicación fueron elaboradas por el área de Desarrollo de Software y son los siguientes:

Requerimientos Hardware:

Mínimo

- 1 procesador Intel Pentium III de 800 Mhz.
- 128 MB de Memoria RAM.
- 1 disco duro de 10GB.
- 1 unidad de respaldo (medio magnético y/o quemador de CD).

Recomendado

- 1 procesadores Intel Pentium IV de 2 Ghz o superior.
- 1024 MB de Memoria RAM.
- 1 disco duro SCSI de 4GB (para el sistema operativo y programas).
- 1 disco duro SCSI de 9GB (para la base de datos).
- 1 unidad de respaldo (medio magnético y/o quemador de CD).

Requerimientos Software:

- Sistema Operativo: Microsoft Windows XP Professional con Internet Information Services (IIS).
- Base de Datos: Microsoft SQL Server 2000 Desktop Engine (MSDE 2000 en ingles) con Service Pack 3.
- NET Framework 1.1
- Internet Explorer 6.0

En el Data Center se encuentran el servidor de desarrollo que utiliza el software Microsoft Visual Source Safe[10] denominado **rev.conectividadglobal.net** para controlar el desarrollo del código fuente de las aplicaciones de la empresa, además con el software .Net Obfuscator instalado sobre el servidor **testserver.conectividadglobal.net** se genera el archivo instalador de este software informático denominada REESetup.msi.

1.2.2.2. Sistema de Gestión Académica FLASH (SGAF)

Es un programa portátil, el cual es distribuido entre los profesores, que tiene como finalidad brindar soporte al trabajo de los profesores en su hogar u oficina fuera de la institución debido al tiempo del que pueden disponer.

Permite optimizar el tiempo para ingresar información al sistema. Presenta una interfaz similar a la del SGA pero no necesita conexión a una base de datos. El profesor puede trabajar desde cualquier computador no conectado a la red y guardar la información en un dispositivo de almacenamiento USB. Al tener acceso a un computador en la red institucional simplemente en una de las opciones del SGA importa los datos desde la unidad USB hacia el servidor SGA a través de archivos .xml que genera la aplicación.

1.2.2.3. Red Educativa Virtual (REV)

Debido a la demanda de los padres de familia en llevar un registro del avance de sus hijos, Conectividad Global Cía. Ltda. desarrolló una herramienta capaz de proveer disponibilidad de la información de las obligaciones, tareas, calificaciones y estado de sus hijos en la institución, en cualquier momento y desde cualquier lugar con acceso a Internet, a través de la infraestructura tecnológica de la empresa y de su red de acceso, los servidores **rev.conectividadglobal.net** y

---

[10] **Microsoft Visual Source Safe:** Sistema de control de versiones en el nivel de archivos, que permite trabajar en distintas versiones de un proyecto al mismo tiempo

sga.conectividadglobal.net que se encuentra en el Data Center, se mantienen en espera de solicitudes Web desde Internet. Cuando llega una solicitud los servidores presentan al usuario la página Web personalizada de autenticación de la Institución Educativa desde el correspondiente servidor. Al momento de ingresar los datos username/password, el servidor envía una solicitud de consulta del username/password mediante lenguaje SQL al servidor SGA de la institución educativa correspondiente, por la red de Acceso Sky Pilot para la autenticación del usuario y la asignación de la respectiva autorización sobre el manejo de la información. Los servidores se convierten en un intermediario de consultas SQL para el usuario que realiza consultas desde Internet.

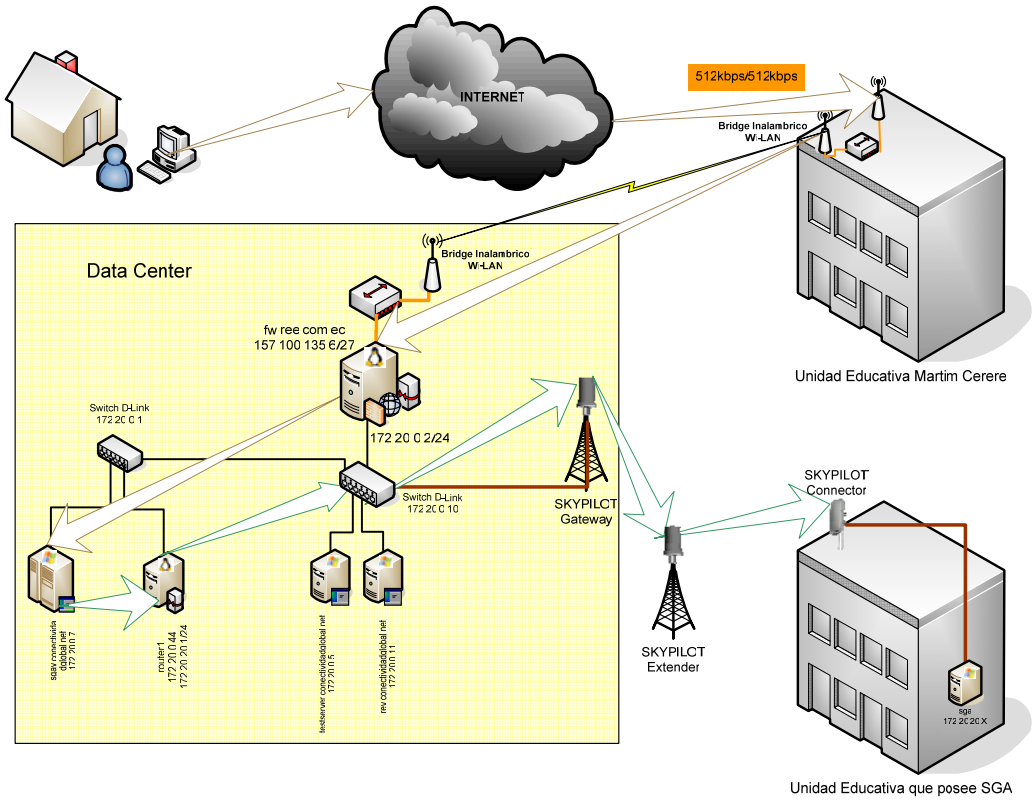


Figura 1.7 Ejemplo de flujo de información asociada a la interacción entre aplicaciones REV y SGA

La Figura 1.7 indica el flujo actual de la información durante las consultas desarrolladas a los servidores SGA. La información necesariamente tiene que

pasar por los servidores del Data Center por lo que se vuelve esencial proveer seguridad durante la ruta de transmisión de la información.

1.2.2.4. Sistema de Seguimiento de Proyectos

El constante crecimiento en las empresas hace imposible manejar proyectos grandes sin una herramienta de administración de proyectos que nos diga con certeza cuál es el avance de cada una de las tareas y el rendimiento de cada uno de sus componentes, los logros y cumplimiento de metas y objetivos, que además nos permita asignar recursos, cambiar tiempos y administrar los proyectos desde cualquier computador conectado al Internet.

Debido a esta demanda se ha utilizado una herramienta prototipo basada en php-mysql la cual permite a una organización el control del desarrollo de proyectos. Su nombre es preliminar debido a que fue desarrollado para un área específica de trabajo del Ilustre Municipio de Distrito Metropolitano de Quito.

Esta herramienta de administración de proyectos se encuentra instalada en el servidor **web.conectividadglobal.net**.

1.2.2.5. Sistema de Educación en Línea

Para proveer este servicio se utiliza la herramienta Moodle, que es un paquete de software open source útil para la administración de cursos y sitios Web de contenido dinámico Web php-mysql, para la enseñanza en las instituciones educativas.

Este paquete, Moodle, para la administración de cursos se encuentra instalada en el servidor **correo.remq.edu.ec** y ha sido incluido en un link del sitio Web www.remq.edu.ec.

1.2.3. INFRAESTRUCTURA DE RED

La infraestructura de una red se refiere a la topología física con sus elementos de hardware, el sistema de cableado estructurado y los dispositivos de conectividad como los routers, switches, servidores, estaciones de trabajo, y la infraestructura lógica, comprende a los protocolos que se vayan a utilizar sobre la infraestructura física.

La red del Data Center de Conectividad Global Cía. Ltda., utiliza a Ethernet como protocolo de capa de enlace de datos con lo cual los dispositivos de conectividad como switches, routers, tarjetas de red de las estaciones de trabajo y de los servidores se comunican. El cableado estructurado comprende segmentos de cable UTP categoría 5e utilizando la norma ANSI/EIA/TIA-568-B, la cual implementa la capa física para Ethernet.

La red de área metropolitana utiliza a equipos Sky Pilot, los mismos que usan su propio protocolo propietario basado en el estándar IEEE 802.11 modificado para redes malladas.

La red de acceso a Internet consta de una infraestructura física basada en bridges inalámbricos punto-punto y utiliza el estándar de comunicaciones IEEE 802.11g.

1.2.3.1. Dispositivos de Conectividad

Los equipos de conectividad son todos aquellos dispositivos que permiten la transferencia de información a nivel de capa 2 y 3 de acuerdo al modelo de referencia ISO/OSI. En la tabla 1.4 se listan todos los elementos que permiten conectividad entre las diferentes ubicaciones físicas de la red.

Función	Modelo/hostname	Interfaces		Ubicación	Enlace	Cantidad
		usadas	totales			
Router con filtrado de paquetes	PC Linux fw.ree.edu.ec	2	2	Data Center	WAN	1
Router con filtrado de paquetes	Server Linux fw.remq.edu.ec	2	2	Data Center	WAN	1
Router con filtrado de paquetes	Server Linux fw.ree.com.ec	2	2	Data Center	WAN	1
Router con filtrado de paquetes	PC Linux gw.conectividadglobal.net	2	2	Data Center	WAN	1
Router	PC Linux router	3	3	Data Center	LAN	1
Router	PC Linux router1	1	1	Data Center	LAN	1
Switch	CNet Port Switch 8	2	8	Martim Cereré	WAN	1
Switch	CNet CNSH 1600	5	16	Data Center	WAN	1
Switch	CNet CSH 1600	3	16	Data Center	LAN	1
Switch	DLink DES1005D	4	8	Data Center	LAN	1
Switch	DLink DES-3326SR	8	16	Data Center	LAN	1
Switch	DLink DES-3326	9	16	Data Center	LAN	1
Switch	AOpen AOW-616	12	16	Data Center	LAN	1
Switch	Advantek ANS-08P	0	8	Data Center	-	1
Switch	DLink DES 1024D	0	16	Data Center	-	1
Switch	CNet Port Switch 8	0	8	Data Center	-	1
Switch	CNet Port Switch 8	0	8	Data Center	-	1
Bridge	Wi-LAN AWE120-58 Tipo RD	2	2	Martim Cereré / Data Center	MAN	2
Gateway	Sky Pilot Gateway	2	2	Data Center	MAN	2
Extender	Sky Pilot Extender	2	2	Puntos de Acceso	MAN	3
Connector	Sky Pilot Connector	2	2	Usuario / Institución	MAN	10

Tabla 1.4 Equipos de Conectividad en la Red

Para obtener las características de los routers, debido a que están basados en Linux se utilizó el software libre lshw-2.09-1.fc3.rf.i386.rpm[11], el cual lista la información necesaria para identificar los componentes de hardware de un equipo con sistema operativo Linux y kernel superior a versión 2.4. Mientras que para el resto de equipos se obtuvo la documentación respectiva del fabricante.

Los dispositivos que actúan como router e interconectan las diferentes redes y enlaces a Internet en su mayoría no trabajan con calidad o diferenciación de servicio, requieren la función de NAT (Traducción de Dirección de red), y no son hardware determinado para esa labor, sino una PC (Computadora Personal) o servidor configurados para este efecto, sobre los cuales se halla instalado Red Hat Linux Enterprise 4 AS. De las características obtenidas de estos dispositivos se puede apreciar que algunos de ellos se han implementado sin consideraciones de planeamiento de capacidad puesto que se han mantenido activos servicios y aplicaciones innecesarias que el sistema instala por defecto y son iniciados desde el momento de arranque del equipo, desperdiciando recursos de hardware. El kernel no ha sido recompilado para desactivar módulos innecesarios y optimizarlo para procesamiento. Algunos de los equipos que realizan funciones de enrutamiento no cuentan con la suficiente capacidad de procesamiento para mantener un nivel aceptable de rendimiento. Se debe considerar que los enrutadores en software dedicados específicamente a esta función requieren un disco duro de baja capacidad, lo cual no se presenta en estos equipos, originando pérdida de recursos al utilizar discos duros de elevada capacidad. La información de enrutamiento y/o de traducción de direcciones de red se almacena en memoria RAM (Memoria de Acceso Aleatorio).

Los dispositivos que realizan funciones de bridge en la red inalámbrica (Tabla 1.5) y sirven para el acceso a Internet son equipos marca WiLan que a pesar de soportar y poseer características importantes no se encuentran configurados correctamente, dejando a un lado parámetros que brinden mejor señal, priorización de tráfico, seguridad, etc.

---

[11] **lshw-2.09-1.fc3.rf.i386.rpm**: Paquete de nombre lshw (list hardware), con extensión rpm (RPM Package Manager)

	Throughput	Alcance	Modulación	Rango de Frecuencia
WiLan AWE 120-58 RD	12 Mbps	25 km	MC-DSSS (Multi-Code Direct Sequence Spread Spectrum)	5.725 – 5.85 MHz

Tabla 1.5 Características Principales de Equipos Bridges Inalámbricos

La arquitectura actual de red combina dispositivos capa dos de baja y alta capacidad (Tabla 1.6). Uno de los principales problemas en el esquema actual es el acceso a Internet, el cual se lo hace a través de un equipo de bajo rendimiento. Algunos de los servicios ofrecidos por los diferentes servidores, en algunos casos necesitan configuración adicional en los equipos que se encuentran en el trayecto de la transmisión de la información, pero estos parámetros no se encuentran configurados en equipo alguno.

La red de acceso inalámbrica está formada por dispositivos que proveen una arquitectura propietaria denominada SyncMesh™, la cual consta de un sistema de conmutación dinámica de un arreglo de ocho antenas directivas (**Dynamic Directional Antenna Switching**) de alta ganancia (18dBi), cada una de ellas cubre 45º con lo cual estos dispositivos pueden cubrir 360º; y de conmutación Sincrónica (**Synchronous Switching**) propietaria de Sky Pilot.

Todos los dispositivos Sky Pilot utilizan el protocolo TDD (Time-division duplex) como protocolo de acceso al medio y es implementado mediante un chip GPS que tienen instalado para proveer un reloj común de sincronización y así permitir transmisiones planificadas entre dispositivos de la red mallada. Toda la arquitectura inalámbrica trabaja a nivel de capa 2 del modelo OSI en la banda de 5 GHz, con modulación OFDM adaptiva permitiendo un alcance de hasta 16Km. Tienen un throughput de hasta 20Mbps para tráfico UDP y de 12 Mbps para tráfico TCP.[26]

Tabla 1.6 Características Principales de los Switches en el Data Center

	capa modelo OSI	# puertos	modo (half-full) / velocidad (10-100 Base T)	Puerto GBIC Gigabit Ethernet	buffer memoria	store and forward	velocidad de conmutación (paquetes/segundo por puerto)		port trunk	vlan	802.1d	802.1p	802.3ad	ACLs	admin. Web SNMP Telnet	QoS	Router	rack
							10 Mbps	100 Mbps										
CNet Port 8	2	8	√	-	256 KBytes	√	148,8	-	-	-	-	-	-	-	-	-	-	-
CNet CNSH 1600	2	16	√	-	-	√	14,881	148,81	4	√	-	-	-	-	-	-	-	√
CNet CSH 1600	2	16	√	-	-	√	14,881	148,81	4	-	-	-	-	-	-	-	-	√
D-Link DES-1005D	2	5	√	-	-	√	-	-	-	-	-	-	-	-	-	-	-	-
DLink DES-3326SR	2 y 3	24	√	√	-	√	-	-	√	√	√	√	√	√	√	√	RIP v1/v2, OSPF v2	√
DLink DES-3326	2 y 3	24	√	-	-	√	-	-	√	√	√	√	√	√	√	√	RIP v1/v2, OSPF v2	√
AOpen AOW-616	2	16	√	-	-	√	-	-	-	-	-	-	-	-	-	-	-	-
Advantek ANS-08P	2	8	√	-	4 kBytes	√	-	-	-	-	-	-	-	-	-	-	-	-
DLink DES 1024D	2	24	√	-	8000 entradas	√	-	-	√	√	√	√	√	√	√	√		√

	Interfaz Ethernet	Wi-Fi	Posición	PoE
SkyPilot Gateway	10/100 Base-T	no	Outdoor	si
SkyPilot Extender	10/100 Base-T	802.11 b/g (ciertos modelos)	Outdoor	si
Sky Connector	10/100 Base-T	no	Indoor/outdoor	si

Tabla 1.7 Características Adicionales de Equipos SkyPilot

La red de acceso inalámbrico no es caso de estudio de este proyecto de titulación por lo que no se considera el análisis actual. En el proceso de reingeniería se considerará dicha red como estable, segura y eficiente.

1.2.3.2. Servidores

Los servidores son equipos computacionales diseñados para procesar solicitudes y entregar datos a múltiples computadores dentro de una red.

Los servidores generalmente son configurados con características especiales como CPU más rápida, gran capacidad de memoria RAM y sistemas de almacenamiento de mayor capacidad dependiendo del servicio que éste proporcione, para manejar múltiples solicitudes concurrentes desde computadores cliente y características extras como redundancia en las fuentes de poder, en las conexiones de red y en dispositivos de almacenamiento.

Para obtener información de las características del hardware de los equipos de computación del Data Center se utilizaron las herramientas de software everest para plataformas Windows y lshw-2.09-1.fc3.rf.i386.rpm para plataformas Linux.

En el Anexo C se describen las características de hardware y de servicios activos de cada uno de los servidores de las tres redes de servicios del Data Center.

Red 192.168.2.0/24

1.2.3.2.1. fw.ree.edu.ec

Este servidor trabaja principalmente como un router básico entre la red pública 157.100.135.0/27 (WAN) y la red privada 192.168.2.0/24 (LAN).

Provee un firewall implementado con el paquete firestarter-1.0.3-1.i386.rpm que tiene funciones como NAT (Network Address Translation), forwarding de puertos (reenvío), filtrado de paquetes. Además es servidor Web del sitio www.ree.edu.ec.

1.2.3.2.2. correo.ree.edu.ec

Proporciona el servicio de correo electrónico para el dominio ree.edu.ec a través del programa comercial Communigate Pro Communication Server versión 5.1-10 cuyo archivo de instalación es CGatePro-Linux-5.1-10.src.rpm. Este servidor se encuentra en fase de prueba.

1.2.3.2.3. router

Este servidor tiene tres interfaces de red Ethernet físicas y dos interfaces virtuales con las cuales provee el enrutamiento entre las diferentes redes del Data Center a través de rutas estáticas para permitir el reenvío de paquetes desde/hacia las diferentes subredes.

Provee la función de NAT (Network Address Translation) implementada con iptables para la comunicación de los servicios basados en TCP/IP.

Red 192.168.1.0/24

1.2.3.2.4. fw.remq.edu.ec

Este servidor trabaja como router básico entre la red pública 157.100.135.0/27 (WAN) y la red privada 192.168.1.0/24 (LAN). Provee un firewall implementado con el paquete firestarter-1.0.3-1.i386.rpm que tiene funciones como NAT (Network Address Translation), reenvío de puertos y filtrado de paquetes.

Actúa como gateway de Internet y alberga a los servicios Web, correo electrónico, DNS, FTP, del dominio remq.edu.ec y el servicio Web del dominio cptquito.org.ec.

El servicio de correo electrónico es provisto con el paquete kerio-kms-6.2.1-1365.linux.i386.rpm que es el software comercial Kerio Mailserver versión 6.2.1. La provisión del servicio Web y DNS se lo realiza a través de Apache Web Server y Bind respectivamente, con el software por defecto en esta distribución de Linux.

Alberga dos tarjetas controladoras SCSI, una tarjeta controladora de arreglos RAID, cuatro discos duros SCSI de 80 Gbytes cada uno, con los cuales se ha configurado un arreglo de discos tipo RAID-5 resultando un total de 204 Gbytes de capacidad de almacenamiento con redundancia mediante paridad.

1.2.3.2.5. asterisk1.local

Este es el servidor de telefonía IP basado en asterisk sobre plataforma operativa Linux que pertenece a la Dirección de Educación del Municipio del Distrito Metropolitano de Quito.

Éste está destinado a proveer telefonía entre las instituciones del Proyecto QuitoEduca.Net y La Dirección De Educación. No se utiliza debido a que el servicio no ha sido requerido por el cliente.

1.2.3.2.6. municipio

Provee el servicio de video conferencia, el cual es utilizado por la Dirección de Educación del Ilustre Municipio Metropolitano de Quito para realizar reuniones que debido a la disponibilidad de tiempo no se hacen de manera presencial con las autoridades de determinado plantel.

Al momento no se pueden realizar sesiones interactivas entre varios establecimientos simultáneamente debido a que la infraestructura de red de acceso inalámbrica no cuenta con la configuración adecuada de Calidad de Servicio.

Red 172.20.0.0/24

1.2.3.2.7. fw.ree.com.ec

Este equipo permite el acceso a los sitios Web ubicados en el servidor web.conectividadglobal.net a través de reenvío de puertos. Adicionalmente permite el redireccionamiento del tráfico SMTP, IMAP, POP3 hacia y desde el servidor correo.conectividadglobal.net.

1.2.3.2.8. asterisk1.local

Éste es el servidor de telefonía IP basado en asterisk sobre plataforma operativa Linux destinado a proveer un servicio agregado de soporte técnico telefónico a los operadores de los Sistemas en las instituciones que lo requieran.

1.2.3.2.9. correo.conectividadglobal.net

Trabaja como servidor de correo para varios dominios entre los cuales están conectividadglobal.net, ree.com.ec, cia.ec, mcerere.ree.edu.ec, además aloja el sitio Web de conectividadglobal.net y ree.com.ec.

Utiliza tres particiones de volúmenes lógicos, Logical Volume Managment (LVM); y una partición ext3 para el punto de montaje /boot.

1.2.3.2.10. testserver.conectividadglobal.net

Sobre éste equipo se encuentran las versiones generadas del Sistema de Gestión Académica (SGA). Aquí se generan los instaladores del SGA, se realizan también pruebas de su funcionamiento y se desarrollan los nuevos requerimientos en la aplicación SGA a través de Visual Source Safe.

Debido a la naturaleza del SGA el sistema operativo es Windows Server 2003 Enterprise Edition.

1.2.3.2.11. web.conectivodadglobal.net

Aloja los sitios Web de las instituciones educativas pertenecientes al Proyecto QuitoEduca.Net. Las páginas en su mayoría están diseñadas en php y son de contenido dinámico.

1.2.3.2.12. firewall01

A pesar de que su nombre sugiere cierta función, éste equipo no se emplea como firewall sino como un servidor de monitoreo principalmente de la red de acceso inalámbrica.

El software que permite cumplir esta labor es OpManager. OpManager permite descubrir redes, dispositivos y categorizarlos, también indica el uso de memoria y la capacidad de disco.

1.2.3.2.13. sga.conectividadglobal.net

Su sistema operativo es Windows Server 2003 Enterprise Edition. Es el medio que permite la interacción de los usuarios de las instituciones que no pertenecen al Proyecto QuitoEduca.Net con el sistema SGA.

1.2.3.2.14. dc.conectividadglobal.net

Su hostname significa "**D**omain **C**ontroller" y es el encargado de proporcionar las funciones de administración de los usuarios y equipos del dominio conectividadglobal.net. Tiene configurado Active Directory.

1.2.3.2.15. rev.conectividadglobal.net

Su nombre hace referencia a "**R**ed **E**ducativa **V**irtual" ya que aloja la aplicación SGA. Es el medio que permite la interacción de los usuarios de las instituciones que pertenecen al Proyecto QuitoEduca.Net con el sistema SGA.

1.2.3.2.16. files.conectividadglobal.net

Utilizado para el servicio de transferencia de archivos en la red interna de empleados de Conectividad Global y en las visitas e instalaciones remotas en los clientes a través de la intranet.

1.2.3.2.17. gw.conectividadglobal.net

Trabaja como un router en su forma más básica permitiendo la salida a Internet a los usuarios de las redes privadas, tiene funciones de firewall básico bloqueando puertos, actúa como DNS local y de caché.

Servidor	Procesador	RAM (Mbytes)	Disco (Particiones)			
			1ra	2da	3ra	4ta
fw.ree.edu.ec	Intel Pentium II 450MHz	512	8927 Mbytes	18 Gbytes	-	-
correo.ree.edu.ec	Intel(R) Pentium(R) III CPU family 1133MHz	256	80 Gbytes	-	-	-
Router	Intel Pentium III (Katmai) 500MHz	512	80000 Mbytes	-	-	-
fw.remq.edu.ec	2 x Intel® Xeon™ MP CPU 2.8GHz	8 x 512	204 Gbytes	-	-	-
asterisk1.local	Intel(R) Xeon(TM) CPU 3.20GHz	1024	34GB	17GB	17GB	-
Municipio	Intel® Xeon™ MP CPU 3.2GHz	2 x 512	33GB	33GB	-	-
fw.ree.com.ec	Intel(R) Pentium(R) III CPU family 1133MHz	256	17 Gbytes	-	-	-
asterisk1.local	2 x Intel(R) Pentium(R) III CPU family 1266MHz	1024 MB	80GB	80GB	-	-
correo.conectividadglobal.net	2 x Cpu:0 à Intel Pentium III (Katmai) 900MHz	1024	68GB	17GB	17GB	-
testserver.conectividadglobal.net	Intel Pentium 4, 2800 MHz (21 x 133)	512	80 GB	-	-	-
web.conectividadglobal.net	2 x Intel(R) Pentium(R) III CPU family 1266MHz	512	74.54GB	-	-	-
firewall01	Intel(R) Pentium(R) 4 CPU 1.50GHz	256	30 Gbytes	-	-	-
sga.conectividadglobal.net	Quad Intel Pentium III Xeon, 550 MHz	1024	18 GB	18 GB	-	-
dc.conectividadglobal.net	Dual Intel Pentium II, 450 MHz (4.5 x 100)	320	80GB	-	-	-
rev.conectividadglobal.net	Intel Pentium II, 448 MHz	384	8675 MB	8754 MB	4338 MB	4338 MB
files.conectividadglobal.net	2 x Intel(R) Pentium(R) III CPU family 1266MHz	512	74.54GB	-	-	-
gw.conectividadglobal.net	Intel Pentium III (Katmai) 500MHz	512	8000 Mbytes	-	-	-

Tabla 1.8 Principales Caracterísiticas de los Equipos Servidores

Del Anexo C (Características de Hardware de los Equipos Servidores) donde se muestran los elementos principales de hardware y software instalado en los servidores podemos concluir que existen varios servicios no relacionados instalados y funcionando sobre un mismo equipo, el número de servicios instalados es superior al número de servicios ofrecidos, y además existe hardware no apto para soportar cierto tipo y volumen de información que generan ciertos servicios.

Existen servidores que contienen información sensitiva, los cuales no poseen algún tipo de sistema de almacenamiento avanzado, es decir, no son tolerantes a fallas. Si se presenta el eventual deterioro de un disco duro, la información no

podría ser recuperada. Por lo que es necesario también realizar el correcto respaldo de la información periódicamente.

No se ha realizado una planificación de software y hardware de acuerdo al servicio ofrecido. Algunos servidores necesitan que el hardware sea configurado de acuerdo al crecimiento futuro para evitar reconfiguraciones totales de los sistemas.

Ciertos equipos no poseen el hardware adecuado para proveer disponibilidad en función de fallas eléctricas. Se puede observar que la mayoría de servidores no poseen fuentes redundantes y que en algunos casos el sistema de enfriamiento interno no funciona adecuadamente ya que algunos ventiladores no se encuentran operando.

1.2.3.3. Sistema de Cableado Estructurado

La instalación del sistema de cableado estructurado realizada por el personal del área de Administración de Redes, consta de cable UTP categoría 5e y la norma EIA/TIA 568B, tomando en cuenta distancias máximas y mínimas del tendido del cable, recomendadas para cable UTP de cuatro pares, categoría 5e.

En las instalaciones del Data Center el tendido de cable entre los servidores y equipos de conectividad se encuentra sobre el techo falso. Desde los patch panels hacia los computadores del personal el cable se encuentra organizado en canaletas decorativas que se ubican en la parte inferior de cada una de las paredes en las se requieren puntos de red. El rack de comunicaciones alberga al patch panel y a los dispositivos de conectividad. El patch panel es de 48 puertos y a él se conectan todos los equipos servidores y los computadores del personal de la empresa.

Los puntos de red no se encuentran etiquetados en ninguno de los dos extremos y no se tiene una documentación del sistema de cableado estructurado.

1.2.3.4. Ubicación Física de Servidores y Equipos de Comunicación

Es importante la organización de los equipos que alojan los sistemas informáticos y los servicios para realizar una mejor administración de la red. En el área de equipos servidores y de conectividad se encuentran tres racks, dos para servidores y uno para equipos.

1.2.3.4.1. Rack de servidores

El primer rack de servidores es un rack de 19 pulgadas (480 mm), donde se han colocado ocho servidores rackeables, es un sistema estandarizado para montaje con varios módulos para equipamiento electrónico. Posee hoyos perforados en intervalos regulares sobre dos soportes metálicos paralelos verticales que permiten que cada hoyo sea parte de su par horizontal a una distancia de 18,3 pulgadas (460 mm). Permite el equipamiento de servidores utilizando dos rieles sobre cada extremo en el rack. Estos rieles son capaces de soportar al equipo en una posición en la cual sea fácilmente desmontado del rack, que es útil para inspección o mantenimiento.

El segundo rack de servidores está conformado por cuatro compartimentos, donde se ubican doce servidores standalone del Data Center. La ubicación física de los servidores en los rack se muestra en la Figura 1.8.

1.2.3.4.2. Rack de equipos

En el rack de equipos se encuentran tres switches rackeables de marca D-Link, un patch panel para 48 puertos RJ-45, un patch panel para 24 puertos RJ-45, dos bandejas donde se encuentran colocados equipos de conectividad y dos organizadores para cable UTP.

La ubicación física de los equipos de conectividad en los racks se describe en la Figura 1.9.

1	fw.ree.com.ec (172.20.0.2)
2	web.conectividadglobal.net (172.20.0.43)
3	correo.ree.edu.ec (192.168.2.2)
4	Servidor para futuros propositos
5	Asterisk1.local (172.20.0.3)
6	sga.conectividadglobal.net (172.20.0.7)
7	correo.conectividadglobal.net (172.20.0.4)
8	dañado
9	fw.ree.edu.ec (192.168.2.1)
10	gw.conectividadglobal.net
11	firewall01 (172.20.0.6)
12	FTP Conectividad Global (172.20.0.12)
13	Router (172.20.0.40)
14	testserver.conectividadglobal.net (172.20.0.5)
15	MUNICIPIO (192.168.1.3)
16	Asterisk1.local (192.168.1.2)
17	rev.conectividadglobal.net (172.20.0.11)
18	Servidor de colegio heidegger
19	dc.conectividadglobal.net (172.20.0.9)
20	fw.remq.edu.ec (192.168.1.1)

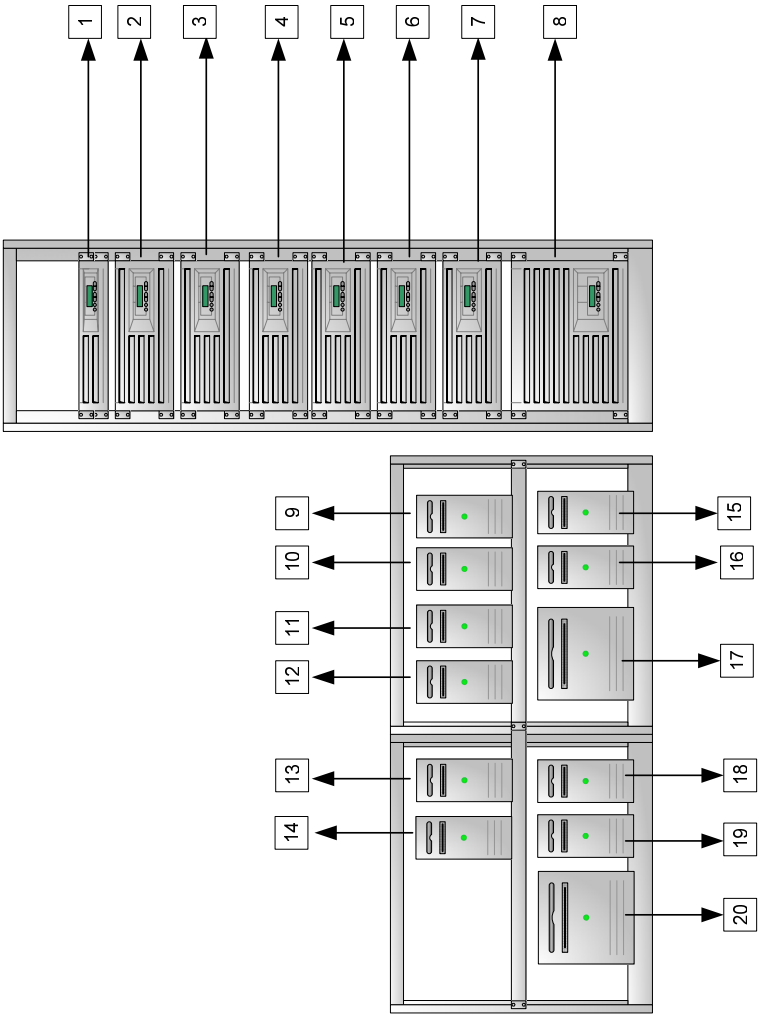


Figura 1.8 Diagrama de localización física de los servidores en los racks

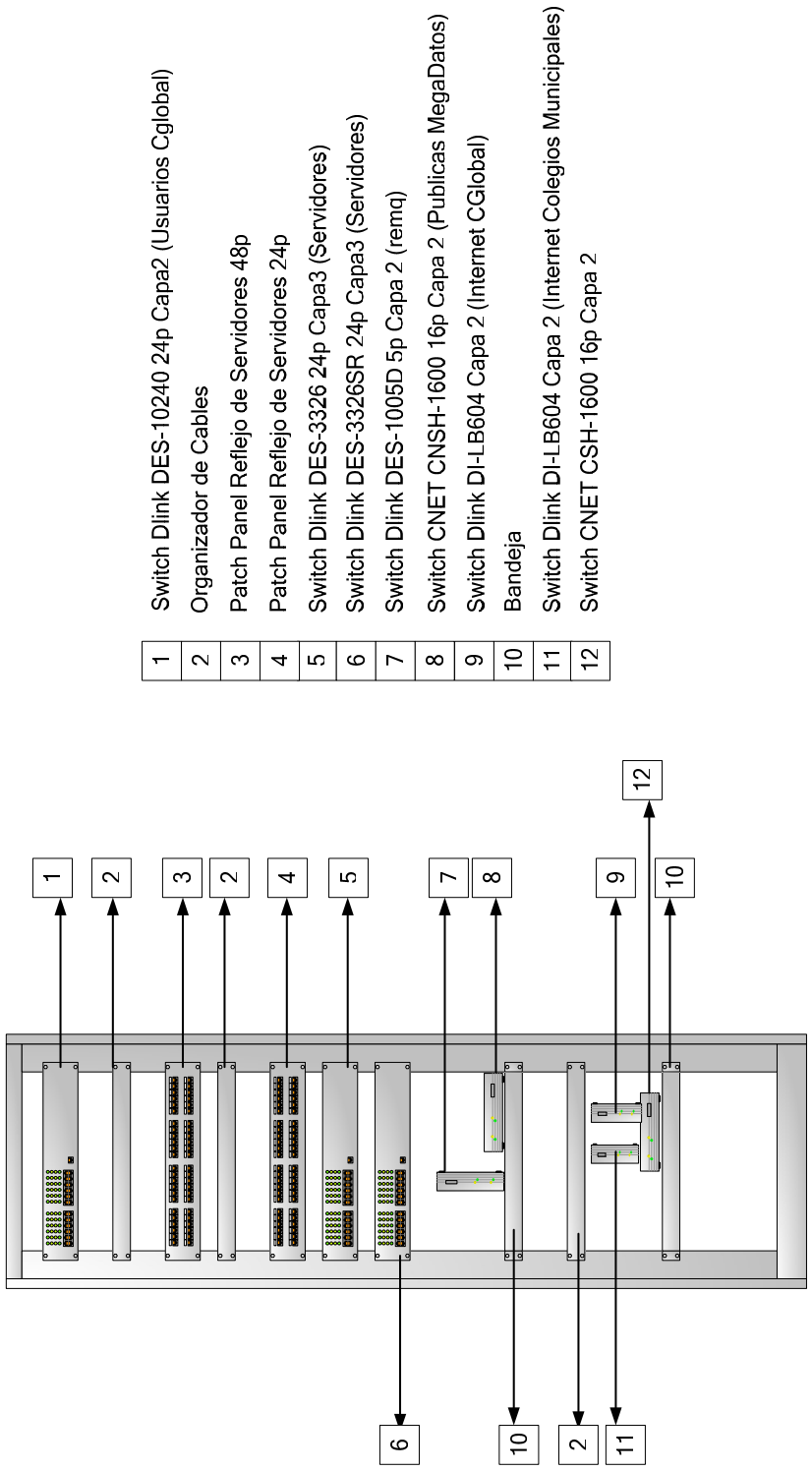


Figura 1.9 Diagrama de localización física de los equipos de ínter conectividad

1.2.3.5. Climatización

El Data Center está provisto de un solo equipo de aire acondicionado ubicado en un extremo de las instalaciones que albergan al Data Center, y se lo ha establecido para mantener la temperatura en 18ºC. En las partes cercanas al equipo se mantiene esta temperatura, mientras que al otro extremo conforme incrementa la distancia la temperatura aumenta, por lo que es necesaria una reubicación de manera que proporcione temperatura constante en todo el Data Center.

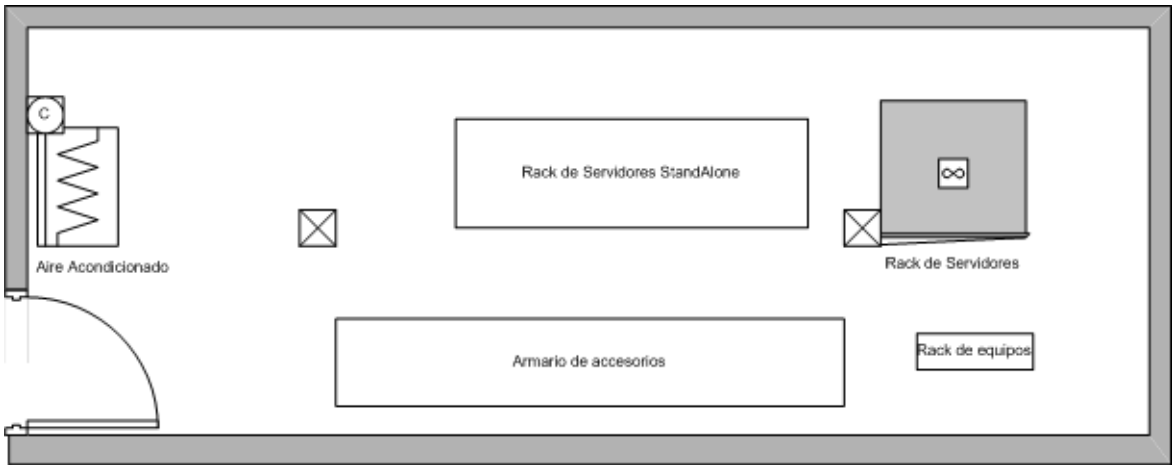


Figura 1.10 Diagrama de la posición del sistema de aire acondicionado en el Data Center (vista Superior)

1.2.3.6. Banco de Baterías

El Data Center no dispone de una planta generadora de electricidad de respaldo para mantener alta disponibilidad, únicamente cuenta con 3 UPS a los que se conectan todos los servidores y equipos de conectividad, que pueden mantenerlos funcionando por aproximadamente 10 minutos. Tiempo en el que se debe proceder a realizar un apagado normal de todos servidores, debido al riesgo de daño del sistema de archivos en servidores Linux si se apaga el equipo abruptamente. Cabe destacar que no se lleva un registro de indisponibilidad del servicio eléctrico en el sector, pero suele ocurrir entre diez minutos y una hora en horario laborable o en fines de semana, y por lo menos una vez cada tres meses.

Para las computadoras de los empleados de la empresa no se cuenta con un UPS propio.

1.2.3.7. Sistema de Tierra

El sistema de Tierra utilizado por el Data Center es el mismo que se utiliza para el edificio, está provisto de una malla metálica instalada debajo de los jardines de la planta baja mediante la cual se conecta a tierra todo el sistema eléctrico del edificio. El voltaje que se obtiene en la línea eléctrica es de 115 voltios, y el voltaje medido entre el neutro y la tierra es de 0.9V. El Data Center debería tener su propio sistema de puesta a tierra.

1.2.4. DIRECCIONAMIENTO IP

La Figura 1.11 muestra el esquema de la infraestructura de red actual y las diferentes redes utilizadas.

La subred de acceso a Internet lo proporciona el ISP Megadatos S.A. quien ha asignado la subred 157.100.135.0/27. El direccionamiento IP de las diferentes redes de servicios que maneja la empresa se lo realizó tomando en cuenta diferentes propósitos.

La red privada 172.20.0.0, con máscara de 24 bits, para la red interna de la empresa, con asignación de direcciones de forma estática debido principalmente a los registros tipo A del servidor de DNS, gw.conectividadglobal.net, que maneja el dominio conectividadglobal.net puesto que dicho servicio es utilizado por varios servicios de esta red.

Las redes privadas clase C 192.168.1.0 para la Red Educativa Metropolitana y 192.168.2.0 para la Red Educativa Ecuatoriana, con asignación de direcciones de forma estática para cada red puesto que se manejan servicios que prescinden de los registros de recursos tipo A de servicios de DNS.

