ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE RED PARA EL MEJORAMIENTO DEL DESEMPEÑO Y LA SEGURIDAD DE LA PLATAFORMA DE RED DE LA AUTORIDAD PORTUARIA DE GUAYAQUIL"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

INGENIERO EN

ELECTRICIDAD ESPECIALIZACIÓN ELECTRÓNICA

ROBERTO JAVIER SERRANO MALDONADO

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A mi familia: a mi papá, mi mamá y mis hermanos por creer siempre en mí.

A Juan Terán por su apoyo y aliento constante.

A José Francisco Rodríguez, Xavier Cárdenas y Amada Velásquez por brindarme ese empujón que necesitaba.

DEDICATORIA

A Dios, por estar siempre presente en mi vida.

A mis padres, por su amor incondicional y su guía constante.

TRIBUNAL DE SUSTENTACIÓN

M.Sc. César Yépez F.

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

Ph.D. Francisco Novillo P.

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en este Informe me corresponde exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

Roberto Javier Serrano Maldonado

RESUMEN

El presente Informe de Proyecto Profesional muestra los cambios que se aplicaron en la plataforma de red de la Autoridad Portuaria de Guayaquil para poder obtener un incremento en el rendimiento y mejoras en la seguridad de la red interna reutilizando equipos con los que contaba la Entidad y planteando un nuevo diseño de la segmentación de la red que existía hasta ese entonces.

ÍNDICE GENERAL

INTRODUCCIÓN

Análisis de la Situación

La Institución sobre la cual se desarrolló el proyecto fue la Autoridad Portuaria de Guayaquil.

La Empresa presentaba los siguientes problemas:

- No existe una estructura jerárquica en capas
- La segmentación de red no estaba realizada de una forma apropiada: Usuarios de distintos departamentos podían acceder a equipos de otros departamentos.
- No poseía un control sobre los dispositivos que se encontraban activos.
- No poseía un control sobre la disponibilidad de los enlaces internos y externos.
- La empresa mantenía enlaces de baja velocidad hacia edificios adjuntos. Había intermitencia en los enlaces.
- El equipo que funcionaba como enrutador de la red de datos, no tenía un nivel de redundancia y confiabilidad adecuados a pesar de la criticidad de la función que desempeñaba dentro del esquema actual de la red.
- No existía presupuesto asignado para la adquisición de nuevos equipos para el área.

El proyecto fue escogido debido a:

- La necesidad de establecer una estructura de red apropiada para el normal desempeño de la Empresa
- La necesidad de establecer seguridades en la red de datos
- La necesidad de mantener un control sobre la disponibilidad de equipos críticos y servicios de los que dispone la Empresa
- La necesidad de mejorar los enlaces hacia los edificios adjuntos tanto en velocidad como en estabilidad

Los objetivos específicos de este proyecto fueron:

- Diseñar e implementar un esquema de red jerárquico en capas
- Diseñar e implementar un nuevo esquema de segmentación de red
- Diseñar e implementar políticas de acceso de red
- Diseñar e implementar un esquema de monitoreo de enlaces y servicios críticos
- Diseñar e implementar un esquema que mejore los enlaces hacia los edificios adjuntos

CAPÍTULO 1

1. METODOLOGÍA IMPLEMENTADA

1.1. Criterios Utilizados

1.1.1. Criterios para el Diseño de Red

Cisco Systems recomienda [1] que en un diseño de red se combine:

- Máxima Disponibilidad
- Flexibilidad
- Seguridad
- Administrabilidad

Los principios sobre los que se basan los lineamientos para el diseño de redes son:

- Jerarquización
    - Facilita el entendimiento del rol de cada dispositivo en cada capa
    - Simplifica el despliegue, operación y mantenimiento
    - Reduce los dominios de falla en cada capa
- Modularidad
    - Permite una expansión transparente de la red y el establecimiento de servicios bajo demanda
- Resiliencia
    - Satisface la expectativa de los usuarios manteniendo la disponibilidad de la red
- Flexibilidad
    - Permite una distribución inteligente de carga utilizada por todos los recursos de la red

1.1.2. Criterios para el Diseño de Jerarquía

Dentro de los dos modelos de diseño de jerarquía [1] están:

- El modelo a tres capas: Núcleo, Distribución, Acceso
- El modelo a dos capas: Núcleo-Distribución Colapsadas, Acceso

Cada capa puede ser vista como un módulo estructurado bien definido, con roles específicos en la red de la empresa. Al introducir el principio de modularidad en el diseño jerárquico de la red Autoridad Portuaria de Guayaquil, se asegura que la red se vuelva resiliente y flexible para

proveer servicios de red críticos a la vez que permite los cambios y el crecimiento que pueden ocurrir a lo largo del tiempo.