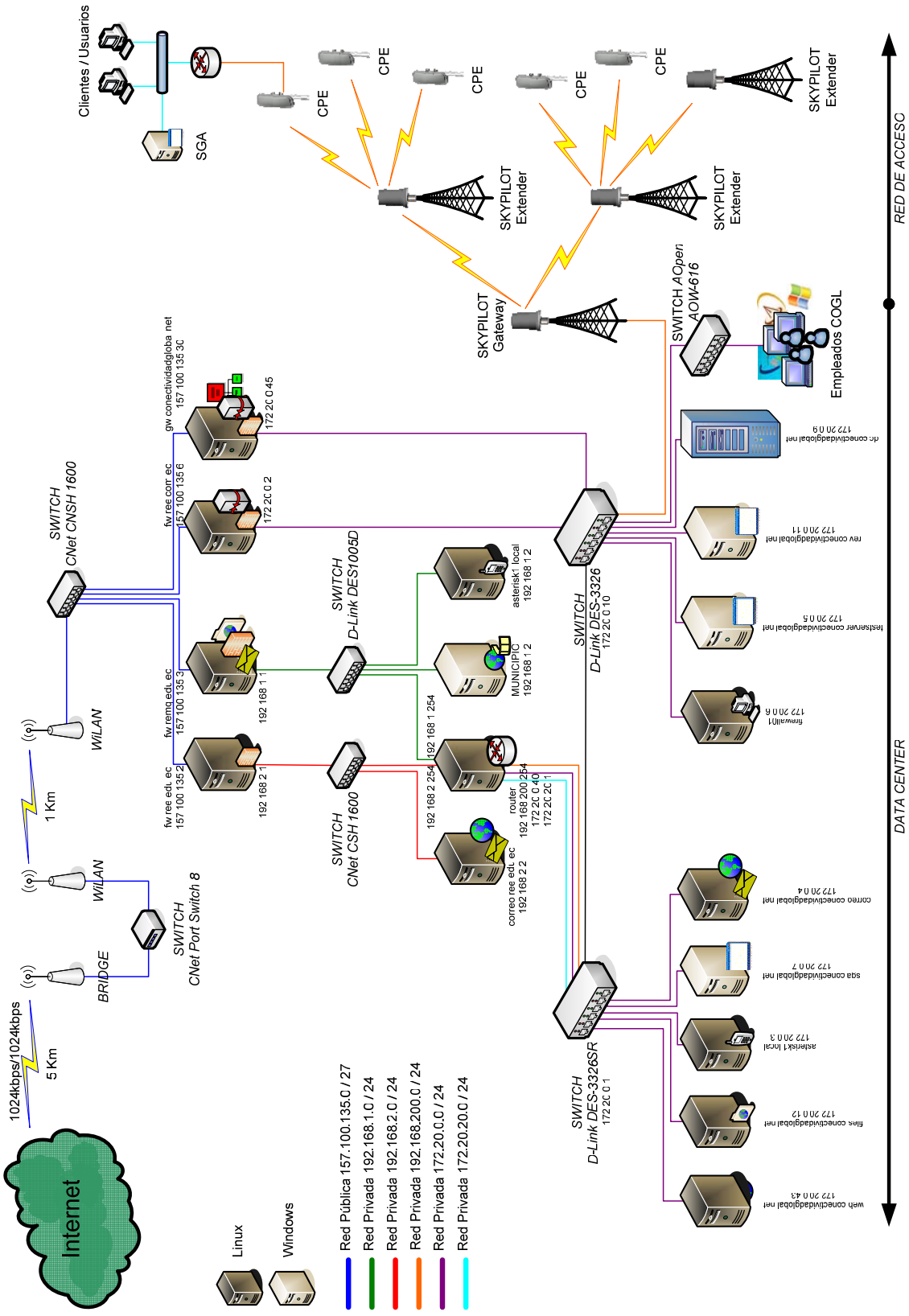


Figura 1.11 Diagrama de la Red de Servicios de Conectividad Global Cía. Ltda.

La red privada 192.168.200.0, con mascara de 24 bits, para la red de administración de los equipos inalámbricos SkyConnector, con asignación de direcciones IP de forma estática y son establecidas en el momento mismo de la configuración de cada equipo SkyConnector.

Para los usuarios finales de los servicios se ha provisto la red 172.20.20.0/24 a través de la cual cada establecimiento configura un equipo capa 3 con una IP estática.

1.2.5. ANÁLISIS DE TRÁFICO

Para analizar el volumen de tráfico generado en la red es necesario implementar software que nos permita obtener lecturas de los niveles de carga que tienen que soportar los enlaces y los servidores. Para el efecto se instaló el paquete MRTG (Multi Routing Traffic Grapher) en el servidor gw.conectividadglobal.net; esta herramienta proporciona información de la monitorización del tráfico sobre enlaces de red que obtiene con ayuda del protocolo snmp (Simple Network Management Protocol), y genera gráficas relacionadas al reporte del tráfico entrante/saliente pico, promedio y mínimo en diferentes periodos que van desde días, semanas, meses y años.

MRTG se ha configurado para recolectar las muestras cada 5 minutos. La línea azul muestra la carga de salida y la verde la de entrada. Además se configuró el nombre de la ***comunidad*** "cogl" en cada equipo ha ser monitorizado. Para análizar el tráfico, se recolectaron los reportes elaborados por MRTG en un lapso de 5 días, desde el día 25 hasta el día 30 de Junio de 2008.

1.2.5.1. Número de Beneficiarios Actualmente

Gracias a la colaboración del personal de la Dirección de Educación, encargado de la ejecución del Proyecto QuitoEduca.Net se obtuvieron las estadísticas de crecimiento de usuarios de los sistemas desde su inicio.

Esta información se vuelve importante para la proyección del crecimiento futuro de la red y el tráfico que generarán los usuarios, tema que se desarrollará en el siguiente capítulo.

La tabla 1.9 muestra varias estadísticas del proceso de integración de algunos centros educativos al Proyecto, indica cuántas instituciones han sido beneficiadas con centros de cómputo, instalaciones eléctricas, software, etc.

ETAPA	I	II	III	IV	V	VI
Año	2002	2003	2004	2005	2006	2007
Centros Beneficiarios	64	43	108	173	184	115
No. Puntos de servicio	444	224	610	1000	1000	1000
No. Estudiantes	27573	13065	54370	36813	28024	29797
No. Maestros	1016	551	1841	2224	1129	2018

Tabla 1.9 Estadísticas de Centros Beneficiados por el Proyecto

La tabla 1.10 indica indica el número de instituciones que se han integrado a la red de datos de Conectividad Global Cía. Ltda. durante los años 2007 y 2008 mediante la red de acceso inalámbrica.

ETAPA	V	VI	VII	TOTALES
Finales de Año	2006	2007	2008	
Centros Integrados a la Red de COGL	0	10	16	26

Tabla 1.10 Estadísticas de los Centros Integrados a la Red de Servicios de Conectividad Global Cía. Ltda.

1.2.5.2. Niveles de Tráfico de Internet

Para la salida hacia Internet Conectividad Global Cía. Ltda. cuenta con un enlace simétrico de 1024 kbps, es decir, 1024 kbps de velocidad tanto para uplink como para downlink.

En la tabla 1.11 se observan las gráficas del consumo del canal de Internet.

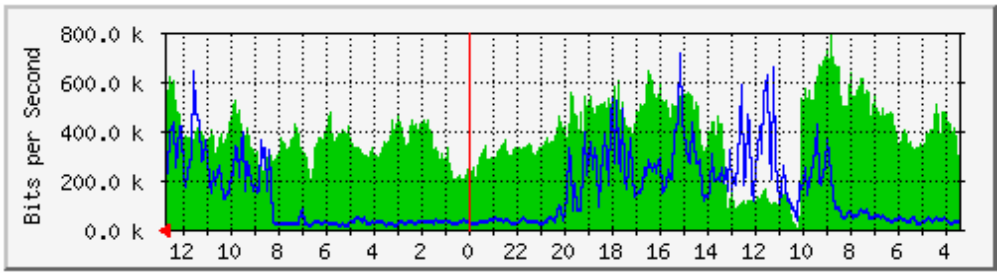
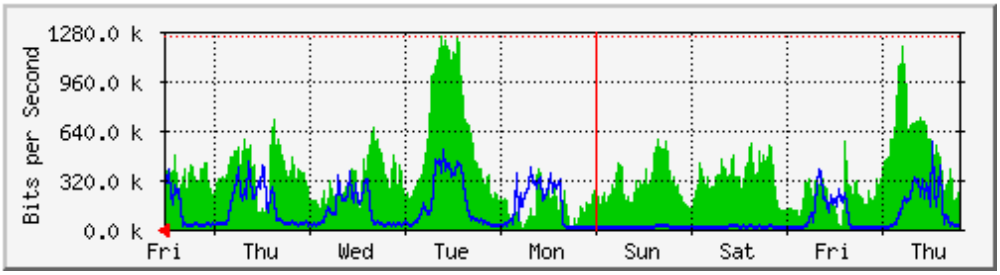
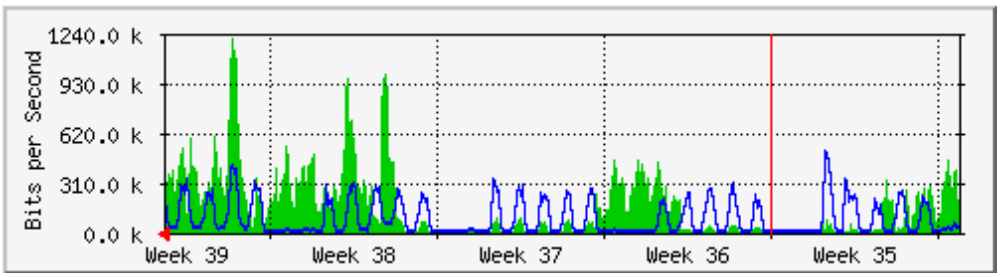
Período de monitoreo	Reporte
Horas	
Días	
Semanas	

Tabla 1.11 Gráficas de reportes de tráfico de Internet.

La tabla 1.12 muestra las estadísticas del reporte de tráfico obtenido en horas, días, y semanas del router 157.100.135.1 perteneciente al proveedor de Servicios de Internet Megadatos S.A. Los valores que conforman esta tabla se encuentran en el Anexo D.

El enlace de Internet es ocupado principalmente por el personal de la Dirección de Educación del Proyecto QuitoEduca.Net y los empleados de Conectividad Global Cía. Ltda.

	CAPACIDAD ENLACE 1024 (kbps)					
	MÁXIMO (kbps)	UTILIZACIÓN (%)	PROMEDIO (kbps)	UTILIZACIÓN (%)	ACTUAL (kbps)	UTILIZACIÓN (%)
	REPORTE EN HORAS					
IN	793,80	77,52	386,30	37,72	520,90	50,87
OUT	711,70	69,50	139,80	13,65	214,30	20,93
	REPORTE EN DÍAS					
IN	1248,60	121,93	367,90	35,93	512,50	50,05
OUT	558,80	54,57	101,00	9,86	372,30	36,36
	REPORTE EN SEMANAS					
IN	1210,50	118,21	165,40	16,15	397,50	38,82
OUT	497,70	48,60	80,80	7,89	220,10	21,49

Tabla 1.12 Mediciones del tráfico de Internet obtenidas por MRTG

Las estadísticas muestran que el enlace no está siendo utilizado en su capacidad máxima, pero cabe aclarar que en el ejercicio de sus funciones, el personal no utiliza Internet las noches ni fines de semana.

Cabe recalcar que existen intermitencias en el servicio de Internet que son propias del enlace de última milla inalámbrico del ISP.

1.2.5.3. Niveles de Tráfico Interno

Para el análisis de tráfico de las redes del Data Center se empleó la herramienta de software libre ***ntop***, la cual permite visualizar las estadísticas de tráfico en cada servidor de la red mediante interfaz Web.

La instalación de este software se la realizó sobre el equipo con hostname **router** de dirección IP 172.20.0.40, encargado de la interconexión de las redes de servicios del Data Center, con el objetivo de analizar el tráfico que fluye a través de sus interfaces físicas. También se lo instaló sobre el equipo fw.ree.com.ec para analizar el tráfico que maneja este servidor, puesto que constituye la puerta de enlace a Internet para algunos servicios y usuarios. Los reportes que este software proporciona se tomaron durante cinco días comprendidos entre el 25 y 30 de Junio de 2008.

1.2.5.3.1. Tráfico en el router 172.20.0.40 y carga en los servidores

La información proporcionada por ntop sobre el router que interconecta las redes 172.20.0.0/24, 192.168.1.0/24 y 192.168.1.0/24 indica y detalla el tipo de tráfico de los diferentes servicios en el Data Center.

Se puede apreciar que los valores promedio no superan la capacidad máxima del protocolo y medio de transmisión que utilizan las interfaces del router. Estos valores están dados en la Tabla 1.13.

Interfaz	eth2	eth1	eth0
Red	***192.168.1.254***	***172.20.0.40 192.168.200.254 172.20.20.1***	***192.168.2.254***
Carga máxima de red (kbps)	989,9	947,9	12700
Carga promedio de red (kbps)	359,	355,8	83,5
Capacidad máxima (kbps)	100000	100000	100000

Tabla 1.13 Tráfico en cada una de las interfaces del router del Data Center

Con el fin de visualizar de mejor manera esta información, se presentan las siguientes gráficas:

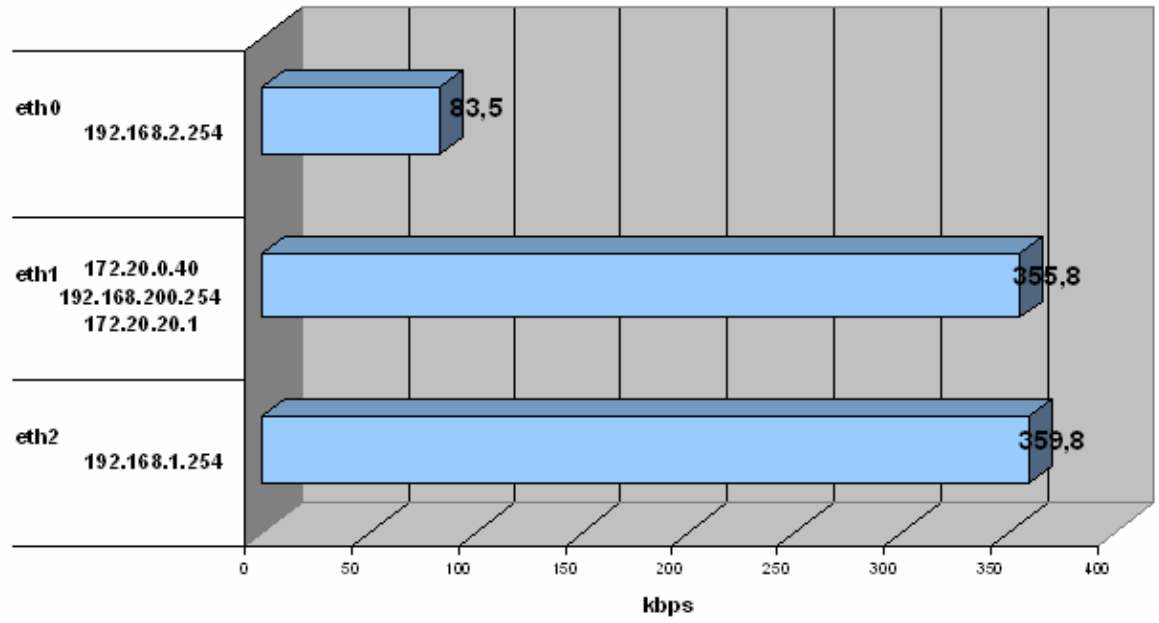


Figura 1.12 Carga Promedio Generada en las Redes

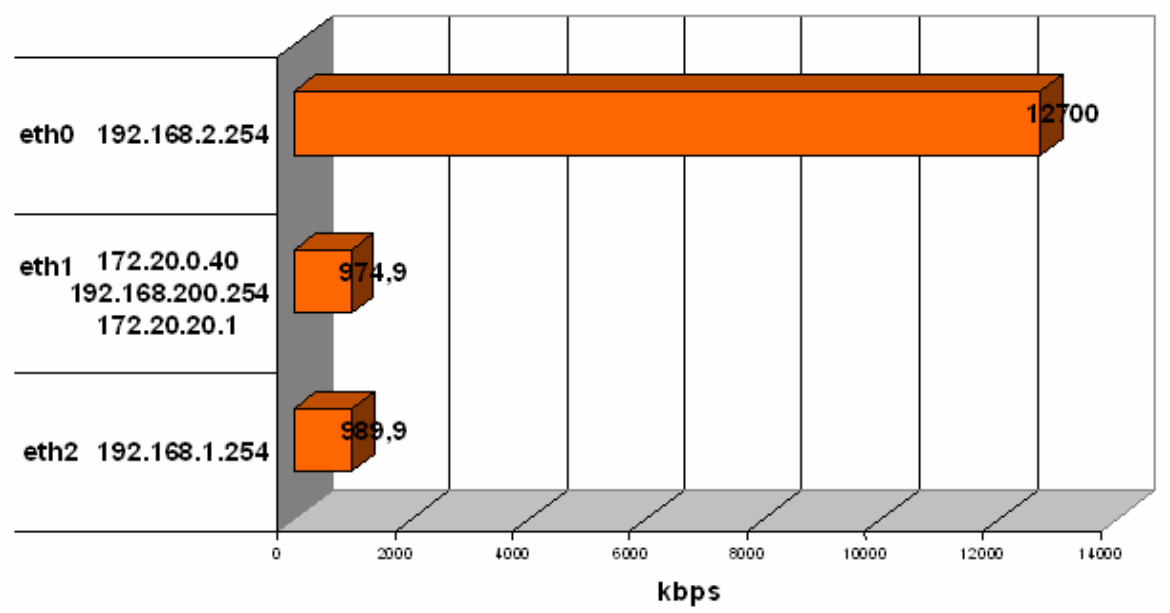


Figura 1.13 Carga Máxima Generada en la Redes

Los valores promedio son bajos debido a que consideran también la carga de red que puede existir en horario no laborable, que en algunos casos es nula.

Observando la Figuras 1.12 se puede concluir que la mayor cantidad de tráfico se enruta a través de las interfaces eth1 y eth2, las cuales representan gateways para los usuarios y para la mayoría de servidores.

La interfaz de la red 192.168.2.0/24 mantiene un nivel de tráfico muy bajo, debido a que sólo mantiene a dos servidores, en los que uno de ellos aloja un solo sitio Web denominado ***www.ree.edu.ec*** y el otro, es servidor de correo para pruebas.

La carga sobre cada servidor constituye una variable de análisis, debido a que, los servicios están limitados por su configuración y por el hardware que disponen. El tiempo de respuesta a una solicitud dependerá del procesamiento y almacenamiento de datos que recibe o entrega. A través de la herramienta PRTG (Paessler Router Traffic Grapher) y ntop se obtuvo información acerca de la carga que procesa cada servidor. Los valores tabulados se encuentran en la Tabla 1.14.

Servidor	Tráfico diario promedio en Interfaces (kbps)		Datos procesados (kbytes)		
	Interna	Externa	Interna	Externa	Total
fw.ree.edu.ec	98,050	1,550	614223,016	8155,265	622378,281
correo.ree.edu.ec	3,270	X	16912,660	X	16912,660
fw.remq.edu.ec	187,346	187,065	987956,317	986476,740	1974433,057
MUNICIPIO	0,630	X	3344,716	X	3344,716
asterisk1.local	0,080	X	407,405	X	407,405
fw.ree.com.ec	142,394	138,754	750905,803	731711,196	1482616,999
gw.conectividadglobal.net	1,55	12,45	8155,265	65627,1	73782,365
asterisk1.local	1,160	X	6134,354	X	6134,354
correo.conectividadglobal.net	4,410	X	23248,893	X	23248,893
testserver.conectividadglobal.net	2,090	X	11004,833	X	11004,833
firewall01	18,810	X	99173,994	X	99173,994
sga.conectividadglobal.net	26,887	X	141785,339	X	141785,339
rev.conectividadglobal.net	3,430	X	18069,635	X	18069,635
files.conectividadglobal.net	22,990	X	121221,236	X	121221,236
dc.conectividadglobal.net	167,790	X	884837,047	X	884837,047

Tabla 1.14 Tráfico generado en los servidores

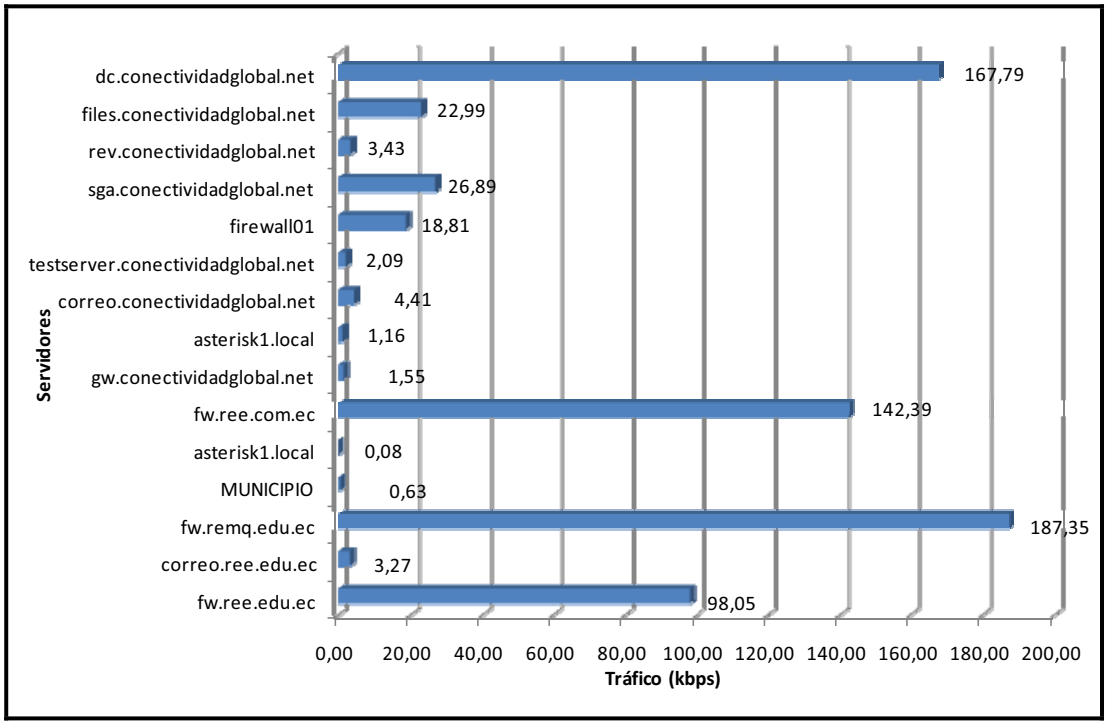


Figura 1.14 Tráfico generado en los servidores

La Figura 1.14 muestra el tráfico que se genera en los servidores. Se observa que el mayor número de solicitudes y respuestas pertenece a los servidores fw.remq.edu.ec, fw.ree.com.ec y dc.conectividadglobal.net. La Figura 1.15 indica la cantidad de datos que los servidores procesan. Se puede ver que en algunos casos los niveles son bajos respecto a los servidores que manejan mayor tráfico.

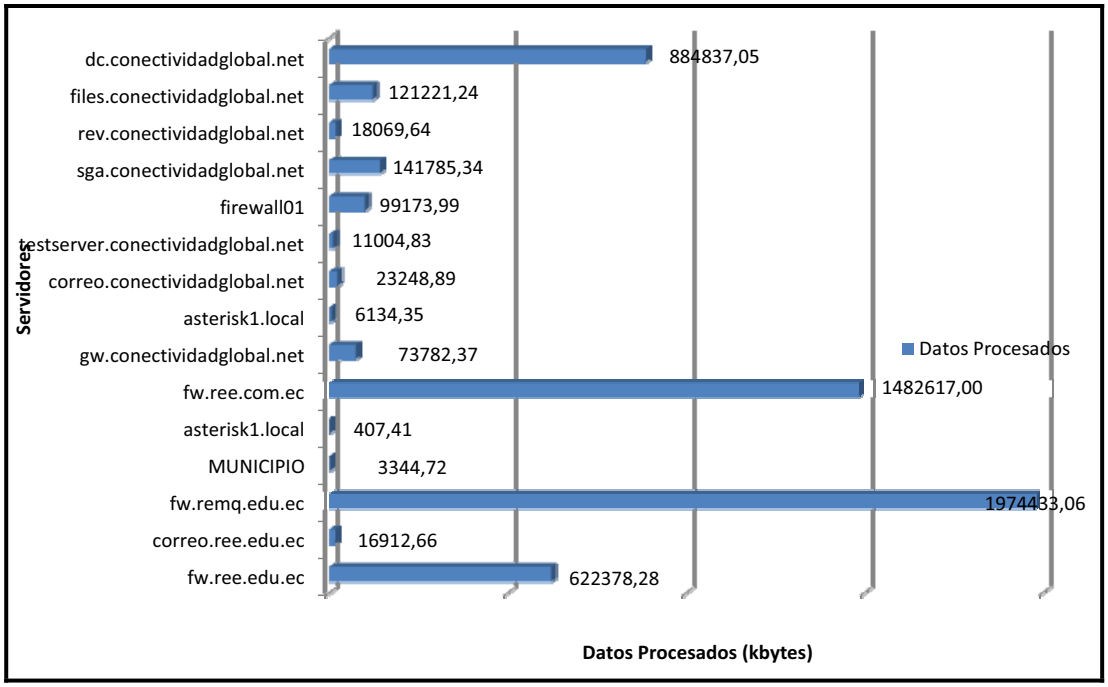


Figura 1.15 Datos Procesados en los servidores

Para un completo análisis, es necesario determinar el tipo de tráfico que provoca este comportamiento. Para esto se realiza un análisis de tráfico generado por aplicación.

1.2.5.3.2. Tráfico por aplicaciones

Para analizar el tráfico por aplicaciones se utilizó el software ntop instaládolo en los equipos de hostname ***router*** de IP 172.20.0.40, sobre el equipo ***fw.ree.com.ec*** de IP 172.20.0.2 y sobre ***fw.remq.edu.ec*** con IP 192.168.1.1 que constituyen routers por los que atraviesa y se enruta todo el tráfico proveniente de usuarios de las Instituciones Educativas que acceden a los servicios del Data Center y de todos los usuarios que acceden a Internet, respectivamente.

Tabla 1.15 Cantidad de datos procesados y porcentaje de utilización por protocolo en la red

PROTOCOLO	Cantidad de datos procesados [Kbytes]							UTILIZACION						
	router			fw.ree.com.ec		fw.remq.edu.ec		router			fw.ree.com.ec		fw.remq.edu.ec	
	eth0	eth1	eth2	eth3	eth4	eth0	eth1	eth0	eth1	eth2	eth3	eth4	eth0	eth1
FTP	33500	102700	110900	182000	111100	111100	182100	0.41%	1.28%	1.48%	2.19%	1.33%	0.88%	1.49%
HTTP	2080866.18	2100677.6	3397965	5400000	5400000	3757615.95	1682378.99	25.70%	26.27%	45.24%	64.86%	64.86%	29.82%	13.78%
DNS	25100	34700	67200	85900	70800	82800	106700	0.31%	0.43%	0.89%	1.03%	0.85%	0.66%	0.87%
Telnet	4000	4000	11.8	17	13.7	32.2	33.8	0.05%	0.05%	0.00%	0.00%	0.00%	0.00%	0.00%
NBios-IP	11300	48.3	43900	77.3	44400	46600	161.6	0.14%	0.00%	0.58%	0.00%	0.53%	0.37%	0.00%
Mail	2284830.66	2258185.24	2107847.25	83700	83700	103100	2178663.71	28.22%	28.24%	28.07%	1.01%	1.01%	0.82%	17.84%
DHCP-BOOTP	294.1		294.2	0.4	369	407.5	1.3	0.00%		0.00%	0.00%	0.00%	0.00%	0.00%
SNMP	66600	0.7	4800		4900	6100		0.82%	0.00%	0.06%		0.06%	0.05%	
NNTP	2.8	2.5		0.5	0.5	3.9	3.9	0.00%	0.00%		0.00%	0.00%	0.00%	0.00%
NFS/AFS	60.6	60.4	20.3	31.5	28.5	76.6	81.8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
VoIP	62.7	63.4	571.6	579.2	579	623.1	623.4	0.00%	0.00%	0.01%	0.01%	0.01%	0.00%	0.01%
X11	10200	10200	106.1	125.9	120.1	16800	16900	0.13%	0.13%	0.00%	0.00%	0.00%	0.13%	0.14%
SSH	21.2	211.11	137400	30100	137400	137400	30100	0.00%	0.00%	1.83%	0.36%	1.65%	1.09%	0.25%
Gnutella	86.4	82.1	552.8	520.1	565.3	1600	1600	0.00%	0.00%	0.01%	0.01%	0.01%	0.01%	0.01%
Kazaa	30	32.9	15.1	36.1	15.1	42.8	64.1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
WinMX	10.5	10.6	3.1	5.6	3.8	14.8	16.6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
eDonkey	2500000	2500000	894000	1100000	1100000	5942384.05	5941957.3	30.88%	31.26%	11.90%	13.21%	13.21%	47.15%	48.67%
BitTorrent	900.8	1000	39400	112200	39400	58700	131500	0.01%	0.01%	0.52%	1.35%	0.47%	0.47%	1.08%
Messenger	44500	44400	30900	32200	32300	37200	36900	0.55%	0.56%	0.41%	0.39%	0.39%	0.30%	0.30%
Other TCP/UDP based Protocols	1033303.16	940237.159	674287.75	979800	1300000	2300000	1900000	12.76%	11.76%	8.98%	11.77%	15.61%	18.25%	15.56%

La tabla 1.15 contiene el porcentaje de utilización de cada una de las aplicaciones manejadas por los tres routers.

Los empleados de Conectividad Global utilizan otro equipo de enrutamiento gw.conectividadglobal.net con dirección IP 172.20.0.45 como puerta de enlace para navegar por Internet.

Como se puede apreciar en la Figura 1.16 el servicio de correo electrónico brindado por ***fw.remq.edu.ec*** es el más requerido en las interfaces de ***router*** por los usuarios que no acceden a través de Internet. fw.remq.edu.ec también constituye la puerta de enlace predeterminada de acceso a Internet para los servicios del dominio remq.edu.ec del Proyecto QuitoEduca.Net.

El tráfico que hace referencia a otros protocolos TCP/UDP contempla las solicitudes hacia el motor RDBMS (Relational Database Management System) de la aplicación SGA, también https, entre otros.

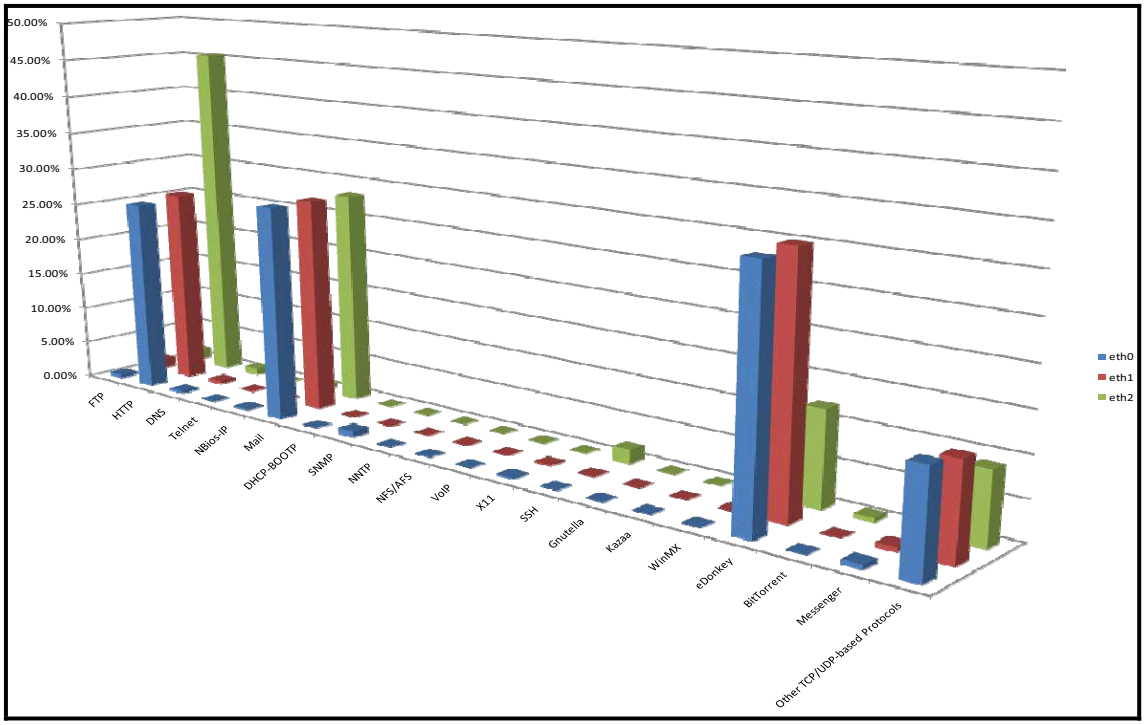


Figura 1.16 Porcentaje de Utilización de Protocolos en "router"

El equipo ***router*** constituye un único punto de falla para los usuarios de los servicios y aplicaciones del Data Center por lo que su disponibilidad debe estar garantizada.

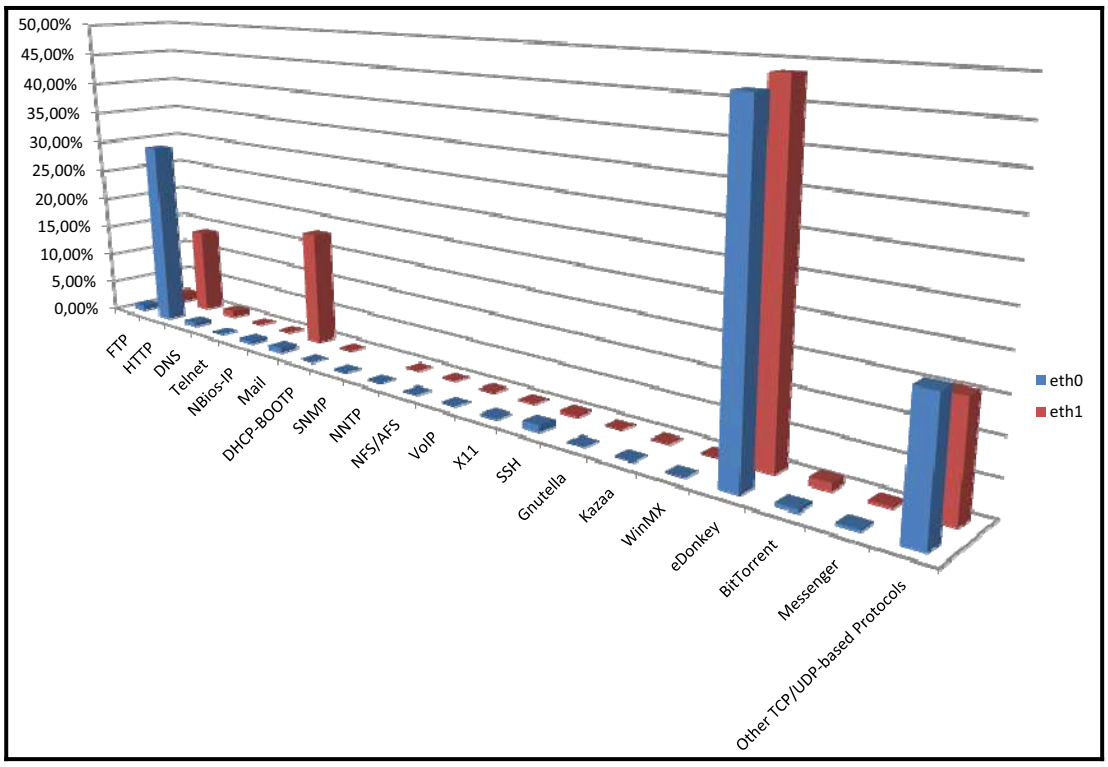


Figura 1.17 Porcentaje de Utilización de Protocolos en "fw.remq.edu.ec"

La Figura 1.17 muestra que la mayor demanda de tráfico de Internet es proveniente de aplicaciones p2p (peer to peer). La mayoría de éstas descargas son innecesarias e inapropiadas para la misión de la empresa, por lo que se debe restringir su utilización.

En la figura 1.18 se observa que la mayor cantidad de solicitudes al servidor fw.ree.com.ec son del tipo http debido a que éste es el equipo que realiza el redireccionamiento de las solicitudes desde Internet hacia el servidor web.conectividadglobal.net que contiene la mayoría de sitios web alojados en el Data Center.

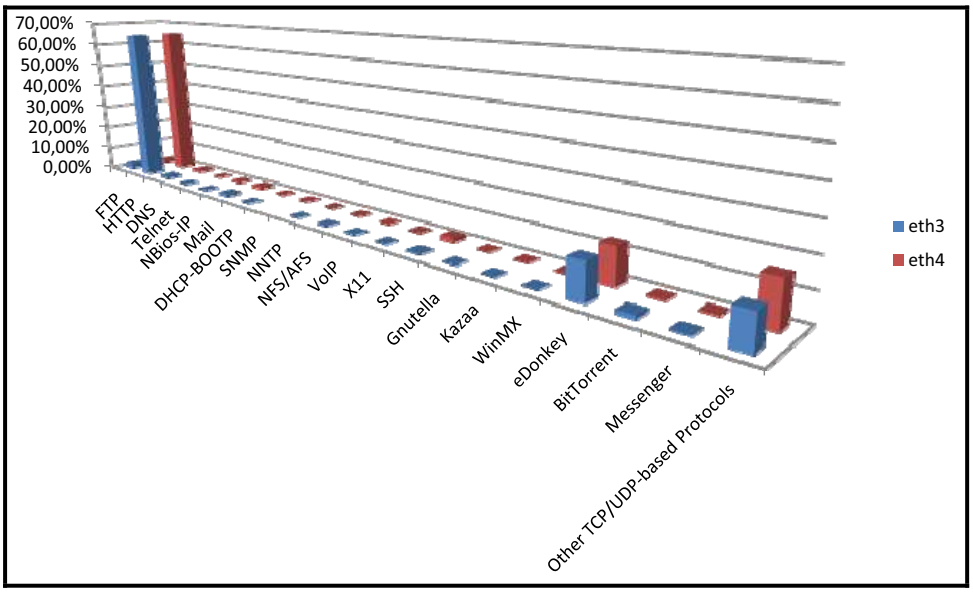


Figura 1.18 Porcentaje de Utilización de Protocolos en "fw.ree.com.ec"

La planificación de la capacidad de un servidor juega un papel importante puesto que al momento no se ha alcanzado el objetivo de vincular al proyecto a todas las instituciones educativas del Distrito Metropolitano de Quito. Si la cantidad de usuarios aumenta, al menos se esperaría que el tráfico crezca en igual magnitud. Como se puede visualizar en las gráficas anteriores el tráfico ya implica una carga de red considerable en algunos servidores, por lo que se debería diseñar una infraestructura que provea capacidad suficiente y disponibilidad de los servicios.

1.3. ESTADO ACTUAL DE LA SEGURIDAD EN LA RED

1.3.1. LEVANTAMIENTO DE LA INFORMACIÓN

El Data Center constituye el pilar principal de Conectividad Global Cía. Ltda., puesto que permite brindar la funcionalidad requerida para el procesamiento de las aplicaciones desarrolladas por la empresa, almacenamiento de datos y ofrecer servicios TCP/IP, que en primera instancia satisfacen necesidades tecnológicas enfocadas a los procesos académicos de instituciones públicas y/o privadas de

nivel prebásico, básico y/o bachillerato del Distrito Metropolitano de Quito y por otro lado permiten ofrecer servicios a empresas privadas que requieran Web Hosting, Housing y correo electrónico.

El levantamiento de la información es necesario para el diagnóstico de la gestión de seguridad de la información de acuerdo a la norma ISO/IEC 17799 y para el respectivo análisis de riesgos.

Conectividad Global Cía. Ltda. no está estructurada de acuerdo a esta norma y consecuentemente la información para el análisis debió obtenerse en colaboración con el administrador de red y del administrador de sistemas de la empresa, documentación impresa y no impresa, y herramientas de software de exploración de redes.

La norma ISO/IEC 17799 considera como información a todas sus formas y medios que puede ésta representar, como por ejemplo: digital, papel, etc., pero sólo nos limitaremos al análisis de la información almacenada, procesada o transmitida a través de los sistemas informáticos del Data Center de Conectividad Global.

Para el análisis de riesgos se identificaron a los sistemas informáticos más críticos desde el punto de vista de seguridad y el análisis se concentró en estos sistemas. A continuación se realizará un análisis de la situación actual de seguridad de los elementos existentes en el Data Center para determinar su grado de seguridad.

1.3.1.1. Documentación Impresa

Conectividad Global, actualmente, no cuenta con una documentación impresa que indique el manejo de la seguridad informática, y no se ha hecho hincapié para establecer una documentación apropiada para el manejo de la seguridad informática, la documentación encontrada en la empresa hace referencia únicamente a las políticas relacionadas al área de Recursos Humanos enfocadas al manejo de personal.

1.3.1.2. Seguridad en el perímetro de red.

Los firewalls son la primera línea de defensa para proteger a la red de información de cualquier organización, análogamente se los puede representar como porteros entre la red interna de la organización y el Internet, y configurados de forma correcta corresponden a una de las herramientas más efectivas para la defensa pero no basta proteger la red sólo con esta herramienta.

1.3.1.2.1. Arquitectura de Firewall

La red informática del Data Center utiliza la arquitectura de firewall, *screened subnet[10]* en los cuatro firewalls para cada red de servicios, implementados sobre servidores basados en plataforma Linux utilizando el software Open Source de firewall *firestarter release 1.0.3*, los mismos que mantienen en una de sus interfaces a las direcciones IP: 157.100.135.2, 157.100.135.3, 157.100.135.6, 157.100.135.30, de la red pública 157.100.135.0/27 del ISP Megadatos.

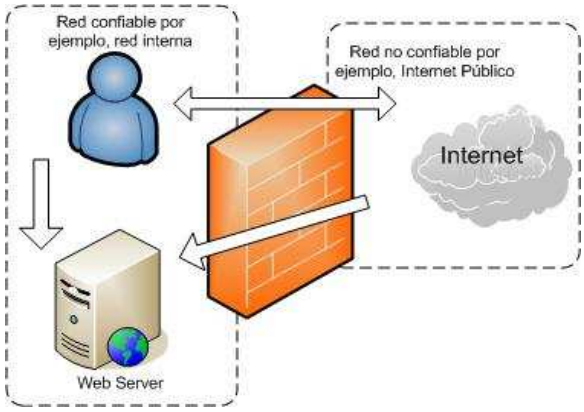


Figura 1.19 Diagrama de arquitectura de firewall screened subnet

Este software utilitario, *firestarter[33]* usa el sistema Netfilter (iptables/ipchains), cuenta con características como monitorización en tiempo real del tráfico de red, reenvío de puertos para la red local, permite compartir la conexión a Internet con otros sistemas sobre una LAN y provee el servicio DHCP, pero tiene el limitante

de que únicamente puede ser configurado para dos interfaces de red, que representan a la red externa y a la red interna.

En el Data Center se han aprovechado las configuraciones de políticas de filtrado de paquetes entrante y saliente, y el reenvío de puertos que este utilitario provee, para cada uno de los equipos con firestarter.

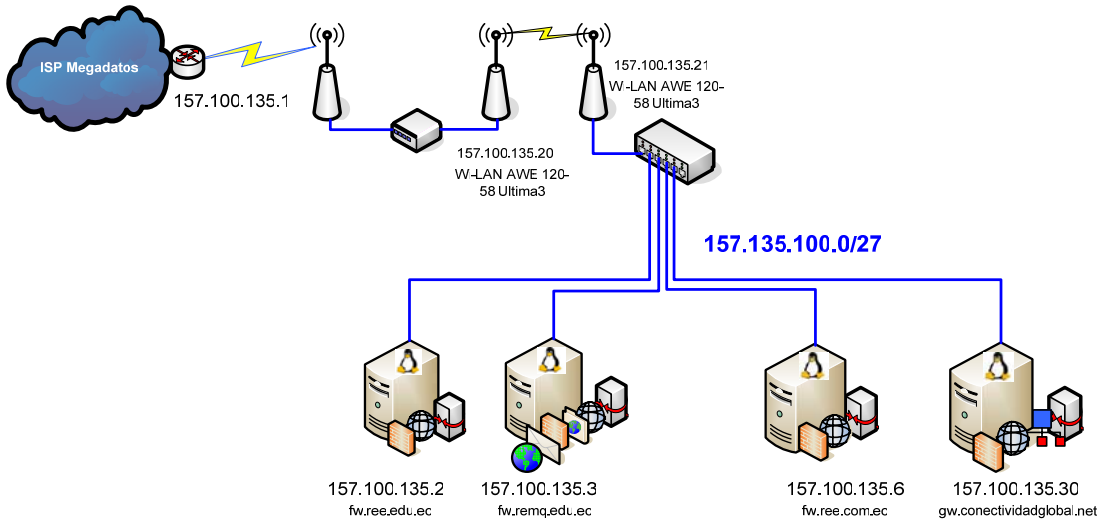


Figura 1.20 Diagrama de arquitectura de firewall del Data Center de Conectividad Global Cia. Ltda.

A continuación, en la Tabla 1.16 se detallan las reglas de filtrado, que especifican los puertos permitidos entrantes/salientes de cada uno de los firewalls, y las reglas de redireccionamiento de puertos.

Hostname	Dirección IP Red Interna	Dirección IP Red Externa	Tráfico permitido				Redireccionamiento de puertos		
			Entrante		Saliente		Puerto entrante	Dirección IP	Puerto Saliente
			Descripción	Puerto	Descripción	Puerto			
fw.ree.edu.ec	192.168.2.1/24	157.100.135.2/27	SSH DNS HTTP WEBMIN	22 53 80 10000	N/A FTP SSH SMTP DNS N/A HTTP APL N/A POP3 IMAP HTTPS SMTPS POP3S SIP N/A N/A WEBMIN	19 20-21 22 25 53 67-68 80 81 106 110 143 443 465 995 5060 8010 8100 10000	19 20-21 25 80 81 106 110 143 443 465 995 5060 8010 10001 2727 3478 4569 5004-5082 5222-5223 10001-20000	192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.1.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2	22 20-21 25 80 81 106 110 143 443 465 995 5060 8010 8100 10000 2727 3478 4569 5004-5082 5222-5223 10001-20000
w.remq.edu.ec	192.168.1.1/24	157.100.135.3/27	FTP SSH SMTP DNS HTTP POP3 N/A IMAP N/A N/A HTTPS N/A N/A N/A N/A MSN MySQL WEBMIN KERIO	20-21 22 25 53 80 110 119 143 389 442 443 465 563 636 993 1863 3306 10000 44337	N/A FTP SSH SMTP DNS DHCP HTTP APL POP3 N/A IMAP N/A N/A HTTPS N/A N/A N/A MSN N/A MySQL RDP N/A N/A N/A N/A WEBMIN N/A KERIO ePOP	19 20-21 22 25 53 67-68 80 81 110 119 143 389 442 443 465 563 636 993 995 1863 2727 3306 3389 4569 5004-5082 5222-5223 8900 9090 10000 10001-20000 44337 61000	19 81 2727 3389 4569 5004-5082 5222-5223 8900 9090 10001-20000 61000 1270 3478	192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.3 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.3 192.168.1.3 192.168.1.2	22 80 2727 3389 4569 5004-5082 5222-5223 10000 9090 10001-20000 61000 1270 3478

Tabla 1.16 Reglas de filtrado de los firewalls alojados en el Data Center de Conectividad Global Cía. Ltda.

fw.ree.com.ec	172.20.0.2/24	157.100.135.6/27	SSH SMTP DNS HTTP N/A POP3 IMAP HTTPS RDP MSN WEBMIN	22 25 53 80 82 110 143 443 3389 1863-65535 10000	FTP SSH SMTP DNS DHCP HTTP APL N/A POP3 HTTPS MSN RDP WEBMIN ePOP	20-21 22 25 53 67-68 80 81 82 110 443 1863 3389 10000 61000	20-21 25 80 81 110 143 443 3389 10100 61000	172.20.0.12 172.20.0.4 172.20.0.4 172.20.0.7 172.20.0.4 172.20.0.4 172.20.0.4 172.20.0.7 172.20.0.45 192.168.1.3	20-21 25 80 80 110 143 443 3389 3000 61000
gw.conectividadglobal.net	172.20.0.45/24	157.100.135.30/27	FTP SSH SMTP DNS HTTP APL POP3 IMAP HTTPS MSN RDP WEBMIN	20-21 22 25 53 80 81 110 143 443 1863-65535 3389 10000	FTP SSH SMTP DNS HTTP APL POP3 IMAP HTTPS MSN RDP N/A N/A WEBMIN	20-21 22 25 53 80 81 110 143 443 1863-65535 3389 8010 8100 10000			

Tabla 1.16 Reglas de filtrado de los firewalls alojados en el Data Center de Conectividad Global Cía. Ltda. (continuación)

Como se puede ver en la tabla anterior, en los firewalls fw.ree.com.ec y gw.conectividadglobal.net existen puertos que se encuentran abiertos desde el Internet a la red interna para aplicaciones como Windows Messenger. Además se puede apreciar que se ha permitido el paso de paquetes entrantes de puertos 1863 hasta el 65535 a la red interna 172.20.0.0/24 de forma innecesaria.

Se puede observar también que en los firewalls fw.ree.edu.ec y fw.ree.com.ec se realiza un redireccionamiento a hosts que se encuentran en otras redes, lo cual no es posible con este utilitario puesto que para este redireccionamiento se requiere de una configuración avanzada de iptables.

1.3.1.3. Seguridad en los recursos de red

La seguridad en las comunicaciones está enfocada a los componentes que se encargan de proveer seguridad a los recursos de la red tal como computadores o servidores.

1.3.1.3.1. Aseguramiento de sistemas informáticos

Para la instalación y puesta en marcha de un nuevo sistema se debe realizar un proceso para el aseguramiento que se denomina ***hardening***[12] con el objetivo de descartar vulnerabilidades inherentes en el sistema operativo. Este proceso involucra implementaciones de seguridad que generalmente se pasan por alto pero que disminuyen significativamente los riesgos que conlleva el acarreo de vulnerablidades.

El personal de Conectividad Global Cía. Ltda., no posee controles o procedimientos que permitan al personal técnico realizar un hardening adecuado a los sistemas informaticos basados en plataformas Linux o Windows que se instalan, configuran y se ponen en funcionamiento.

1.3.1.3.2. Firewalls personales

Personal Firewall es un término que se refiere a los firewalls que protegen al único host sobre el cual ellos residen.

El firewall de Windows está instalado y habilitado por defecto en los sistemas operativos modernos (superiores a Windows XP y Windows 2003). El firewall personal para Linux, está implementado mediante Netfilter.

En la empresa, los servidores con plataformas Windows utilizan Windows Firewall, con la configuración por defecto. Los diferentes servidores con

---

[12] **Hardening**: proceso de aseguramiento de un sistema al reducir su rango de vulnerabilidades.

plataformas Linux no tienen reglas de filtrado de paquetes que realicen funciones de firewall personal.

1.3.1.3.3. Antivirus

Conectividad Global Cía. Ltda. no cuenta con software Antivirus licenciado, por lo que se ha instalado antivirus de ediciones libres como el AVG Free Edition (que no hace un escaneo en tiempo real cuando se suscita un ataque de virus) en los computadores cliente de la empresa que tienen instalado Windows XP, pero no se ha estandarizado un software de antivirus para la empresa.

Cabe destacar que se generaron problemas en el mes de Febrero con el troyano Kavo.exe en las máquinas cliente, que se transmitía por los dispositivos de almacenamiento USB de los empleados de la empresa.

La responsabilidad por mantener al antivirus actualizado va por cuenta del usuario del computador. No se hacen escaneos periódicos de los computadores, no hay un procedimiento, ni se asignó algún responsable para que realice esta tarea.

Además no se cuenta con políticas o procedimientos de análisis de virus en dispositivos de almacenamiento extraíbles o Laptops, los cuales no están siempre conectados a la red, o acerca de descargas de software desde el Internet.

Los servidores de la empresa implementados sobre plataformas Windows como: dc.conectividadglobal.net, sga.conectividadglobal.net, rev.conectividadglobal.net, testserver.conectividadglobal.net, no tienen ningún software antivirus instalado.

Sin embargo, los servidores Linux de Correo Electrónico: correo.conectividadglobal.net y correo.remq.edu.ec, son los únicos que cuentan con motor Antivirus McFee, por defecto, embebido en el software Kerio MailServer version 6.2.1 para el servicio de correo electrónico, pero no está actualizado, puesto que este requiere de una licencia anual, que no ha sido renovada desde el año 2007.

1.3.1.3.4. Encriptación de Información Sensitiva

La información sensitiva y que representa una ventaja competitiva de la empresa está plasmada por las aplicaciones desarrolladas, y el control del desarrollo de código fuente de las aplicaciones se realiza mediante el programa ***Microsoft Visual Source Safe***, el cual no permite una encriptación de los datos.

Respecto a la protección del código fuente de los instaladores de las aplicaciones, se puede mencionar que es realizado utilizando la herramienta comercial Dotfuscator Professional. Pero los respaldos del código fuente o de otro tipo de información que generalmente se realiza sobre unidades externas como cds o dvds no se encuentran encriptados.

1.3.1.4. Seguridad en los Servicios

La seguridad en los servicios está dirigida a los componentes que se encargan de proporcionar los servicios TCP/IP implementados en el Data Center.

Cabe recalcar que algunos equipos ejecutan varios servicios simultáneamente por lo que se repetirán las referencias de análisis.

1.3.1.4.1. Correo Electrónico

Conectividad Global Cía. Ltda. administra dos sistemas de correo electrónico comercial: uno denominado Kerio Mail Server versión 6.2.1 que sirve a la intranet de la empresa y a usuarios de los servicios de la Red Educativa Metropolitana, el cual está implementado bajo plataforma Linux; otro servidor de correo electrónico que utiliza el software Communigate Pro Communication Server version 5.1-10 sobre el servidor correo.ree.edu.ec, maneja el dominio ree.edu.ec para correos internos de la empresa debido a que está en pruebas para posteriormente sacarlo a producción.

El manejo de Kerio Mail Server se lo realiza a través de una consola de administración gráfica propietaria accedida mediante autenticación de contraseña, a través de la dirección IP y del puerto 44337 del servidor permitiendo realizar tareas de gestión sobre Kerio Mail Server. El Web Mail que maneja este aplicativo utiliza HTTP sobre Secure Sockets Layer, HTTPS, implementado a través de un certificado digital con un esquema de 1024 bits con algoritmo de firma md5RSA no firmado por una entidad certificadora instalado sobre el mismo servidor, que es presentado a los usuarios que utilizan un web browser para acceder y utilizar a sus cuentas de correo.

Los servidores de correo elelctrónico basados en Kerio Mail Server están configurados para no permitir a usuarios de Internet usar el servidor de correo electrónico como un Mail Relay, no tienen establecido el tamaño máximo de mensajes entrantes, el número de conexiones SMTP concurrentes desde una misma dirección IP, ni el máximo número de recipientes desconocidos que previenen ataques de Directory Harvest, y no tienen configurado de forma correcta el motor antivirus Mcfee puesto que no se encuentra actualizado por lo que no se realiza un chequeo de virus para mensajes que entran y salen del servidor. Además este software cuenta con un filtro antispam utilizando la aplicación SpamAssassin.

Kerio Mail Server permite asegurar protocolos necesarios para el envío/recepción de correo electrónico utilizando Secure Sockets Layer (SSL) como Secure POP3 (POP3S), Secure SMTP (SMTPS), Secure IMAP (IMAPS).

Cuando el servidor SMTP intenta enviar un mensaje a un servidor SMTP remoto usa en primer lugar una conexión encriptada (SSL), si SSL no es soportada, por dicho servidor SMTP remoto será usada una conexión desencriptada.

Se tiene configurados respaldos de forma automática sobre el mismo equipo en periodos semanales, realizando respaldos diferenciales diarios a la 1:00 a.m. y respaldos totales los días domingos a la 1 a.m.

El personal de administración de red del Data Center tiene la responsabilidad de mantener los servicios de correo electrónico disponibles en ambos equipos, se

encarga de la inserción de nuevos dominios, administración de usuarios del servicio de todos los dominios excepto del dominio remq.edu.ec puesto que el personal técnico del Proyecto QuitoEduca.Net se encarga de la administración de las cuentas de usuarios.

1.3.1.4.2. Sistema de Nombres de Dominio

El Data Center utiliza los servidores fw.ree.edu.ec, fw.remq.edu.ec, fw.ree.com.ec y gw.conectividadglobal.net configurados de forma autoritativa para su propio dominio e implementados sobre la distribución de Linux Red Hat Enterprise release 4 mediante el paquete bind versión 9.2.4, la misma que tiene la característica de enjaular al servicio named, que provee la resolución de nombres de dominio, de forma que pueda ser ejecutado como usuario no–root.

Ambos equipos se usan para la resolución de nombres del Internet y de la intranet, es decir, que se revela información interna a usuarios de Internet. Además no se cuenta con registros reversos de los recursos en el DNS del ISP Megadatos.

En la configuración de este servicio no se ha considerado características de seguridad que permitan el uso adecuado de este servicio, puesto que no se han establecido las opciones que permiten:

- Especificar desde que host se reciben actualizaciones de las zonas de transferencia de forma automática.
- Enviar las zonas de transferencia a otros servidores de DNS.
- Especificar que hosts pueden realizar consultas sobre las zonas y sus reversas.

1.3.1.4.3. Web

Apache Web Server ofrece seguridad cuando inicia el servicio con usuario root en el puerto TCP 80 y lo cambia al usuario y grupo de los demonios httpd hijos establecidos en el archivo de configuración httpd.conf. La configuración por

defecto, de este usuario y grupo es “nobody”, permitiendo con ello no proveer privilegios de root a los procesos de Apache. No se revisan liberaciones de nuevas actualizaciones de este software para su posterior actualización, tampoco se han considerado las vulnerabilidades de la versión de Apache instalada.

Servicio Web para las aplicaciones Sistema de Gestión Académica y Red Educativa Virtual

No se han realizado procedimientos para una configuración apropiada para asegurar el servicio web basado en Internet Information Server para la instalación de las aplicaciones de la empresa sobre los equipos de las Instituciones Educativas.

Portal de Administración de Contenido

Para la creación y administración de contenido de páginas web se utilizan paquetes de Código Abierto, que usan php4 y MySQL Database Server, que permiten un nivel de autenticación a través de usuario-contraseña para el acceso a la administración del contenido del sitio Web.

No se han establecido usuarios específicos para el acceso a cada base de datos que requiere cada uno de los sitios Web en el servidor MySQL Server, sino que utilizan la cuenta de usuario root de MySQL Server para el acceso a cada base de datos que contiene la información de cada sitio Web alojado.

1.3.1.4.4. Ssh y scp

Para acceder a los distintos servidores del Data Center cuyo sistema operativo sea una distribución de Linux se utiliza este protocolo desde una terminal virtual en equipos cliente Linux utilizando el comando ssh <user@host>, o desde equipos cliente con sistema operativo Microsoft Windows utilizando el aplicativo putty.exe.

Además se utiliza el protocolo Secure Copy, ***SCP***, para copiar un archivo desde un equipo a otro. En ocasiones también se utiliza la aplicación WinSCP para copiar archivos desde Linux hacia Windows.

1.3.1.4.5. Seguridad en las aplicaciones

La instalación y operación del Sistema de Gestión Académica se la realiza sobre un servidor en la red de las instituciones Educativas, requiriéndose para ello programas complementarios: Microsoft .Net Framework version 1.1 y version 2.0, y SQL Server Database Engine 2005, y si se requiere utilizar la Red Educativa Virtual se necesita de un equipo Terminal SkyConnector instalado en la institución Educativa para la importación/exportación de consultas SQL desde/hacia la aplicación de la Red Educativa Virtual ubicada en el Data Center hasta el Sistema de Gestion Académica ubicado en las instalaciones del establecimiento educativo mediante el uso de las clases y librerias del Microsoft Framework.

Cabe destacar que existen controles y procedimientos que no se han considerado en el diseño de estas aplicaciones como la generación de registros de error de la aplicación.

1.3.1.4.6. Sistema de Gestión Académica

Esta aplicación alberga la página Web y la base de datos pertenecientes a la institución educativa. Se puede acceder desde cualquier sitio de su red interna mediante autenticación de usuario/password de los profesores, alumnos y padres de familia cuyos registros se encuentran en la base de datos del SGA.

Los niveles de autorización de la conexión de Internet Information Server con la base de datos no han sido planificados debido a que se utiliza la cuenta de super usuario de SQL Server Database Engine 2005 cuando la información de la base de datos es solicitada por la interfaz de usuario de la aplicación.

Para la actualización de una calificación, el SGA durante el proceso genera un registro en el que constan los siguientes campos: usuario, fecha, valores involucrados en una actualización de calificación. En el caso de una nota mal ingresada, no se han creado responsabilidades de ingreso de datos pero verbalmente se ha establecido que, en el caso de suscitarse esta acción la responsabilidad recaerá sobre el profesor de la institución que ha ingresado de forma incorrecta la calificación.

Para verificar que los datos hayan sido correctamente ingresados, no se han implementado controles que permitan la detección de datos corrompidos por errores de procesamiento o por actos deliberados.

El control de errores del procesamiento interno de la aplicación se lo ha realizado a través de clases de control de excepciones para personalizar el mensaje de error, salvo los casos en los cuales dichos errores sean de tipo desconocido, para este tipo de excepciones se generará un mensaje de error del sistema.

Además no se ha llevado a cabo una evaluación de riesgos para determinar si es requerida la confidencialidad en las transacciones.

1.3.1.4.7. Red Educativa Virtual

La Red Educativa Virtual permite la publicación de los datos de consultas de Microsoft SQL Server Engine a través de un portal Web basado en código HTML desde el cualquier equipo conectado a Internet.

Esta aplicación aloja la página Web de login de cada institución educativa. Es utilizada para acceder a la información desde el Internet previa autenticación de los registros de usuarios ubicados en la base de datos del SGA. Un ejemplo de la página de autenticación se muestra en la Figura 1.21.

Al igual que el SGA, la conexión que se realiza desde la aplicación Red Educativa Virtual a la base de datos del equipo de la Institución Educativa que tiene

instalado el SGA utiliza niveles de autorización a nivel de super usuario del Microsoft SQL Server Engine.

Figura 1.21 Portal de autenticación presentado por la aplicación Red Educativa Virtual

1.3.1.5. Seguridad Física

Control de acceso físico al Data Center

Previo a la implementación del Data Center no se efectuó un análisis acerca de los controles de acceso físico requeridos.

El Data Center se encuentra ubicado en un cuarto que permanece con cerradura mecánica, y de la llave son custodios las personas que integran el área de administración de redes y el gerente general de la empresa, quienes tienen acceso autorizado al Data Center. Éste es el único lugar en el que se tiene control de acceso en la empresa. Además las personas externas a la empresa como personal de soporte técnico de ISPs que requieren acceso a algunos de los equipos del Data Center, son supervisadas por personal del área de

administración de redes, pero no se registra la hora y/o fecha del ingreso, ni la tarea realizada.

La empresa cuenta con guardias de seguridad; en horarios laborales se ubican en el exterior del edificio, mientras que fuera de estos horarios el servicio de vigilancia privada permanece en la planta baja. No hay tarjetas magnéticas de entrada ni llaves cifradas requeridas para controles de autenticación en ningún lugar de la empresa.

Control de acceso a los sistemas

Todos los equipos servidores permiten la instalación de hardware de almacenamiento externo como disqueteras, unidades lectoras de CD/DVD, y dispositivos de almacenamiento USB. No existe ningún control sobre el acceso de estos dispositivos al Data Center, los servidores no tienen establecida una contraseña en el BIOS.

Para los servidores que tienen instalados sistemas operativos Linux se puede cambiar la contraseña del usuario root debido a que no se tiene establecida una contraseña que impida la modificación del programa GRUB.

Además cabe recalcar que no se ha hecho una gestión de usuarios sobre los servidores sino que, cuando un empleado del área de Tecnologías de la Información solicita acceso a un servidor, se le permite utilizar la cuenta root o administrador que proporciona acceso total a los recursos del servidor desde la intranet. Se puede acceder a los equipos que realizan tareas de firewall a través del protocolo ssh versión 2 con la cuenta root desde Internet.

No se realizan controles periódicos sobre los dispositivos de hardware instalados en las computadoras de los empleados de la empresa, de manera que alguien podría extraer o instalar algún dispositivo. No se encuentran deshabilitados las interfaces USB de los equipos del personal de desarrollo.

Una vez que se ha completado la instalación de algún servidor, el administrador de la red no realiza chequeos rutinarios o periódicos del hardware, solo revisa los equipos ante fallas de los mismos, o por un problema reportado por algún usuario.

Estructura del Edificio

Las paredes externas del cuarto que alberga al Data Center son de concreto y del mismo grosor que las paredes de todo el piso del edificio, no tiene ventanas, pero posee un techo falso sobre el cual pasa el cableado de la red de datos.

1.3.1.6. Herramientas de Software

Las herramientas de escaneo de red se utilizan para probar la efectividad de los controles de seguridad de un sistema IT y cómo han sido aplicados en un ambiente operacional sobre la red interna.

Para el escaneo de redes, se utilizó el software ***Nessus***, para lo cual se instaló en un computador de escritorio desde el cual se realizó la tarea de exploración de vulnerabilidades. Cabe aclarar que esta herramienta de escaneo de redes puede producir falsos positivos.

La Figura 1.22 muestra un ejemplo del escaneo de vulnerabilidades realizado para el servidor correo.conectividadglobal.net. y testserver.conectividadglobal.net.

producir falsos positivos.

La Figura 1.22 muestra un ejemplo del escaneo de vulnerabilidades realizado para el servidor correo.conectividadglobal.net. y testserver.conectividadglobal.net.

producir falsos positivos.

La Figura 1.22 muestra un ejemplo del escaneo de vulnerabilidades realizado para el servidor correo.conectividadglobal.net. y testserver.conectividadglobal.net.

172.20.0.4

Scan time :

Start time :	Wed Jul 2 18:33:46 2008
End time :	Wed Jul 2 21:36:08 2008

Number of vulnerabilities :

Open ports :	27
Low :	87
Medium :	25
High :	3

Information about the remote host :

Operating system :	Linux Kernel 2.6 on Red Hat Enterprise Linux 4
NetBIOS name :	(unknown)
DNS name :	(unknown)

[^] Back to 172.20.0.4

[^] Back

172.20.0.5

Scan time :

Start time :	Tue Jul 22 17:58:49 2008
End time :	Tue Jul 22 18:01:58 2008

Number of vulnerabilities :

Open ports :	22
Low :	41
Medium :	5
High :	8

Information about the remote host :

Operating system :	Microsoft Windows Server 2003
NetBIOS name :	TESTSERVER
DNS name :	(unknown)

[^] Back to 172.20.0.5

Figura 1.22 Reporte general del escaneo de vulnerabilidades utilizando Nessus para un servidor en Linux y uno en Windows

1.3.2. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA RED INFORMÁTICA DEL DATA CENTER

El objetivo del diagnóstico es identificar las falencias de la seguridad informática del Data Center respecto a la norma ISO/IEC 17799 [13] para la determinación de controles a implementarse para asegurar la disponibilidad, integridad y confidencialidad de la información y de la infraestructura informática que dispone el Data Center. Para este diagnóstico se examinó la manera como Conectividad Global Cía. Ltda. gestiona la seguridad usando como referencia cada una de las áreas de la norma, y además tomando en cuenta los indicadores enfocados a cada área de gestión de seguridad de esta norma, documentados en el Anexo E.

1.3.2.1. Política de Seguridad

Conectividad Global Cía. Ltda. no cuenta con normas, políticas o procedimientos de seguridad formales, aprobados y respaldados por el personal de la empresa, esta es la mayor debilidad en la gestión de seguridad de información. Ante la ausencia de una política de seguridad, cada grupo o persona del Departamento de Tecnologías de la Información ha definido su propia política de seguridad.

1.3.2.2. Organización de la Seguridad de la Información

Conectividad Global Cía. Ltda. no cuenta con una estructura organizativa de seguridad que se responsabilice de la gestión de la seguridad, ni una asignación de responsabilidades de los activos puesto que no se cuenta con políticas de seguridad definidas o documentadas, razón por la cual no se realizan actividades enfocadas a la seguridad de la información con el personal que labora en la empresa de forma que no existe una coordinada gestión de la seguridad ya que se encuentra dispersa en las diferentes áreas del Departamento de Tecnologías

de la Información, y no se han hecho esfuerzos en involucrar a esta gestión con el establecimiento de políticas de seguridad, aspectos legales y gestión de riesgos.

No se han establecido acuerdos de confidencialidad o de no-divulgación para los empleados que laboran en la empresa, que son necesarios para la protección de la información confidencial de forma legal.

Los requisitos de seguridad necesarios para asegurar el acceso a la información o a los sistemas de procesamiento a la que pueden acceder los usuarios de las instituciones educativas a través de la red Inalámbrica MAN Skypilot no han sido definidos. No se ha realizado o planificado ningún tipo de auditoría de seguridad.

1.3.2.3. Organización de Activos

No existe un inventario de los activos informáticos de la empresa (hardware, software, datos, servicios, etc.) que los abarque de forma completa y detalle su importancia para la organización. Al no existir este inventario el nivel de protección en términos de confidencialidad, integridad y disponibilidad u otro requerimiento de seguridad, no podría ser claramente establecido.

Se ha delegado por parte del gerente de la empresa como custodios o propietarios[13] de las aplicaciones SGA y REV al Jefe del área de desarrollo de Software; de los sistemas de procesamiento de información a los administradores de sistemas, y de elementos o dispositivos que permiten la conectividad entre los sistemas de información a los administradores de Red. De forma que el personal designado se responsabilice del funcionamiento y de seguridad de los activos que le corresponden.

Con respecto a la clasificación de la información como activo de la empresa, no se ha asignado un valor de protección adecuado a todos los activos en términos de valor monetario, requisitos legales, criticidad y sensibilidad.

---

[13] **Propietario:** identifica al individuo o entidad que ha probado habilidades de gestión para controlar la producción, mantenimiento, uso y seguridad de un activo. El término propietario no significa que la persona tienen efectivamente derechos de propiedad sobre el activo.

1.3.2.4. Seguridad de Recursos Humanos.

En la empresa existen políticas para esta área, enfocadas en el servicio al cliente y al personal que labora en la empresa para Personal en Relación de Dependencia o Prestador de Servicios, pero no se hace mención a la gestión de seguridad de la información, referida a roles y responsabilidades que deben cumplir cada uno de los empleados y seguridad en la selección de personal. Tampoco se han definido condiciones de confidencialidad y responsabilidades en los contratos puesto que la empresa no cuenta con políticas de seguridad establecidas claramente.

No existe una formación para el personal nuevo en materia de seguridad en el que se expliquen canales y procedimientos a seguir en caso de incidentes de seguridad y para informar sobre vulnerabilidades observadas o sospechadas.

1.3.2.5. Seguridad Física y del Ambiente

El Data Center cuenta con su propio perímetro de seguridad física, puesto que se encuentra operando en un área aislada del resto de la empresa, con una puerta asegurada con llave, de la que son custodios el área de Administración de redes y el gerente de la empresa.

Cuenta con protecciones físicas contra fuego y acceso indebido. Los Sistemas de energía ininterrumpida (UPSs) se encargan de la protección eléctrica. Sin embargo, las condiciones ambientales como humedad y temperatura del Data Center no son monitorizadas periódicamente.

Cabe recalcar que cuando se suscita una suspensón del servicio eléctrico sólo puede ser soportada por un lapso de 10 minutos puesto que no se cuenta con un sistema de Energía eléctrica ininterrumpida (UPS) óptima, razón por la cual no se puede asegurar la disponibilidad de los servicios.

El sistema de cableado estructurado de la red de datos, se encuentra asegurado contra daños puesto que el cable UTP categoría 5e no apantallado se encuentra montado sobre las paredes de las instalaciones de la empresa y recubierto por canaletas. El acceso físico a los puestos de trabajo de los empleados, donde existen estaciones de trabajo, impresoras y otros equipos, no está regulado por mecanismos y procedimientos formales que limiten el acceso a terceros o personas externas a la empresa.

El mantenimiento de los equipos se lo realiza de manera general cada 6 meses por personal del área de administración de Red y de Sistemas y no se documenta el estado de los equipos en revisión. Las bitácoras de eventos que son generadas por el sistema operativo de los sistemas no son almacenadas, y sólo se revisan cuando se realiza un mantenimiento correctivo del equipo. Se informa al Gerente General si se requiere un mantenimiento correctivo de un equipo por una empresa externa.

1.3.2.6. Gestión de las Comunicaciones y Operaciones.

La gestión básica de los sistemas computacionales y de comunicación (operación, cambios, actualización de antivirus, etc.) no se realiza con procedimientos operativos formales ni documentados. La empresa dispone de ambientes independientes de desarrollo y producción (desarrollo y pruebas de nuevos servicios y/o productos).

A continuación se detallarán ciertos aspectos de la empresa relacionadas a esta gestión que no se encuentran establecidas ni documentadas:

- Establecimiento claro de responsabilidades y tareas para un control de cambio en los equipos.
- Manejo de incidentes de seguridad para asegurar una respuesta rápida, ordenada y efectiva que incluya auditoria, planes de contingencia y recuperación.

- Controles que permitan evitar mal uso de datos, privilegios y servicios de las Instituciones Educativas con la empresa, como para el mejoramiento de su provisión.
- Planeamiento de Capacidad para evitar fallas de los sistemas y asegurar un adecuado desempeño de proceso y almacenamiento de información para los requerimientos futuros.
- Procedimientos de actualización y/o aceptación de nuevas versiones de los servicios de Intranet.
- Controles para prevención de software malicioso sobre servidores y computadores del personal.
- Gestión de bitácoras de eventos de las actividades realizadas por los operadores y administradores.
- Copias de backup de la información esencial para la empresa.
- Procedimientos de seguridad en el acceso a recursos de la intranet sobre redes públicas de datos.
- Intercambio controlado con otras empresas en relación a acuerdos de datos y software, acuerdos de acceso a sistemas y seguridad de correo electrónico.
- Documentación y aseguramiento de los Sistemas de Información.
- Protección de los medios de almacenamiento de acceso no autorizado, robo o corrupción de datos.
- Políticas y procedimientos para proteger los sistemas de información de amenazas provenientes de la red SkyPilot.
- Procedimientos de instalación, configuración, aseguramiento y mantenimiento de servidores, routers y switches.

1.3.2.7. Control de Acceso.

Conectividad Global Cía. Ltda. no cuenta con una política y procedimientos de control de acceso para la gestión de acceso a los recursos informáticos y computacionales de la empresa que expresen una administración de usuarios en relación al registro y dada de baja de usuarios, passwords, niveles de autorización para control y restricción de asignación de privilegios en entornos multiusuario, acceso a la red, acceso remoto, ni registros de eventos de acceso y auditoria sobre los recursos informáticos de la empresa.

Para acceder remotamente a los sistemas basados en distribuciones de Linux se utiliza el servicio ssh con autenticación username/password.

Además cabe recalcar que la administración de usuarios se la realiza de manera irregular puesto que se trabaja con plataformas Windows y Linux y no se ha hecho hincapié en cuentas de usuario que definan un nivel de autorización para cada servidor al que se necesite acceder a sus recursos, puesto que para el control de acceso a los recursos de la intranet de la empresa que sean de plataformas Windows se lo realiza a través del Controlador de dominios de Microsoft Windows Server 2003 utilizando el servicio de Active Directory, y el acceso a los sistemas operativos Linux se permite a cualquier empleado del departamento de Tecnologías de la Información que lo requiera utilizando la cuenta de súper usuario.

1.3.2.8. Desarrollo y Mantenimiento de los Sistemas de Información.

No existen controles o procedimientos documentados a seguir para el aseguramieto de nuevos sistemas computacionales que se instalen. Este tipo de aseguramientos generalmente no son considerados.

Los sistemas computacionales que utilizan sistemas operativos Microsoft Windows son instalados de acuerdo a las caracteristicas de seguridad

configuradas por defecto por el fabricante y no son personalizadas de acuerdo a los activos de información que éstos alberguen.

Los sistemas computacionales que utilizan sistemas operativos basados en disctribuciones de Linux, no tienen configuradas caracteristicas adicionales de seguridad como: aseguramiento de los sistemas de archivos, recompilacion del kernel, aplicaciones de parches, configuración de firewall personal basado en iptables, actualización de paquetes instalados, desactivación de servicios innecesarios, etc.

En las aplicaciones desarrolladas por la empresa los requerimientos de seguridad para el desarrollo y mantenimiento de éstas se han considerado parcialmente, puesto que existen controles que no han sido considerados en la fase de diseño de estas aplicaciones, entre ellos se podría mencionar que estas aplicaciones no cuentan con registros de error de ingreso de datos, pero existen clases basadas en lenguaje C#, que se encargan del control de excepciones de error, dando respuesta a errores de ingreso de datos al momento que se susciten, salvo el caso en los cuales dichos errores sean de tipo desconocido, en este caso de excepciones se genera un mensaje de error del sistema. Para verificar que los datos hayan sido correctamente ingresados, no se han implementado controles que permitan la detección de datos corrompidos por errores de procesamiento o por actos deliberados pero podrían hacerse mediante consultas manuales a la base de datos del SGA. Existen procedimientos documentados acerca de la instalacion del Sistema de Gestión Académica (SGA) pero no se han documentado controles acerca de otro software que podría ser instalado sobre los sistemas operacionales que tengan instalado el SGA. La información para el procesamiento de estas aplicaciones es obtenida de una base de Datos utilizando el motor del sistema de gestión de base de datos relacionales Microsoft SQL Server 2005.

El control para modificaciones al código fuente de las aplicaciones “Sistema de Gestión Académica” y “Red Educativa Virtual” es realizado a través del programa Microsoft Visual Source Safe. El acceso al código fuente de las aplicaciones no está estrictamente controlado puesto que cualquier empleado que se encuentre

registrado en el Controlador del Dominio puede acceder al equipo que aloja al código fuente.

1.3.2.9. Gestión de los Incidentes de la Seguridad de la Información

No se han establecido canales de administración que permitan comunicar eventos de seguridad de información y debilidades asociadas con los sistemas de información para permitir una acción correctiva lo más pronto posible.

1.3.2.10. Gestión de la Continuidad del Negocio.

No existe un plan de continuidad del negocio para afrontar eventos catastróficos. Existen algunas medidas informales que han sido tomadas por diferentes áreas del departamento IT, de manera aislada e independiente:

- El código Fuente de las aplicaciones desarrolladas por la empresa se encuentra en custodia en el domicilio del gerente general de la empresa.
- Respaldo o recuperación de las bases de datos del Sistema de Gestión Académica y de la Red Educativa Virtual por parte del Área de desarrollo pero sin hacer seguimiento de procedimientos.
- Se realizan respaldos automáticos de los archivos de correo electrónico sobre los servidores que proveen este servicio, pero no se copian en medios extraíbles.
- No se ha documentado procedimientos para respaldar y recuperar los portales de administración de contenido que utilizan LAMP, sino que se los realiza de manera informal.

1.3.2.11. Cumplimiento

Esta es un área que se ha pasado por alto debido principalmente a que no se mantiene ninguna política que defina el uso o derechos de propiedad intelectual de las aplicaciones creadas por la empresa. Tampoco se han especificado claúsulas en los contratos de los empleados que protejan a los datos, activos contra própositos no autorizados, e información privada de la organización.

1.3.3. ANÁLISIS DE RIESGOS.

El diagnóstico previo nos permitió mostrar las distintas debilidades de la gestión de la seguridad en la información. Estas debilidades pueden generar riesgos para la seguridad de la información y afectar de forma negativa la operación de los servicios del Data Center.

Por lo expuesto anteriormente se debe efectuar una administración de riesgos para su identificación y valoración, para implementar medidas que reduzcan los riesgos a un nivel aceptable, permitiendo a los administradores IT balancear los costos económicos y operacionales de medidas de protección para el cumplimiento de la misión de la organización al proteger lo sistemas IT y los datos que mantiene.

Existen varias metodologías de administración de riesgos. Se ha seleccionado la ***Guía de la Administración de Riesgos para los Sistemas de Información Tecnológica SP800-30*** del Instituto Nacional de Estándares y Tecnología (NIST)[14] para este propósito, debido a que esta metodología está más acorde con la situación actual de la infraestructura tecnológica del Data Center. Cabe recalcar que no se ha realizado un análisis de riesgos y, mediante esta metodología se proporcionará un inicio para el desarrollo de un programa de administración de riesgos, con el fin de proteger a la organización y su habilidad para cumplir su misión, conteniendo tanto las definiciones, así como, una guía para la valoración de riesgos identificados dentro de los sistemas IT.

La metodología NIST se refiere precisamente a la valoración de riesgos describiendo el proceso de valoración, identificación, su impacto y una recomendación de medidas para su reducción.

1.3.3.1. Valoración de Riesgos

La administración de riesgos es el primer proceso en esta metodología y se usa generalmente para determinar la medida de las amenazas potenciales y el riesgo asociado con el sistema IT para identificar apropiados controles para reducir o eliminar riesgos. Esta guía define al riesgo como "una probabilidad de que una amenaza dada aproveche una particular y potencial vulnerabilidad, y el impacto resultante de ese evento hostil sobre la organización". Para determinar la probabilidad de un futuro evento de naturaleza hostil, se debe analizar las amenazas a un sistema IT.

1.3.3.1.1. Identificación de Amenazas

En la valoración de la fuente de las amenazas, es importante considerar todos los conjuntos de amenazas que sean aplicables y que puedan causar daño a un sistema IT y a su ambiente de procesamiento. La Tabla 1.17 muestra los diferentes tipos de amenazas.

Humanas	Naturales	Entorno
Empleado Forcejeo de la seguridad Hacker Cracker Ex-empleado Asociados Asociados de negocios Clientes	Fuego Vibración Terremotos	Infraestructura interna: Servicio Eléctrico Agua Aire Acondicionado Red Interferencia Infraestructura externa: Servicio Eléctrico Internet DNS Interferencia Infraestructura del sistema:

		Hardware Software Aplicación

Tabla 1.17 Tipos de Amenazas

A continuación, en la Tabla 1.18 se puntualizará la motivación y las acciones para llevar a cabo un ataque por parte de las amenazas humanas, cabe destacar que el personal de la empresa no ha llevado reportes de incidentes de la seguridad que afecten a los sistemas IT y a sus datos.

AMENAZA	MOTIVACIÓN	ACCIONES
Hacker, cracker	Reto Ego Rebelión	• Hacking • Ingeniería Social • Intrusión al sistema, robos de información • Acceso no autorizado al sistema
Empleados: Personal del área de desarrollo de software de la empresa no calificado	Curiosidad Errores no intencionales u omisiones	• Errores de Actualización de software • Errores de programación • Datos corruptos • Errores del sistema • Código malicioso (virus, bomba lógica, caballo de Troya) • Manipulación de la configuración • Brechas en la seguridad no detectadas • Negación de Servicio
Usuarios de las aplicaciones desarrolladas por la empresa	Errores no intencionales u omisiones	• Manipulación de la configuración • Error en el ingreso de datos • Errores de Actualización de software • Datos corruptos
Empleados: Personal de la empresa no confiable (deshonestos, descontentos, maliciosos o despedidos)	Ego Inteligencia Ganancia Monetaria Venganza	• Desperdicio • Abuso • Fraude y Robo de información • Sabotaje del sistema • Venta de información de la empresa • Datos corruptos • Errores del sistema • Código malicioso (virus, bomba lógica, caballo de Troya)

		• Copia no autorizada de software • Intrusiones al sistema • Ingeniería Social • Abuso de la autorización en los accesos al Data Center • Manipulación de la configuración • Negación de Servicio • Instalación no autorizada o cambios en software • Búsqueda de Información de la empresa

Tabla 1.18 Amenazas en los recursos Humanos

Empleados: Personal de la empresa pobremente capacitado	Errores no intencionales y omisiones	• Manipulación de la configuración de los sistemas • Divulgación de la Información • Alteración de la configuración de los sistemas • Indisponibilidad del personal • Brechas de seguridad no detectadas • Virus de computación, Fuerza Bruta y ataques de diccionario • Errores de Administración • Instalación no autorizada de software
Intrusos, personal no autorizado	Ganancia monetaria	• Robo • Pérdida de elementos del Data Center • Robo de Información
Asociados de Negocios	Ganancia Monetaria	• Acceso no autorizado y robo de información clasificada y/o propietaria • Copia no autorizada de software

Tabla 1.18 Amenazas en los recursos Humanos (continuación)

El análisis de las amenazas naturales mostrado en la Tabla 1.19 indica las posibles acciones que pueden ocasionar daños sobre el sistema IT. Si no se prepara a la organización ante las posibles acciones de estas amenazas o no son controladas debidamente, pueden ocacionar pérdidas monetarias y de información.

AMENAZA	ACCIONES
Fuego Calor Humedad Vibración Terremoto	• Daño de los activos de la empresa • Afectación a la disponibilidad e integridad de los servicios del Data Center • Pérdida o deterioro de la información de la empresa

Tabla 1.19 Amenazas ambientales

Las amenazas del entorno y sus posibles acciones para afectar la operatividad de la organización se decriben en la Tabla 1.20.

	AMENAZA	ACCIONES
Infraestructura interna	Indisponibilidad del Servicio eléctrico en el Data Center	• afectación a la disponibilidad e integridad de los servicios del Data Center • Pérdida o deterioro de la información albergada en sistemas de información
	Agua	• Daño de los activos de la empresa • Pérdida o deterioro de la información de la empresa
	Interferencia	• Perturbación en la transmisión de información desde/hacia el Data Center
Infraestructura externa	Indisponibilidad del Servicio Eléctrico en lugares donde se hallen instalados los equipos terminales de red inalámbrica	• Afectación a la disponibilidad, integridad de los servicios del Data Center para los usuarios
	Internet DNS Interferencia	• Afectación a la disponibilidad, integridad de los servicios para los usuarios que acceden a través del Internet
Infraestructura del sistema	Fallo o daño en los componentes de Hardware mantenido por el Data Center	• Afectación a la disponibilidad, integridad de los servicios del Data Center • Intrusión al sistema • Daño del sistema • Brecha de seguridad • Pérdida o deterioro de la información de la empresa • Falla en la Configuración de los sistemas • Mantenimiento pobre de los sistemas
	Arquitectura de Seguridad no definida	
	Falla en la Configuración de los sistemas	
	Instalación de Software no autorizado	
	Código malicioso: Virus, gusanos, backdoors, troyanos, etc.	