En redes con pocos usuarios accediendo a la red, o en empresas que consistan de un solo edificio, el tener la capa de núcleo y distribución puede no ser necesario.

Es por esto que se siguió la recomendación de Cisco Systems [1] en utilizar el diseño de red de núcleo colapsado, en el cual las capas de núcleo y distribución se combinan en una sola capa.

Para esto, se utilizarían los conmutadores Cisco WS-C2950T-24 dentro de la capa de núcleo-distribución colapsada y los conmutadores no administrables se utilizarían en la capa de acceso.

1.1.3. Criterios para el Diseño de Seguridad

Para incrementar la seguridad dentro de la red de la Autoridad Portuaria de Guayaquil, se utilizaron los criterios expresados en el estándar ISO 27002:2005 [2], que indican:

11.1.1: …"*establecimiento de reglas basadas en la premisa 'En general, todo está prohibido, a menos que esté expresamente permitido' y no en la regla más débil de 'En general, todo está permitido, a menos que esté expresamente prohibido'"…*

11.2.2: …"*Se deberían asignar los privilegios a usuarios sobre los principios de necesidad-de-uso y evento-por-evento, y de manera acorde*

con la política de control de acceso, es decir, el requisito mínimo para su función, sólo cuando sea necesario"….

11.4.5: …"*En las redes, se deberían separar los grupos de servicios de información, usuarios y sistemas de información*"….

11.4.7: …"*Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio*"….

Por ello, se optó por segmentar de manera más agresiva la red, en la medida de las posibilidades, definiendo como unidad de aislamiento para asignación de privilegios los departamentos de la Institución. Así, a éstos se les iba a asignar los privilegios de acceso de acuerdo a las necesidades de acceso a información y servicios puntuales de cada departamento.

Además, utilizando el criterio del mismo estándar [2]:

10.4: …"*Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados*"….

Se optó por aprovechar las ventajas que poseen los equipos Fortigate 500A en la prevención de ataques en la red interna o alertas en caso de actividades sospechosas de equipos administrados o desconocidos.

1.1.4. Criterios para Resiliencia

Dentro de las consideraciones que hubo para mejorar la disponibilidad de

la red estuvieron:

- Colocar en alta disponibilidad los equipos que iban a realizar las funciones de enrutamiento de la red de datos de la Autoridad Portuaria de Guayaquil
- Reemplazar los enrutadores y módems que conectaban los edificios adjuntos por módems VDSL, así, se incrementaba la disponibilidad de ancho de banda y se eliminaba la intermitencia de conexiones que hasta el momento existía en las comunicaciones
- Utilizar una herramienta para verificar la disponibilidad de los enlaces de comunicaciones y de los equipos críticos

1.2. Diseño de la nueva segmentación de la Red

En concordancia con el criterio de seguridad seleccionado, se realizaría la segmentación de la red por departamentos. Esto garantizaría un control granular sobre el flujo de información entre las distintas áreas de la Autoridad Portuaria de Guayaquil.

1.2.1. VLANs

Para la segmentación de las redes se utilizaron LANs Virtuales (VLANs). Esto aislaría de manera lógica las redes asociadas con cada VLAN.

Una VLAN [3] (acrónimo de Virtual LAN, “red de área local virtual”) es un grupo de dispositivos sobre una o más LANs que son configuradas de tal forma que pueden comunicarse como si estuvieran sobre el mismo

dispositivo físico, cuando de hecho pueden estar localizados sobre un número de segmentos LAN diferentes. Debido a que las VLANs están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

1.2.2. Troncales VLAN

Todas las VLANs creadas fueron troncalizadas y enviadas a un dispositivo que se encargaría del enrutamiento y filtrado de paquetes.

Las troncales [4] son utilizadas para transportar el tráfico que pertenece a múltiples VLANs entre dispositivos sobre el mismo enlace. Un dispositivo puede determinar a cuál VLAN pertenece el tráfico mediante su identificador VLAN. El identificador VLAN es un tag que se encapsula junto con los datos.

1.2.3. Criterio de Asignación de VLANs

La asignación de VLANs fue estática. Cada puerto del conmutador fue etiquetado dependiendo del departamento al que iba a estar asignado.

1.2.4. Subredes

Fue necesaria la creación de nuevas subredes para cada departamento. La máscara de subred sería dimensionada de acuerdo a la cantidad de equipos que tuviera cada departamento.

1.2.5. Servidores DHCP

Fue necesaria la creación de servidores DHCP (Dynamic Host Configuration Protocol) para garantizar la distribución centralizada de direcciones IP a equipos en la red. Sólo un equipo va a estar encargado de dicha distribución, a diferencia de antes, donde equipos enrutadores hacían las funciones de servidores DHCP.

1.2.6. Configuración de Accesos

Las reglas anteriores tuvieron que ser desechadas por fallas o inconsistencias al momento de filtrar accesos.

Se realizó un estudio de los accesos que irían a tener cada departamento hacia los servidores del Centro de Cómputo. Se crearon reglas acordes a las necesidades de acceso de cada departamento. Dichas reglas serían implantadas posteriormente.

1.2.7. Reemplazo de Equipos

Se hicieron los siguientes reemplazos de equipos:

1.2.7.1. Conmutadores

Se reemplazaron los 4 conmutadores 3Com 3C16471 de 24 puertos Fast Ethernet y el conmutador CNet CNSH-800 de 8 puertos Fast Ethernet por 4 conmutadores Cisco Catalyst WS-C2950T-24 de 24 puertos Fast Ethernet y 2 puertos Gigabit Ethernet.

Los conmutadores Catalyst WS-C2950T-24 son administrables, permiten la creación de VLANs y enlaces troncales de VLANs. Además, facilita la configuración de VLANs mediante el protocolo propietario VTP (VLAN Trunking Protocol).

Se reemplazó además el conmutador DLink DES-3226 de 24 puertos Fast Ethernet por el conmutador 3Com 4400 SE de 24 puertos Fast Ethernet y 1 puerto Gigabit Ethernet.

1.2.7.2. Equipo Enrutador

Se reemplazó el equipo Clon que tenía las funciones de enrutamiento y filtrado de paquetes con los equipos Fortigate 500A que tenía la empresa y se los colocó en modo de alta disponibilidad.

El Equipo Fortigate 500A posee 1 conmutador Fast Ethernet de 4 puertos, 4 puertos Fast Ethernet y 2 puertos Gigabit Ethernet, soporta VLANs, permite la creación de servidores DHCP y filtrado de paquetes.

1.2.7.3. Equipos para Enlaces hacia Edificios Adjuntos

Los equipos reemplazados en los enlaces hacia los edificios adjuntos de la Autoridad Portuaria de Guayaquil son cubiertos en detalle en la sección 1.4 “Diseño de la solución para la mejora de los enlaces hacia los edificios adjuntos”.

1.3. Diseño de la solución para el monitoreo del enlace de Internet y de servicios críticos

Para el monitoreo de enlaces y servicios críticos, se instalaría un servidor con Friendly Pinger 5.0.

1.3.1. Friendly Pinger

Friendly Pinger es una aplicación orientada a la administración de redes, monitoreo e inventario.

Entre las ventajas que la aplicación ofrece están:

- Monitoreo de disponibilidad de dispositivos de red,
- Notificaciones cuando un servidor se cae o se levanta,
- Envío de paquetes ICMP a dispositivos en paralelo,
- Monitoreo de servicios HTTP, FTP, SMTP entre otros

1.3.2. Monitoreo del Enlace de Internet

1.3.2.1. Última Milla

Para el monitoreo de la última milla, se utiliza el envío de paquetes ICMP (Internet Control Message Protocol) Echo Request hacia el enrutador del proveedor. Además, se establecen sesiones hacia el puerto 53 TCP para la comprobación del servicio de DNS.

1.3.2.2. Salida Internacional

Para el monitoreo de la salida internacional del enlace de Internet se va a monitorear el servicio HTTP de dos sitios web conocidos.

1.3.3. Monitoreo de Servicios Críticos

Se definieron como servicios críticos:

- DNS
- Mensajería Interna
    - SMTP
- Bases de Datos Internas
    - SQL
    - Informix
- Portales Internos
    - HTTP
- Equipos Biométricos

El período de muestreo es de 60 segundos.

1.4. Diseño de la solución para la mejora de los enlaces hacia los edificios adjuntos

Los equipos que comunicaban al edificio central con las sedes eran equipos Cisco 805, 828, y 1760. Las tasas de transferencia máxima que podían alcanzar estos equipos estaban entre los 128kbps y los 512kbps. Aunque los edificios a los

cuales comunicaban se encontraban a menos de 1 Km de distancia, éstos eran tratados como una red WAN.

1.4.1. Reemplazo de Equipos

Se reemplazarían los routers y módems por Módems VDSL.

Con la eliminación de los routers en las localidades, se eliminaron también los servidores DHCP que ellos tenían. Esto brindaba la oportunidad de centralizar la distribución de direcciones IP.