Tabla 1.20 Amenazas del entorno

1.3.3.1.2. Identificación de las vulnerabilidades

Para el análisis de las vulnerabilidades se toma en cuenta la asociación amenazas-vulnerabilidades, y se genera una lista de vulnerabilidades que puedan ser explotadas por potenciales fuentes de amenazas a los recursos de red del Data Center clasificándolos de acuerdo a los servicios que éstos proporcionan.

Para la identificación de las vulnerabilidades de los activos de la empresa se utilizó como fuente de vulnerabilidades al sitio Web http://www.securityfocus.com, las herramientas de software de escaneo de red nmap y Nessus; y la información obtenida en el análisis y diagnóstico de la situación actual de la seguridad de la información antes expuesta. La Tabla 1.21 muestra la identificación de las vulnerabilidades de acuerdo al recurso que podría generarla, la amenaza específica y la acción que ésta podría tomar.

RECURSOS	VULNERABILIDAD	AMENAZA FUENTE	ACCIÓN DE LA AMENAZA
Recursos Humanos	Cuentas de usuario de los empleados que salen de la empresa no son removidas de los sistemas IT	Empleados que salen de la empresa	Ingresar de forma no autorizada a los recursos del dominio de la intranet de la compañía
	Cuentas de usuario del sistema que hayan sido creadas sobre equipos que accedan de forma directa al Internet	Empleados que salen de la empresa	Deteriorar la integridad del servicio que es realizado por el equipo
	No existen acuerdos de confidencialidad	Empleados que salen de la empresa	Divulgación de información de la empresa
	Manipulación errores de la configuración de los sistemas	Personal de la empresa pobremente capacitado	Indisponibilidad de los servicios del Data Center
	No existen acuerdos definidos para el reemplazo de empleados	Insuficiente Personal	Mantenimiento y indisponibilidad incumplida de los sistemas de Información
	Capacitación inadecuada de usuarios y administradores	Personal de la empresa no calificado.	Sistemas IT no manejados competitivamente
Usuarios de las aplicaciones desarrolladas por la empresa	Falta de planificación en las capacitaciones de las aplicaciones a los usuarios	Personal de la empresa no calificado	Hay errores en la entrada, modificación y eliminación de datos
Firewalls	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker. Personal de la empresa no calificado. Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso. Manipulación de la configuracion
	No existe un procedimiento formal para la realización de respaldos periódicos de los sistemas	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Afectación a la disponibilidad, integridad de los servicios del Data Center

Tabla 1.21 Identificación de las Vulnerabilidades

	No se han establecido reglas de filtrado para contrarrestar ataques de falsificación de direcciones IP	Hackers, crackers	Ataques provenientes del Internet
	No se ha establecido una correcta arquitectura de firewall, donde exista una segmentación DMZ	Hackers, crackers	Intrusiones o acceso no autorizado a los sistemas IT de la red interna
	Este equipo tiene instalado el software Webmin: webmin(10000/tcp)	Hackers, crackers	No se configurado el control de acceso de forma correcta a la herramienta de administración Webmin, el username/password son enviados en texto plano sobre el Internet
	Habilitado el acceso al sistema con cuenta de root, utlizando protocolo Secure shell (ssh)	Hackers, crackers	A través de un ataque de fuerza bruta o por diccionario se podria descubrir la cuenta root del sistema
	Servicios ejecutandose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad
	Demasiados servicios sobre un mismo equipo	Hackers, crackers	Demasiados servicios activos que se ofrezcan al mundo exterior por este equipo incrementan el riesgo de un posible agujero de seguridad sobre este equipo
	Demasiados puertos permitidos en el firewall	Hackers, crackers	El atacante puede usar los puertos abiertos para conectarse al sistema y atacarlo
	Sistemas de tecnologías de la información pobremente mantenidos	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Agujeros de seguridad sobre el sistema operativo y en el software instalado en los servidores. Mayor deterioro de los sistemas por virus o gusanos, o intrusiones por no chequear ni instalar los parches de seguridad disponibles de cada fabricante de software o hardware
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauracion
Servicio de Correo Electrónico kerio Mail Server	Incapacidad para distinguir peticiones autenticas de falsas	Hackers, crackers	Negación de Servicio
	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso. Manipulación de la configuracion
	No existe un procedimiento formal para la realización de respaldos periódicos de la información.	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la información de correos electronicos de los usuarios

Tabla 1.21 Identificación de las Vulnerabilidades (continuación)

	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de correo electronico	Hackers, crackers, spammers	Ataques de virus, spam, archivos adjuntos peligrosos permitiendo su envio/recepcion, y de esta manera se podria comprometer a los equipos remotos desde donde se accedan a estos correos electronicos. El atacante puede conseguir información interna que podria comprometer al sistema como userids, hostnames, etc.
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio de correo electronico
	Este equipo tiene instalado el software Webmin: webmin(10000/tcp)	Hackers, crackers	No se configurado el control de acceso de forma correcta a la herramienta de administración Webmin, el username/password son enviados en texto plano sobre el Internet
	Servicios ejecutandose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad
	La versión 6.2.1 de la aplicación Kerio Mail Server no esta actualizada y tiene vulnerabilidades en el core	Hacker, cracker	Este servidor se halla direccionado desde un firewall a los puertos IMAP, POP, HTTP, HTTPS y SMTP y os atacantes podrían realizar ataques al filtro de vinculación del servicio de correo electrónico, y una posible corrupción de la memoria
	El motor Antivirus embebido en el servicio de correo electrónico no se encuentra actualizado	Código malicioso	Los nuevos virus o algún otro código malicioso sobre archivos adjuntos de correos electrónicos no podrán ser detectados y se pude correr el riesgo de infectar al sistema y/o a los usuarios
	Se encuentra ejecutándose el servicio LDAP de forma innecesaria sobre el servicio de correo electrónico	Hacker, cracker. Personal de la empresa no calificado	Existiría un ataque de negación de Servicio de correo electrónico, si se usase LDAP para autenticar a los usuarios de correo electronico, si el atacante utilizando el usuario anónimo enviase solicitudes de búsqueda malformadas, negaría el acceso al servicio a usuarios legítimos
Servicio de Correo Electrónico Communigate Pro Communication Server	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de correo electronico	Hackers, crackers, spammers	Ataques de virus, spam, archivos adjuntos peligrosos, y no se puede comprometer al servidor de correo electronico. El atacante puede conseguir información interna que podria comprometer al sistema como userids, hostnames, etc.
	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso Manipulación de la configuracion

Tabla 1.21 Identificación de las Vulnerabilidades (continuación)

	Este equipo tiene instalado el software Webmin: webmin(10000/tcp)	Hackers, crackers	No se configurado el control de acceso de forma correcta a la herramienta de administración Webmin, el username/password son enviados en texto plano sobre el Internet
	Servicios ejecutandose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad
	No se encuentran instalados programas antivirus, ni antispam para chequeos de correos electrónicos	Hackers, crackers, spammers	Ataques de virus, spam, archivos adjuntos peligrosos permitiendo su envio/recepcion, y de esta manera se podria comprometer a los equipos remotos desde donde se accedan a estos correos electronicos El atacante puede conseguir información interna que podria comprometer al sistema como userids, hostnames, etc.
Servicio DNS	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de correo electronico	Fuego Hackers, crackers, spammers	Ataques de virus, spam, archivos adjuntos peligrosos, y no se puede comprometer al servidor de correo electronico. El atacante puede conseguir información interna que podria comprometer al sistema como userids, hostnames, etc.
	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso. Manipulación de la configuracion
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio DNS.
	Este equipo tiene instalado el software Webmin: webmin(10000/tcp)	Hackers, crackers	No se configurado el control de acceso de forma correcta a la herramienta de administración Webmin, el username/password son enviados en texto plano sobre el Internet
	Servicios ejecutandose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad
	Demasiados servicios sobre un mismo equipo	Hackers, crackers	Demasiados servicios activos que se ofrezcan al mundo exterior por este equipo incrementan el riesgo de un posible agujero de seguridad sobre este equipo
	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de resolucion de nombres	Hackers, crackers, spammers	El mismo equipo se encarga de la resolución de nombres del Internet y de la intranet, permitiendo la revelación de información interna a usuarios de Internet

Tabla 1.21 Identificación de las Vulnerabilidades (continuación)

	No se cuenta con un servidor secundario para respaldo.	Fallo o daño en los componentes de Hardware mantenido por el Data Center	Afectación a la disponibilidad, integridad de los servicios del Data Center
Servidores de VoIP Asterisk	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso Manipulación de la configuracion
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio de Voz sobre IP
	Los nuevos parches no han sido aplicados al sistema	Hacker, cracker	El servicio Web del servidor Trixbox contiene un script PHP que es susceptible a ataques puesto que le atacante podria ver archivos en el sistema o ejecutar codigo php arbitrario con privilegios del usuario del servicio Web
	Servicios ejecutandose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad
Servidor de Video Conferencia ePoP	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso Manipulación de la configuracion
	Sistemas de tecnologías de la información pobremente mantenidos	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Agujeros de seguridad sobre el sistema operativo y en el software instalado en los servidores. Mayor deterioro de los sistemas por virus o gusanos, o intrusiones por no chequear ni instalar los parches de seguridad disponibles de cada fabricante de software o hardware
Servicio Web	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio de Voz sobre IP
	No existen políticas de control de acceso a los sistemas.	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso Manipulación de la configuracion
	Servicios ejecutandose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad

Tabla 1.21 Identificación de las Vulnerabilidades (continuación)

	Sistemas de tecnologías de la información pobremente mantenidos	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Agujeros de seguridad sobre el sistema operativo y en el software instalado en los servidores. Mayor deterioro de los sistemas por virus o gusanos, o intrusiones por no chequear ni instalar los parches de seguridad disponibles de cada fabricante de software o hardware
	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la información de la empresa
Instalaciones del Data Center	Inadecuada protección contra intrusos y daño de componentes del Data Center	Intrusos, personal no autorizado	Robo o pérdida de componentes del Data Center
	Falta de sistema de deteccion y supresion de incendio	Fuego	Pérdida o deterioro de componentes del Data Center
	Funcionamiento no adecuado del UPS	Indisponibilidad del Servicio eléctrico en el Data Center	Afectación a la disponibilidad, integridad de los servicios del Data Center, y la pérdida o deterioro de la información albergada en sistemas de información
Computadores Personales de Oficina	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la información de la empresa
	Falta de sistema de deteccion y supresion de incendio	Fuego	Pérdida o deterioro de información contenida en los computadores
	No existen programas antivirus.	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Daño o deterioro del sistema operativo contenido en las computadores
	Sistemas de tecnologías de la información pobremente mantenidos	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Agujeros de seguridad sobre el sistema operativo y en el software instalado en los servidores. Mayor deterioro de los sistemas por virus o gusanos, o intrusiones por no chequear ni instalar los parches de seguridad disponibles de cada fabricante de software o hardware
Documentación.	Falta de sistema de deteccion y supresion cde incendio	Fuego	Perdida o deterioro de Información documentada
	Perdida de Informacion	Personal de la empresa no calificado	Perdida de Información que podria ocurrir por negligencia de los empleados o por un almacenamiento no protegido
	Documentación incorrecta o errónea del sistema	Personal de la empresa no calificado Empleados que salen de la empresa	Incapacidad de restauración de los sistemas de Información
	Modificacion no autorizada de la información documentada del sistema	Personal de la empresa no calificado Empleados que salen de la empresa	Incapacidad de restauración de los sistemas de Información

Tabla 1.21 Identificación de las Vulnerabilidades (continuación)

Aplicaciones desarrolladas por la empresa.	Falta de conocimiento del uso de la aplicación	Usuarios de las aplicaciones desarrolladas por la empresa	Errores de los usuarios en el uso del sistema
	Errores de configuracion	Personal de la empresa no calificado	Indisponibilidad de la aplicacion
	Manipulación de la configuracion	Personal de la empresa no calificado	Indisponibilidad de la aplicacion
	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que llevan embebido software mailicioso Manipulación de la configuracion
	Abuso de los privilegios de usuario de la base de datos de la aplicacion	Personal de la empresa no calificado Personal de la empresa pobremente capacitado	Pérdida o deterioro de la base de datos que maneja la aplicacion
	Negacion de servicio	Personal de la empresa pobremente capacitado. Empleados que salen de la empresa	Aprovecharse de las vulnerabilidades a nivel de aplicacion a través consultas SQL
	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la base de datos que maneja la aplicaicon

Tabla 1.21 Identificación de las Vulnerabilidades (continuación)

1.3.3.1.3. Análisis de controles actuales

No se han documentado controles para la seguridad, cada área del Departamento de Tecnologías de Información se ha impuesto sus propios controles de seguridad para resguardar los activos de la empresa.

1.3.3.1.4. Determinación de la probabilidad

Para estimar la tasa de probabilidad e indicar la posibilidad de que una potencial vulnerabilidad pueda ser ejercida dentro del ambiente de las amenazas asociadas, los siguientes factores deben ser considerados: fuentes de amenazas, motivación y capacidad, naturaleza de la vulnerabilidad, efectividad y existencia de los controles. La probabilidad de la fuente de amenazas puede ser descrita como alta, media y baja, a continuación la Tabla 1.22 muestra estos tres niveles de probabilidad.

NIVEL DE PROBABILIDAD	DEFINICIÓN
Alto	La fuente de amenazas es altamente motivada y suficientemente capaz, y los controles para prevenir esta vulnerabilidad son inefectivos.
Medio	La fuente de amenazas es motivada y capaz, pero los controles pueden impedir el ejercicio exitoso de la vulnerabilidad.
Bajo	La fuente de amenazas carece de motivación o capacidad, o los controles para la prevencion, o al menos significativamente impiden, que la vulnerabilidad sea ejercida.

Tabla 1.22 Definiciones de probabilidades de amenazas

1.3.3.1.5. Analisis de impacto

Este análisis consiste en la medición del nivel de riesgo para determinar el impacto que podría ser resultado de una exitosa amenaza sobre una vulnerabilidad considerando la misión, importancia, y sensitividad de los datos y activos para la organización.

La sensitividad del sistema y de los datos puede ser determinada basándose en el nivel de protección requerida para mantener la disponibilidad, integridad y confidencialidad del Data Center y de sus datos.

Por lo tanto, el impacto de un evento de seguridad puede ser descrito en términos de pérdida o degradación, o una combinación de cualquiera de los siguientes tres objetivos de seguridad: disponibilidad, confidencialidad e integridad.

A continuación en la Tabla 1.23 se describe cada objetivo de seguridad y el impacto que éste acarrea.

Magnitudes de impacto	Definición de Impacto
Alto	La vulnerabilidad puede resultar en una pérdida de altos costos de los activos tangibles o recursos; puede significativamente violar, dañar o impedir la misión, reputación o intereses de la organización; o puede resultar en pérdidas humanas o lesiones serias.
Medio	La vulnerabilidad puede resultar en una pérdida de altos costos de los mayores activos tangibles o recursos; puede significativamente violar, dañar o impedir la misión, reputación o intereses de la organización; o puede resultar en lesiones serias.
Bajo	La vulnerabilidad puede resultar en la pérdida de algunos activos tangibles o recursos; puede notablemente afectar a la misión, reputación o intereses de la organización.

Tabla 1.23 Magnitudes de definiciones de impacto

1.3.3.1.6. Determinación del Riesgo

La determinación del riesgo es la evaluación del nivel de riesgo del sistema IT. Para una particular amenaza/vulnerabilidad puede ser expresada en función de su probabilidad, magnitud de impacto y del ajuste del planeamiento de controles de seguridad existentes para eliminar o reducir riesgos asociados. Para su medición se debe desarrollar una matriz de nivel de riesgos.

Matriz de nivel de riesgos

La determinación final del riesgo es obtenida multiplicando las tasas asignadas por la probabilidad de la amenazas y del impacto de la amenaza.

La probabilidad asignada para cada nivel de amenaza es de 1.0 para un nivel de amenaza alto, 0.5 para un medio y 0.1 para un nivel bajo.

El valor asignado para cada nivel de impacto es de 100 para alto, 50 para medio y 10 para bajo.

La Tabla 1.24 describe la matriz de nivel de impacto de los activos informáticos de la empresa Conectividad Global Cía. Ltda. con la que se determina el nivel de riesgos y su priorización. Esto permite recomendar qué controles deberían ser implantados para mitigación o disminución del impacto a cada uno de los recursos analizados.

Activos / Recursos	Vulnerabilidad	Amenaza Fuente	Acción de la amenaza	Nivel de probabilidad de la amenaza	Magnitud de impacto	Riesgo
Recursos Humanos	Cuentas de usuario de los empleados que salen empresa no son removidas del dominio	Empleados que salen de la empresa	Ingresar de forma no autorizada a los recursos del dominio de la intranet de la compañía	Alto 1.0	Medio 50	50
	Cuentas de usuario del sistema que hayan sido creadas sobre equipos que se puedan acceder desde Internet	Empleados que salen de la empresa	Deteriorar la integridad del servicio que es ofrecido por el equipo	Medio 0.5	Medio 50	25
	No existen acuerdos de confidencialidad	Empleados que salen de la empresa	Divulgación o robo de información de la empresa	Alto 1.0	Alto 100	100
	Manipulación erronea de la configuración de los sistemas	Personal de la empresa pobremente capacitado	Indisponibilidad de los servicios del Data Center	Medio 0.5	Medio 50	25
	No existen acuerdos definidos para el reemplazo de empleados	Insuficiente Personal	Mantenimiento y disponibilidad incumplida de los sistemas de Información	Medio 0.5	Medio 50	25
	Capacitación inadecuada de usuarios y administradores sobre el uso de los servicios	Personal de la empresa no calificado	Falla en la conectividad a los servicios del Data Center por parte de los usuarios	Medio 0.5	Medio 50	25
Usuarios de las aplicaciones desarrolladas por la empresa	Falta de planificación en las capacitaciones de las aplicaciones a los usuarios	Personal de la empresa no calificado	Hay errores en la entrada, modificación y eliminación de datos	Medio 0.5	Medio 50	25
Firewalls	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que lleva embebido software malicioso. Manipulación de la configuración	Medio 0.5	Medio 50	25

Tabla 1.24 Matriz de Nivel de Impacto

	No existe un procedimiento formal para la realización de respaldos periódicos de la configuración de los sistemas	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Afectación a la disponibilidad, integridad de los servicios del Data Center	Medio 0.5	Medio 50	25
	Configuración pobre de las reglas de filtrado para contrarrestar ataques provenientes de Internet	Hackers, crackers	Reconocimiento de la red interna y intrusiones a los sistemas interno	Medio 0.5	Medio 50	25
	No se ha establecido una correcta arquitectura de firewall, donde exista una segmentación DMZ	Hackers, crackers	Intrusiones o acceso no autorizado a los sistemas IT de la red interna	Medio 0.5	Medio 50	25
	Este equipo tiene instalado el software Webmin (10000/tcp)	Hackers, crackers	Se accede a la herramienta de administración Webmin con autenticación de super usuario al sistema y son enviados en texto plano sobre el Internet	Medio 0.5	Medio 50	25
	Habilitado el acceso al sistema con cuenta de root, utilizando protocolo Secure shell (ssh)	Hackers, crackers	A través de un ataque de fuerza bruta o por diccionario se podría descubrir la cuenta root del sistema	Medio 0.5	Medio 50	25
	Demasiados servicios sobre un mismo equipo	Hackers, crackers	Demasiados servicios activos que se ofrezcan al mundo exterior incrementan el riesgo de un posible agujero de seguridad sobre este equipo	Medio 0.5	Medio 50	25
	Demasiados puertos permitidos en el firewall	Hackers, crackers	El atacante puede usar los puertos abiertos para conectarse al sistema y atacarlo	Medio 0.5	Medio 50	25
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración	Bajo 0.1	Medio 50	25
Servicio de Correo Electrónico kerio Mail Server	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que lleva embebido software malicioso Manipulación de la configuración de los sistemas	Medio 0.5	Medio 50	25

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la información de correos electrónicos de los usuarios	Medio 0.5	Alto 100	50
	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de correo electrónico	Hackers, crackers, spammers	Pérdida de confidencialidad o integridad de la información de correos electrónicos de los usuarios	Medio 0.5	Alto 100	50
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio de correo electrónico	Medio 0.5	Medio 50	25
	Este equipo tiene instalado el software Webmin (10000/tcp)	Hackers, crackers	Se accede a la herramienta de administración Webmin con autenticación de super usuario al sistema y son enviados en texto plano sobre el Internet	Medio 0.5	Alto 50	50
	La versión 6.2.1 de la aplicación Kerio Mail Server no esta actualizada y tiene vulnerabilidades en el core	Hacker, cracker	Existe una vulnerabilidad no especificada en el filtro de archivos adjuntos del servidor	Medio 0.5	Medio 50	25
	El motor Antivirus embebido en el servicio de correo electrónico no se encuentra actualizado	Código malicioso	Los nuevos virus o algún otro código malicioso sobre archivos adjuntos de correos electrónicos no podrán ser detectados	Alto 1.0	Medio 50	25
	Se encuentra ejecutándose el servicio LDAP de forma innecesaria sobre el servicio de correo electrónico	Hacker, cracker. Personal de la empresa no calificado	Existiría un ataque de negación por el atacante utilizando al usuario anónimo para enviar solicitudes de búsqueda malformadas	Bajo 0.1	Bajo 10	1
Servicio de Correo Electrónico Communigate Pro Communication Server	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de correo electrónico	Hackers, crackers, spammers	Ataques de virus, spam, archivos adjuntos peligrosos, y no se puede comprometer al servidor de correo electrónico El atacante puede conseguir información interna que podría comprometer al sistema como userids, hostnames, etc.	Medio 0.5	Bajo 10	5

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

	Este equipo tiene instalado el software Webmin: webmin(10000/tcp)	Hackers, crackers	No se configurado el control de acceso de forma correcta a la herramienta de administración Webmin, el username/password son enviados en texto plano sobre el Internet	Medio 0.5	Bajo 10	5
	No se encuentran instalados programas antivirus, ni antispam para chequeos de correos electrónicos	Hackers, crackers, spammers	Ataques de virus, spam, archivos adjuntos peligrosos permitiendo su envío/recepción	Alto 1.0	Bajo 10	10
Servicio DNS	No se encuentra establecida una arquitectura de seguridad que asegure el servicio de DNS	Hackers, crackers, spammers	El atacante puede conseguir información interna que podría comprometer al sistema como userids, hostnames, etc.	Medio 0.5	Alto 100	50
	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio DNS	Medio 0.5	Alto 100	25
	Este equipo tiene instalado el software Webmin (10000/tcp)	Hackers, crackers	Se accede a la herramienta de administración Webmin con autenticación de super usuario al sistema y son enviados en texto plano sobre el Internet	Medio 0.5	Alto 100	50
	No se cuenta con un servidor secundario para respaldo	Fallo o daño en los componentes de Hardware mantenido por el Data Center	Afectación a la disponibilidad, integridad de los servicios del Data Center	Medio 0.5	Alto 100	100
Servicio FTP	Ganar acceso al servidor FTP	Hacker, cracker	Búsqueda de passwords de usuarios del sistema utilizando ataques de fuerza bruta o diccionario	Alto 1.0	Alto 100	100
	Captura de usernames/passwords de usuarios del sistema	Hacker, cracker	Capturar las contraseñas utilizando sniffing	Medio 0.5	Alto 100	50
Servicio Web	Falta de Planes de continuidad del negocio	Personal de la empresa no calificado	Incapacidad de restauración del servicio Web	Medio 0.5	Medio 50	25
	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la información de la empresa	Alto 1.0	Alto 100	100

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

	No existe una configuración adecuada de este servicio	Hacker, cracker	Negación de servicio	Alto 1.0	Alto 100	100
	Acceso a la cuenta de usuario root a las bases de datos de administradores de contenido	Hackers, crackers. Personal no calificado de la empresa. Personal pobremente capacitado	Daño o deterioro de los sitios Web de contenido dinámico basados en php-mysql	Alto 1.0	Alto 100	100
Acceso a Internet	No existe filtrado de URLs que obedezcan a políticas de seguridad	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Acceso a sitios Web de alto riesgo	Alto 1.0	Alto 100	100
Instalaciones del Data Center	Inadecuada protección contra intrusos y daño de componentes del Data Center	Intrusos, personal no autorizado	Se protege con cerradura metálica y se descuida que la puerta este cerrada	Medio 0.5	Medio 50	25
	Falta de sistema de detección y supresión de incendio, solo se cuenta con un extinguidor en las instalaciones del Data Center	Fuego	No existe un sistema de detección y supresión de Incendio	Bajo 0.1	Alto 100	10
	Funcionamiento no adecuado del UPS	Afectación a la disponibilidad, integridad de los servicios del Data Center, y la pérdida o deterioro de la información albergada en sistemas de información	No existe una alta confiabilidad en el desempeño de los sistemas UPS que se encuentran en el UPS puesto que son sistemas antiguos, que solo soportan la carga de todo el Data Center por 10 minutos	Alto 1.0	Medio 50	50
Equipos servidores	No existe procedimientos para la instalación de nuevos sistemas	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Sistemas nuevos vulnerables	Alto 1.0	Alto 100	100
	No se realiza Instalación de parches legítimos del sistema operativo	Código malicioso: Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker	Agujeros de seguridad sobre el sistema operativo y/o software instalado, No existen procedimientos de descarga y verificación de legitimidad de parches	Medio 0.5	Alto 100	50

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

	No se recompila el kernel	Hacker, cracker	Si no se deshabilita el soporte de módulos un hacker puede cargar un modulo que contenga código malicioso	Medio 0.5	Alto 100	50
	No se establece una contraseña en el BIOS del equipo	Empleados no confiables, personal no autorizado	Modificación de la configuración del x BIOS para arrancarlo desde un dispositivo extraíble	Bajo 0.1	Medio 50	5
	No se realizan consideraciones respecto al uso de cuentas del sistema que vienen por defecto	Hacker, cracker	Acceso no autorizado al sistema	Medio 0.5	Alto 100	50
	Servicios ejecutándose de forma innecesaria	Hackers, crackers	Servicios activos innecesarios que se ofrezcan al mundo exterior acompañado por reglas de filtrado mal configuradas o demasiado permisivas incrementan el riesgo de un posible agujero de seguridad	Medio 0.5	Medio 50	50
	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que lleva embebido software malicioso Manipulación de la configuración	Alto 1.0	Alto 100	100
Computadores Personales de Oficina	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la información de la empresa	Medio 0.5	Alto 100	50
	Falta de sistema de detección y supresión de incendio	Fuego	Pérdida o deterioro de información contenida en los computadores	Bajo 0.1	Alto 100	10
	Los programas antivirus solo son versiones de evaluación	Código malicioso: Virus, gusanos, backdoors, troyanos, etc.	Daño o deterioro del sistema operativo contenido en las computadores	Alto 1.0	Medio 50	50
	Falta de sistema de detección y supresión de incendio	Fuego	Pérdida o deterioro de Información documentada	Baja 0.1	Alto 100	10

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

Documentación	Pérdida de Información	Personal de la empresa no calificado	Pérdida de Información que podría ocurrir por negligencia de los empleados o por un almacenamiento no protegido	Medio 0.5	Alto 100	50
	Documentación incorrecta o errónea del sistema	Personal de la empresa no calificado Empleados que salen de la empresa	Incapacidad de restauración de los sistemas de Información	Medio 0.5	Alto 100	50
	Modificación no autorizada de la información documentada del sistema	Personal de la empresa no calificado. Empleados que salen de la empresa.	Incapacidad de restauración de los sistemas de Información.	Medio 0.5	Bajo 10	5
Aplicaciones desarrolladas por la empresa	Falta de conocimiento del uso de la aplicación	Usuarios de las aplicaciones desarrolladas por la empresa	Errores de los usuarios en el uso del sistema	Bajo 0.1	Medio 50	5
	Errores de configuración	Personal de la empresa no calificado	Indisponibilidad de la aplicación	Medio 0.5	Medio 50	25
	Manipulación de la configuración	Personal de la empresa no calificado	Indisponibilidad de la aplicación	Medio 0.5	Medio 50	25
	No existen políticas de control de acceso a los sistemas	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Instalación de software no autorizado que lleva embebido software malicioso. Manipulación de la configuración	Medio 0.5	Medio 50	25
	No existen procedimientos para la instalación de las aplicaciones	Virus, gusanos, backdoors, troyanos, etc. Hacker, cracker Personal de la empresa no calificado Empleados que salen de la empresa	Comprometimiento de la base de datos de la aplicación	Alto 1.0	Alto 100	100
	Abuso de los privilegios de usuario de la base de datos de la aplicación	Personal de la empresa no calificado Personal de la empresa pobremente capacitado	Pérdida o deterioro de la base de datos que maneja la aplicación	Medio 0.5	Alto 100	50

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

	Negación de servicio	Personal de la empresa pobremente capacitado Empleados que salen de la empresa	Aprovecharse de las vulnerabilidades a nivel de aplicación a través consultas SQL	Medio 0.5	Alto 100	50
	No existe un procedimiento formal para la realización de respaldos periódicos de la información	Fuego Fallo o daño en los componentes de Hardware mantenido por el Data Center	Pérdida o deterioro de la base de datos que maneja la aplicación	Medio 0.5	Alto 100	50

Tabla 1.24 Matriz de Nivel de Impacto (continuación)

1.4. REQUERIMIENTOS

Ante el análisis realizado, se concluye que no existe una arquitectura definida de red. Los servicios, aplicaciones y acceso han sido agregados sin un previo análisis de capacidad y sin definir algún esquema que provea seguridad, ni mucho menos escalabilidad. Claramente se aprecia que algunos de los equipos servidores soportan dos o más servicios, y en algunos casos no relacionados; mientras que existen equipos subutilizados.

Si bien los equipos de conectividad se encuentran funcionando sin problema, es necesario involucrar equipos que provean disponibilidad garantizada. Además la configuración de los mismos podría realizarse de manera óptima aprovechando las capacidades de cada uno de ellos.

Se debe definir también un esquema de configuración óptima de cada servicio con el fin de aprovechar el hardware para cierta función específica.

Tanto los elementos de hardware como de software del Data Center deben garantizar disponibilidad, integridad y confidencialidad, lo que nos señala que es necesario un rediseño basado en arquitecturas de seguridad.

1.4.1. SÍNTESIS DE REQUERIMIENTOS

Entre los requerimientos considerados necesarios para rediseñar la infraestructura de red están los siguientes:

Brindar servicios de manera ordenada, óptima y eficaz para satisfacer las necesidades de los clientes.

Proveer a los equipos servidores del Data Center tolerancia ante fallas a través de mecanismos de redundancia en sus servicios y en lo posible del hardware.

Garantizar escalabilidad a través del planeamiento básico de capacidad en los servidores, y un diseño de red que permita a futuro involucrar y brindar más beneficios y servicios a los clientes y usuarios.

Determinar el flujo de Información para proponer niveles de acceso a los usuarios.

Establecer políticas y procedimientos de seguridad para el Data Center y los servicios que ofrece, con el fin de precisar que es lo que se quiere proteger y los mecanismos que se requieren para cumplirlo.

Proveer al Data Center un adecuado diseño de arquitectura de seguridad con el fin de garantizar disponibilidad, integridad y confidencialidad de la información, y una correcta administración de los recursos.

Utilizar dispositivos apropiados para incrementar el nivel de seguridad de la red en profundidad.

Proponer un sistema de monitoreo y registro de eventos de los recursos informáticos del Data Center utilizando herramientas de software existentes en el Data Center o bien herramientas de software Libre.

CAPÍTULO 2. REINGENIERÍA DE LA INFRAESTRUCTURA DE RED Y SERVICIOS

2.1. DISEÑO DE LAS POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD PARA EL DATA CENTER

Antes del desarrollo de las políticas y procedimientos de seguridad es necesario realizar un análisis acerca de la mitigación de los riesgos.

2.1.1. MITIGACIÓN DE RIESGOS

Para el proceso de mitigación de riesgos se realizará un plan de mitigación de acuerdo a las Recomendaciones NIST que permita priorizar, evaluar e implementar los controles apropiados para la reducción de los riesgos a un nivel aceptable con el objetivo de minimizar el impacto sobre la misión y los recursos de la organización. La metodología para mitigación de los riesgos sirve para seleccionar controles apropiados de los riesgos encontrados en el Data Center, que permitirán una reducción del riesgo a un nivel aceptable o su eliminación. En la Tabla 2.1 se realizará la mitigación de riesgos utlizando esta metodología.

Recurso	Riesgo (Amenaza /Vulnerabilidad)	Nivel de Riesgo	Controles Recomendados	Prioridad de Acción	Controles Seleccionados
Recurso Humano	Las cuentas de usuario de los empleados sobre los servidores internos que salen de la empresa se mantienen habilitadas	Medio	Establecimiento de privilegios para el acceso remoto a los servidores únicamente desde los computadores de administradores de red	Medio	Establecimiento de privilegios para el acceso remoto a los servidores únicamente desde los computadores de administradores de red
			Determinación de los privilegios de los usuarios para acceso a los sistemas		Determinación de los privilegios de los usuarios para acceso a los sistemas

Tabla 2.1 Metodología para mitigación de Riesgos

Recurso Humano			Eliminación de la cuenta de usuario del ex-empleado		Mantenimiento de una documentación para administración de las cuentas de usuario en cada servidor
			Mantenimiento de una documentación para administración de las cuentas de usuario en cada servidor		
	Cuentas de usuario del sistema pertenecientes a empleados que hayan salido de la empresa que hayan sido creadas sobre los equipos firewall	Medio	Deshabilitar o eliminar las cuentas de usuario del ex-empleado en todos los sistemas.	Alto	Deshabilitar o eliminar las cuentas de usuario del ex-empleado en todos los sistemas.
			Registro para control de las cuentas de usuario en cada servidor		Registro para control de las cuentas de usuario en cada servidor
	El empleados de la empresa no firman acuerdos de confidencialidad	Alto	Acuerdos de confidencialidad con los empleados de la empresa	Alto	Acuerdos de confidencialidad con los empleados de la empresa
			Conocimiento, educación y entrenamiento de la seguridad de información		
	Personal de la empresa configura incorrectamente a los sistemas.	Medio	Conocimiento, educación y entrenamiento de la seguridad de información a los empleados nuevos	Medio	Conocimiento, educación y entrenamiento de la seguridad de información a los empleados nuevos
			Proceso disciplinario		Proceso disciplinario
			Selección y política del personal		Selección y política del personal
			Establecimiento de responsabilidades		Establecimiento de responsabilidades
	Comprometimiento de los sistemas por politicas inexistentes de control de acceso	Medio	Establecimiento de procedimientos para impedir acceso de red no autorizado a los sistemas	Medio	Procedimiento para inserción y eliminación de las cuentas de usuario en los sistemas
			Procedimiento para insercion y eliminacion de las cuentas de usuario en los sistemas		La asignacion de privilegios sobre los sistemas debe ser controlada
			La asignacion de privilegios sobre los sistemas debe ser controlado		Implementacion de Politicas de control de acceso
			Apropiada autenticacion para el acceso		Registrar intentos exitosos y fracasos de autenticacion al sistema
			Implementacion de Politicas de control de acceso		
			Definicion de procedimiento para continuidad del negocio		

Tabla 2.1 Metodología para mitigación de Riesgos (continuación)

			Registrar intentos exitosos y fracasos de autenticación al sistema		
	Usuarios maliciosos pueden aprovecharse de la configuración de los equipos firewalls	Medio	Planificación adecuada para accesibilidad a los servicios a través del firewall.	Bajo	Implementar una arquitectura de seguridad adecuada para la red
			Implementar una arquitectura de seguridad adecuada para la red		Definición de procedimiento para restauración
			Definición de procedimiento para restauración		
Servidor de correo electrónico Kerio Mail Server	Usuarios maliciosos pueden aprovecharse de las vulnerabilidades del webmin para acceder al Servidor de correo electrónico kerio MailServer	Medio	Usar privilegios a nivel de sistema operativo para evitar instalaciones no autorizadas	Medio	Usar privilegios a nivel de sistema operativo para evitar instalaciones no autorizadas
			Política de seguridad para un manejo general de sistemas multiusuario		Política de seguridad para un manejo general de sistemas multiusuario
			Crear y mantener al día procedimientos operativos sobre el uso de cada sistema		Proporcionar una capacitación sobre el uso de los sistemas
			Proporcionar una capacitación sobre el uso de los sistemas		
			Investigar alternativas que provean seguridad al software instalado		
	Deterioro del equipo servidor de correo electrónico kerio Mailserver por fuego o daño en el hardware	Medio	Mejoramiento de la seguridad física de las Instalaciones del Data Center	Medio	Mejoramiento de la seguridad física de las Instalaciones del Data Center
			Mantenimiento regular apropiado de los equipos		Mantenimiento regular apropiado de los equipos
	Hackers o crackers podrian aprovechar del pobre diseño de red del servicio de correo electrónico	Medio	Diseñar una adecuada red de servicios con características de seguridad	Medio	Diseñar una adecuada red de servicios con características de seguridad
	Usuarios Maliciosos pueden aprovecharse del pobre mantenimiento del software Kerio Mail Server	Medio	Mantener actualizado al software Kerio Mail Server y deshabilitar los servicios extras que no sean necesarios	Medio	Mantener actualizado al software Kerio Mail Server y deshabilitar los servicios extras que no sean necesarios
	Incapacidad de restauración del servidor kerio Mail Server	Medio	Gestión interna de respaldo de información	Alto	Gestión interna de respaldo de información

Tabla 2.1 Metodología para mitigación de Riesgos (continuación)

			Desarrollo e implantación de planes de contingencia para mantener disponiblidad del servicio		Desarrollo e implantación de planes de contingencia para mantener disponiblidad del servicio
Servidor de correo electrónico Communigate Pro Communication Server	Usuarios maliciosos pueden aprovecharse de las vulnerabilidades del webmin para acceder al Servidor de correo electrónico Communigate Pro Communication Server	Medio	Usar privilegios a nivel de sistema operativo para impedir que software vulnerable pueda ser instalado sobre los sistemas	Bajo	Usar privilegios a nivel de sistema operativo para evitar instalaciones no autorizadas
			Política de seguridad para un manejo general de sistemas multiusuario		Política de seguridad para un manejo general de sistemas multiusuario
			Crear y mantener al día procedimientos operativos sobre el uso de cada sistema		Proporcionar una capacitación sobre el uso de los sistemas
			Proporcionar una capacitación sobre el uso de los sistemas		
			Investigar alternativas que provean seguridad al software instalado		
	Virus, gusanos, backdoors, troyanos pueden infectar al sistema o a los equipos que usen el servicio de correo electrónico desde este servidor	Medio	Proveer la instalación de un sistema de detección de intrusos basado sobre la red en la encuentre el servidor	Medio	Proveer la instalación de un sistema de detección de intrusos basado sobre la red en la encuentre el servidor
			Instalar software antivirus y antispam para el servicio de correo electrónico		Instalar software antivirus y antispam para el servicio de correo electrónico
	Hackers o crackers podrían aprovechar del pobre diseño de red del servicio de correo electrónico	Medio	Diseñar una adecuada infraestructura de red de servicio de correo electrónico con características de seguridad	Medio	Diseñar una adecuada red de servicios con características de seguridad
Servicio DNS	Hackers o crackers podrían aprovechar del pobre diseño de red del servicio DNS	Medio	Diseñar una adecuada infraestructura de red de servicio DNS con características de seguridad	Medio	Diseñar una adecuada infraestructura de red de servicio DNS con características de seguridad
	Incapacidad de restauración del servicio DNS al no contar con un servidor secundario de respaldo	Medio	Desarrollo e implantación de planes de contingencia para mantener disponiblidad del servicio	Medio	Desarrollo e implantación de planes de contingencia para mantener disponiblidad del servicio
	Usuarios maliciosos pueden aprovecharse de las vulnerabilidades del webmin para acceder al Servidor de correo electrónico kerio MailServer	Medio	Usar privilegios a nivel de sistema operativo para evitar instalaciones no autorizadas	Medio	Usar privilegios a nivel de sistema operativo para evitar instalaciones no autorizadas

Tabla 2.1 Metodología para mitigación de Riesgos (continuación)

			Política de seguridad para un manejo general de sistemas multiusuario		Política de seguridad para un manejo general de sistemas multiusuario
			Crear y mantener al día procedimientos operativos sobre el uso de cada sistema		Proporcionar una capacitación sobre el uso de los sistemas
			Proporcionar una capacitación sobre el uso de los sistemas		
			Investigar alternativas que provean seguridad al software webmin		
Servicio FTP	Hacker , cracker gane acceso al servidor FTP	Alto	Proveer la instalación de un sistema de detección de intrusos basado sobre la red en la que se encuentre el servidor	Medio	Proveer la instalación de un sistema de detección de intrusos basado sobre la red en la que se encuentre el servidor
Servicio Web	Incapacidad de restauración del servicio Web	Medio	Gestión interna de respaldo de información	Alto	Gestión interna de respaldo de información
			Desarrollo e implantación de planes de contingencia para mantener disponiblidad del servicio		Desarrollo e implantación de planes de contingencia para mantener disponiblidad del servicio
	Hacker, crackers pueden comprometer las bases de datos de los sitios Web dinámicos por una inadecuada administración de usuarios	Medio	Proporcionar seguridad en el control de acceso al RDBMS MySQL	Medio	Proporcionar seguridad en el control de acceso al RDBMS MySQL
			Investigar alternativas que provean seguridad al RDMS MySQL		
Acceso a Internet	Acceso a sitios Web de contenido pornográfico y violento	Medio	Proveer de un servicio de fltrado URL para el acceso a Internet	Alto	Proveer de un servicio de fltrado URL para el acceso a Internet
Instalaciones del Data Center	Acceso no autorizado por falta de seguridad física	Medio	Establecimiento de políticas y procedimientos para impedir acceso no autorizado a los sistemas	Medio	Establecimiento de políticas y procedimientos para impedir acceso no autorizado a los sistemas
			Mantener un inventario de los activos		Mantener un inventario de los activos
	Falta de sistema de detección y supresión de incendios	Medio	Adquirir un sistema de detección y supresión de incendios	Alto	Adquirir un sistema de detección y supresión de incendios
	Falta de sistema de energía ininterrumplible	Medio	Diseñar un óptimo sistema de energía initerrumpible	Alto	Diseñar un óptimo sistema de energiá initerrumpible

Tabla 2.1 Metodología para mitigación de Riesgos (continuación)

			Procedimientos para mantenimiento del suministro eléctrico en caso de una prolongada demora de corte eléctrico		Procedimientos para mantenimiento del suministro eléctrico en caso de una prolongada demora de corte eléctrico
Equipos Servidores	Usuarios y código malicioso puede comprometer a nuevos sistemas que no cuenten con un correcto aseguramiento a nivel de sistema operativo	Alto	Procedimientos de instalación que mejoren la seguridad de los sistemas operativos de nuevos sistemas	Medio	Procedimientos de instalación que mejoren la seguridad de los sistemas operativos de nuevos sistemas
	Falta de mantenimiento de los sistemas	Medio	Procedimientos para instalación y mantenimiento de actualizaciones y parches de seguridad de las aplicaciones y/o sistemas operativos	Medio	Procedimientos para instalación y mantenimiento de actualizaciones y parches de seguridad de las aplicaciones y/o sistemas operativos
	Empleados no confiables podrían acceder no autorizadamente valiéndose de la configuración del BIOS	Bajo	Configurar una contraseña en el BIOS	Bajo	Configurar una contraseña en el BIOS
	Acceso indebido por usuarios maliciosos utilizando puertos que se ejecutan innecesariamente .	Medio	Permitir el acceso hacia el servidor únicamente por un puerto por el que se provee el servicio	Medio	Permitir el acceso hacia el servidor únicamente por un puerto por el que se provee el servicio
Computadores personales de oficina	Incapacidad de restauración	Medio	Gestión interna de respaldo de información	Alto	Gestión interna de respaldo de información
	Contaminación por código malicioso por no contar con software antivirus con licencia	Medio	Guías para instalación y mantenimiento de Antivirus	Alto	Guías para instalación y mantenimiento de Antivirus
	Falta de sistema de detección y supresión de incendios	Bajo	Adquirir un sistema de detección y supresión de incendios para los lugares donde se encuentran los pcs de oficina	Bajo	Adquirir un sistema de detección y supresión de incendios para los lugares donde se encuentran los pcs de oficina
documentación	Falta de sistema de detección y supresión de incendios	Medio	Adquirir un sistema de detección y supresión de incendios para los lugares donde se encuentran la documentación	Medio	Adquirir un sistema de detección y supresión de incendios para los lugares donde se encuentran la documentación

Tabla 2.1 Metodología para mitigación de Riesgos (continuación)

	Personal no calificado puede provocar pérdida de información, deterioro de la documentación o realizar una modificación no autorizada de un sistema	Medio	Políticas de control de acceso a la documentación	Medio	Políticas de control de acceso a la documentación
	Incapacidad de recuperación de la información	Bajo	Gestión interna de respaldo de información	Medio	Gestión interna de respaldo de información
Aplicaciones desarrolladas por la empresa	Los usuarios administradores del sistema SGA pueden provocar errores de la configuración	Bajo	Proporcionar una capacitación sobre el uso de los sistemas	Medio	Proporcionar una capacitación sobre el uso de los sistemas
	Personal de la empresa no confiable puede acceder a información confidencial de la empresa	Alto	Políticas de control de acceso al código fuente de las aplicaciones	Alto	Políticas de control de acceso al código fuente de las aplicaciones
	Personal de la empresa no calificado puede realizar instalaciones descuidando la seguridad	Medio	Procedimientos para la instalación estandarizada de las aplicaciones.	Alto	Procedimientos para la instalación estandarizada de las aplicaciones.
	Incapacidad de restauración	Medio	Gestión interna de respaldo de la base de datos de la aplicación	Alto	Gestión interna de respaldo de la base de datos de la aplicación
			Desarrollo e implantación de planes de contingencia para mantener disponibilidad del servicio que proporcionan las aplicaciones		Desarrollo e implantación de planes de contingencia para mantener disponibilidad del servicio que proporcionan las aplicaciones

Tabla 2.1 Metodología para mitigación de Riesgos (continuación)

Los campos que se encuentran en la Tabla 2.1 se refieren a los siguientes pasos:

Priorizar acciones: basados en el nivel de riesgo de la Tabla 1.24 (Matriz de Nivel de Impacto) las acciones para la implementación son priorizadas. Al par amenaza/vulnerabilidad con los más altos niveles de riesgo se les asignará recursos de forma inmediata ya que requieren de acción correctiva inmediata para la protección de los intereses y misión de la organización.

Evaluación de las opciones de controles recomendados: se debe seleccionar la opción de control más apropiada para reducir el riesgo.

Selección de controles: se determina los mejores controles para reducir los riesgos a la misión de la organización.

2.1.2. POLÍTICAS PARA LA ADMINISTRACIÓN DE SEGURIDAD DEL DATA CENTER

Para el diseño de las políticas y procedimientos para la administración de la seguridad se tomó en cuenta los controles seleccionados de la Tabla 2.1 de mitigación de riesgos y la metodología de la arquitectura de red propuesta.

2.1.2.1. Recursos Humanos

2.1.2.1.1. Propósito

Establecer las reglas de contratación y responsabilidades de seguridad para los empleados actuales y nuevos de la empresa Conectividad Global Cia. Ltda.

2.1.2.1.2. Alcance

Esta política se aplica sin excepciones a todos los empleados nuevos y actuales de la empresa Conectividad Global Cia. Ltda.

2.1.2.1.3. Exposición de Políticas

- Los términos y condiciones de empleo de la empresa deben contener requerimientos para el cumplimiento con la seguridad de la información.
- Las referencias de los nuevos empleados deberán ser verificadas, y los empleados deberán comprometerse con las políticas de seguridad de la información de la empresa.
- Todos los proveedores externos que sean contratados para proveer servicios a la empresa deberán estar de acuerdo en seguir las políticas de seguridad de la empresa. Un apropiado resumen de las políticas de

seguridad de la información deberá ser formalmente entregado al proveedor previo a cualquier provisión de servicios.

- Los acuerdos de confidencialidad deberán ser usados en todas las situaciones donde la confidencialidad, sensitividad o valor de la información siendo divulgada es clasificada como propietaria.
- Los papeles membretados por la empresa, formularios impresos y otros documentos deberán ser manejados de forma segura para evitar accesos indebidos.
- El préstamo de llaves físicas está prohibido.
- Todos los empleados deberán cumplir con las políticas de seguridad, cualquier acción de no cumplimiento resultará en una acción disciplinaria.
- Todos los empleados de la empresa y contratistas deberán firmar un contrato de trabajo respetando derechos de propiedad intelectual durante los términos que el contrato lo indique.
- Todos los empleados requerirán firmar un acuerdo formal concerniente a la necesidad de proteger la confidencialidad de la información tanto durante como después de las relaciones contractuales con la empresa.

2.1.2.2. Seguridad física del Data Center

2.1.2.2.1. Propósito

Establecer las normas para el perímetro de seguridad del Data Center con controles físicos de entrada para proteger a los recursos de hardware frente a robos y para la protección del sistema de cableado estructurado de manipulación no autorizada.

2.1.2.2.2. Alcance

Esta política se aplica a todos los equipos de comunicación, sistemas informáticos y cableado físico que se encuentre dentro de las instalaciones de la empresa.

2.1.2.2.3. Exposición de políticas

- La infraestructura de red y de servicios del Data Center deberá estar ubicada en una sección física aislada del resto de las instalaciones de la organización, estar protegidos por paredes y puertas externas con cerradura, y contar con un sistema de alarma contra robos.
- La infraestructura de red y servicios del Data Center deberá contar con alimentación eléctrica regulada y con su propio sistema de puesta a tierra.
- Las condiciones ambientales de los equipos del Data Center deberán cumplir estándares de temperatura y humedad.
- Las personas ajenas a la empresa que accedan a las instalaciones del Data Center deberán ser supervisadas por algún empleado del área de administración de red.
- Se deberá proveer de un apropiado equipo de detección y supresión de incendios.

2.1.2.3. Administración de operaciones del Data Center

2.1.2.3.1. Propósito

Establecer el perfil de responsabilidad y procedimientos para el uso aceptable de los recursos informáticos de la empresa Conectividad Global Cia. Ltda. para una segura y correcta operación.

2.1.2.3.2. Alcance

Esta política se aplica a todos los empleados del departamento de Tecnologías de la Información, practicantes, pasantes y otros trabajadores que se encarguen de la infraestructura tecnológica del Data Center; y a todos los equipos de comunicación, sistemas informáticos de propiedad o administrados por Conectividad Global Cia. Ltda.

2.1.2.3.3. Exposición de políticas

- Los procedimientos operativos de los sistemas de información deben ser documentados.
- Las modificaciones a los sistemas de información o dispositivos de comunicación deben ser controladas.
- Debe haber una separación de ambientes de pruebas, desarrollo y producción de los sistemas informáticos para evitar cambios no intencionados a la aplicación o a la información y se debe procurar emular a un entorno de pruebas lo más parecido posible al ambiente de producción.
- Los requerimientos de capacidad de los recursos informáticos deben ser claramente identificados.
- Se deberán revisar los respaldos de los sistemas y aplicaciones periódicamente.
- Los procedimientos de restauración desde los respaldos deberán ser regularmente chequeados y probados.

2.1.2.4. Control de acceso

2.1.2.4.1. Propósito

Establecer las reglas para las cuales la organización establece controles de acceso a los activos de la empresa Conectividad Global Cia. Ltda. y deberán ser incorporados para balancear restricciones al acceso no autorizado contra la necesidad de proveer un acceso libre a las necesidades de la empresa.

2.1.2.4.2. Alcance

Esta política se aplica a todos los empleados del departamento de Tecnologías de la Información, practicantes, pasantes y otros trabajadores que se encarguen de la infraestructura tecnológica del Data Center; y a todos los equipos de comunicación, sistemas informáticos propiedad o administrados por Conectividad Global Cia. Ltda.

2.1.2.4.3. Exposición de políticas

- El acceso a todos los sistemas informáticos y equipos de comunicación debe ser autorizado por el encargado del sistema y dicho acceso deberá tener los apropiados privilegios y ser registrado en una lista de control de acceso.
- El equipo debe estar siempre protegido apropiadamente, incluso el equipo desatendido.
- El uso de los recursos de red debe ser estrictamente controlado para prevenir el acceso no autorizado. El acceso a todos los sistemas de computación, información y periféricos deberá ser restringido a menos que sea explícitamente autorizado.
- El acceso a los comandos del sistema operativo deberá ser permitido sólo para personal de Administración de redes.
- La selección de passwords, su uso y administración para brindar un control de acceso deberán seguir las siguientes reglas:
    - Los passwords nunca serán escritos sobre un papel o documento.
    - Los passwords deberán ser cambiados en intervalos regulares de tiempo y ser manejados de forma privada e individual.
    - No se deben compartir los passwords porque podría darse un acceso no autorizado a los sistemas de información.
- El acceso debe ser registrado y monitorizado para identificar potenciales accesos indebidos a la información o a sistemas.
- El acceso a la información y documentación debe ser cuidadosamente controlado asegurando que sólo personal autorizado pueda tener acceso a información sensitiva.

2.1.2.5. Reenvío automático de correo electrónico

2.1.2.5.1. Propósito

Impedir la divulgación no autorizada o inadvertida de información sensitiva de la compañía.

2.1.2.5.2. Alcance

Esta política cubre al reenvío automático de correo electrónico, y por consiguiente la transmisión potencial e inadvertida de información sensitiva por los empleados, vendedores, y agentes que operen en patrocinio de Conectividad Global Cia. Ltda.

2.1.2.5.3. Exposición de políticas

Los empleados deben ser precavidos cuando envíen cualquier correo electrónico desde el interior de Conectividad Global Cia. Ltda. hacia una red exterior. A menos que sea aprobado por el personal de Administración de redes, el correo electrónico de Conectividad Global Cia. Ltda no será automáticamente reenviado a un destino externo. La información sensitiva, es decir bases de datos del SGA de las instituciones no será reenviada, a menos que ese correo electrónico sea crítico para el negocio.

2.1.2.6. Uso Aceptable

Los sistemas relacionados a los servicios de Internet, Extranet o Intranet, servidores, computadores, software, sistemas operativos, medios de almacenamiento, cuentas de correo electrónico, navegación Web y FTP que formen parte del Data Center son propiedad de Conectividad Global Cia. Ltda. Estos sistemas son usados para propósitos comerciales y educativos y para la prestación de servicio para clientes e intereses de la compañía.

La efectividad de la seguridad es un esfuerzo del equipo implicando la participación y soporte de cada empleado de la empresa Conectividad Global Cia. Ltda. y de cada usuario que se ocupe de la información y/o sistemas de información. Es la responsabilidad de cada usuario de las aplicaciones conocer estas líneas directivas, y conducir sus actividades consecuentemente.

2.1.2.6.1. Propósito

El propósito de esta política es indicar acerca del uso del equipo computacional en Conectividad Global Cia. Ltda. Estas reglas son para la protección del empleado de Conectividad Global Cia. Ltda. y del usuario. El uso inapropiado expone a Conectividad Global Cia. Ltda a riesgos que incluyen ataques de virus, que podrían comprometer a sistemas de información y servicios de la red.

2.1.2.6.2. Alcance

Esta política se aplica a los empleados, los contratistas, asesores, terceras partes, y otros trabajadores de Conectividad Global Cia. Ltda incluyendo todos los empleados contratados por terceros. Esta política se aplica a todos los equipos propios o alojados en las instalaciones del Data Center de Conectividad Global Cia. Ltda.

2.1.2.6.3. Exposición de políticas

Uso General

- Mientras el personal de la administración de la red del Data Center de la empresa desea proveer un nivel razonable de privacidad, los usuarios deberían ser conscientes que los datos creados por los sistemas de información permanecen como propiedad de Conectividad Global Cía. Ltda. La administración no puede garantizar la confidencialidad de información almacenada sobre cualquier dispositivo de la red no perteneciente al Data Center de Conectividad Global Cia. Ltda.

- Los departamentos individuales son responsables por la creación de las guías relacionadas al uso personal de sistemas del Data Center. En ausencia de estas políticas, los empleados deberían ser guiados por políticas departamentales acerca del uso personal, y si hay cualquier duda, los empleados deberían consultar a su supervisor o su gerente.

- Se recomienda que cualquier información que el usuario considere sensitiva o vulnerable sea encriptada.

- Para la seguridad y los propósitos de mantenimiento de la red, sólo las personas autorizadas de Conectividad Global Cia. Ltda pueden monitorear equipo, sistemas y tráfico de la red del Data Center en cualquier momento.

- Conectividad Global Cia. Ltda reserva el derecho para realizar la auditoría de sistemas y redes periódicamente para asegurar conformidad con esta política.

Seguridad e Información Propietaria

- El acceso a la información por los usuarios contenida en los sistemas del Data Center debería ser clasificada como confidencial o no confidencial, Los ejemplos de información confidencial incluyen: datos privados de la compañía, las estrategias corporativas, información competitiva, y datos de desarrollo de software. Los empleados deberán llevar todos los pasos necesarios para impedir el acceso no autorizado a esta información.

- Mantener contraseñas seguras y no compartir cuentas. Los usuarios autorizados son responsables de la seguridad de sus contraseñas y cuentas. Las contraseñas a nivel de sistema y de usuario deberán cambiarse frecuentemente.

- Todos los PCs, laptops y estaciones de trabajo deberían ser asegurados con un screensaver con activación automática de 10 minutos o menos y ser protegido en contraseña, o para salir del sistema cuando el host esté sin usar.

- La información contenida en computadoras portátiles es especialmente vulnerable, se debe tener un cuidado especial.

- Todos los hosts usados por el empleado que están conectados a la infraestructura de Red del Data Center, ya sean propiedad del empleado o de Conectividad Global Cia. Ltda deberán continuamente ser escaneados por un software antivirus aprobado y se debe contar con la base de datos de virus actualizada.

- Los empleados deben usar extrema precaución cuando abran archivos adjuntos a correo electrónico recibidos por un remitente desconocido, puesto que puede contener virus, bomba de correo electrónico, o código de caballos de Troya.

Uso inaceptable

Las siguientes actividades son, en general, prohibidas. Los empleados pueden estar liberados de estas restricciones durante el curso de sus responsabilidades legítimas de trabajo, por ejemplo: el grupo de administradores de sistemas puede tener una necesidad para desactivar el acceso a la red de un host si está desestabilizando servicios de producción.

- De ninguna manera un empleado de Conectividad Global Cia Ltda. puede involucrarse en cualquier actividad ilegal utilizando los recursos de Conectividad Global Cia. Ltda.

Actividades del Sistema y de la red

Las siguientes actividades estarán estrictamente prohibidas, sin excepciones:

- Las violaciones de los derechos de autor, patente, propiedad intelectual, u otras regulaciones o leyes similares de cualquier ciudadano o compañía, incluyendo la instalación o la distribución de software pirata u otros productos que no se encuentren apropiadamente autorizados para su uso por Conectividad Global Cia. Ltda.

- No se autoriza copia de material que cuente con derechos de copia, incluyendo digitalización, distribución de fotos de revistas, libros u otras fuentes, música y la instalación de cualquier software con derechos de copia que Conectividad Global Cia. Ltda. o el usuario final no tengan licencia activa, está estrictamente prohibido.

- La introducción de programas maliciosos en la red o el servidor como por ejemplo virus, gusanos, caballos de Troya, etc.

- Revelación de contraseña a otros o permitir el uso de la cuenta. Esto incluye a la familia y otros miembros familiares.

- Usar un activo de Conectividad Global Cia. Ltda. para proxenetismo o transmitir material pornográfico.

- Hacer ofertas fraudulentas de productos, artículos, o servicios desde cualquier cuenta de correo que maneje Conectividad Global Cia. Ltda.

- Hacer declaraciones acerca de garantía, expresamente o implícito, a menos que sea una parte de derechos normales de trabajo.

- Hacer brechas de seguridad o alteraciones en la comunicación de la red. Las brechas de seguridad se refieren a ganar acceso a los datos de los cuales el empleado no es propietario o acceder a un servidor con una cuenta que el empleado no está expresamente autorizado a utilizar. Para los propósitos de esta sección, "la interferencia" se refiere a sniffing a la red, inundaciones de pings, falsificación de paquetes, negación de servicio, y provisión de información falsificada de enrutamiento para los propósitos maliciosos.

- El escaneo de puertos o escaneo de seguridad está expresamente prohibido a excepción de previa notificación a los administradores de sistemas.

- Ejecutar cualquier formalidad de monitoreo de red en la que se intercepten datos, no está permitido para los hosts de los empleados, a menos que esta actividad sea una parte del trabajo o tarea normal del empleado.

- Evadir la autenticación del usuario o seguridad de cualquier host, red o cuenta.

- Interferir con o negando el servicio para cualquier usuario o para el host del empleado (por ejemplo, el ataque de negación de servicio).

- Usando cualquier programa, software o script, o enviar mensajes de cualquier tipo, con la intención de interferir, o deshabilitar una sesión terminal de usuario, por cualquier manera, y sea de forma local o por la Extranet, Intranet o Internet.

- Proveer información acerca, de listas de empleados de Conectividad Global Cia. Ltda. a terceras partes externas a Conectividad Global Cia. Ltda.

Actividades del Correo Electrónico

- Enviar mensajes no solicitados del correo electrónico, incluyendo envío de mensajes de correo electrónico no solicitado u otro material publicitario para personas quienes específicamente no solicitaron dicho material (spam).

- El uso no autorizado o la falsificación de información del encabezado del correo electrónico.

- Crear o reenviar "cadena de mensajes", "pirámide" o esquemas de cualquier tipo.

- El uso de correo electrónico no deseado originado desde la red de Conectividad Global Cia. Ltda, desde otro proveedor de servicios de

Internet, anunciado desde cualquier servicio alojado por la empresa o a través de la red de Conectividad Global Cia. Ltda.

2.1.3. PROCEDIMIENTO PARA LA ADMINISTRACIÓN DE SEGURIDAD DEL DATA CENTER

2.1.3.1. Seguridad física

El personal del área de Administración de red se encargará de supervisar la seguridad física de la infraestructura de red y de servicios del Data Center, y monitorizando frecuentemente la humedad y la temperatura en las instalaciones. La alarma deberá ser encendida durante los periodos no laborables de la empresa.

No debe modificarse la ubicación o posición de los equipos, o configuracion del hardware o software establecida.

No se debe ingresar con alimentos, bebidas, ni tampoco se puede fumar dentro de las instalaciones del Data Center.

La infraestructura de red y servicios del Data Center deberán contar con un sistema de puesta a tierra independiente de la instalaciones eléctricas del edificio, de un suministro eléctrico regulado y de un sistema de fuentes de energía ininterrumpible (UPS) para mantener la disponibilidad de las operaciones de la infraestructura de red. Además se deberá contar con un generador eléctrico de respaldo que use gasolina en caso de falla del UPS o para periodos prolongados de ausencia del suministro eléctrico.

Las personas ajenas a la empresa deberán identificarse, esperar la autorización para ingresar a las instalaciones del Data Center y ser escoltadas por el personal del área de administración de redes.

Se deberá mantener registros con sus respectivas horas y fechas de las tareas realizadas sobre los equipos y servicios por personal de mantenimiento externo o interno a la empresa.

Las instalaciones del Data Center contarán con un sistema de alarma para detección de incendios y se utilizará un extinguidor de incendio a base de dióxido de carbono que será ubicado dentro de las instalaciones del Data Center y deberá ser continuamente mantenido.

Los equipos que no se encuentren en producción y los respaldos de información deberán ubicarse fuera de las instalaciones del Data Center.

Se contratarán servicios para la instalación del sistema de cableado estructurado y eléctrico que deberá ser instalado de forma separada para prevenir interferencia y el personal del área de Administración de redes deberá realizar la documentación de la etiquetación en los cables y equipos.

2.1.3.2. Administración de operaciones del Data Center

El personal de Departamento de Tecnologías de la Información deberá documentar los procedimientos relacionados a las actividades que se realicen en los sistemas informáticos y equipos de comunicación de una forma detallada manteniendo niveles de acceso para cada área del Departamento.

El área de administración de redes se encargará de las modificaciones a los sistemas de información y a los dispositivos de comunicación y deberán ser identificadas, registradas, probadas y formalmente aprobadas por el Jefe del área para posteriormente comunicar los detalles de los cambios a todos los usuarios. Antes de cualquier modificación se deberá establecer un procedimiento para abortar y recuperar la configuración inicial. El jefe del área de administración de redes definirá las tareas de los empleados para reducir el riesgo de modificación no intencional, no autorizada o uso indebido de los recursos informáticos.

Los recursos informáticos requeridos por el área de desarrollo de software y por el área de administración de redes deberán ser separados en ambientes de prueba, desarrollo y producción utilizando segmentación de red.

Para la obtención de los requerimientos de capacidad de los recursos informáticos se debe proveer una monitorización de la utilización de los servicios que proporciona cada equipo.

Para los respaldos de información se deberá realizar procedimientos rutinarios como revisión del respaldo sobre el medio de almacenamiento, frecuencia, extensión (respaldo total o diferencial) de acuerdo al tipo de información que deberán ser almacenados en una localización remota utilizando la debida protección física y ambiental. En la Tabla 2.2 se muestra la frecuencia de realización y chequeo de los respaldos que debería ejecutarse.

Tipo de Información	Frecuencia	Extensión	Medio de almacenamiento	Chequeo de integridad del medio de almacenamiento
Sitios Web Apache (archivo de configuración de servidor Web y contenido del sitio)	mensual	Total	Servidor FTP corporativo y en DVDs	Cada quince días en DVDs.
Portales Web IIS de REV y SGA	trimestral	Total	Servidor FTP corporativo y en DVDs	Cada dos meses en los DVDs.
Correos electrónicos	Diariamente	Diferencial	Servidor FTP corporativo y en DVDs	Semanalmente en los DVDs.
	Semanalmente	Total		
Bases de datos de los sitios Web de contenido dinámico	mensual	Total	Servidor FTP corporativo y en DVDs	Cada quince días en DVDs.
Bases de datos del SGA de las instituciones educativas	mensual	Total	Servidor FTP corporativo y en DVDs	Cada quince días en los DVDs
Código fuente actualizado de las aplicaciones desarrolladas por la empresa	Cada quince dias	Total	DVDs	Semanalmente
Archivos de configuración de los servidores de DNS	mensual	Total	Servidor FTP corporativo y en DVDs	Cada quince días en DVDs.

Tabla 2.2 Frecuencia de los respaldos y chequeo de sus medios de almacenamiento

Servidor de VoIP Asterisk	Trimestral	Total	Servidor FTP corporativo y en DVDs	Cada dos meses en los DVDs
Servidor de VoIP Asterisk	Trimestral	Total	Servidor FTP corporativo y en DVDs	Cada dos meses en los DVDs

Tabla 2.2 Frecuencia de los respaldos y chequeo de sus medios de almacenamiento (continuación)

El área de administración de redes deberá chequear regularmente los procedimientos de restauración y probarlos para asegurar su efectividad y que puedan ser completados dentro de un tiempo estipulado.

2.1.3.3. Control de acceso

Deberán ser removidos cuadros de diálogo de autenticación o banners que provean información sobre el sistema, previo al proceso de una autenticación exitosa para evitar que puedan ayudar a usuarios autorizados a ganar acceso al sistema. Debe haber una apropiada asignación de privilegios que debe ser documentada y regulada para evitar que usuarios no experimentados cometan errores accidentales o provoquen problemas en el procesamiento de los sistemas.

El equipo desatendido puede resultar un objetivo de ataque de personal inescrupuloso de la empresa o de personas ajenas a la empresa. El acceso no autorizado a un sistema de computación desatendido puede resultar en daño o modificación del sistema, intentos fraudulentos como modificación o eliminación de datos o uso fraudulento del correo eletrónico.

El acceso no autorizado a programas o aplicaciones puede conducir a transacciones falsas o fraudulentas. El acceso lógico y físico interno también deberá ser controlado para evitar que usuarios puedan encontrar rutas de acceso a sistemas y recursos de red.

Se deberán establecer perfiles de usuario para acceso a la red manteniendo información correcta y completa para evitar la modificación, eliminación o acceso a información confidencial contenida en recursos de red. La modificación de estos perfiles se deberá realizar con un procedimiento de control de cambios para evitar un inesperado acceso inautorizado a recursos de red.

Todos los sistemas desde computadores a servidores deberán seguir un proceso de hardening[14] para remover todas las herramientas innecesarias de desarrollo y utilitarios previo a la entrega de los equipos computacionales y servicios a los usuarios.

El uso de programas utilitarios instalados sobre los sistemas que podrían ser capaces de causar un gran impacto en el rendimiento deberá estar restringido o ser estrictamente controlados.

En los sistemas de computación que son accedidos a través de cuentas de usuarios utilizando la autenticación de UserID y password, se debe realizar un cambio frecuente de los passwords que podría ser regulado implementando un periodo de expiración para dichos passwords. El acceso a los sistemas debe ser monitorizado regularmente para frustar intentos de acceso no autorizado utilizando para ello sistemas de detección de intrusos.

2.1.3.4. Guías para el procedimento de uso y mantenimiento del software Anti-Virus

Los procesos recomendados para impedir problemas de virus son:

- Siempre se debe ejecutar el software de antivirus estándar Corporativo soportado y verificar que esté disponible del sitio de descarga. Descargar y ejecutar la versión actual; descargar e instalar actualizaciones del software de antivirus como sean disponibles.

---

[14] **Hardening**: proceso de aseguramiento de un sistema al reducir su rango de vulnerabilidades.

- Nunca abrir cualquier archivo o macros adjuntos a los correos electrónicos de una fuente desconocida, sospechosa o de dudosa procedencia. Suprimir estos anexos inmediatamente, luego suprimirlos completamente eliminándolos de la papelera de reciclaje.

- Suprimir spam, cadenas, u otros correos electrónicos no solicitados sin reenviarlos, de acuerdo con la *Política De Uso Aceptable* de Conectividad Global Cia. Ltda.

- Nunca se debe descargar archivos de fuentes desconocidas o sospechosas.

- Evitar uso compartido del disco directamente con acceso de lectura / escritura a menos que sea un requerimiento del negocio hacerlo.

- Siempre escanear un disquete flexible o dispositivo USB de almacenamiento de fuente desconocida en busca de virus antes de usarlo.

- Respaldar los datos críticos y las configuraciones del sistema sobre bases regulares y almacenarlos en un lugar seguro.

- Si los laboratorios de prueba están en conflicto con software antivirus, ejecutar el utilitario del antivirus para asegurar una máquina limpia, deshabilitar el software, ejecutar la prueba del laboratorio. Después de la prueba del laboratorio, habilitar el software de antivirus. Cuando el software de antivirus es deshabilitado, no ejecutar más aplicaciones que pudiesen transferir un virus, por ejemplo correo electrónico o compartir archivos.

2.1.3.5. Fortalecimiento de los sistemas informáticos

Es importante tomar ciertas consideraciones de seguridad en cada equipo realizando hardening de servidores y proveyendo a los equipos parámetros eléctricos específicios como fuentes redundantes y soporte de UPS.

2.1.3.5.1. Sistemas Linux

Es necesario proveer seguridad individual a cada uno de los servidores, por lo que después de la instalación de Linux se debe ir al sitio Web y descargar e instalar todos los parches que hayan sido liberados desde el sitio oficial de la Distribución, no es recomendable hacerlo desde otras fuentes diferentes, pues pueden contener troyanos, además revisar la suma de verificación MD5 y la firma GPG[15] del paquete. Los parches son generalmente distribuidos en RPMs. Adicionalmente se debe actualizar el kernel de una forma apropiada, es decir nunca se debe actualizar el kernel, sino instalarlo como si se tratase de un nuevo paquete, posteriormente se debe reiniciar el sistema y desinstalar el kernel antiguo.

Luego de la instalación de Linux, se necesita recompilar el kernel permitiendo[3]:

- Deshabilitar todo el soporte de hardware que no está disponible en este equipo, debido a que se desperdicia espacio en disco, en memoria, o podría ser usado para ataques de negación de servicio (DoS – Deny of Service), para ataques de intrusión si un agujero de seguridad es encontrado en una pieza de código.

- Elegir el uso del equipo, como router, host o servidor debido a que, si se requiere configurar como router se permite que los paquetes IP tomen otra ruta mediante el código del kernel lo cual mejora el desempeño para paquetes que necesitan ser enrutados, pero reduce el desempeño para paquetes que tienen al mismo equipo como destino.

- No cargar todos los módulos por completo y deshabilitar su soporte para mantener al kernel con los módulos necesarios. Deshabilitando el soporte mejora el rendimiento, pero la ventaja principal es que un hacker no podría cargar ningún módulo personalizado que pueda contener algún tipo de código malicioso.

---

[15] **GPG:** GNU Privacy Guard. Es una herramienta para cifrado y firmas digitales que protege la información distribuida a través de Internet garantizando su libre distribución, modificación y uso.

- Añadir características de seguridad que no hayan sido instaladas dentro del kernel inicial, por ejemplo, existen parches que permiten al kernel detectar exploración de puertos, que sería útil para ser usado sobre un firewall.

- En el caso que surgieran problemas de seguridad en el kernel actual y no haya sido liberado un nuevo kernel que arregle dichos problemas, poder aplicar el parche y recompilar el kernel.

- Si se requiere, soporte para hardware especial.

En los equipos servidores se debe: determinar claramente si los servicios que se están ejecutando son críticos para la función del servidor Linux que se está configurando, permitir el arranque únicamente desde el disco duro, habilitar la protección antivirus, establecer contraseña en el BIOS, establecer una contraseña en el GRUB, deshabilitar o modificar la opción Ctrl-Alt-Del, deshabilitar la interfaz gráfica (X Window System), cambiar el nombre de usuario de la cuenta root a cualquier otro, eliminar todas las cuentas de usuario por defecto, tener una cuenta de usuario para cada administrador y así posteriormente cambiarse a la cuenta root si se necesita utilizando el comando su, modificar o eliminar el contenido los archivos /etc/issue y /etc/issue.net puesto que en algunas distribuciones este archivo revela el tipo de sistema operativo y su versión a la persona que intenta acceder al sistema antes de loguearse y un hacker podría aprovechar las vulnerabilidades para esa versión en particular de sistema operativo y atacarlo.

2.1.3.5.2. Sistemas Windows

En primer lugar se debe renombrar la cuenta de Administrador de los sistemas y la cuenta de Administrador del Dominio, debido principalmente a que son cuentas especiales que gozan de un alto nivel de acceso, y son análogas a la cuenta root sobre sistemas Linux, por lo que esta cuenta es el primer blanco de ataques sobre sistemas operativos Microsoft. Deshabilitar la cuenta de invitado, utilizar una cuenta estándar para operaciones comunes con el objetivo de limitar que un virus,

o cualquier otro malware, sea capaz de comprometer el sistema, puesto que generalmente, suelen intentar modificar el Registro o realizar otras acciones para incrustarse en el sistema; lo cual no podrían realizar si no se encuentran con privilegios adecuados.

Habilitar controles de acceso a nivel de archivos, remover software innecesario, deshabilitar servicios innecesarios, parchar el sistema operativo y cualquier software instalado, configurar cuentas de usuario y grupo para proveer solo el mínimo acceso requerido y configurar la red para permitir sólo la mínima conectividad que sea requerida (IP/puerto).

Aplicar configuraciones de seguridad basadas en Group Policies Objects (GPOs) a nivel de dominio o computadores individuales.

2.2. ARQUITECTURA DE RED

Para el diseño se utiliza una solución de arquitectura de red definida, la cual sirve como guía de diseño ya que permite visualizar aspectos relativos a funcionalidad que pasarían por alto si se realizase únicamente en función de requerimientos, especialmente si éstos tienen caraterísticas de seguridad.

A través de Cisco SAFE[11], que es una arquitectura de red desarrollada por ingenieros de Cisco Systems se consideran requerimientos de seguridad en el diseño de redes. Esta arquitectura basa su diseño en forma modular utilizando para ello todos los bloques funcionales de la red, permitiendo de esta forma implementar la seguridad módulo a módulo y no de forma global con un método de defensa en profundidad. Se enfoca esencialmente en las amenazas y en sus métodos de mitigación, en vez de la ubicación de firewalls, IDS y de otras tecnologías.

El diseño se lo hace en forma de capas para no comprometer los recursos de red por si llegase a fallar un sistema de seguridad y se asume que se cuenta con políticas de seguridad establecidas.

A continuación se realiza una revision de los White papers[16] de SAFE que pueden ser considerados para el diseño

SAFE: A Security Blueprint[17] for Enterprise Networks.

Permite la incorporación de seguridad en el diseño de una red empresarial, dividéndola en varios módulos conformados por elementos de común funcionalidad pero con diferentes niveles de obligaciones y confianza con el objetivo de ayudar a mitigar vulnerabilidades y ataques que puedan ocurrir a través de esos dispositivos.

SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks.

Extiende los principios de SAFE Enterprise y los adecua para redes más pequeñas como implementaciones de red autónomas, pequeñas o medianas. Descarta la redundancia de dispositivos de red presente en el SAFE Enterprise con el objetivo de reducir costos y proporcionar seguridad en profundidad a la red incluyendo sistemas de detección de intrusos basados en red.

En este blueprint, la complejidad del módulo de Internet Corporativo es mayor en relación al blueprint para redes pequeñas por el acceso remoto implementado a través de VPNs.

Acorde con los requerimientos de disponibildad de los servicios y aspectos de redundancia en los elementos de la infraestructura de red del Data Center, se realizará el diseño acogiendo las recomendaciones de SAFE Enterprise Network Design del White paper "*SAFE: A Security Blueprint for Enterprise Networks*".

---

[16] **White Paper:** es un informe o guía que aborda problemas y la manera de cómo resolverlos.

[17] **Blueprint:** es un tipo de reproducción de esquemas técnicos que describen una arquitectura o diseño de ingeniería.

2.3. DISEÑO DETALLADO DE RED

Siguiendo la arquitectura de red de Cisco SAFE Enterprise Network el nuevo diseño de la red del Data Center cumplirá con los requerimientos mencionados en el capítulo anterior, para brindar servicios de calidad manteniendo disponibilidad, integridad y confidencialidad de la información para los usuarios del proyecto QuitoEduca.Net.

Para el diseño se pueden identificar a seis módulos autónomos con funcionalidades propias que se encuentran enlazados entre sí.

El módulo de administración contiene a los equipos y elementos necesarios para proveer una administración y gestión segura de los hosts del Data Center utilizando una arquitectura de administración in-band[18].

El módulo núcleo se responsabiliza de que el tráfico que circulan entre las redes sean entregadas rápidamente y de forma confiable mediante conmutación considerando latencia y throughput.

Módulo del edificio se refiere a la porción de la red que provee servicios para las estaciones de trabajo, teléfonos IP y demás dispositivos de capa 2 utilizados por los usuarios de la empresa.

Módulo de Servidores provee los servicios y aplicaciones del Data Center proporcionados para los usuarios de la intranet.

Módulo Internet Corporativo provee acceso a los servicios de Internet a los usuarios internos de la empresa y acceso a los servidores públicos de la empresa por parte de los usuarios de Internet.

Módulo MAN se refiere al tráfico enrutado desde los usuarios remotos de la red SkyPilot al Data Center.

---

[18] **In-band:** arquitectura de administración que utiliza la misma interfaz de red tanto para transmisión de información como para tráfico de administración.

Cada uno de ellos tendrá asignada su propia red, a excepción de los módulos núcleo que se encargarán de la conmutación de las redes pertenecientes a los módulos del Data Center.

2.3.1. MÓDULO DE ADMINISTRACIÓN

La Figura 2.1 muestra el diagrama de red para el módulo de administración.

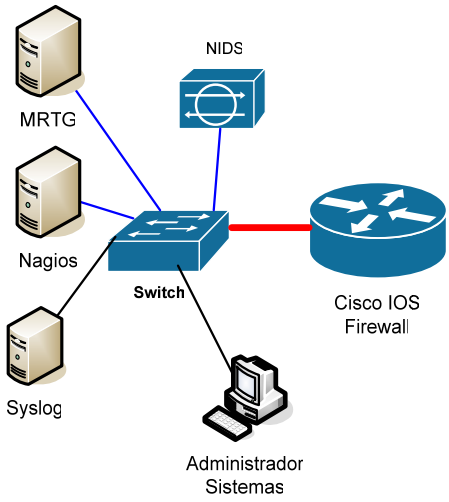


Figura 2.1 Diagrama de red del módulo Administración

Como ya se indicó antes, este módulo se encargará de una administración y monitorización segura de todos los hosts de la red, de la información de los registros para identificación y reportes dirigidos a los hosts de administración, establecimiento de nuevas configuraciones, capacidad de instalación de software desde los hosts de administración a los dispositivos. Para el diseño no se dedicará una interfaz de red exclusiva para tareas de administración sino que se utilizará una arquitectura de administración in-band por lo que requerirá del uso de tuneles basados en IPSec.

La información recogida permitirá determinar configuraciones más eficientes de los sistemas del Data Center y su proyección para futuros requerimientos de capacidad.

En este módulo se considera la instalación de un router con soporte de terminación de VPNs para el tráfico de administración que se transmitirá en el Data Center utilizando IPSec. Además se deberá permitir un acceso remoto y seguro al personal técnico de administración de red para los equipos de este módulo.

2.3.1.1. Elementos de Hardware y Software del módulo de administración

Los principales dispositivos en este módulo son servidores para la administración, servidores para registro de eventos, equipos para administración de sistemas, sistemas de detección o prevención de intrusos basados en red que dependerán de la tecnología o protocolo que se vaya a utilizar. Desde este módulo se realizarán actualizaciones de software, modificación de configuraciones, administración SNMP y de registro de eventos, monitoreo de las interfaces de los hosts de la red, y operará sobre una subred privada completamente aislada del resto de la red con el objetivo de no ser anunciada por algún protocolo de enrutamiento.

2.3.1.1.1. Servidor de administración de Red

Este sistema deberá poseer las herramientas y utilitarios necesarios para el monitoreo, reporte y almacenamiento de los registros de las actividades de los dispositivos, y registro del tráfico manejado por las interfaces de cada host para su análisis.

Este servidor deberá utilizar al protocolo SNMP, mismo que deberá estar instalado en los dispositivos administrados en modo de “sólo lectura” para la obtención de la información de administración.

La capacidad de hardware de este servidor dependerá de las especificaciones del fabricante y de las aplicaciones que se vayan a utilizar para este próposito.

2.3.1.1.2. Sistema de detección y prevención de Intrusos basado en Red.

Se utilizará un sistema de detección y prevención de Intrusos basado en red, IPS, que es un sensor que se encargará de monitorear e inspeccionar todo el tráfico de esta red de administración buscando cualquier actividad maliciosa o de uso indebido en tiempo real comparándolas con una librería embebida de firmas para consecuentemente tomar las medidas necesarias. Cuando este dispositivo detecta una actividad no autorizada las medidas de respuesta pueden ser: terminar con la conexión, bloquear permanentemente al host atacante, registrar el incidente y enviar una alerta al administrador.

2.3.1.1.3. Router

El requerimiento para el Gateway de salida en todos los dispositivos de la red del módulo de administración será un router que permita realizar terminaciones de VPN para manejar el tráfico de administración Syslog y snmp transmitido en texto plano sobre la misma interfaz de red; y el filtrado stateful Inspection para control granular de tráfico entrante y saliente.

Para la implementación de las VPNs se elegirá a IPSec como protocolo de intercambio seguro por su interoperabilidad en la encriptación para garantizar confidencialidad de los datos en tránsito.

Las asociaciones de seguridad se realizarán desde cada sistema y equipo de conectividad de los otros módulos hacia el router del módulo de administración.

El extremo de la red privada virtual será implementada mediante el programa ***racoon***[19] para los sistemas de plataformas Linux, y mediante las directivas de seguridad IP de la Consola de administración Microsoft para las plataformas Windows.

---

[19] **Racoon:** paquete de software para implementaciones de VPN basadas en IPSec.

El protocolo de encripción que se utilizará para las VPN IPSec será ESP[20] debido al soporte para la traducción de dirección de red, con algoritmo de encripción DES[21] porque se trata de un servicio sencillo y no se establecerán funciones de integridad. Cabe aclarar que los dispositivos que se encuentren a lo largo de cada ruta que tomará cada VPN IPSec deben tener establecidas listas de control de acceso que permitan el tráfico para el protocolo UDP en el puerto 500 para ISAKMP, y el puerto 50 para ESP.

A continuación se resume las características mínimas del router basándose en los requerimientos antes mencionados:

- Soporte de VPN basadas en IPSec.
- Firewall Stateful Inspection.
- Soporte para listas de control de acceso.

2.3.1.1.4. Host de administración de sistemas

Desde este equipo se deberán realizar los cambios de las configuración, cambios en el contenido y software de los dispositivos administrados utilizando en lo posible el protocolo secure shell (SSH).

2.3.1.1.5. Switch capa 2

Este switch proveerá la conmutación de los diferentes equipos del módulo y debe permitir establecer un puerto con características de port mirroring o algún otro tipo de protocolo que permita la captura de todo el tráfico de la red para el IPS.

---

[20] **ESP**: Encapsulation Security Payload, añade confidencialidad al tráfico de datos.
[21] **DES:** Data Encryption Standard, posee una clave de 56 bits.

La Tabla 2.3 muestra las caracteristicas requeridas para los equipos de este módulo.