CAPÍTULO 2

2. RESULTADOS OBTENIDOS

2.1. Implementación de la nueva segmentación de la Red

2.1.1. VLANs

Cada departamento estaría alojado en una VLAN como unidad de aislamiento.

Dentro del área de Sistemas se hicieron tres subdivisiones adicionales: la existencia de un segmento en el que estuvieran únicamente los administradores de infraestructura de servidores, un segmento para la división de producción y un segmento para la división de desarrollo.

2.1.2. Subredes

Con la separación departamental en unidades lógicas es necesaria la

creación de subredes para cada VLAN. La máscara de subred se seleccionó de acuerdo a la cantidad máxima de equipos existentes.

2.1.3. Servidores DHCP

Para minimizar la carga administrativa para la asignación de direcciones IP, se crearon servidores DHCP para cada una de las 18 subredes.

Los parámetros comunes de los servidores DHCP son:

- Dominio: puertodeguayaquil.corp
- DNS Primario: 10.1.0.237
- DNS Secundario: 10.1.0.238
- WINS Primario: 10.1.0.237
- WINS Secundario: 10.1.0.238

2.1.4. Equipos Fortigate

2.1.4.1. Hardware y Software

Los equipos Fortigate tenían las siguientes características:

- Modelo: 500A
- Firmware: 3.00 Maintenance Release 4 Patch 2 (26/01/2007)
- Interfases de Red: 1 conmutador Fast Ethernet de 4 puertos, 4 interfases Fast Ethernet, 2 interfases Gigabit Ethernet

2.1.5. Políticas de Acceso

En concordancia con el criterio de seguridad seleccionado, se establecieron las siguientes políticas, de manera general:

- Ningún segmento de red de usuarios va a tener acceso entre sí
- Todos los segmentos de red van a tener acceso a:
    - Servicios de infraestructura
    - Correo Electrónico
    - Navegación mediante un servidor proxy
    - Aplicativos de uso común de la Institución
- El segmento de servidores no va a tener acceso a la red de usuarios, salvo para envío de tareas de impresión
- El segmento de desarrollo accede únicamente a los servidores donde se encuentran los códigos fuentes de sus aplicativos
- Una regla activada bajo demanda permite que un equipo del segmento de administradores pueda comprobar la disponibilidad de equipos en toda la red

2.2. Implementación de la solución para el monitoreo del enlace de Internet y de servicios críticos

2.2.1. Hardware y Software

Se preparó un servidor virtual bajo VMWare ESX 3.5. El equipo tuvo las

siguientes características:

- Procesador: 2.8 GHz
- Memoria: 512 MB
- Tarjetas de Red: 1 interfaz Gigabit Ethernet
- Sistema Operativo: Microsoft Windows Server 2003 Enterprise Edition Service Pack 2
- Software de Monitoreo: Friendly Pinger 5.0

2.2.2. Configuración de la Interfaz de Red

La interfaz en el equipo estaba configurada de la siguiente forma:

- Dirección IP: 10.1.0.240
- Máscara de Red: 255.255.255.0
- Puerta de Enlace: 10.1.0.225
- Servidores DNS: 10.1.0.237, 10.1.0.238
- Servidores WINS: 10.1.0.237, 10.1.0.238

2.2.3. Configuración del Software de Monitoreo

Para el monitoreo del enlace de internet, se seleccionaron dos sitios para comprobar la conexión al puerto HTTP, y se comprobó la disponibilidad del enrutador del proveedor mediante el envío de paquetes ICMP Echo Request.

Para el monitoreo de los servicios críticos, se seleccionaron puertos apropiados para la comprobación de disponibilidad del servicio de

acuerdo al rol de cada equipo (bases de datos, servidores de nombre de dominio, correo electrónico, etc). Se enviaron paquetes ICMP Echo Request a equipos a los que únicamente se requería comprobar su disponibilidad.

2.3. Implementación de la solución para la mejora de los enlaces hacia los edificios adjuntos

2.3.1. Hardware

Se reemplazaron los módems y los enrutadores hacia los edificios adjuntos por Módems VDSL Zyxel Prestige 841C. Con los equipos, se pretendía alcanzar tasas de transferencia de hasta 16 Mbps sobre par de cobre.

2.4. Situación Actual de la Autoridad Portuaria de Guayaquil

La Autoridad Portuaria de Guayaquil actualmente posee:

- Una red de 18 segmentos
- Reglas de acceso entre segmentos de red
- Distribución de direcciones IP centralizada
- Control sobre los dispositivos que se encuentran activos mediante la herramienta Friendly Pinger
- Control sobre la disponibilidad de los enlaces internos y externos

mediante la herramienta Friendly Pinger, y

- Enlaces de 16 Mbps hacia los edificios adjuntos por medio de Módems VDSL.

CONCLUSIONES

La Autoridad Portuaria de Guayaquil obtuvo las siguientes ventajas producto los cambios realizados:

1. Jerarquización, Modularidad y Resiliencia al utilizar un diseño de red de núcleo colapsado
2. Administrabilidad al utilizar equipos que permitan su gestión remota en la capa de núcleo-distribución colapsada, centralización de las configuraciones de distribución de direcciones IP, centralización en la configuración de políticas de acceso
3. Seguridad, al seguir lineamientos del estándar ISO 27002:2005 en la creación de políticas de control de acceso y al aprovechar las ventajas que poseen los equipos Fortigate 500A en la prevención de ataques en la red interna o alertas en caso de actividades sospechosas de equipos administrados o desconocidos.

4. Resiliencia al implementar alta disponibilidad en el equipo de enrutamiento interno, incrementar los anchos de banda de los enlaces de comunicaciones hacia los edificios adjuntos y el monitoreo constante de la disponibilidad de enlaces y equipos críticos

ANEXOS

Abreviaturas

ATM: Asynchronous Transfer Mode

CIDR: Classless Inter-Domain Routing

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

Eth: Ethernet

FTP: File Transfer Protocol

HTTP: Hyper-Text Transfer Protocol

HTTPS: Hyper-Text Transfer Protocol Secure

ICMP: Internet Control Message Protocol

IOS: Internetwork Operating System

IP: Internet Protocol

ISAKMP: Internet Security Association and Key Management Protocol

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

LPD: Line Printer Daemon

MAC: Media Access Control

MB: Megabytes

Mbps: Megabits per second

NAT-T: Network Address Translation - Transversal

NetBIOS: Network Basic Input/Output System

NTDS: New Technology Directory Service

NTFRS: New Technology File Replication Service

NTP: Network Time Protocol

POP3: Post-Office Protocol v.3

PVC: Private Virtual Circuit

RPC: Remote Procedure Protocol

SHDSL: Single-pair high-speed digital subscriber line

SMTP: Simple Text Transfer Protocol

SQL: Structured Query Language

TCP: Transfer Control Protocol

UDP: User Datagram Protocol

VDSL: Very-high-bit-rate digital subscriber line

VLAN: Virtual Local Area Network

VTP: VLAN Trunking Protocol

WINS: Windows Internet Naming Service

Equipos y Configuraciones Anteriores

La Autoridad Portuaria de Guayaquil poseía un computador de escritorio clon con sistema operativo Linux que funcionaba como enrutador de la red de datos, servidor DHCP y smarthost SMTP.

Las redes utilizadas por la empresa eran:

- 10.3.10.x Usuarios,
- 10.3.20.x Sistemas,
- 10.3.30.x Presidencia e Ingeniería,
- 10.3.61.x Operaciones y Seguridad Física, y
- 10.1.0.x Servidores.

La segmentación de la red era física: cada red convergía a un conmutador no-administrable y éste, a su vez, a una interfaz del enrutador.

Los equipos que poseía el Área de Sistemas eran:

- 2 Firewall Fortigate 500A
- Conmutador 3Com 4226T
- Conmutador D-Link DES 3226
- Conmutador Cisco 2950
- Conmutador 3Com Baseline
- Conmutador 3Com Superstack 4400 SE
- Enrutador Cisco 1760
- Enrutador Cisco 2600

El edificio principal se conectaba a los edificios adjuntos mediante par de cobre.

Tabla 1: Configuración IP de las Interfases de Red del Enrutador

Interfaz	Direccionamiento	Dirección	Máscara de Red	Puerta de Enlace	Red	Dirección de Broadcast
Eth0	Estático	10.100.0.25	255.255.255.248	10.100.0.26	10.3.10.255	10.100.0.31
Eth5	Estático	10.3.10.254	255.255.255.0	-	10.3.10.0	10.3.10.255
Eth2	Estático	10.3.20.33	255.255.255.224	-	10.3.20.32	10.3.20.63
Eth3	Estático	10.3.30.33	255.255.255.224	-	10.3.30.32	10.3.30.63
Eth4	Estático	10.3.40.33	255.255.255.224	-	10.3.40.32	10.3.40.63
Eth6	Estático	10.3.60.5	255.255.255.252	-	10.3.60.4	10.3.60.7
Eth7	Estático	10.3.60.9	255.255.255.252	-	10.3.60.8	10.3.60.11