EQUIPO	DESCRIPCIÓN
Router	Capacidad de manejo de tráfico del módulo Administración
	Soporte de protocolos IP, telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	2 Interfaces Fast Ethernet 10/100 Mbps
	Soporte de enrutamiento estático y dinámico como OSPF, RIP v1, RIP v2
	Soporte de DHCP y NAT
	Soporte de QoS
	Características de seguridad, encriptación y autenticación
	Altamente administrable y monitorizable
	Soporte de transmisión de voz
	Soporte de Link Aggregation (LACP-802.3ad) y otro protocolo para tolerancia a fallas
	Manejo de control de acceso a nivel de capa de red (filtrado de paquetes)
	Soporte de IPsec para terminación de VPNs para todos los hosts administrados (100 hosts)
Switch Capa 2	Puerto uplink Gigabit Ethernet para fibra óptica multimodo
	Velocidad de backplane mínima: 1 Gbps
	Auto-negociación de la velocidad de puerto
	Soporte de protocolos telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	Conmutación a nivel de capa 2
	Soporte de Port Mirroring
	Altamente administrable y monitorizable
Sistema de Prevención de Intrusos	1 puerto Fast Ethernet para Monitoreo
	Detectar tráfico malicioso dentro del modulo de usuarios.
	Altamente administrable y monitorizable

Tabla 2.3 Requerimientos en equipos de conectividad del módulo Administración

2.3.2. MÓDULO NÚCLEO

Este módulo se encarga del transporte de grandes cantidades de tráfico provenientes de los diferentes módulos de la red. Debe ser eficiente, robusto y tolerante a fallas.

La Figura 2.2 muestra el diagrama para el módulo núcleo.

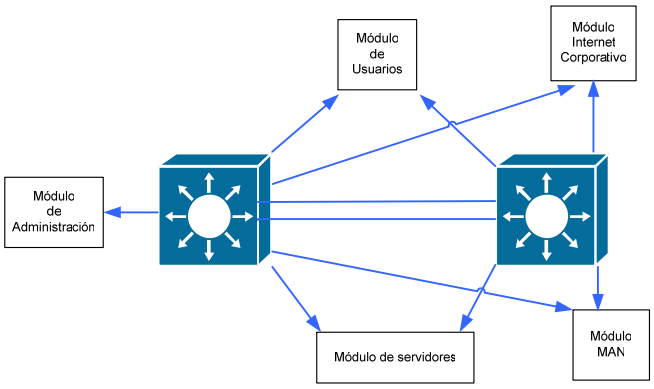


Figura 2.2 Diagrama de red del módulo Núcleo

2.3.2.1. Elementos de Hardware y Software.

Este módulo estará conformado por switches para el manejo del tráfico que provean alta disponibilidad en la conectividad hacia los servicios del Data Center, por lo que se requerirá de dos switchs multicapa con funcionalidades de tolerancia a fallas y redundancia, que deberán tener soporte para el estánndar 802.3ad Link aggregation.

Además para manejar velocidades de transmisión altas se requiere que los enlaces del núcleo hacia los módulos, utilicen un medio fisico de alta velocidad de transmisión. Estos switches mantendrán una configuración similar entre ellos y tendrán las características presentadas en la Tabla 2.4.

EQUIPO	DESCRIPCIÓN
Switches Capa 3	Velocidad de conmutación mínima de 2 000 Mbps
	Autonegociación de la velocidad de los puertos
	Conmutación a nivel de capa de 2 y 3
	Soporte de enrutamiento estático y dinámico como OSPF, RIP v1, RIP v2.
	Soporte de protocolos telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON.
	Calidad de servicio QoS del estándar IEEE 802.1p para priorizar tráfico para aplicaciones en tiempo real
	Protocolo Spanning Tree (IEEE 802.1d)
	Protocolo IPv6
	Enrutamiento InterVLAN
	Soporte de VLAN Trunking
	Soporte de VLANs (IEEE 802.1q)
	Puertos Gigabit Ethernet
	Puertos Fast Ethernet
	Protocolo para redundancia de enlaces Link Aggregation (IEEE 802.3ad)
	Soporte de control de acceso a nivel de capa de red
	Altamente administrable y monitorizable

Tabla 2.4 Requerimientos en equipos de conectividad del módulo Núcleo

2.3.3. MÓDULO DE USUARIOS.

A este módulo pertenecen las estaciones de trabajo, impresoras, cámaras IP, teléfonos IP de la red interna de la empresa, los cuales pueden pertenecer a varios grupos de trabajo. Las estaciones deberán tener instalado un software antivirus utilizando el procedimiento de Guias de Antivirus del numeral 2.1.3.4, y contar con un sistema de protección de intrusos basados en Host para la prevención de software malicioso como virus o caballos de troya.

El diseño del módulo usuarios se realizará de acuerdo al diagrama de red de la Figura 2.3.

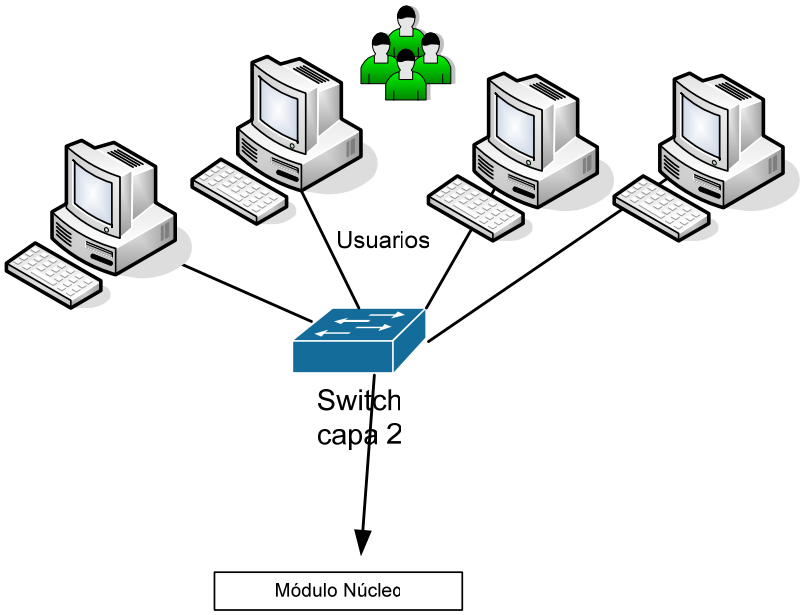


Figura 2.3 Diagrama de red del módulo Usuarios

El switch para este módulo deberá permitir un manejo de VLANs que dependerán del número de empleados y usuarios internos que requierán acceso a los servicios del Data Center. Los grupos de usuario de la empresa estarán establecidos de acuerdo a la Tabla 2.5.

Grupo de Usuarios	Número de Usuarios
Gerencia	1
Proyectos	2
Administrativo/Financiero	2
Diseño	3
Desarrollo de software	3
Soporte de software	5

Tabla 2.5 Número de usuarios conectados a la Intranet de la empresa

No se consideraron hosts para administración de red puesto que estos se encontrarán conectados al módulo de administración.

La configuración de acceso a Internet para las estaciones de trabajo de los usuarios internos se lo realizará a través de un proxy ubicado en el módulo de Internet Corporativo con el que se realizará filtrado de contenido, horarios de acceso y bloqueo de servicios por grupo de usuarios o por usuario.

Además se recomienda el uso de un software antivirus para mitigar ataques de virus, spyware, troyano u otro programa malicioso para implementar la seguridad a nivel de estación de trabajo. Los equipos de este módulo deben cumplir con los requerimientos de la Tabla 2.6.

EQUIPO	DESCRIPCIÓN
Switch	Puerto uplink Gigabit Ethernet para fibra óptica multimodo
	Soporte de VLANs (IEEE 802.1Q)
	Soporte de Port Trunking y VLAN Trunking Protocol
	Auto-negociación de la velocidad de puerto
	Soporte de protocolos telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	Conmutación a nivel de capa 2
	Altamente administrable y monitorizable

Tabla 2.6 Requerimientos en equipos de conectividad del módulo Usuarios

El control de acceso para este módulo, a nivel de capa de red, será proporcionado por los switches capa 3 que se encuentra en el módulo núcleo.

2.3.4. MÓDULO SERVIDORES

El diseño de este módulo será de acuerdo al diagrama de red de la Figura 2.4.

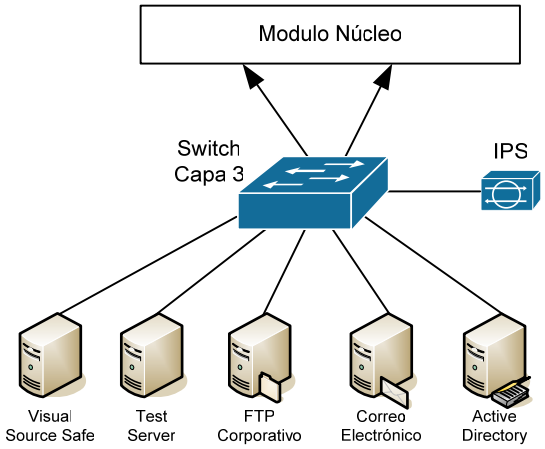


Figura 2.4 Diagrama de red del módulo Servidores

Éste módulo se encuentra conformado por los siguientes servidores que alojan a los servicios de la Intranet.

- Active Directory.
- DNS interno.
- Correo electrónico.
- Servidor de pruebas de software.
- Visual Source Safe.
- NTP.

Para la conectividad de los servidores hacia el resto del Data Center se utilizarán un switch capa 2 que se encargará de evitar la falsificación de direcciones IP al bloquear los paquetes salientes cuya dirección IP origen no pertenezca a la red de servidores. Además con este dispositivo se implementarán redes privadas virtuales asociando la funcionalidad de cada servidor con el personal de la empresa que requiera uso exclusivo del equipo o desde los servidores de la DMZ que requieran una conexión hasta uno de ellos.

Se utilizará además dos sensores IPS basados en red conectados a una de las interfaces del switch que deberán estar configurados con port mirroring con el fin de detectar ataques de capa aplicación sobre los equipos servidores.

A continuación, en la Tabla 2.7 se detallan las características requeridas para los dispositivos de conectividad en este módulo.

EQUIPO	DESCRIPCIÓN
Switch	Puerto uplink Gigabit Ethernet para fibra óptica multimodo
	12 Puertos Fast Ethernet 10/100 Mbps (Autonegociación de la velocidad de los puertos)
	Soporte de VLANs (IEEE 802.1Q)
	Soporte de Port Trunking y VLAN Trunking Protocol
	Auto-negociación de la velocidad de puerto
	Soporte de protocolos telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	Conmutación a nivel de capa 2
	Altamente administrable y monitorizable
	Soporte de Port Mirroring
Sistema de Prevención de Intrusos	1 puerto Fast Ethernet para Monitoreo
	Detectar tráfico malicioso dentro del modulo de usuarios.
	Altamente administrable y monitorizable

Tabla 2.7 Requerimientos en equipos de conectividad del módulo Servidores

2.3.5. MÓDULO INTERNET CORPORATIVO

El diseño de este módulo será de acuerdo al diagrama de red de la Figura 2.5.

Este módulo provee la conectividad necesaria de los usuarios internos hacia el Internet y a los servicios públicos de la DMZ, y el acceso de los usuarios de Internet a los servicios públicos como Web/FTP, REV, Mail Relay, DNS y Filtrado de URLs.

Por motivos de disponibilidad se contratará dos enlaces de Internet con proveedores diferentes para realizar un balanceo de carga y proveer redundancia para el acceso a los servicios desde Internet.

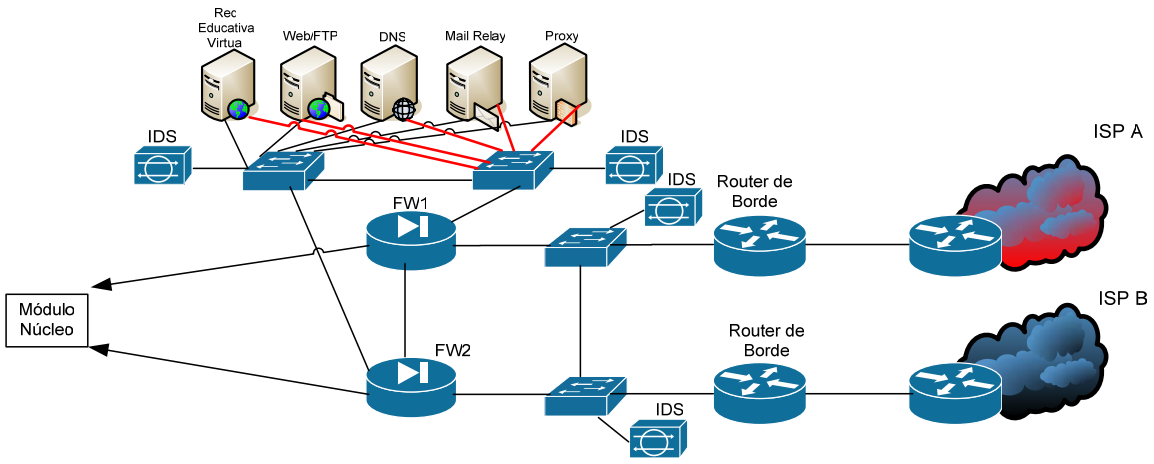


Figura 2.5 Diagrama de red del módulo Internet Corporativo

Cada ISP deberá proveer una subred de direcciones IPs públicas con máscara 255.255.255.252 y con la respectiva responsabilidad de delegación de los registros de mapeado para esa subred.

2.3.5.1. Elementos de Hardware y Software.

2.3.5.1.1. Routers de borde

Además del enrutamiento proveerán de un balanceo de carga y tolerancia a fallas mediante la utilización del protocolo HSRP[22], que es propietario de Cisco.

Las listas de control de acceso impedirán ataques de falsificación de direccion IP origen, filtrará el tráfico de acuerdo al servicio esperado y bloquearán paquetes IP fragmentados.

El balanceo de carga de los enlaces a Internet para acceso a los servicios se realizará utilizando el procedimiento Round Robin DNS.

---

[22] **HSRP:** Hot Standby Router Protocol. Aumenta la disponibilidad de la puerta de enlace por defecto mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico.[12]

2.3.5.1.2. Servidores

En la red de servidores se alojarán los equipos necesarios para la provisión de los servicios de Mail Relay, DNS externo, REV y Web, estos servidores se encontrarán conectados al segmento de red DMZ.

2.3.5.1.3. Firewall

El firewall Stateful inspection[34] analizará el inicio de cualquier flujo de datos y mantendrá la información de estado del flujo correspondiente a las direcciones IP, números de secuencia y puertos usados. Se encargarán del redireccionamiento de puertos hacia cada servicio que provee cada servidor de la DMZ.

El firewall utilizará tres direcciones IP para los segmentos DMZ, externa e interna. Además deberá tener funciones de NAT y PAT para proveer servicios utilizando una única dirección IP pública en la interfaz externa de forma que los diferentes tipos de tráfico FTP, HTTP y DNS puedan completarse.

El firewall se encargará de mitigar ataques de acceso no autorizado y falsificación de direcciones IP mediante listas de control de acceso, además ayudará a impedir ataques de negación de servicio utilizando controles en las conexiones TCP.

Se dispondrá de dos equipos firewalls para mantener una alta disponibilidad al incorporar redundancia.

2.3.5.1.4. Sistema de prevención de Intrusos

Los sistemas de prevención de intrusos basados en red se ubicarán en los puntos clave de la red trabajando en modo promiscuo para actuar automáticamente contra posibles amenazas que pudieren suscitarse. Su ubicación será:

Segmento de red de los servicios públicos del firewall, para el monitoreo y detección de ataques complejos de capas 4 a 7 como ataques de password contra un servicio protegido que el firewall no puede detectar.

Lado público del firewall, se encargará de la monitorización de ataques analizando el tráfico de capa 4 a capa 7 y comparándolos contra firmas conocidas. Las alarmas deberán estar establecidas a un bajo nivel porque en este lado no pueden suscitarse brechas de seguridad sino sólo intentos.

2.3.5.1.5. Switch de capa 2

Los switches se encargarán de la conmutación entre los diferentes elementos de la red, además deberán tener configurado un puerto como port mirroring para monitoreo de amenazas realizadas por el IPS que trabajará en modo promiscuo.

Las características de los equipos de conectividad para este módulo se detallan en la Tabla 2.8.

EQUIPO	DESCRIPCIÓN
Switches Servidores DMZ	12 Interfaces Fast Ethernet 10/100 Mbps, Auto-negociación de la velocidad de puerto
	Soporte de protocolos telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	Conmutación a nivel de capa 2
	Altamente administrable y monitorizable
	Puerto Port Mirroring
Switches Outside	8 Interfaces Fast Ethernet 10/100 Mbps, Auto-negociación de la velocidad de puerto
	Soporte de protocolos telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	Conmutación a nivel de capa 2
	Altamente administrable y monitorizable
	Puerto Port Mirroring
Routers de Borde Intranet/DMZ	Capacidad de manejo de tráfico contratado para el acceso a Internet
	Soporte de protocolos IP, telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	2 Interfaces Fast Ethernet 10/100 Mbps
	Soporte de enrutamiento estático y dinámico como OSPF, RIP v1, RIP v2
	Soporte de QoS
	Soporte de DHCP y NAT

Tabla 2.8 Requerimientos en equipos de conectividad del módulo Internet Corporativo

	Características de seguridad, encriptación y autenticación
	Altamente administrable y monitorizable
	Soporte de transmisión de voz
	Soporte de Link Aggregation (LACP-802.3ad) y otro protocolo para tolerancia a fallas
	Manejo de control de acceso a nivel de capa de red. (filtrado de paquetes)
Routers internos	Capacidad de manejo de tráfico del módulo Internet corporativo
	Soporte de protocolos IP, telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	2 Interfaces Fast Ethernet 10/100 Mbps
	Soporte de enrutamiento estático y dinámico como OSPF, RIP v1, RIP v2
	Soporte de QoS
	Características de seguridad, encriptación y autenticación
	Altamente administrable y monitorizable
	Soporte de transmisión de voz
	Soporte de Link Aggregation (LACP-802.3ad) y otro protocolo para tolerancia a fallas.
	Manejo de control de acceso a nivel de capa de red. (filtrado de apquetes)
Firewalls	Stateful Inspection
	Soporte de NAT/PAT
	2 Interfaces 10/100 Mbps Fast Ethernet, Half/Full Duplex
	Redundante contra fallas para proveer alta disponibilidad
	Soporte de VLANs (IEEE 802.1Q).
	Soporte de SNMP y syslog
	Altamente administrable y monitorizable
	Soporte de VPNs
Sistema de Prevención de Intrusos	4 puertos Fast Ethernet de Monitoreo
	Detectar tráfico malicioso dentro del modulo de usuarios.
	Altamente administrable y monitorizable

Tabla 2.9 Requerimientos en equipos de conectividad del módulo Internet Corporativo

2.3.6. MÓDULO MAN

La Figura 2.6 representa el diagrama de red del módulo MAN.

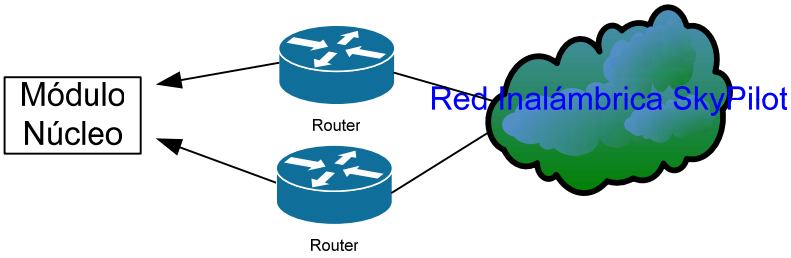


Figura 2.6 Diagrama de red del Módulo MAN

Está conformado por un router y por la infraestructura de red de acceso inalámbrico Skypilot. El router se encargará de proveer enrutamiento IP hacia el núcleo desde la red inalámbrica Skypilot, evitará ataques de falsificación de direcciones IP origen mediante un filtrado capa 3 y un control de acceso al núcleo permitiendo el ingreso de paquetes de protocolos específicos como Web, DNS, imap, pop3 y smtp. Las características de estos routers están en la Tabla 2.9.

EQUIPO	DESCRIPCIÓN
Routers	Capacidad de manejo de tráfico del módulo MAN
	Soporte de protocolos IP, telnet, SNMPv1, SNMPv2, SNMPv3, syslog, RMON
	2 Interfaces Fast Ethernet 10/100 Mbps
	Soporte de enrutamiento estático y dinámico como OSPF, RIP v1, RIP v2
	Soporte de DHCP y NAT
	Soporte de QoS
	Características de seguridad, encriptación y autenticación
	Altamente administrable y monitorizable
	Soporte de transmisión de voz
	Soporte de Link Aggregation (LACP-802.3ad) y otro protocolo para tolerancia a fallas
	Manejo de control de acceso a nivel de capa de red. (filtrado de paquetes)

Tabla 2.9 Requerimientos en equipos de conectividad del módulo MAN

2.4. DIRECCIONAMIENTO IP

Debido al número de los dispositivos de red y servidores del Data Center y los equipos servidores SGA remotos conectados a la red inalámbrica Skypilot, se escoge la red clase C: 192.168.100.0, que forma parte del rango de direcciones privadas. Todos los equipos que incluyen estaciones de trabajo, servidores, routers, firewalls, switches administrables mantendrán un direccionamiento estático por el manejo de registros del servicio de DNS.

A toda la red se la dividirá en subredes de acuerdo al número de equipos que contenga y el enrutamiento se lo realizará utilizando el protocolo RIP versión 2.

La asignación y los rangos para el direccionamiento IP de las subredes se encuentran en la Tabla 2.10.

SEGMENTO	SUBRED/MASK	DIRECCIONES IP VÁLIDAS		PUERTA DE ENLACE PREDETERMINADA
		INICIAL	FINAL	
Administración	192.168.100.0/29	192.168.100.1	192.168.100.5	192.168.100.6
Desarrollo	192.168.100.8/29	192.168.100.9	192.168.100.13	192.168.100.14
Proyectos	192.168.100.16/29	192.168.100.17	192.168.100.21	192.168.100.22
Diseño	192.168.100.24/29	192.168.100.25	192.168.100.29	192.168.100.30
Gerencia	192.168.100.32/29	192.168.100.33	192.100.100.37	192.168.100.38
Servidores de desarrollo software	192.168.100.40/29	192.168.100.41	192.168.100.45	192.168.100.46
Servidores	192.168.100.48/29	192.168.100.49	192.168.100.53	192.168.100.54
dmz	192.168.100.64/28	192.168.100.64	192.168.100.77	192.168.100.78
Soporte técnico	192.168.100.80/28	192.168.100.81	192.168.100.93	192.168.100.94
Administración de red	192.168.100.96/28	192.168.100.97	192.168.100.109	192.168.100.110
MAN	192.168.100.128/25	192.168.100.129	192.168.100.253	192.168.100.254
Conexión Administración de red-core	192.168.100.112/30	192.168.100.113	192.168.100.114	
Conexión1 Internet-core	192.168.100.116/30	192.168.100.117	192.168.100.118	
Conexión2 Internet-core	192.168.100.120/30	192.168.100.121	192.168.100.122	
Conexión MAN-core	192.168.100.124/30	192.168.100.125	192.168.100.126	

Tabla 2.10 Direccionamiento IP de los segmentos de red

2.5. DISEÑO DE VLAN

Algunos de los segmentos de red utilizarán VLANs para proveer seguridad y para agrupar dominios de broadcast en el acceso a los recursos. Estará conformada

por ocho subredes asociadas con VLANs independientes para cada uno de los siguientes departamentos de trabajo de la empresa: Gerencia, administración, Servidores, Desarrollo de software, proyectos, soporte técnico, servidores de desarrollo de software y diseño Web. Para esto se requiere establecer dominios para la administración de usuarios y servicios que contendrán computadores o servidores. En la Tabla 2.11 se especificará la asociación del nombre de las VLAN con los segmentos realcionados a cada departamento de la empresa.

SEGMENTO	VLAN	SUBRED/MASK	DIRECCIONES IP VÁLIDAS		PUERTA DE ENLACE
			INICIAL	FINAL	
Administración	COGLADMIN	192.168.100.0/29	192.168.100.1	192.168.100.5	192.168.100.6
Desarrollo	COGLDES	192.168.100.8/29	192.168.100.9	192.168.100.13	192.168.100.14
Proyectos	COGLPRO	192.168.100.16/29	192.168.100.17	192.168.100.21	192.168.100.22
Diseño	COGLDIS	192.168.100.24/29	192.168.100.25	192.168.100.29	192.168.100.30
Gerencia	COGLGER	192.168.100.32/29	192.168.100.33	192.100.100.37	192.168.100.38
Servidores de desarrollo software	SRVDES	192.168.100.40/29	192.168.100.41	192.168.100.45	192.168.100.46
Servidores	COGLSRV	192.168.100.48/29	192.168.100.49	192.168.100.53	192.168.100.54
Soporte técnico	COGLSOP	192.168.100.80/28	192.168.100.81	192.168.100.93	192.168.100.94

Tabla 2.11 Direccionamiento IP de las VLANs

Para las VLANs se requerirá de los protocolos IEEE 802.1Q VLAN y del protocolo VTP[23] para su administración a lo largo de toda la red.

Se utilizará el modo Servidor del protocolo VTP sobre el switch de core, y los demás swtiches estarán configurados en modo cliente. Todos los switches se mantendrán en el dominio VTP *cogl* con password *coglsafe*. Se proporcionará un enrutamiento InterVLAN sobre los switches del núcleo y utilizando listas de control de acceso se filtrará para bloquear o permitir la comunicación entre las diferentes subredes y VLANs como se indica en la Tabla 2.12.

[23] **VTP:** VLAN Trunking Protocol, usado para configurar y administrar VLANs en equipos Cisco.

Tabla 2.12 Control de acceso entre las diferentes subredes

Outbound/Inbound	*Administración*	*Desarrollo*	*Proyectos*	*Diseño*	*Gerencia*	*Servidores de desarrollo software*	*Servidores*	*DMZ*	*Soporte técnico*	*Administración de Red*	*MAN*
Administración		negar	negar	negar	negar	negar	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicio Web	negar	Permitir acceso a solo a los puertos de los servicios de administración	negar
Desarrollo	negar		negar	negar	negar	permtir	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicio Web	negar	Permitir acceso a solo a los puertos de los servicios de administración	negar
Proyectos	negar	negar		negar	negar	negar	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicio Web	negar	Permitir acceso a solo a los puertos de los servicios de administración	negar
Diseño	negar	negar	negar		negar	negar	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicio Web	negar	Permitir acceso a solo a los puertos de los servicios de administración	negar
Gerencia	negar	negar	negar	negar		permitir	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicio Web	negar	Permitir acceso a solo a los puertos de los servicios de administración	negar
Servidores de desarrollo software	negar	permtiir	negar	negar	permitir		Permitir acceso solo a servicios DNS, NTP. FTP, NetBIOS	Negar	negar	Permitir acceso a solo a los puertos de los servicios de administración	negar
Servidores	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicios DNS, NTP. FTP, NetBIOS		Permitir acceso solo a servicios DNS, NTP, SMTP	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso a solo a puertos de protocolos de administración y a servicios DNS, NTP, SMTP, IMAP, POP3	Permitir acceso solo a servicios DNS, NTP, SMTP, IMAP, POP3, M-SQL
DMZ	permitir	permitir	permitir	permitir	permitir	negar	Permitir acceso solo a servicios DNS, NTP, SMTP.		permitir	Permitir acceso a solo a los puertos de los servicios de administración	permitir
Soporte técnico	negar	negar	negar	negar	negar	negar	permitir	Permitir acceso solo a servicio Web		Permitir acceso a solo a los puertos de los servicios de administración	permitir
Administración de red	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración	Permitir acceso a solo a los puertos de los servicios de administración y Web	Permitir acceso a solo a los puertos de los servicios de administración		Permitir acceso a solo a los puertos de los servicios de administración
MAN	negar	negar	negar	negar	negar	negar	puertos	Permitir acceso solo a servicio Web	permtir	Permitir acceso a solo a los puertos de los servicios de administración	

2.6. PROYECCIÓN DE CRECIMIENTO A TRES AÑOS

Previo al dimensionamiento de las capacidades de los enlaces y equipos importantes del Data Center, se debe analizar la proyección de crecimiento de la intranet y conocer quiénes tendrán acceso a los servicios con el fin de proporcionar una visión del número de usuarios futuros.

Es importante determinar el crecimiento futuro de la red ya que se debe garantizar la estabilidad del hardware y software.

Se puede determinar una proyección de futuros usuarios, considerada por el número de instituciones que serán integradas a la red de servicios.

En la Tabla 1.9 se puede observar el número de instituciones que se han ido integrando al Proyecto QuitoEduca.Net durante los años 2007 y 2008, gracias a estos valores se puede obtener una tendencia de la integración de nuevas instituciones en los siguientes tres años.

Esta línea de tendencia representa la posible proyección de crecimiento futuro de usuarios que solicitarán servicios.

Pueden considerarse tendencias de crecimiento exponencial, lineal, logarítmico, polinómico y potencial.

Se ha seleccionado una tendencia polinómica debido a que su curva (mostrada en color rojo en la Figura 2.7) se aproxima mejor al incremento de instituciones en los años anteriores, y permite un crecimiento similar en los años siguientes.

Una vez completa la lista de instituciones que serán integradas a los beneficios del Proyecto QuitoEduca.Net, la curva se mantiene constante.

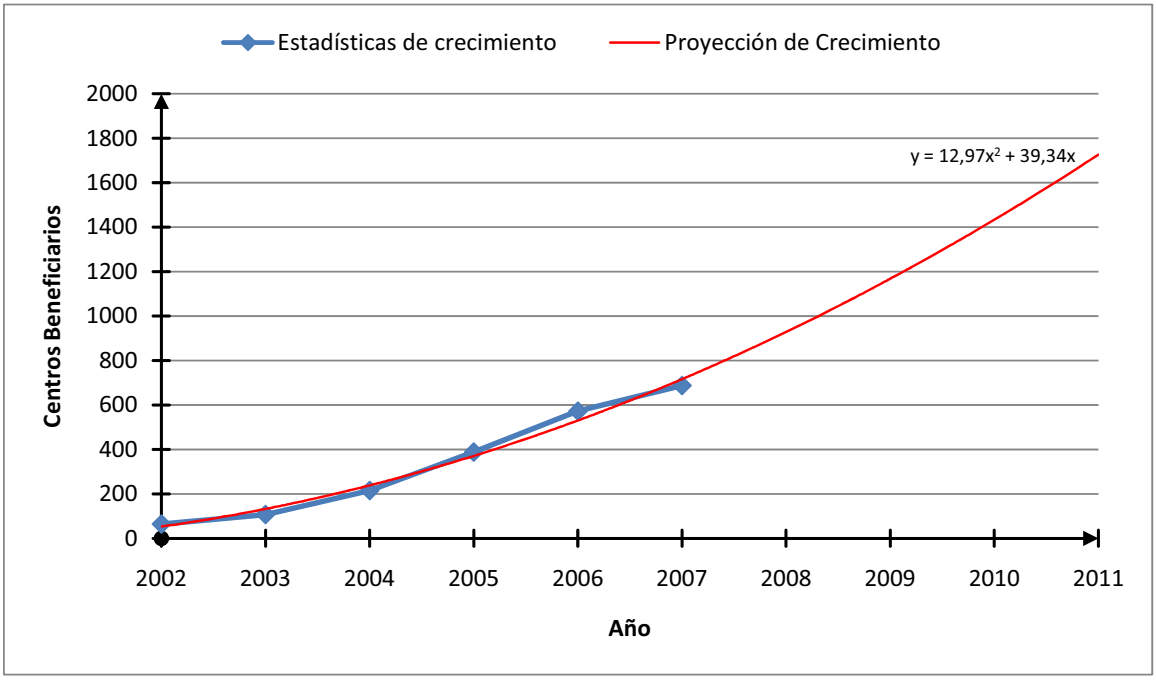


Figura 2.7 Estadísticas y Proyección de Integración de los Centros Educativos al Proyecto QuitoEduca.Net

La proyección de integración, obtenida gracias a la herramienta de cálculo Microsoft Excel está determinada por la ecuación 2.1:

$$y = 12.97x^2 + 39.34x$$

Ecuación 2.1 Proyección de integración de centros educativos al Proyecto

Donde:

$y \rightarrow$ Número de instituciones beneficiarias del Proyecto QuitoEduca.Net

$x \rightarrow$ Número de años desde que se inició el proyecto.

La Tabla 1.10 muestra el número de instituciones que se han integrado a la red de datos de Conectividad Global Cía. Ltda. La implementación de puntos de acceso, es decir, la instalación y configuración de los dispositivos SkyConnector no ha tenido un crecimiento rápido. Se proyecta un crecimiento igual durante los siguientes tres años por lo que se considera una proyección de tendencia lineal (mostrada en color rojo en la Figura 2.8).

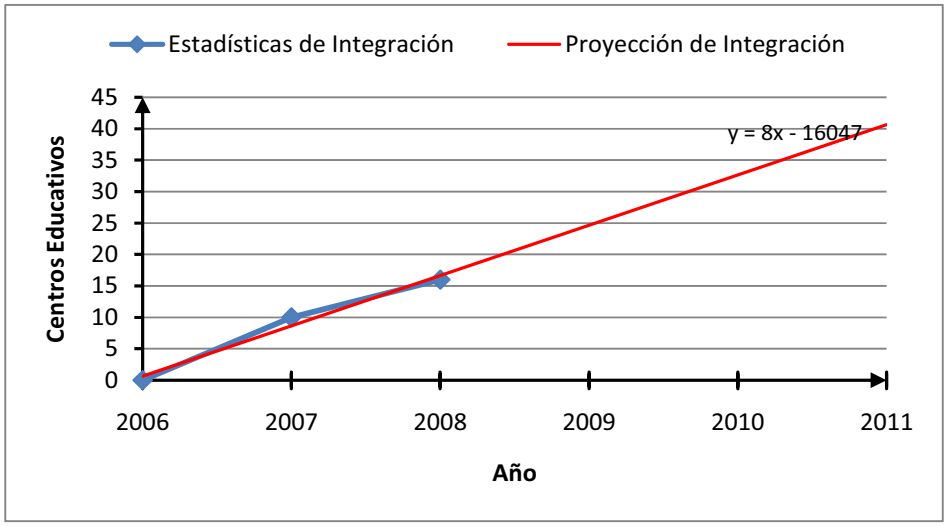


Figura 2.8 Estadísticas y Proyección de Integración de los Centros Educativos a la Red de Servicios del Proyecto QuitoEduca.Net

La línea de proyección, obtenida a través de las herramientas Microsoft Excel está determinada por la ecuación 2.2:

$$y = 8x - 16047$$

Ecuación 2.2 Proyección de integración de centros educativos a la red de servicios del Proyecto

Donde:

$y \rightarrow$ Número de instituciones integradas a la red de servicios del Data Center.

$x \rightarrow$ Año en el que se estima la proyección.

2.7. ANÁLISIS DE LA CAPACIDAD REQUERIDA PARA LOS MÓDULOS DE LA RED

La capacidad de los enlaces en cada uno de los módulos del diseño propuesto se calculará en base a la proyección de uso de los diferentes servicios en la red.

2.7.1. ESTIMACIÓN DE LA CAPACIDAD DE LOS ENLACES A INTERNET

Se analiza la capacidad necesaria del enlace a Internet tanto para uplink (tráfico hacia Internet) como para downlink (tráfico desde Internet).

2.7.1.1. Enlace Downlink

Solamente se considerará al tráfico generado por los usuarios del servicio de correo electrónico que acceden por Internet y el porcentaje de correos que ingresan desde dominios externos hacia los dominios locales del servidor de correo. Las solicitudes hacia las aplicaciones y sitios web en el Data Center se consideran despreciables.

2.7.1.1.1. Correo Electrónico

Usuarios de Internet

El personal administrativo de las instituciones participantes del proyecto que no se encuentren en la Intranet acceden a este servicio a través de Internet utilizando WebMail. Para estimar la capacidad de este enlace se tomará como punto de partida el servidor fw.remq.edu.ec debido a que contiene el 79.01% de cuentas de correo alojadas en el Data Center (Dato obtenido de la Tabla 1.2). Los valores mostrados en el Anexo F.4 fueron recolectados durante 34 días, 21 horas y 4 minutos por la consola de administración Kerio Mail Server y sirvieron para realizar algunas de las siguientes consideraciones:

- Tamaño promedio del correo electrónico es de 24 KBytes.

$$\frac{\text{Volumen de mensajes recibidos}}{\text{Número de mensajes recibidos}} = \frac{393\text{MB}}{16961} * \frac{1024\text{KB}}{1\text{MB}} = 23.72KB \approx 24KB$$

- Simultaneidad promedio de uso del servicio de correo electrónico por parte de usuarios que acceden desde Internet es de 5%. Dato obtenido del

Anexo F.4 tomando el valor promedio aproximado de la gráfica de Conexiones SMTP.

$$\frac{75 \text{ conexiones}}{1591 \text{ cuentas}} * 100 = 4.71 \approx 5\%$$

- Tiempo aceptable de entrega de 60 segundos.
- El 17% del tráfico de correo electrónico que ingresa al servidor proviene de dominios externos. Dato obtenido de la relación:

$$\frac{(\text{mensajes RX por el servidor} - \text{mensajes entregados a dominios locales}) * 100}{\text{mensajes RX por el servidor}}$$

$$= \frac{16961 - 14070}{16961} * 100 = 17\%$$

- El número total de cuentas que se almacenarán en el servidor será de cinco para cada institución educativa integrada de acuerdo a la proyección determinada por la ecuación 2.1, es decir, 1691 instituciones para el 2011.

$$\#\text{Usuarios} = \#instituciones\ educativas \times 5$$
$$\#Usuarios = 1691 \times 5 = 8455$$

Ecuación 2.3 Cálculo del número de usuario con cuentas de correo electrónico

$$C_{Usuario} = \frac{\text{Tamaño E-mail}}{\text{Tiempo de Entrega}} = \frac{24k \times 8}{60s} = 3.2[kbps]$$

Ecuación 2.4 Cálculo de la capacidad necesaria para envío de e-mail por Usuario

$$C_{correoElectronicoDL} = C_{Usuario} \times \#\text{usuarios} \times \text{simultaneidad} = 3.2[kbps] \times 8455 \times 0.05 = 13528[kbps]$$

Ecuación 2.5 Cálculo de la capacidad downlink del servicio de correo electrónico en el Data Center

$$C_{Downlink} = 13528[kbps] \approx 1408[kbps]$$

Ecuación 2.6 Capacidad necesaria downlink de Internet

2.7.1.2. Enlace uplink

Para el cálculo se considerará el tráfico de los distintos servicios que se proveen en la DMZ como correo electrónico, servicio y aplicaciones web.

2.7.1.2.1. Correo electrónico

Para dimensionar la capacidad del enlace necesario para el envío de correo electrónico se considerará a los usuarios que forman parte de la Intranet y el total de correos enviados hacia dominios externos.

Cada usuario de la empresa Conectividad Global Cia. Ltda. tendrá una cuenta de correo electrónico sumando un total de 20.

Grupo de Usuarios	Número de Usuarios
Gerencia	1
Proyectos	2
Administrativo/Financiero	2
Diseño	3
Desarrollo de software	3
Soporte de software	5
Administración de Red	4
Total	20

Tabla 2.13 Número de cuentas de correo electrónico del personal de Conectividad Global Cia. Ltda.

Usuarios Totales.

Del Anexo F.4 se obtiene que aproximadamente el 12.72% de los mensajes de correo tienen como destino dominios externos, por lo que la consideración de que el 15% de los correos enviados a otros dominios es acertada. Es necesario realizar algunas consideraciones:

$$\text{Destino dominios externos} = \frac{\text{mensajes enviados a servidores remotos}}{\text{mensajes transmitidos por el servidor}} * 100 =$$

$$= \frac{2050}{16120} * 100 = 12.72\%$$

- Tamaño promedio de e-mail de 25 kBytes.

$$\frac{\text{Volumen de mensajes transmitidos}}{\text{Número de mensajes transmitidos}} = \frac{398.9\,\text{MB}}{16120} * \frac{1024\,\text{KB}}{1\,\text{MB}} = 25.34KB$$

- Tiempo aceptable de entrega de 60 segundos.

- Factor de uso del 3%. Número de conexiones obtenido del Anexo F.3 y número de cuentas de la Tabla 1.3.

$$\frac{40 \text{ conexiones}}{1591 \text{ cuentas}} * 100 = 2.51 \approx 3\%$$

- El 15 % del tráfico de correo electrónico sale al exterior.

- El número total de cuentas que se almacenarán en el servidor será de cinco para cada institución educativa integrada a la Intranet de acuerdo a la proyección determinada por la ecuación 2.2, es decir, 41 instituciones para el 2011. Se considera también los usuarios que acceden al servicio vía web para enviar correo a dominios externos.

$$\#\,\text{Usuarios} = \#\,\text{instituciones educativas} \times 5 + \#\,\text{usuarios de Conectividad Global}$$
$$\#\,Usuarios = 1691 \times 5 + 20 = 8475$$

Ecuación 2.7 Cálculo del número de usuarios que usan correo electrónico.

$$C_{Usuario} = \frac{\text{Tamaño E-mail}}{\text{Tiempo de Entrega}} = \frac{25k \times 8}{60s} = 3.33[kbps]$$

Ecuación 2.8 Cálculo de la capacidad del enlace requerida para envío de correo electrónico por usuario.

$$C_{correoElectrónicoInternet} = C_{Usuario} \times \#usuarios simultaneidad = 3.33[kbps] \times 8475 \times 0.03 = 84665[kbps]$$

Ecuación 2.9 Cálculo de la capacidad del enlace para correo electrónico en la Intranet.

$$C_{InternetcorreoElectronico} = 0.15 \times C_{CorreoElectronico} = 0.15 \times 84665[kbps] = 12699[kbps]$$

Ecuación 2.10 Capacidad del enlace para correo electrónico saliente a dominios externos.

2.7.1.2.2. Web

Se establecerán las siguientes consideraciones para la provisión de este servicio:

- El tamaño promedio de una página Web es de 150 kbytes para un sitio Web Joomla o Moodle.
- El número promedio de páginas descargadas por día desde el servidor es de 5329. Valor obtenido del Anexo G.

$$Pág/seg = \frac{5329 \text{ páginas descargadas}}{86400 \text{ segundos}} = 0.062\left[\frac{\text{pág}}{\text{seg}}\right]$$

- Actualmente existen 58 sitios web alojados en el Data Center, el número máximo de sitios para el 2011 será de 1691. Por lo que la tasa de crecimiento será de 29,2 veces.

$$C_{Web} = Pág/seg \times \text{tamaño de página} \times \text{tasa de crecimiento} =$$
$$0.062\left[\frac{pág}{s}\right] * (150 * 8)\left[\frac{\text{kbits}}{\text{pág}}\right] * 29 = 2146.4[kbps]$$

Ecuación 2.11 Capacidad uplink para el servidor Apache.

La capacidad requerida para Uplink será de:

$$C_{Uplink} = C_{Web} + C_{CorreoElectronico} = 21464 + 12699 = 227339[kbps]$$

Ecuación 2.12 Cálculo para la capacidad Uplink a Internet.

$$C_{Uplink} = 227339[kbps] \approx 2304[kbps]$$

Ecuación 2.13 Capacidad para el enlace Uplink a Internet.

Se contratarán dos enlaces simetricos iguales en capacidad pero de proveedores diferentes. La capacidad de cada enlace será la mitad del total requerido ya que se piensa proveer balanceo de carga y redundancia para tolerancia a fallas. La capacidad excedente en downlink se utilizará para navegación web.

$$C_{Internet\,simetrico} \approx 2 \times 1152[kbps]$$

Ecuación 2.14 Capacidad a contratar del enlace a Internet.

2.7.2. CÁLCULO DE TRÁFICO EN EL MÓDULO INTERNET CORPORATIVO

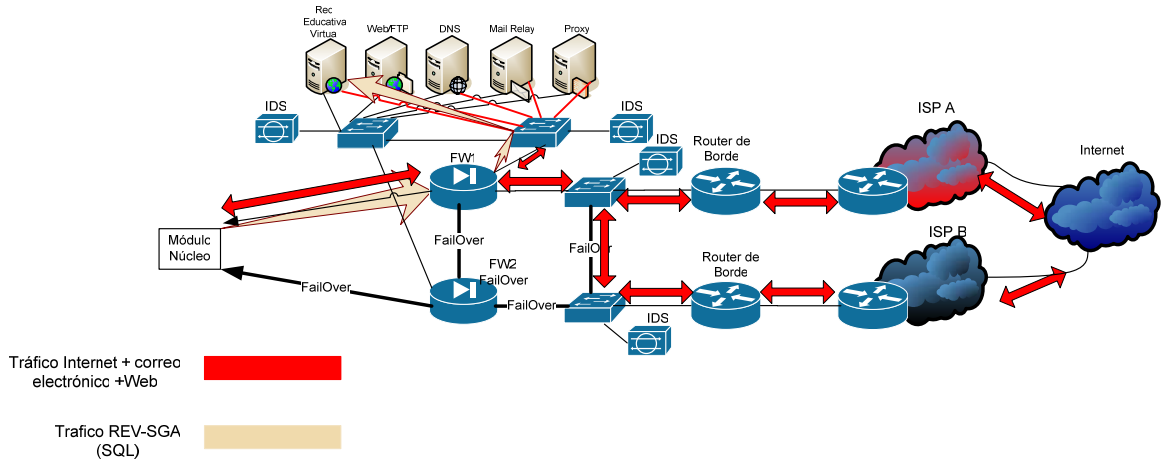


Figura 2.9 Flujo de tráfico del módulo Internet Corporativo

Para el cálculo del tráfico en este módulo se considerará el tráfico de las consultas realizadas a las bases de datos Microsoft SQL Server de la aplicación SGA a los 41 establecimientos educativos que se encontrarán conectados a la Intranet más el tráfico de Internet.

El tráfico hacia los sitios Web desde la Intranet se considerará despreciable por ser esta una red de alta velocidad.

La aplicación REV de las instituciones educativas consulta a las bases de datos de la aplicación SGA instalada sobre cada una de la 61 institutciones educativas. Para el cálculo de la capacidad se harán las siguientes consideraciones:

- La capacidad promedio necesaria para consultas transaccionales a las bases de datos es de 30kbps de acuerdo al reporte del tráfico del servidor sga.conectividadglobal.net que tiene instalado a la aplicacion REV de la Tabla 1.14.

$$C_{BD\text{-}REV} = 30[\text{kbps}]$$

Ecuación 2.15 Capacidad para transacciones con las bases de datos SGA.

El tráfico manejado por el módulo será:

$$C_{INTERNET\text{-}CORPORATIVO} = C_{INTERNET} + C_{BD} = 2304 + 30 = 2360[kbps]$$

Ecuación 2.16 Cálculo del tráfico total del módulo Internet Corporativo.

2.7.3. CÁLCULO DE TRÁFICO EN EL MÓDULO MAN

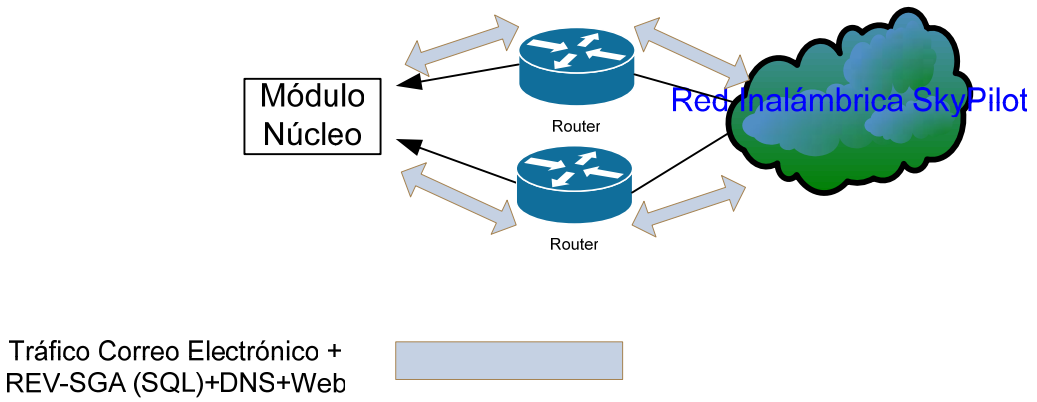


Figura 2.10 Flujo de tráfico del Módulo MAN

El tráfico de este módulo esta constituido por el tráfico de las bases de datos de las aplicaciones SGA de las instituciones educativas más el tráfico de correo electrónico de los usuarios de la Intranet.

$$\#\,\text{Usuarios} = \#\,\text{institucio nes educativas} \times 5$$
$$\#\,Usuarios = 41 \times 5 = 205$$

Ecuación 2.17 Cálculo del número de usuarios de la red MAN que usan correo electrónico.

$$C_{MAN\text{-}Email} = C_{Usuario} \times \#\text{usuarios simultaneos} = 1.33[kbps] \times 205 \times 0.03 = 27.27[kbps]$$

Ecuación 2.18 Capacidad del enlace para correo electrónico de la red MAN.

$$C_{MAN} = C_{MAN\text{-}Email} + C_{BD\text{-}REV} = 27.27 + 30 = 57.27[kbps]$$

Ecuación 2.19 Cálculo del tráfico total del módulo MAN.

2.7.4. CÁLCULO DE TRÁFICO EN EL MÓDULO DE SERVIDORES

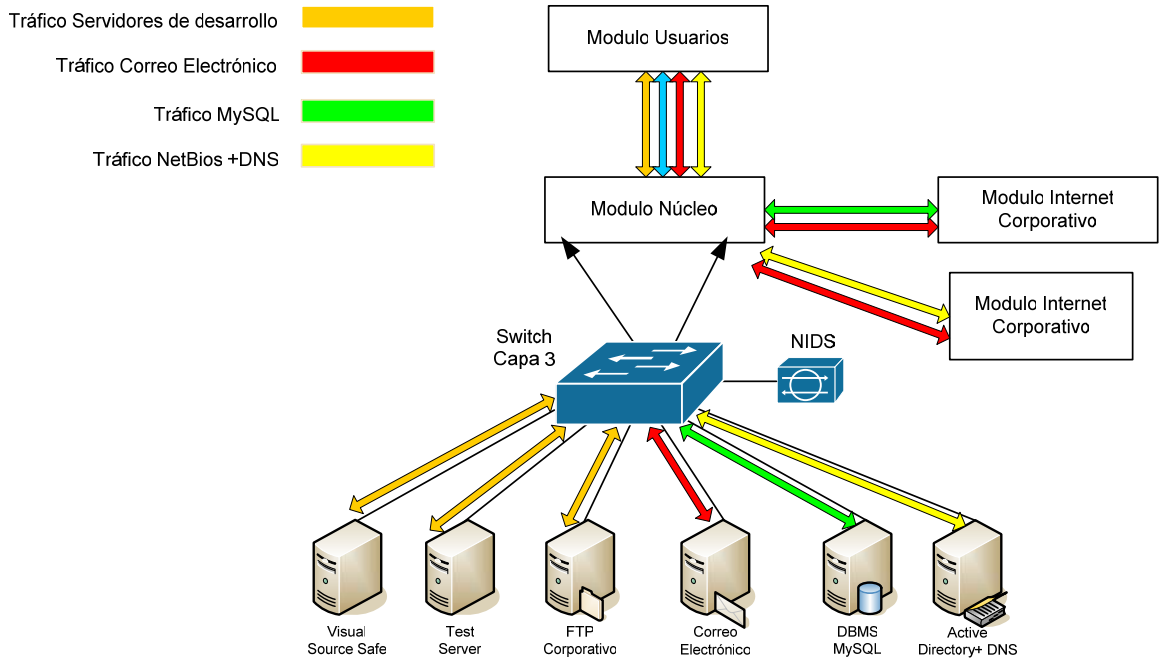


Figura 2.11 Flujo de tráfico del módulo servidores

Para éste análisis se utilizan únicamente los servicios FTP y correo electrónico. Se considera que los servidores NTP, Active Directory (NetBIOS) y DNS generan tráfico despreciable sobre la red interna. El tráfico generado por el servidor de video confrerencia no puede ser tomado en consideración debido a que su uso debe ser programado.

2.7.4.1. FTP

La capacidad de este servicio solo es aproximada porque FTP usa la capacidad (ancho de banda) máxima disponible en el momento. Además maneja velocidades variables dependiendo del tráfico y velocidad de transmisión disponible.

Este servicio se lo utilizará para respaldar la información generada por otros servidores y por usuarios de la empresa, por lo que podrá ser utilizado sólo por el personal de Conectividad Global Cia. Ltda.

Los requerimientos minimos para la provisión de este servicio y su uso dentro de la Intranet son:

- El tamaño promedio de un archivo de 500 kbytes.
- El tiempo promedio de descarga de un archivo de estas caracteristicas será de treinta segundos.
- El factor de simultaneidad de este servicio será del 5%.

$$C_{FTP-USER} = \frac{TamañoArchivo}{Tiempode\,desc\text{arg}a} = \frac{500k*8}{30} = 133.33[kbps]$$

Ecuación 2.20 Cálculo del tráfico por usuario del servicio FTP.

$$C_{FTP} = C_{FTP-USER} \times \#usuarios \times simultaneidad = 13333 \times 20 \times 0.05 = 13333 [kbps]$$

Ecuación 2.21 Cálculo del tráfico del servicio FTP.

2.7.4.2. Mail Server

El tráfico generado por este servicio será la suma de la capacidad calculada en las ecuaciones 2.6 y 2.9.

$$C_{correo-electrónico} = C_{correoElectrónicoInternet} + C_{correoElectrónicoDL} = 84665 + 1408 = 225465 [kbps]$$

Ecuación 2.22 Calculo del tráfico generado por el servidor de correo electrónico Interno.

El cálculo del tráfico total de este módulo corresponderá a la suma de las ecuaciones 2.21 y 2.22.

$$C_{servidores} = C_{FTP} + C_{correo-electrónico} = 13333 + 225465 = 238798 [kbps]$$

Ecuación 2.23 Cálculo del tráfico del módulo Servidores.

2.7.5. CÁLCULO DE TRÁFICO EN EL MÓDULO USUARIOS INTERNOS

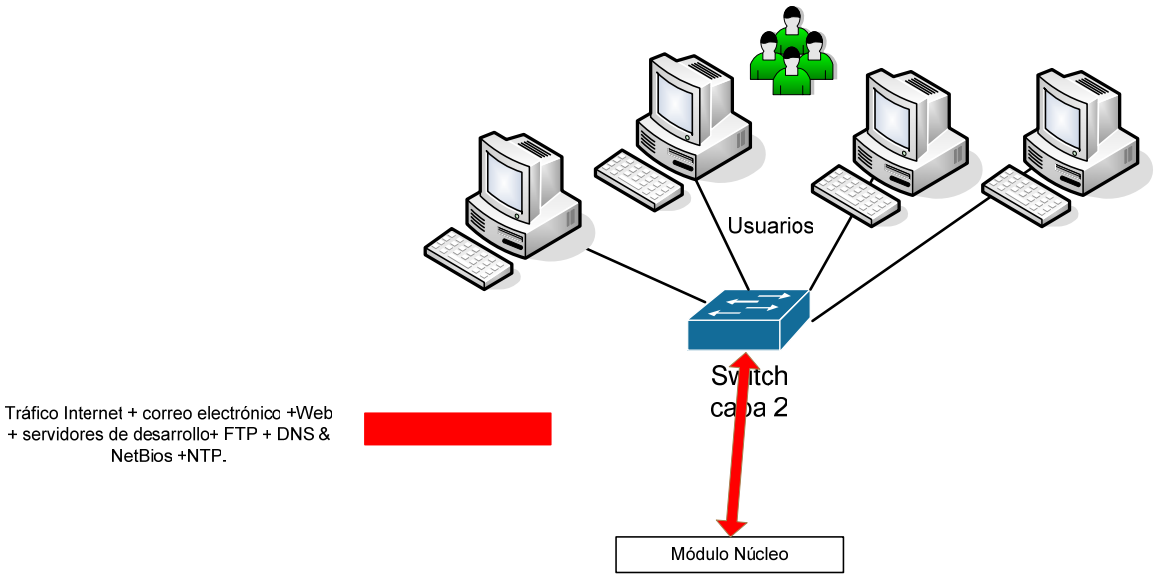


Figura 2.12 Flujo de tráfico del módulo usuarios

Para este módulo se considerará al tráfico generado por el personal de Conectividad Global Cia. Ltda. de los servicios FTP corporativo y correo electrónico.

Para el tráfico del servicio FTP se considerará a los resultados de la ecuación 2.21 que considera el tráfico mínimo para servicio FTP.

$$C_{correoElectronico} = C_{Usuario} \times \#usuarios\ simultaneidad = 1.33[kbps] \times 20 \times 0.1 = 2.66[kbps]$$

Ecuación 2.24 Cálculo del tráfico del servicio de correo electrónico del personal de la empresa

El cálculo del tráfico total de este módulo corresponderá a la suma de las ecuaciones 2.21 y 2.24.

$$C_{usuarios} = C_{FTP} + C_{correoElectronico} = 133.33 + 2.66 = 135.99[kbps]$$

Ecuación 2.25 Cálculo del tráfico del módulo Usuarios.

2.7.6. CÁLCULO DE TRÁFICO EN EL MÓDULO DE ADMINISTRACION

El tráfico para este módulo se lo considerará despreciable por la naturaleza de los protocolos utilizados por los sistemas de administración.

El MRTG utiliza al protocolo SNMP para obtención de la información de tráfico que será programada para envíar cada tres minutos a la interfaz de cada host administrado, un paquete de SNMP cuyo tamaño por defecto es de 1500 bytes.

El protocolo Syslog utiliza un paquete de tamaño de 1024 bytes y todos los hosts de la Intranet enviarán sus paquetes Syslog con nivel de severidad warn o superior a un servidor de recolección de eventos.

2.7.7. CÁLCULO DE TRÁFICO EN EL MÓDULO NÚCLEO

Todos los módulos requieren del núcleo para el enrutamiento y conmutación del tráfico del Data Center, por lo que el cálculo de tráfico de este módulo será la suma de los los valores de los tráficos estimados de todos los módulos obtenido a partir de las ecuaciones 2.16, 2.19, 2.23 y 2.25.

$$C_{Core} = C_{Internet-Corporativo} + C_{MAN} + C_{Administración} + C_{Servidores} + C_{usuarios}$$
$$C_{Core} = 2360 + 57.27 + 0 + 2387.98 + 135.99 = 4941.24[kbps]$$

Ecuación 2.26 Cálculo del tráfico del módulo Núcleo.

2.8. PROPUESTA DE EQUIPOS

Utilizando los requerimientos antes expuestos de acuerdo a la proyección de crecimiento se propondrán los equipos de cada módulo que formarán parte de la nueva infraestructura de red del Data Center.

La selección de la tecnología de red será Ethernet debido a que está difundida ampliamiente y por los requerimientos de la capacidad de tráfico a manejarse. Se utilizará Fast Ethernet en la conexión de los servidores o equipos de computación con los dispositivos de conectividad que comprendan cada módulo, y a Gigabit Ethernet para enlazar los módulos con los switches del núcleo.

2.8.1. MÓDULO ADMINISTRACIÓN

En este módulo se encontrarán los diferentes sistemas de administración y monitoreo de la red del Data Center de los cuales se encargará el personal de administración de red de la empresa. El direccionamiento IP de sus hosts se encuentra en la Tabla 2.14.

Servidor	Dirección IP	Mascara	Gateway	Dirección del DNS
Syslog	192.168.100.97	255.255.255.240	192.168.100.110	192.168.100.54
Nagios	192.168.100.65	255.255.255.240	192.168.100.110	192.168.100.54
MRTG	192.168.100.66	255.255.255.240	192.168.100.110	192.168.100.54
Host de	192.168.100.67	255.255.255.240	192.168.100.110	192.168.100.54

administración de sistemas				

Tabla 2.14 Direccionamiento IP de los hosts de administración

2.8.1.1. Sistema de Prevención de Intrusos

Se seleccionará al sistema de prevención de intrusos Cisco IPS 4240-DC Sensor Appliance por cumplir con los requerimientos y adiciona además características con funcionalidad para mantener un mejor nivel de seguridad en profundidad. A continuación se enumeran sus características básicas:

- Puede trabajar las interfaces en modo promiscuo o en modo en línea.

El modo promiscuo se refiere a los paquetes que no fluyen a través del sensor, sólo analiza una copia del tráfico monitoreado en vez del paquete actual reenviado. La ventaja de este modo es que el sensor no afecta el flujo de paquetes del tráfico reenviado. Pero su desventaja es que el sensor no puede impedir que el tráfico malicioso de ciertos ataques tenga éxito sino que requiere de la asistencia de otro dispositivo de red manejado por éste como firewall, router o switch para responder al ataque.

En el modo inline en cambio, el IPS se coloca directamente entre el flujo del tráfico afectando el flujo normal de paquetes añadiendo cierta latencia, deteniendo los ataques antes de que alcancen su objetivo proveyendo de esta forma un servicio de protección. La información que puede analizar este dispositivo puede ser desde capa de red a la capa aplicación del modelo OSI, de forma que podría detener los ataques que pudieren pasar a través del firewall. Las carácterísticas necesarias para este dispositivo son:

- Cuatro puertos Ethernet 10/100/1000 Base T.
- Puede ayudar a detectar, clasificar y mitigar amenazas como gusanos, spyware y adware, virus de red y abuso en las aplicaciones sobre los

sistemas de computación en los que se tenga instalado el Cisco IPS software version 5.0.

- Soporte de IEEE 802.1q.
- Múltiples acciones de respuestas automatizadas que incluyen bloqueo de paquetes, terminación de la conexión e implementación de listas de control de acceso sobre cisco routers, switches y firewalls.
- Capacidad para detectar y detener amenazas sobre VoIP.
- Opciones de administración y monitorización embebidas que soportan comunicaciones encriptadas.
- Interfaz de comando y control 10/100 Base T.

Las interfaces de red del sensor que analizan el tráfico por violaciones de seguridad serán configuradas en modo promiscuo y desde ella enviará paquetes TCP reset al equipo firewall para tratar de cancelar la conexión del host atacante.

Es necesario aclarar que para este módulo se utilizará únicamente una interfaz de monitoreo del IPS para ser conectada al puerto del switch con características de port mirroring, en este caso configurando a un puerto del switch en modo SPAN[24], configuración similar a port mirroring, para que analice todo el tráfico que atraviese por este switch. Otra de las cuatro interfaces de monitoreo del IPS será conectada un puerto configurado con SPAN del switch del módulo de servidores.

2.8.1.2. Servidor Syslog

Este servidor proporcionará información valiosa acerca de lo que ocurre en un sistema y/o aplicación por lo que resultan ser más apropiados para este tipo de componentes de la red.

---

[24] **SPAN:** Switched Port Analyzer,

Cuando se intenta proponer un registro de eventos se debe tomar en cuenta los formatos con los que este tipo de información pueda operar en forma centralizada, que dependerán de los registros generados y de quién recibe esos registros. Estos formatos de la información de registro de eventos dependen de los sistemas operativos. La plataforma Windows proporciona esta información a traves de la herramienta propietaria ***Visor de Sucesos***, en cambio, los sistemas basados en Unix tienen instalado por defecto a ***Syslog*** que es un software libre.

Para operar de forma centralizada se debe manejar la información de registro de eventos en el mismo formato para sistemas basados en plataformas Windows y Linux que mantenga el Data Center por lo que utilizará al servicio Syslog.

Para sistemas basados en Linux se utilizará a Syslog y se configurará para enviar todos los eventos al servidor.

La herramienta de software NTSyslog para sistemas operativos Microsoft Windows permite reformatear los registros de eventos a un formato para su correcto envío a un servidor Syslog especificado por su dirección IP. El reformateo de los registros de eventos se lo realiza mediante el establecimiento de la equivalencia de cada evento de información, advertencia, error, auditoría exitosa o fallas en la auditoría con los niveles de severidad de Syslog: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), information (6) y debug (7) para los diferentes subsistemas del sistema operativo: Aplicación, Sistema, Internet Explorer y Seguridad.

Para la recolección de la información del servidor Syslog que utiliza el puerto UDP 514 se utlizará un equipo con sistema operativo Fedora Core 3 y el software KiwiSyslog. KiwiSyslog es un software comercial basado en Syslog que tiene la ventaja de permitir la implementación de alarmas en tiempo real para los diferentes eventos de los sistemas con el fin de lograr una corrección inmediata de problemas y para su análisis posterior.

La capacidad de almacenamiento en disco es el factor más relevante para el dimensionamiento de este servidor debido a qué dependerá del número de eventos que generan los distintos sistemas y de acuerdo a las políticas de

auditoría que generan dichos eventos que posteriormente son recibidos en el servidor.

2.8.1.3. Agentes SNMP

Son programas instalados en los sistemas basados en sistemas operativos Unix o Microsoft Windows, y en algunos dispositivos que permiten la obtención de información de monitorización de estado y actividades basándose en el protocolo SNMP. SNMP usa passwords llamados nombres de comunidad enviados en ***texto plano***[25] sobre el mensaje por lo que la seguridad debería implementarse utilizando control de acceso sobre el dispositivo a administrar para permitir consultas sólo a los hosts de administración y además la comunidad debe ser configurada en modo solo lectura.

2.8.1.4. NMS

Las NMS (Network Management Station) o consolas de administración son paquetes de software que utilizando a los agentes instalados en los equipos administrados permiten visualizar el seguimiento del estado actual de la red.

A continuación se listarán las NMS comerciales y de código abierto:

- HP OpenView. (Comercial para plataformas Windows, HP-UX, Solaris).
- OpenNMS (software Libre Licencia GPL[26] para cualquier plataforma que soporte Java).
- Nagios (software Libre Licencia GPL para plataformas Unix).

---

[25] **Texto plano**. Información sin encripción enviada a través de un medio de transmisión.
[26] **GPL**: GNU Public License, licencia aplicada a software para mantenerlo libre de forma que cualquiera puede adaptarlo a sus necesidades sin depender de la voluntad del autor.

- Big Brother (software Libre y comercial para plataformas Unix, Windows 2000/2003/NT).

- Ipswitch WhatsUp (comercial para plataformas Windows).

Es necesario aclarar que las soluciones de NMS de software libre para la implementación de una NMS son una buena opción debido a los costos por licencias y a la alta funcionalidad de administración de red que poseen si se las configura apropiadamente.

Para esta propuesta de diseño utilizaremos a Nagios que además de permitir una revisión del estado de los dispositivos y de sus recursos, permite una supervisión de host y servicios TCP/IP alertando si se suscita algún tipo de imprevisto, una característica adicional es su gran extensibilidad ofrecida por plug-ins adicionales. Sus requisitos de instalación no requieren del protocolo SNMP, salvo casos en los que los plug-ins adicionales que se instalen lo demanden.

Los requerimientos de hardware para este NMS debe ser de al menos de un procesador de 3 GHz, de 512 Mbytes a 1 Gbyte de memoria RAM, y un disco duro cuya capacidad dependerá del tipo de complementos a usarse y del número de hosts a monitorizarse. El disco duro deberá ser preferentemente de tipo UltraSCSI o IDEs de acceso rápido para garantizar un alto desempeño.

Además se requiere de la instalación de un agente software sobre equipos con sistemas operativos Windows llamado NSClient++.

2.8.1.5. Monitorizadores de tráfico

Es necesario poseer algún tipo de registro histórico que permita revisar la información del tráfico de las interfaces de red en los diferentes dispositivos.

Existen varios paquetes de software que permiten obtener esta información, entre las que se tienen a MRTG (Multi-Router Traffic Grapher) que es un software libre de fácil manejo y configuración. La información que se necesita para la

generación de los reportes se la obtiene a tráves de una agente basado en SNMP que debe ser configurado en los hosts a monitorear.

Para la determinación de los requerimientos de hardware necesarios para un servidor de administración de tráfico que utilice MRTG serán necesarias variables como el número de interfaces de red totales de todos los dispositivos del Data Center debido a que cada interfaz genera un reporte con un tamaño en disco aproximado de 150 KBytes conformado por un archivo HTML, un archivo log, un archivo old y cuatro archivos gif.

2.8.1.6. Switch Capa 2

Se seleccionará al switch Cisco Catalyst 2950-12 cuyas características se encuentran en el Anexo K.2 porque cumplie con los requerimientos mencionados anteriormente.

Se configurará uno de los puertos del switch como SPAN para uso de una interfaz de monitoreo dell sistema de detección y prevención de intrusos.

2.8.1.7. Router IOS Firewall

Se seleccionará al router Cisco Router 1710 cuyas características se encuentran en el Anexo K.1 por cumplir con los requerimientos antes mencionados.

Este router usará al Cisco IOS Firewall para stateful inspection y será la puerta de enlace para la red de administración de red, se encargará de realizar las terminaciones VPN de los túneles IPSec que transmite protocolos de administración como syslog y SNMP desde/hacia todos los host administrados del Data Center.

El servidor de monitoreo con el software Nagios no utilizará IPSec sino que tendrá acceso a los servicios de los hosts del Data Center que requieran ser monitoreados directamente.

Este router además utilizará sus características de firewall statefull inspection para bloquear todo el tráfico entrante que no sea respuesta de solicitudes de los paquetes o datagramas salientes de los hosts de administración.

2.8.2. MÓDULO NÚCLEO

Por la importancia de este módulo se realizará un estudio para la elección de los dispositivos switches donde se evaluarán cuatro propuestas, dos de ellas correspondientes a equipos que forman parte de la infraestructura de la red actual. Las caracterisiticas de los cuatro equipos se encuentran en el Anexo H.

2.8.2.1. Switch capa 3

Tanto el Switch Cisco Catalyst 3550 24 DC como el Cisco Catalyst 4948 Switch del Anexo H cumplen con todos los requerimientos básicos, pero se seleccionará al Cisco 3550 24 DC debido a que cuenta con el número de puertos necesarios.

Utilizando un par de Switch Cisco Catalyst 3550 24 DC se proveerá enlaces redundantes utlizando link agreggation (estandar IEEE 802.3ad) y con el protocolo HSRP se conseguirá tolerancia a fallas de estos equipos. Se configurará el enrutamiento InterVLAN para VLANs basadas en el protocolo IEEE 802.1q, se proporcionará enrutamiento IP estático entre los distintos segmentos de red del Data Center.

Además estos equipos realizarán el control de acceso para prevenir la falsificación de las direcciones IP de origen y se encargarán de filtrar el tráfico entrante no esencial desde los dispositivos de los módulos de usuarios, Internet Corporativo y MAN para evitar ataques pasivos de reconocimientos de red.

2.8.3. MÓDULO INTERNET CORPORATIVO.

Las subredes que este módulo manejará serán *DMZ*, *Conexión DMZ-Core1 y Conexión DMZ-Core2.* Las subredes de la Conexión DMZ-Core1 y Conexión DMZ-Core2 serán manejadas por los equipos firewall y el core.

Por motivos de seguridad la interfaz externa de los equipos Firewall se encontrará en otra red para conectarse con los routers de borde. En la Tabla 2.15 se muestra la configuración IP de los dispositivos de red de este módulo.

Equipo	Dirección IP	Máscara
Firewall1-interfaz Externa	172.16.31.2	255.255.255.248
Firewall1-interfaz Interna	192.168.100.118	255.255.255.252
Firewall1-interfaz DMZ	192.168.100.68	255.255.255.240
Firewall2-interfaz Externa	172.16.31.3	255.255.255.248
Firewall2-interfaz Interna	192.168.100.122	255.255.255.252
Firewall2-interfaz DMZ	192.168.100.68	255.255.255.240
Routers de Borde Interfaz virtual HSRP interna	172.16.31.5	255.255.255.248
Router de Borde1 Interfaz Externa	Red pública del ISP1	-
Router de Borde2 Interfaz Externa	Red pública del ISP2	-

Tabla 2.15 Configuración IP de los dispostivos de capa de red del módulo Internet Corporativo

Los servidores de la DMZ se encontrarán formando parte del segmento de Red DMZ y mantendrán la configuración de red mostrada en la Tabla 2.16.

Servidor	Hostname	Dirección IP	Máscara	Gateway	Dirección del DNS
Web/FTP	web	192.168.100.64	255.255.255.240	192.168.100.68	DNS1:192.168.100.65 DNS2:192.168.100.66
DNS-Primario	ns1	192.168.100.65	255.255.255.240	192.168.100.68	DNS1 → ISP1 DNS→ ISP2
DNS-Secundario	ns2	192.168.100.66	255.255.255.240	192.168.100.68	DNS1 → ISP1 DNS2 → ISP2
Red Educativa Virtual	rev	192.168.100.67	255.255.255.240	192.168.100.68	DNS1:192.168.100.65 DNS2:192.168.100.66

Mail Relay	mrelay	192.168.100.68	255.255.255.240	192.168.100.68	DNS1:192.168.100.65 DNS2:192.168.100.66

Tabla 2.16 Configuración IP de los servidores de la DMZ del módulo Internet Corporativo.

2.8.3.1. Router de borde

Para los routers de borde se ha seleccionado al Cisco Security Acces Router 1710 por cumplir con los requerimientos mínimos. Estos routers proveerán el balanceo de carga y tolerancia a fallas al utilizando el protocolo HSRP.

2.8.3.2. Firewall

Para este diseño se ha seleccionado al equipo appliance de seguridad Cisco PIX 515E con licencia de software no restringida debido a sus características de redundancia y tolerancia a fallas porque con un par de estos dispositivos que mantengan la misma configuración se podrá mantener alta disponibilidad de forma automática. Sus características se encuentran en el Anexo I.

2.8.3.3. Switches.

Los switches seleccionados son los switches Cisco Catalyst 2950-12 y 2940-8TT por tener características que cumplen con los requerimientos mínimos. Estos switches se encargarán de la conmutación de los equipos de las subredes de los servidores de la DMZ y de la red en la que se conectan los routers de borde, firewalls e IPS.

2.8.3.4. Sistema de Prevención de Intrusos.

Se ha seleccionado al sistema de prevención de intrusos Cisco IPS 4240-DC Sensor Appliance cuyas caracterisiticas se encuentran en el Anexo J debido a

que cuenta con con el número de interfaces de monitoreo necesarias y la capacidad requerida para la inspección de tráfico en las interfaces de los switches capa 2 de este módulo. Uno de los puertos de cada switch de este módulo deberá estar configurado con SPAN para monitorear, repeler y reportar violaciones a la seguridad de la red.

2.8.4. MÓDULO DE USUARIOS

Se utilizarán VLANs para segmentar las subredes del este módulo y se contará únicamente con un switch Cisco Catalyst 2950-24 cuyas características cumplen con los requerimientos. En la Tabla 2.17 se muestra la configuración IP de los hosts pertenecientes a distintos segmentos de red del módulo.

Segmento de red	Subred/máscara	Gateway	Dirección del DNS
Administración	192.168.100.0/29	192.168.100.6	192.168.100.54
Desarrollo de Software	192.168.100.8/29	192.168.100.14	192.168.100.54
Proyectos	192.168.100.16/29	192.168.100.22	192.168.100.54
Diseño Web	192.168.100.24/29	192.168.100.30	192.168.100.54
Gerencia	192.168.100.32/29	192.168.100.38	192.168.100.54
Soporte Técnico	192.168.100.80/28	192.168.100.94	192.168.100.54

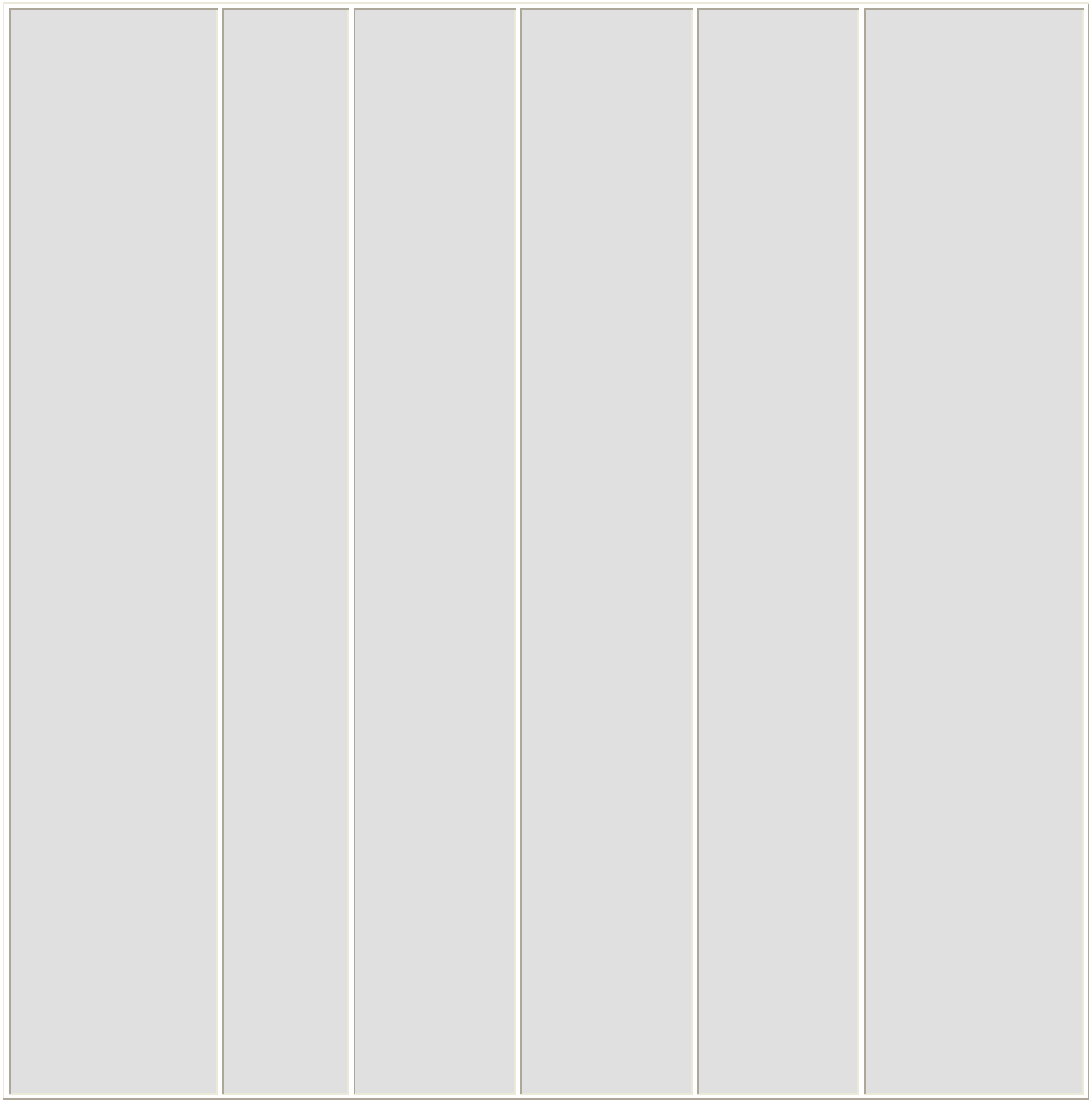
Tabla 2.17 Direccionamiento IP del módulo Usuarios.

El enrutamiento y filtrado de paquetes a nivel de capa 3 será realizado a través de las características de enrutamiento Inter-vlan y de las listas de control de acceso que poseen los switches capa 3 del módulo Núcleo.

Tanto el switch de core como el switch del módulo de usuarios se conectarán a través de puertos configurados como port trunking utilizando el estándar IEEE 802.1Q.

2.8.5. MÓDULO SERVIDORES

Mediante un switch Cisco Catalyst 2950SX-24 se proporcionará seguridad a los equipos de desarrollo de software diferenciándolos del resto de servidores haciendo uso de dos VLANs. Éste se conectará con los switches del módulo núcleo haciendo uso de los puertos 1000BASE-SX con fibra óptica multimodo y serán configurados como port trunking. Los switches del módulo núcleo también proporcionarán el control de acceso a nivel de VLANs para el personal del departamento de Desarrollo de Software. La Tabla 2.18 muestra el esquema de direccionamiento IP a utilizarse.



de los puertos 1000BASE-SX con fibra óptica multimodo y serán configurados como port trunking. Los switches del módulo núcleo también proporcionarán el control de acceso a nivel de VLANs para el personal del departamento de Desarrollo de Software. La Tabla 2.18 muestra el esquema de direccionamiento IP a utilizarse.

de los puertos 1000BASE-SX con fibra óptica multimodo y serán configurados como port trunking. Los switches del módulo núcleo también proporcionarán el control de acceso a nivel de VLANs para el personal del departamento de Desarrollo de Software. La Tabla 2.18 muestra el esquema de					

direccionamiento IP a utilizarse.

direccionamiento IP a utilizarse. Servidor					
FTP + NTP	COGLSRV	192.168.100.49	255.255.255.248	192.168.100.54	192.168.100.54
Active Directory + DNS.	COGLSRV	192.168.100.50	255.255.255.248	192.168.100.54	DNS1:192.168.100.65 DNS:192.168.100.66
Correo Electronico	COGLSRV	192.168.100.51	255.255.255.248	192.168.100.54	192.168.100.54
Test Server	SRVDES	192.168.100.41	255.255.255.248	192.168.100.46	192.168.100.54
Visual Source Safe	SRVDES	192.168.100.42	255.255.255.248	192.168.100.46	192.168.100.54

Tabla 2.18 Direccionamiento IP de los servidores de la DMZ del módulo Servidores.

Uno de los puertos de este switch será configurado en modo SPAN y se conectará con una de las tres interfaces de monitoreo disponibles del equipo Cisco IPS 4240 Appliance Sensor para detectar amenazas originadas por tráfico malicioso.

2.8.6. MÓDULO MAN

A través de este módulo se conseguirá el acceso a los diferentes sistemas de Gestión Académica de las institutciones Educativas interconectadas a la Intranet del Proyecto utilizando un router que permite la interconexión con la red Inalámbrica Skypilot. Los routers que se han seleccionado son Cisco 1605-R cuyas características se encuentrane en el Anexo K.4.

2.9. DIAGRAMA FINAL DEL DISEÑO DE RED

La Figura 2.13 muestra el esquema de la unión de los diferentes módulos que conforman la arquitectura de red. Éste es el diagrama final de la red que proporcionará seguridad y disponibilidad de los servicios y aplicaciones alojados en el Data Center.

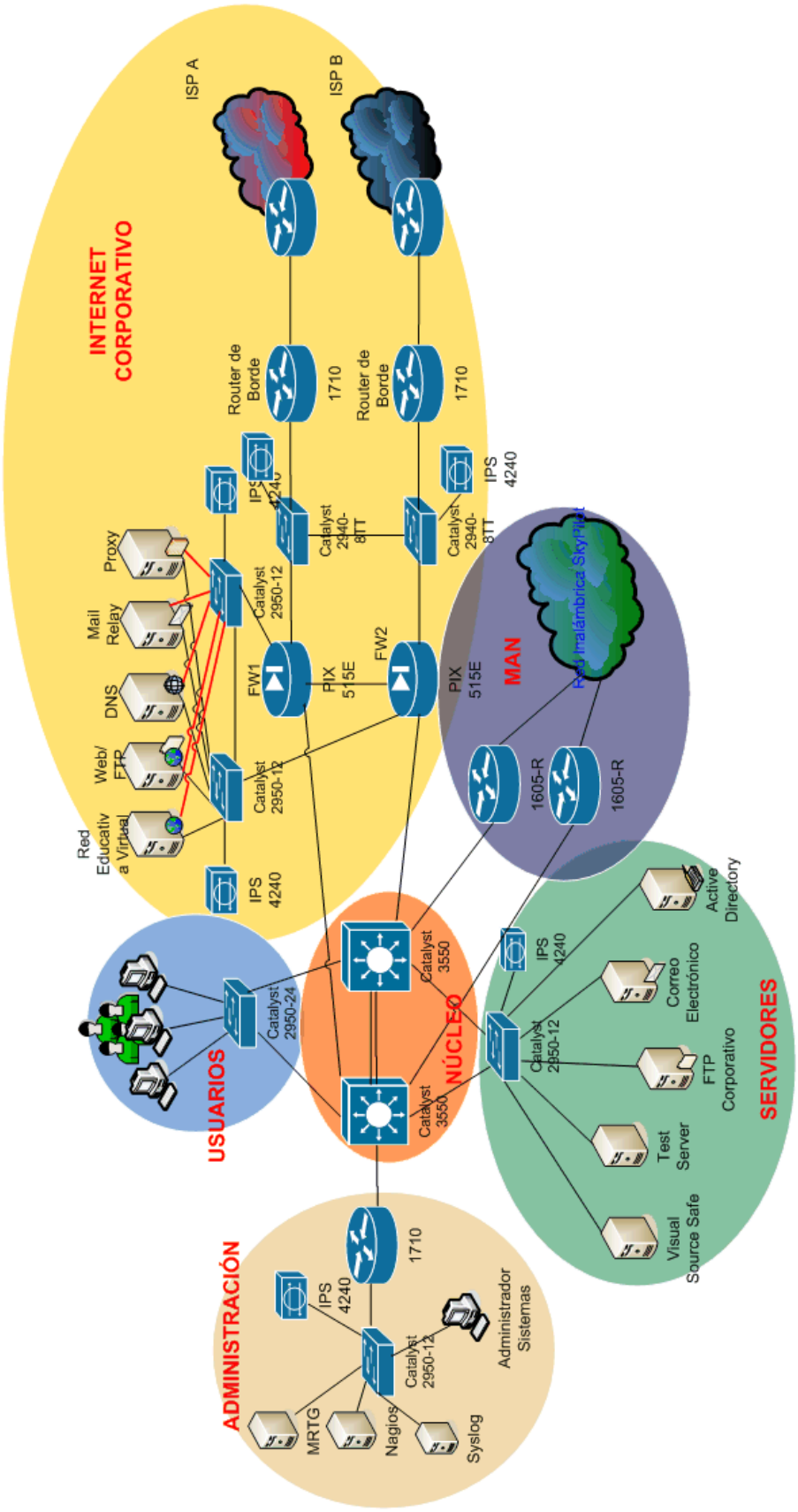


Figura 2.13 Diagrama Final de la Red de Servicios

2.10. PLANEAMIENTO DE SERVIDORES

Para proveer servicios de alta disponibilidad se debe tomar en consideración la capacidad de los recursos de hardware de un servidor, la plataforma operativa que correrá sobre éstos y el software que permitirá brindar dichos servicios. Además es importante que se provean técnicas de respaldo de información, redundancia y balanceo de carga. Todos estos parámetros permiten a los servidores ofrecer disponibilidad de servicios frente a solicitudes, tráfico en sus interfaces y carga generada.