Figura A1.1: Conexiones de Equipo Enrutador

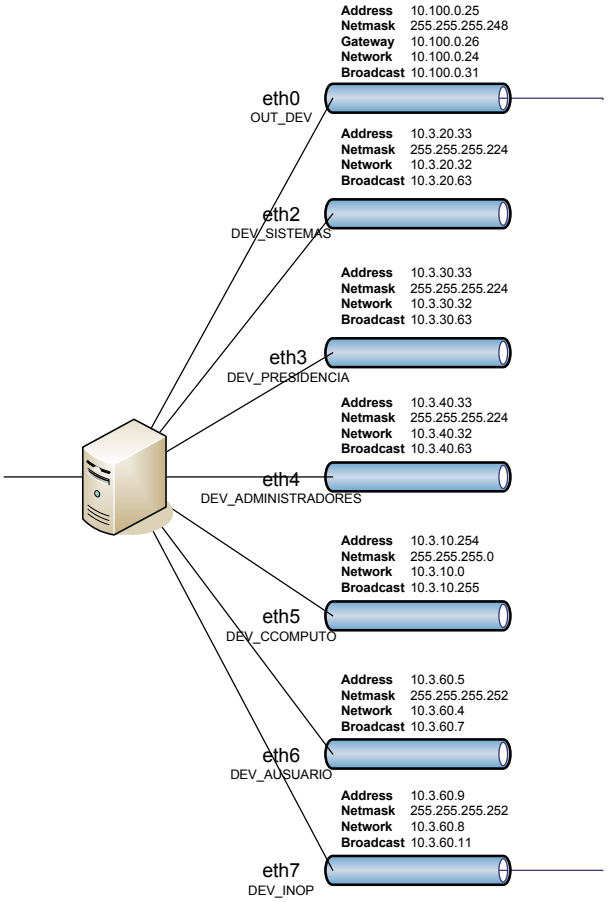

Tabla 2: Configuración DHCP de Enrutador

Subred	Máscara de Red	Rango	Puerta de Enlace	Dirección de Broadcast
10.3.10.0	255.255.255.0	10.3.10.50-10.3.10.199	10.3.10.254	10.3.10.255
10.3.20.32	255.255.255.224	10.3.20.34-10.3.20.62	10.3.20.33	10.3.20.63
10.3.30.32	255.255.255.224	10.3.30.34-10.3.30.60	10.3.30.33	10.3.30.63

Tabla 3: Reservaciones DHCP

Equipo	Dirección MAC	IP	Equipo	Dirección MAC	IP
imp_audit	00:20:00:4a:6d:4c	10.3.10.20	pclbeltran	00:0f:fe:b0:ed:fd	10.3.10.52
pctvega	00:0d:60:07:c7:9f	10.3.10.53	pcrfarfan1	00:0d:60:a8:9b:b0	10.3.10.54
pcmnavas	00:11:25:67:5d:8f	10.3.10.55	pcsagreda	00:0a:5e:41:a1:77	10.3.10.56
pcanevarez	00:60:94:51:9a:13	10.3.10.57	pctrivino	00:0d:60:41:46:64	10.3.10.59
pcmerchan	00:08:0d:f2:7a:f7	10.3.10.61	pcmsolis	00:60:97:57:40:0d	10.3.10.62
jastudillo	00:0d:60:41:6f:3a	10.3.10.63	pclgarcia1	00:0d:60:a7:1e:8f	10.3.10.64
pcpadilla1	00:0d:60:a5:64:f8	10.3.10.65	pcrnorero	00:08:0d:c4:0f:fc	10.3.10.66
laptopdtorres	00:08:0d:ea:7a:f7	10.3.10.68	libre_69	00:00:01:45:ea:bb	10.3.10.69
pcesanchez-	00:0d:60:a7:19:8e	10.3.10.70	pccabina	00:0d:60:41:46:66	10.3.10.71
pcdaniel	00:0f:fe:b1:79:da	10.3.10.73	pcwmartinez1	00:02:e3:33:cb:75	10.3.10.74
pcndominguez	00:04:ac:25:b0:86	10.3.10.75	pcnyela	00:6f:fe:b1:97:8c	10.3.10.76
pcmguerrero	00:0d:60:a7:0c:01	10.3.10.77	pcmrivadeneyra	00:04:ac:25:ae:8a	10.3.10.78
pccartagena	00:60:94:51:a7:39	10.3.10.79	pcaruiz	00:0f:fe:b1:96:e8	10.3.10.80
pcjrrhhmg	00:0d:60:a5:af:00	10.3.10.81	pcpfarfan	00:0d:60:a7:18:20	10.3.10.82
pcsrodriguez	00:0f:fe:b0:56:02	10.3.10.83	pcimontalvo	00:08:0d:10:09:fc	10.3.10.84
pcwmarinezg	00:08:0d:89:c7:f8	10.3.10.86	sapg18	00:10:18:0a:56:e5	10.3.10.87
pcpbarreiro	00:0f:fe:b0:f4:c7	10.3.10.88	pcrpogo	00:02:e3:33:ba:65	10.3.10.90
pcpvintimilla	00:0d:60:41:55:a9	10.3.10.91	pcpparedes	00:0d:60:3d:31:32	10.3.10.92
pcmcarranza	00:02:e3:31:91:14	10.3.10.93	impresora_fx_2b7e2a	08:00:37:2b:7e:2a	10.3.10.94
pcjbravo	00:0d:60:41:54:8e	10.3.10.95	miguel	00:0D:60:41:74:FF	10.3.10.96
pccontr01	00:04:ac:25:df:71	10.3.10.97	lxk4d0a4d	00:04:00:b2:50:b2	10.3.10.99
pcaias01	00:08:0d:03:0f:fc	10.3.10.100	mandino	00:0d:60:41:54:ff	10.3.10.101
bas_int_01	00:11:25:66:69:69	10.3.10.102	pcddunn	00:09:6b:d5:71:31	10.3.10.103
pc_gmacias	00:0d:60:a7:0c:37	10.3.10.104	pcmcedeno	00:0D:60:3D:31:A3	10.3.10.106
pcdhernandez1	00:0d:60:41:3d:7f	10.3.10.107	pchmerchan1	00:0d:60:41:55:ef	10.3.10.109
pcjchavez1	00:0d:60:41:65:56	10.3.10.110	pcgcasanova	00:0f:fe:43:24:4d	10.3.10.111
pcgvilla	00:04:ac:25:52:f6	10.3.10.112	pckortiz	00:50:ba:a7:56:30	10.3.10.113
pcgabriela	00:60:94:51:a7:61	10.3.10.114	libre_115	11:10:01:45:aa:bb	10.3.10.115
libre_116	00:38:01:45:aa:bb	10.3.10.116	libre_118	00:00:e1:75:aa:bb	10.3.10.118
pcsadi02	00:11:25:66:69:ed	10.3.10.119	pcltorres	00:0b:cd:a9:33:66	10.3.10.120
pcdigita01	00:11:25:66:74:78	10.3.10.121	pcsildeyg	00:04:ac:25:4a:c5	10.3.10.123
pcfguevara	00:09:6b:9d:73:3b	10.3.10.125	rvalle	00:0d:60:69:bb:8a	10.3.10.126
pcvvelez1	00:09:6b:d5:71:36	10.3.10.127	pcmaritzan	00:0d:60:a7:2b:c5	10.3.10.128
pctramon	00:09:6b:d5:f7:08	10.3.10.129	pchmerchan	00:0f:fe:b1:97:05	10.3.10.130
pctguerrero	00:06:1b:c2:53:21	10.3.10.133	pcsmartinez	00:08:0d:b3:0f:fc	10.3.10.134
pcontabilidad0	00:0d:60:41:3a:c4	10.3.10.13	pclsantos	00:0d:60:a7:0b:27	10.3.10.13