La plataforma operativa para los servicios de red será Linux por su alto desempeño, y porque es la actual plataforma en los servidores alojados en el Data Center, lo que implica cierto grado de manejo y configuración por parte de los administradores de red. La plataforma que brindará el soporte necesario para las aplicaciones, debido a su naturaleza será Microsoft Windows Server.

El dimensionamiento de la capacidad de un servidor no es puntual, depende de muchos factores aleatorios como el tráfico, el uso, la concurrencia, el peso de las solicitudes y respuestas, etc. Debido a esto se realizará un cálculo aproximado de los requerimientos de hardware necesarios para proveer los servicios suponiendo y asumiendo el uso del equipo de acuerdo a las estadísticas y el análisis realizado en el capítulo 1. El cálculo del CPU requerido se lo realizará en base a Capacity Planning de Microsoft Learning mostrado en el Anexo L. [35]

Cabe aclarar que el planeamiento de capacidad puede ser sub o sobredimensionado por lo que se recomienda realizar pruebas de saturación al servidor, al canal y a los dispositivos que interconectan los servidores, ya que son las únicas pruebas reales que permitirán conocer a ciencia cierta cuántos requerimientos soportan los equipos.

2.10.1. WEB

El servidor Web debe soportar HTTP desde su versión 1.1 en adelante debido a que este protocolo utiliza conexiones persistentes que permiten al navegador de

Internet recuperar múltiples items de las páginas web en una sola conexión al servidor.

Debe soportar la mayoría de lenguajes de programación como Java, JavaScript, Perl, PHP, etc., basados en scripts que permitan conectar a bases de datos y desplegar páginas web dinámicas, además, que se ejecuten sobre cualquier plataforma.

Tiene que proporcionar alto desempeño, ser altamente configurable, y deben existir actualizaciones continuamente.

El servidor que cumple con las características mencionadas es ***Apache*** el cual además funciona sobre cualquier sistema UNIX y Windows, es open source y es gratuito.

La versión 2.0 de Apache basa su modelo de procesamiento en múltiples hilos, utiliza módulos de multiprocesamiento, consta de una Interfaz de Programación de Aplicaciones avanzada, soporta IPv6 y su configuración es fácil.

Previo a la instalación y configuración de este servidor se debe tomar en cuenta parámetros de dimensionamiento, es decir el número de sitios web que se van a almacenar, el espacio en disco destinado a cada uno de ellos y la velocidad de procesamiento con la que se debe responder a las solicitudes generadas al servidor.

De la ecuación 2.1 se obtiene que el número de centros beneficiados que podrían requerir hosting en el servidor web del Data Center es aproximadamente 1691. Si bien, según la ecuación 2.2 aproximadamente hasta el año 2011 se integrarán 41 centros educativos a la red del Proyecto QuitoEduca.Net, este servicio se puede brindar también a las instituciones no integradas. Frente a este cálculo, se consideran despreciables los clientes privados de conectividad Global Cía. Ltda.

Los sitios desarrollados en html permiten visualizar páginas estáticas, mientras que los desarrollados con Joomla asocian bases de datos y despliegan páginas dinámicas. El espacio en disco que ocupa un sitio web se determina de acuerdo

al nivel de complejidad de diseño de cada página, pero se debe tener en cuenta que una página realmente bien diseñada es aquella que no demora en desplegar toda la información necesaria.

Actualmente existen 58 sitios albergados en los servidores web del Data Center, utilizando el comando ***du –s ** sobre la carpeta /var/www/html del servidor web.conectividadglobal.net se obtuvo que en promedio un sitio ocupa un tamaño de 66972 KBytes, aproximadamente 65,4 MBytes. El tamaño en disco necesario para alojamiento de sitios web se determina por la ecuación 2.27.

$$Espacio en disco = Número de sitios web * Tamaño por sitio web$$
$$Espacio en disco = 1691 * 65.4[MBytes] = 107.99[GBytes]$$

Ecuación 2.27 Capacidad de disco duro para alojamiento de sitios web

Se debe considerar además el espacio en disco necesario para la instalación del Sistema Operativo, para la aplicación servidor y para los paquetes adicionales con los que se va a trabajar.

En un servidor web se necesita proveer disponibilidad y velocidad de acceso al disco. El método de dispositivos de bloque virtuales que permite proveer lo antes mencionado es RAID (Redundant Array of Inexpensive Disks). Para elegir el nivel de RAID adecuado podemos basarnos en la Tabla 2.19.

RAID	Mínimo número de discos	Desempeño de lectura(*)	Desempeño de escritura(*)	Redundancia	Capacidad de almacenamiento si se dispone de N discos	Otros aspectos
Linear	2	Igual	Igual	No	N	Puede usarse con discos de tamaños diferentes
0	2	Rápido	Rápido	No	N	
1	2	Rápido	Algo más lento	Si	1	Puede soportar el colapso de N-1 discos.
4	3	Algo más rápido	lento	Si	N-1	Puede soportar el colapso de un disco
5	3	Algo más rápido	Algo más rápido	Si	N-1	Puede soportar el colapso de un disco. Consumo alto de CPU

Tabla 2.19 Carácterísticas de selección de un dispositivo de bloque tipo RAID

Debido a que se necesita de acceso rápido, es decir, lectura rápida de la información almacenada en disco, por su alta capacidad de almacenamiento N-1 y redundancia se debe implementar RAID 4 en el servidor. A pesar de que RAID 5 tiene las mismas características, y una adicional, el desempeño de escritura rápido, no se selecciona este tipo de dispositivo de bloque por el consumo elevado de CPU que demanda.

Para dimensionar el CPU requerido es necesario considerar una velocidad de referencia de un procesador. Debido a que se cuenta con hardware en los servidores web actuales, de entre ellos, por poseer procesadores de alto rendimiento destinados a servidores se escoge como base para el cálculo al Intel Xeon de 2.8GHz del servidor fw.remq.edu.ec. Se considera que el porcentaje de disponibilidad y utilidad que debe brindar el procesador sea del 80%.

En el servidor web.conectividadglobal.net, debido a que es el que contiene mayor número de sitios web almacenados, se instaló una herramienta denominada Webalizer, que permite el análisis del log del servidor Apache y lo muestra en gráficas estadísiticas.

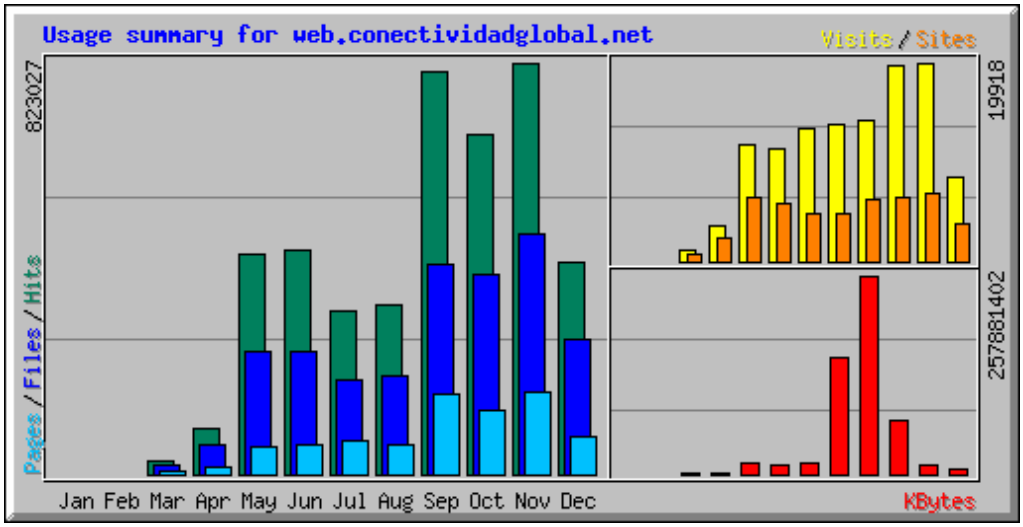


Figura 2.14 Estadísiticas del Servicio Web Apache en el equipo servidor web.conectividadglobal.net

Como se puede ver en la Figura 2.14, uno de los meses con mayor actividad durante el 2008 es Septiembre, tomando como referencia la carga de éste se realizará el dimensionamiento del nuevo servidor web.

En la Figura 2.14, los valores de Hits hacen referencia al número de solicitudes realizadas hacia el servidor web, los valored Files son el número de páginas, archivos, imágenes, etc. que han sido descargados desde el servidor hacia el agente de usuario o explorador de Internet; y Pages es el número de archivos considerados páginas web; KBytes es el tráfico que genera el servidor para atender las solicitudes de los clientes; Sites indica el número de direcciones IP desde las que se han realizado solicitudes al servidor; Visits son las solicitudes al servidor para consultar una página.

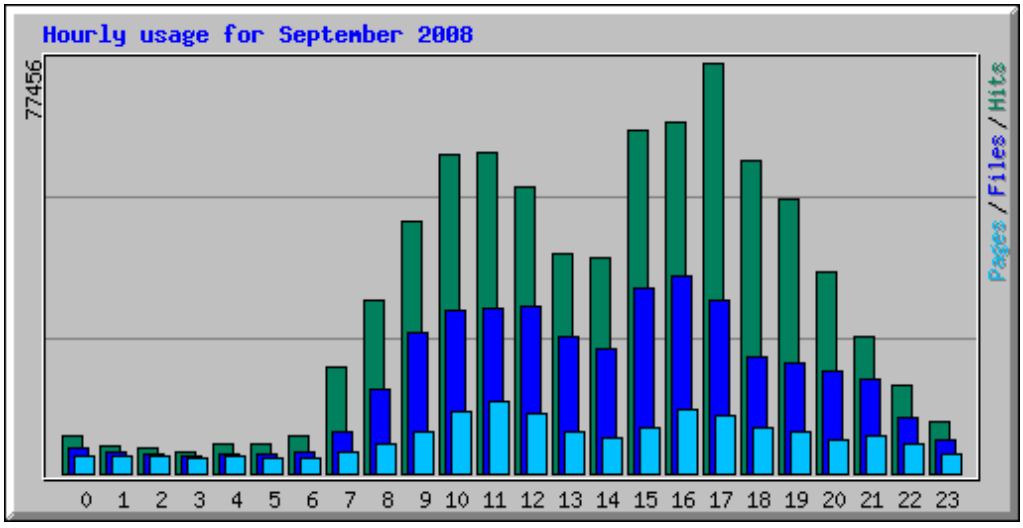


Figura 2.15 Estadísticas por hora del servidor Apache en web.conectividadglobal.net durante el mes de Septiembre de 2008

En la Figura 2.15 se observa que la hora de mayor tráfico es de 17:00 a 18:00, por lo que se tomará como referencia este rango de tiempo. Del Anexo G se obtiene que se han realizado 2581 solicitudes al servidor durante el tiempo especificado. Dos son el número de solicitudes al procesador para realizar una operación sobre un sitio web, las operaciones pueden ser: acceder a la página por

defecto o principal, solicitar una página, realizar búsquedas, descargas, subir archivos, etc. Se considera que un usuario normal podría permanecer en el sitio web durante diez minutos y realizar alrededor de seis operaciones, y que la concurrencia, es decir el número de clientes solicitando el mismo servicio a la vez, será de veinte por ciento.

uso CPU	% uso CPU	×	# CPU	×	vel. CPU [MHz]
4480,00	0,80		2,00		2800,00

solicitudes / segundo	# solicitudes	÷	tiempo [s]	×	simultaneidad
14,34	2581,00		3600,00		20,00

solicitudes / operación	# solicitudes	÷	# operaciones
2,00	2,00		1,00

costo / operación	uso CPU	÷	solic / seg	×	solic / oper
624,87	4480,00		14,34		2,00

operaciones / segundo	# ope / cliente	÷	tiempo [s]
0,0100	6,00		600,00

costo / usuario	costo / oper	÷	oper / seg
6,25	624,87		0,0100

CPU [MHz]	concurrencia	×	Costo / usuario
3225,60	516,20		6,25

Tabla 2.20 Cálculo del procesador requerido para el servidor Web

El valor que tenemos como resultado es 3225,6 MHz, el cual es inferior al valor del CPU establecido como base para el cálculo ya que al tener doble núcleo se empezó con 5600 MHz. Entonces se puede afirmar que el procesador utilizado para este análisis puede ser utilizado para la provisión de este servicio ya que cumple los requisitos necesarios.

2.10.2. DNS

Para la configuración del servicio de DNS se utilizarán dos conjuntos de servidores de DNS: para la DMZ constituido por el servidor Maestro y Esclavo para necesidades del Internet, y para la intranet se utilizará un servidor Maestro.

El conjunto de servidores DNS de la DMZ serán autoritativos para los dominios que maneja la empresa y contendrán los registros de recursos asociados a las direcciones IP de los servidores de la DMZ con sus zonas de reversa. El servidor DNS primario de la Intranet será autoritativo para un dominio creado para própositos locales a los servicios de la Intranet y para los dominios de la DMZ, pero únicamente contendrá a los registros de reversa del dominio local.

Para proporcionar seguridad frente a intrusos en el servicio se instalará BIND para que el demonio ***named*** corra enjaulado en un directorio en particular considerado como el directorio raíz de este sistema de ficheros.

El espacio en disco necesario es el que demanda el sistema operativo y los paquetes adicionales mencionados. Se considera suficiente 10 GB en disco duro.

En el caso de necesitar un servidor web adicional se puede tener ciertas configuraciones de balanceo de carga en los servidores DNS, lo cual implica redundancia de los servicios de la DMZ.

Al momento de la adquisición de los registros de los dominios se deberán configurar para que apunten a los servidores DNS primario y secundario de la DMZ del Data Center por lo que la configuración del dominio se establecerá como dirección IP del DNS primario del dominio a la de la interfaz WAN del router de borde de la empresa que se conecta al primer ISP y como dirección IP del segundo DNS a la del otro router de borde que se conecta con el segundo ISP con el fin de brindar redundancia en los DNS que maneja la empresa.

Para redundancia y balanceo de carga de los servicios que provee la DMZ se utilizará el algoritmo de round robin DNS, de la siguiente forma: todos los servidores de la DMZ tendrán asignadas direcciones IPs privadas en sus interfaces de red y las solicitudes de consulta DNS de usuarios de Internet

ingresarán por el router de borde de la empresa hacia el servidor DNS primario el mismo que responderá de forma alternada con las direcciones IP públicas de estos routers de borde. El servidor DNS secundario tendrá funcionalidad de backup para el servicio de DNS de la DMZ.

Para balancear el acceso a Internet a los diferentes servicios proporcionados se configurará la directiva de opciones del archivo de configuración del demonio named, named.conf.

Con el fin de establecer varios registros de recursos asociados a un mismo hostname se especificarán varias direcciones IP asociadas a un mismo registro de recurso.

Como ambos equipos en la DMZ deben soportar una carga similar pueden considerarse iguales.

2.10.3. CORREO ELECTRÓNICO

El sistema de correo electrónico, debe permitir que los usuarios internos de la red sean capaces de enviar o recibir correos a su propio dominio o a cualquiera ya sea externo o interno.

Para dimensionar el servidor de correo se toma como punto de partida el servidor fw.remq.edu.ec debido a que contiene el 79.01% de cuentas de correo alojadas en el Data Center. La consola de administración del servicio muestra los datos recopilados durante 34 días, 21 horas y 4 minutos, éstos se pueden ver en el Anexo F.4. En la Figura 2.16 se observa un alto porcentaje de spam detectado en el servidor de correo fw.remq.edu.ec. Dentro de los esquemas de correo electrónico que proveen alta seguridad, está el uso de un servidor en la DMZ que realizará tareas como análisis y escanéo de ***malware***[27] y spam del correo entrante y saliente (**mail filter**), relevo de correo desde dominios externos (**mail relay**) y envío de correo hacia dominios externos (**Mail Gateway**). Para que el

[27] **malware**: **Mal**icious Soft**ware**.

servidor interno de correo tenga un mejor desempeño éste limitará el tamaño de los mensajes salientes o entrantes.

desempeño éste limitará el tamaño de los mensajes salientes o entrantes.

desempeño éste limitará el tamaño de
los mensajes salientes o entrantes.

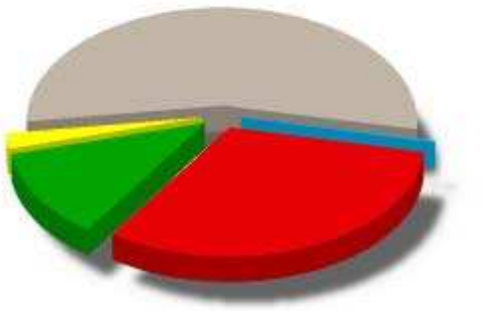


Figura 2.16 Estadísticas del tipo de tráfico en el servidor de correo fw.remq.edu.ec

El Mail Gateway será ubicado sobre la DMZ, y ningún cliente de correo electrónico podrá establecer conexiones con éste. El único servidor con el cual los clientes de correo deben conectarse es el servidor de la red Interna.

El servidor de correo que se utiliza sobre los equipos servidores actualmente es KerioMailServer, pero debido al número de usuarios y al costo de su licencia por usuario, se puede proponer una solución en software de libre distribución para servidores de alta capacidad como sendmail o postfix. De entre éstos, sendmail es el paquete por defecto en las distribuciones de Fedora, mientras que postfix en las distribuciones de Suse. Debido a que el personal de Administración de la Red tiene conocimientos de Fedora, mas no de Suse, por conveniencia se utilizará sendmail.

Dependiendo del destinatario en el mensaje de correo, el servidor interno decidirá si envía el mensaje al buzón /var/spool/mail/***nombre_del_usuario*** o enviarlo hacia el mail gateway. Esta consideración es importante para dimensionar la capacidad en disco del servidor y su estructura de dispositivos de bloque virtuales.

En el Anexo F.4 se observa que el mensaje de mayor tamaño recibido por el servidor fw.remq.edu.ec es de 18 [MB]. Por la que se considerado necesario y suficiente asignar una capacidad de 50 MBytes de espacio en disco para cada usuario.

$$\text{Capacidad en disco servidor interno} = \#\text{cuentas} * 50[\text{MB}]$$
$$Capacidad\,en\,disco\,servidor\,interno = (1691 * 5 + 20) * 50 = 42375[MB] = 413[GB]$$

Ecuación 2.28 Cálculo de la capacidad de disco duro para el servidor interno de correo electrónico.

Del Anexo F.4 se obtiene que aproximadamente el 12.71% de los mensajes de correo tienen como destino dominios externos, y un valor muy cercano de 12.77% es el porcentaje de cuentas de correo que enviaron esos mensajes, por lo que la consideración de que el 20% de los usuarios puedan enviar mensajes hacia otros dominios es acertada. Además se permitirá solamente el envío de mensajes con un tamaño máximo de 10 MB. El servidor mail gateway deberá permitir encolar todos estos mensajes.

$$\text{Capacidad en disco servidor DMZ} = \#\text{cuentas} * 0.2 * \text{Tamaño máximo de mensaje}$$
$$Capacidad\,en\,disco\,servidor\,DMZ = (1691 * 5 + 20) * 0.2 * 10[MB] = 16950[MB] = 16.55[GB]$$

Ecuación 2.29 Cálculo de la capacidad de disco duro para el servidor relay de correo electrónico

Debido a que las capacidades calculadas estarán dentro de la partición /var del disco, es necesario proveer un mecanismo que permita redimensionar dicha partición cuando sea necesario. Para esto se utilizarán dispositivos de bloque virtuales LVM (Logical Volume Management), donde uno o más volúmenes físicos (PV) que pueden ser discos duros o particiones de éstos, forman parte de un Grupo de Volúmenes (VG); un volumen físico puede dividirse en varias Extensiones Físicas (PE) de igual tamaño y varias PE de un mismo VG pueden combinarse para formar un Volumen Lógico (VL).

Con este esquema se prefieren discos de menor tamaño para ir incrementándolos según sean necesarios.

Para el cálculo del procesador es necesario tomar como referencia el servidor asterisk1.local que tiene un procesador Intel Xeon con CPU de 3.20GHz. Considerando que las solicitudes hacia el servidor son los mensajes transmitidos y recibidos por éste, del Anexo F.4 se obtienen los valores 16961 como mensajes recibidos y 16120 como enviados. La suma de éstos da 33081 solicitudes. Se consideran 3 operaciones: solicitud, procesamiento y respuesta del servidor por cliente cada cinco minutos. Para propósitos de dimensionamiento se considera que el servidor soporta concurrencia del 20% en las solicitudes realizadas.

uso CPU	% uso CPU	×	# CPU	×	vel. CPU [MHz]
2560,00	0,80		1,00		3200,00

solicitudes / segundo	# solicitudes	÷	tiempo [s]	×	simultaneidad
72,63	33081,00		3013440		6616,20

solicitudes / operación	# solicitudes	÷	# operaciones
2,00	2,00		1,00

costo / operación	uso CPU	÷	solic / seg	×	solic / oper
70,49	2560,00		72,63		2,00

operaciones / segundo	# ope / cliente	÷	tiempo [s]
0,0100	3,00		300,00

costo / usuario	costo / oper	÷	oper / seg
0,70	70,49		0,0100

CPU [MHz]	concurrencia	×	Costo / usuario
2331,97	3308,10		0,70

Tabla 2.21 Cálculo del CPU requerido en el servidor de correo interno

Según el resultado de la Tabla 2.21 es necesario un procesador de 2.33 [GHz], por lo cual el procesador tomado como referencia se lo puede utilizar en el nuevo servidor interno de correo.

El servidor de correo interno se configurará para proveer el servicio utilizando el protocolo POP3 a través del demonio ***dovecot*** para no mantener los mensajes en el buzón de cada cliente ya que provocaría pérdida de información cuando el buzón se encuentre lleno. Adicionalmente se configurará el servicio de administración de mensajes vía web utilizando ***squirrelmail*** ya que permite los controles necesarios para leer, escribir, archivar correos, y su administración es sencilla.

Como se analizó en el capítulo anterior, es necesario proveer de este servicio a dominios externos, para lo cual se utilizarán "dominios virtuales" y el tipo de reenvío utilizado será de una cuenta de correo en un dominio hacia el mismo nombre de usuario pero en el dominio conectividadglobal.net. Para esto se debe pedir que los registros MX de ese dominio apunten hacia el servidor de correo en el Data Center. Para calcular el requerimiento de procesador en el servidor de correo en la DMZ se propone como referencia el CPU del servidor con hostname router, Intel Pentium III de 500 MHz. La Tabla 2.22 muestra el cálculo del CPU requerido para este servidor.

uso CPU	% uso CPU	×	# CPU	×	vel. CPU [MHz]
400,00	0,80		1,00		500,00

solicitudes / segundo	# solicitudes	÷	tiempo [s]	×	simultaneidad
0,28	2050,00		3013440		410,00

solicitudes / operación	# solicitudes	÷	# operaciones
3,00	3,00		1,00

costo / operación	uso CPU	÷	solic / seg	×	solic / oper
4302,35	400,00		0,28		3,00

operaciones / segundo	# ope / cliente	÷	tiempo [s]
0,0017	1,00		600,00

costo / usuario	costo / oper	÷	oper / seg
7,17	4302,35		0,0017

CPU [MHz]	concurrencia	×	Costo / usuario
1469,97	205,00		7,17

Tabla 2.22 Cálculo del CPU requerido en el servidor de correo de la DMZ

Para el servidor de correo en la DMZ se necesita un CPU mínimo de 1.4 GHz. Se utilizará entonces el procesador del servidor con hostname firewall01. Sobre este servidor se instalará software adicional antispam y antivirus para lo cual se puede utilizar ***MailScanner*** o por separado ***SpamAssassin*** y ***AMaViS*** (A Mail Virus Scan). Es necesario que estos programas corran como demonios en el sistema.

Como medidas de seguridad se permitirán solamente conexiones en el puerto 25, se bloquearán los servicios adicionales como telnet, ssh desde redes y usuarios no autorizados. Hará falta agregar registros en los DNS tanto de la DMZ como interno.

2.10.4. ACTIVE DIRECTORY Y DNS INTERNO

Este servidor proveerá de los beneficios de autenticación y seguridad para redes Microsoft a los diferentes servidores y a los usuarios internos, es decir empleados de la empresa Conectividad Global Cía. Ltda.

El dimensionamiento o planeamiento de capacidad de éste se realizó utilizando la herramienta Microsoft Active Directory Sizer Tool, la cual basada en el perfil de la organización, la información del dominio y la topología de la red permite estimar el hardware necesario para proveer los servicios de autenticación y privacidad.

Se estima un total de 65 usuarios para el dominio conectividadglobal.net, donde se incluyen los usuarios de los distintos servidores, tanto de las instituciones en la red, como los empleados de la empresa. El porcentaje de concurrencia en horas pico se considera del 50% de usuarios.

El número de atributos por usuario es asignado automáticamente por esta herramienta, basada en el número de atributos que provee Active directory para cada usuario, es decir 25.

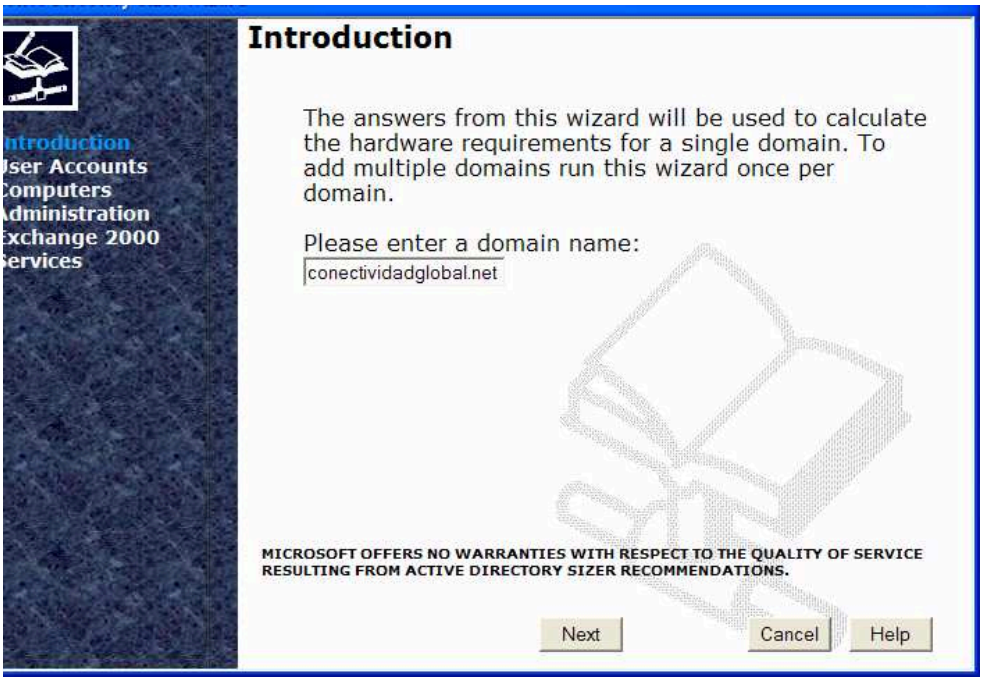


Figura 2.17 Active Directory Sizer

El número estimado de grupos de usuarios es seis: gerencia - financiero - proyectos, diseño web, desarrollo de software, soporte de software y administración de red. Se programará para que el sistema pida cambio de password cada 15 días. La tasa promedio de inicio de sesión por segundo en horas pico se estima con la herramienta incluida “Estimate logon Rates”.

El número estimado de equipos será la suma de servidores internos como rev.conectividadglobal.net, testserver.conectividadglobal.net; servidores en las instituciones dentro de la red interna, es decir 41; y las estaciones de trabajo de los empleados de la empresa haciendo un total de 65 hosts que accederán a los servicios de Active Directory.

Se considera que otros objetos como impresoras compartidas, carpetas de uso común y grupos de usuarios pueden llegar a ser 10.

Se decide el promedio de utilización del CPU para el único controlador de dominio del 80%.

Se realizarán cambios de los objetos, es decir parámetros de la administración diariamente en un promedio de una actividad para agregar, borrar y modificar objetos.

No se utilizará correo electrónico basado en Microsoft Exchange Server, pero si se utilizará el servicio de DNS.

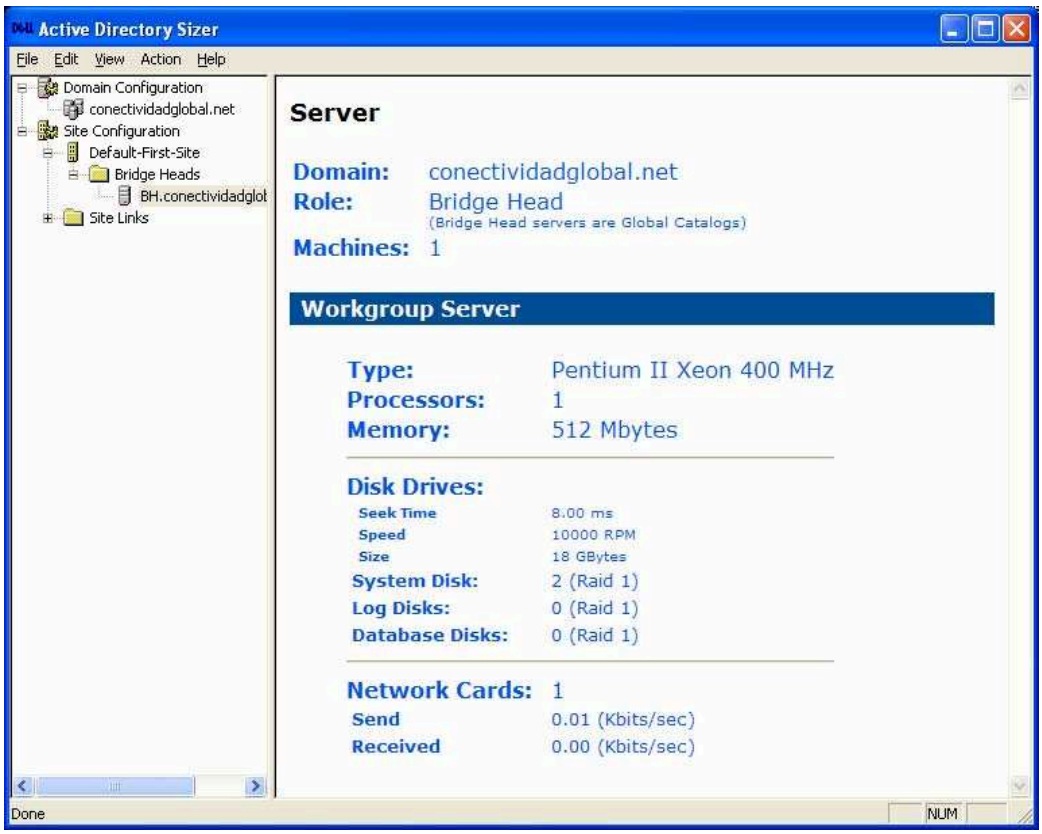


Figura 2.18 Cálculo de la capacidad necesaria para el servidor Active Directory

La Figura 2.18 muestra el resultado general del planeamiento de capacidad obtenido. La herramienta de dimensionamiento de hardware nos permite conocer que es necesario almenos un procesador a 400 MHz, 512 MBytes en RAM y un disco de 18 GBytes.

2.10.5. FTP Y NTP

Debido a la necesidad de tener registros de eventos de los sistemas, las autenticaciones realizadas, la hora a la que se realizaron las acciones sobre un servidor, el tiempo de asignación de los servicios, en el caso del correo, tener el tiempo real de envío de los mails, para auditoría, etc. Se hace necesario implementar un servidor que permita mantener la hora real en todos los sistemas, esto se logra con NTP (Network Time Protocol) que sincroniza la hora entre los sistemas con una precisión en microsegundos.

Los métodos para proveer comunicaciones NTP son del tipo unicast, broadcast y multicast. Debido a que se trata de tráfico y procesamiento despreciable se unirá este servicio con el de respaldos a través de FTP.

El servidor FTP debe soportar respaldos diarios del servidor de correo y de los servidores de aplicaciones, en los sistemas Linux se debe configurar un crontab que permita realizar un backup en una hora determinada.

El protocolo FTP permite el uso del máximo ancho de banda disponible en una conexión para transferencia de información. Debido a que es un servidor de respaldos, es necesario considerar algún tipo RAID que provea alta disponibilidad. La capacidad de disco puede calcularse de acuerdo al número de cuentas en el servidor de correo, al espacio en disco asignado a cada una de ellas y al volumen de información en los servidores de aplicaciones. Se debe tomar en cuenta que solamente se almacenará la información durante una semana debido a que es obligación del personal de Administración de Servidores respaldar la información en medios de almacenamiento extraibles.

2.10.6. SGA

Se utilizarán las sugerencias en cuanto a hardware de los desarrolladores de software de la empresa debido a que el personal realiza pruebas constantemente y sabe por experiencia lo que se necesita.

Mínimo

- 1 procesador Intel Pentium III de 800 MHz o superior.
- 128 MB de Memoria RAM mínimo.
- 1 disco duro de 10GB.
- 1 unidad de respaldo (medio magnético y/o quemador de CD).

Recomendado

- 1 procesadores Intel Pentium IV de 2 GHz o superior.
- 1024 MB de Memoria RAM.
- 1 disco duro SCSI de 4GB (para el sistema operativo y programas).
- 1 disco duro SCSI de 9GB (para la base de datos).
- 1 unidad de respaldo (medio magnético y/o quemador de CD).

Requerimientos Software:

- Sistema Operativo: Microsoft Windows XP Professional con Internet Information Services (IIS).
- Base de Datos: Microsoft SQL Server 2000 Desktop Engine (MSDE 2000 en ingles) con Service Pack 3.
- NET Framework 1.1
- Internet Explorer 6.0

2.10.7. TESTSERVER

Se acogen las sugerencias del equipo de desarrolladores de software.

Mínimo

- 1 procesador Intel Pentium IV de 2400 MHz o superior.
- 1024 MB de Memoria RAM mínimo.
- 1 disco duro de 100GB.
- 1 unidad de respaldo (medio magnético y/o quemador de CD).

Recomendado

- 1 procesadores Intel Pentium IV de 3200 Ghz o superior.
- 2048 MB de Memoria RAM.

- 1 disco duro SCSI de 18GB (para el sistema operativo y programas).
- 1 disco duro SCSI de 72GB (para la base de datos).
- 1 unidad de respaldo (medio magnético y/o quemador de CD).

Requerimientos Software:

- Sistema Operativo: Microsoft Windows Server 2003.
- Base de Datos: Microsoft SQL Server 2000 Desktop Engine (MSDE 2000 en ingles) con Service Pack 3.
- NET Framework 1.1.
- Internet Explorer 6.0.

CAPÍTULO 3. CONCLUSIONES Y RECOMENDACIONES

3.1. CONCLUSIONES

- Del análisis de la situación actual se pudo apreciar que el Data Center no posee una arquitectura de red definida que permita implementar seguridad en los puntos clave de la infraestructura de red.

- El análisis de tráfico generado en el Data Center es el punto de partida principal para la elaboración de un esquema de red que soporte todos los requerimientos de los usuarios y permita la implementación de nuevos servicios y aplicaciones.

- El diseño actual de red no provee mecanismos de seguridad, ni de respaldo de los recursos de la organización, por lo que es necesario acogerse a un nuevo esquema que brinde los beneficios de una red segura y confiable con el fin de garantizar la integridad y disponibilidad de la información.

- El análisis de la seguridad en base a la norma ISO/IEC17799 permitió obtener una adecuada y conjunta auditoría de los activos en materia de administración de la seguridad informática.

- Las políticas y procedimientos para la administración de las seguridades propuestas basadas en el análisis de riesgos definen el manejo de los activos de la empresa y los lineamientos de seguridad para protegerlos contra ataques internos y externos.

- El diseño de la arquitectura de red basándose en el Blueprint Cisco SAFE que utiliza una amplia variedad de equipos propietarios de la empresa Cisco, provee un esquema de seguridad en profundidad sobre cada módulo para mitigación de amenazas internas y externas de los diferentes sistemas informáticos, y además proporciona redundancia en su diseño.

- La estimación de tráfico del nuevo diseño del Data Center de acuerdo a la proyección hasta el 2011 permitió una selección de equipos de conectividad de acuerdo a requerimientos de capacidad de transporte y procesamiento de tráfico y la capacidad de los enlaces a Internet que se deberían contratar.

- El segmento de red Administración se encargará de recopilar información necesaria para análisis futuros de planeamiento de capacidad y evitar posibles cuellos de botella o procesamiento limitado por el hardware de los distintos sistemas de información y dispositivos de conectividad.

- El planeamiento de capacidad para los servidores juega un papel importante en el diseño debido a que basado en el tráfico actualmente generado se puede proyectar una tendencia de crecimiento del mismo y dimensionar equipos que soporten todos los requerimientos de los clientes.

- La seguridad de la información defe ser considerada como un proceso de mejoramiento contínuo en base a nuevos requerimientos de seguridad que se ajusten a los cambios de la empresa.

3.2. RECOMENDACIONES

- La implementación del proyecto debe ser por etapas, permitiendo la adaptabilidad tanto organizacional como de infraestructura.

- Rediseñar el software Sistema de Gestión Académica (SGA) para permitir la integración de la administración de las base de datos Microsoft SQL Server de los Sistemas de Gestión Académica de las instituciones educativas de la intranet con el Active Directory de Windows Server 2003 que mantiene el Data Center.

- Integrar el controlador de dominios de los sistemas de computación utilizando Active Directory para plataformas Windows 2000 o superior con Samba para los que utilicen plataformas Linux para una mejor administración de los usuarios y de los recursos.

- Se debe exigir al personal técnico de la empresa la documentación de los procedimientos operativos describiendo en lo posible tareas de requerimientos de programación, independencias con otros sistemas, tareas de mantenimiento, previstas y procedimientos de recuperación ante incidentes. Además se deberá mantener un inventario actualizado en los que se registren los cambios en las configuraciones, instalación o desinstalación de software de los sistemas informáticos utilizando las plantillas del Anexo C.

- Se debe realizar capacitación al personal nuevo contratado acerca de las políticas y procedimientos de seguridad que se manejan en la empresa y conjuntamente con la Gerencia se debería promover un cambio de cultura y concientización en su cumplimiento.

- Al realizar una reingeniería de red, es posible minimizar los costos de inversión que involucra su instalación y puesta en marcha determinando cuidadosamente los elementos de red que puedan ser reutilizados, sin afectar el rendimiento de la misma.

- Se debe realizar un proyecto que brinde una tecnología de acceso a usuarios apropiada y su análisis deberá partir del estudio realizado en este proyecto.

REFERENCIAS BIBLIOGRAFÍCAS

LIBROS

[1] International Business Machines Corporation. (2005). Linux Power User (course Code QLX02). Student Notebook.

[2] International Business Machines Corporation. (2005). Linux Network Administration I: TCP/IP and TCP/IP Services (course Code QLX07). Student Notebook. Linux Web.

[3] International Business Machines Corporation. (2005). Linux Network Administration II: Network Security and Firewalls (course Code QLX24). Student Notebook.Linux Web.

[4] International Business Machines Corporation. (2002). Linux as Web Server (Apache) (course Code QLX25). Student Notebook. Linux Web.

[5] Comer, Douglas E., y David L. Stevens. (2001). Internetworking with TCP/IP Volume 3: Client-server programming and applications. Linux/POSIX Sockets Version. New Jersey : Prentice Hall.

[6] Libro de Red de Área Local del Ingeniero Pablo Hidalgo.

[7] CHAMPLAIN JACK J.; Auditing Information Systems, 2003, Second Edition.

[8] KRAMER JOHN; The CISA Prep Guide: Mastering the certified Information System Auditor Exam.

[9] KRUTZ RONALD L., DEAN VINES RUSSEL; The CISSP Prep Guide: Mastering the ten domains of computer security

[10] SEAGREN ERIC; Securing your Network for Free, 2007

[11] Cisco SAFE Implementation - Student Guide Version 2.0, 2004.

[12] WADE EDWARDS, TERRY JACK, TODD LAMMLE, ROBERT PADJEN, ARTHUR PFUND, TOBY SKANDIER, CARL TIMM. CCNP® Complete Study Guide. Copyright © 2005 SYBEX Inc.,

NORMAS

[13] INTERNATIONAL STANDARD ISO/IEC 17799 Information technology — Security techniques — Code of practice for information security management.

MANUALES

[14] STONEBURNER GARY, GOGUEN ALICE, FERINGA ALEX; Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, Special Publication 800-30, October 2001

PÁGINAS WEB

[15] http://en.wikipedia.org/wiki/Data_center

[16] http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

[17] http://www.pc-doctor.com.mx/Radio%20Formula/temas/Redes.htm

[18] http://en.wikipedia.org/wiki/Root_nameserver

[19] http://download.kerio.com/archive

[20] http://www.slacksite.com/other/ftp.html

[21] http://en.wikipedia.org/wiki/Proxy_server

[22] http://luxik.cdi.cz/~devik/qos/htb/manual/userg.htm

[23] http://es.wikipedia.org/wiki/Videoconferencia

[24] http://www.wiredred.com/web-conferencing

[25] http://es.wikipedia.org/wiki/Capa_de_aplicaci%C3%B3n#Capa_de_aplicaci.C3.B3n_.28Capa_7.29

[26] http://www.skypilot.com/technology/

[27] http://www.skypilot.com/pdf/ds_skygateway.pdf

[28] http://www.skypilot.com/pdf/ds_skyextender.pdf

[29] http://www.skypilot.com/pdf/ds_SkyConnectorPro.pdf

[30] http://www.trepcom.com/Instalacion-wireless-Montevideo-Uruguay.pdf

[31] http://manageengine.adventnet.com/products/opmanager/documents.html#whitepaper

[32] http://www.fs-security.com/

[33] http://es.wikipedia.org/wiki/Firestarter

[34] http://en.wikipedia.org/wiki/Stateful_firewall

[35] http://www.microsoft.com/mspress/books/sampchap/5357.aspx