Equipo	Dirección MAC	IP	Equipo	Dirección MAC	IP
5		5			6
pcpfarfan1	00:0d:60:41:89:bb	10.3.10.13	pceayala	00:0d:60:3d:33:ef	10.3.10.13
		7			8
pclochoa	00:04:ac:25:51:06	10.3.10.13	libre_140	00:00:01:c2:c2:bb	10.3.10.14
		9			0
pcfacturac03	00:0f:fe:b0:f4:9f	10.3.10.14	pcfcaux01	00:0d:60:41:59:42	10.3.10.14
		1			2
pcpatriciag	00:11:25:67:24:7c	10.3.10.14	concesiones_temp	00:08:02:63:8e:be	10.3.10.14
		3			4
pcfflores	00:0d:60:41:45:4f	10.3.10.14	pcmalvarado	00:0d:60:41:65:5e	10.3.10.14
		5			6
pcmguevara_	00:0d:60:41:47:5b	10.3.10.14	pcpriscilar	00:09:6b:d5:25:8d	10.3.10.14
		8			9
pcjbriones	00:0d:60:41:59:42	10.3.10.15	pc_rrosero	00:06:1b:c2:54:84	10.3.10.15
		2			3
fx-2b12cc	08:00:37:2B:12:C	10.3.10.15	pccgarcia	00:0D:60:41:6D:D	10.3.10.15
	C	4		B	5
pcdgarofalo	00:0D:60:A7:1F:1	10.3.10.15	pccbenitez	00:0d:60:41:85:92	10.3.10.16
	B	9			1
sipa2	00:08:02:38:0A:72	10.3.10.16	pcpbriones	00:0d:60:a5:c3:75	10.3.10.16
		3			4
ogallo	00:0d:60:6b:6a:f5	10.3.10.16	pcmmontalvo	00:06:1b:c2:53:ff	10.3.10.16
		5			8
libre_169	00:00:01:78:78:78	10.3.10.16	libre_170	00:33:33:33:aa:bb	10.3.10.17
		9			0
pcmmoncayo	00:09:6b:d5:75:74	10.3.10.17	pcjvergara	00:0d:60:a7:1c:29	10.3.10.17
		2			3
pcgalcivar	00:0d:60:3d:30:e5	10.3.10.17	pclramos	00:06:1b:c2:f1:36	10.3.10.17
		4			5
pcwmartinez_	00:0d:60:3d:10:04	10.3.10.17	pccontr02	00:08:0d:f5:7a:f7	10.3.10.17
		6			7
pchmoreno	00:09:6b:d5:75:12	10.3.10.17	pcicelleri	00:0d:60:a5:d6:6d	10.3.10.17
		8			9
pcleonor	00:0d:60:41:6e:84	10.3.10.18	pcgpavon	00:0f:fe:b0:5d:dd	10.3.10.18
		0			1
pcksolorzano	00:0D:60:A4:74:8	10.3.10.18	pcbasc_problema	00:0d:60:41:70:4c	10.3.10.18
	E	2			3
pc_rfarfan	00:09:6b:d5:25:c9	10.3.10.18	pcabecerra	00:0d:60:41:54:55	10.3.10.18
		4			5
pcdtorres	00:06:1b:c2:52:f1	10.3.10.18	pclarrese	00:0d:60:a7:20:24	10.3.10.18
		6			7
pcletamendi1	00:0d:60:63:ff:90	10.3.10.18	pcjsanlucas	00:0d:60:41:78:5b	10.3.10.18
		8			9
pcbalvarez	00:04:ac:25:db:87	10.3.10.19	pc_abrito	00:0d:60:a7:04:b2	10.3.10.19
		1			2
pcnjacome	00:0d:60:41:57:45	10.3.10.19	pcagonzalezz	00:0d:60:41:53:dc	10.3.10.19
		3			6
Libre_197	00:0d:4d:4d:4d:db	10.3.10.19	narteaga	00:0d:60:41:57:6a	10.3.10.19
		7			8
pcjorge	00:0e:7f:a4:2a:3d	10.3.10.19	pcrquiroz	00:11:25:65:15:07	10.3.20.35
		9			
pccarrasco2	00:0d:60:a4:87:75	10.3.20.36	pcmmorales	00:11:25:65:06:79	10.3.20.37
christian	00:02:e3:31:ab:49	10.3.20.38	jsanlucas	00:0D:60:A7:1F:1B	10.3.20.42
pccmanrique	00:0d:60:a7:16:e9	10.3.20.43	pcraguirre	00:11:25:65:0a:07	10.3.20.44
pccramirez1	00:0d:60:a7:13:78	10.3.20.45	pcamoreno	00:0d:60:a5:9b:f3	10.3.20.46
pcdrueda1	00:06:1b:c6:4f:89	10.3.20.47	impresoralx	00:04:00:52:36:99	10.3.20.48
pclnieves	00:0d:60:3d:20:84	10.3.20.49	pcjcordova	00:0d:60:a7:16:e9	10.3.20.50
sapg05	00:06:29:50:a9:17	10.3.20.51	sapg11	00:02:a5:ea:45:2b	10.3.20.52
pcbackup02	00:0d:60:a8:ba:58	10.3.20.53	pcintercambio	00:04:ac:ae:ec:c7	10.3.20.54
laptopraul	00:0f:b0:01:c8:6f	10.3.20.55	sapg03-b	00:0b:cd:4d:ec:c1	10.3.20.59
pcwsamaniego	00:0d:60:63:f7:62	10.3.20.61	pcing	00:20:af:b6:c7:85	10.3.30.39
pcrordonez	00:0f:fe:b1:78:c0	10.3.30.40	pcjberta	00:03:47:19:31:f2	10.3.30.43
pcfalquez2	00:0d:60:41:6e:08	10.3.30.45	pcsluna	00:0d:60:a7:01:0e	10.3.30.47
pcavillacis	00:0d:60:41:53:fa	10.3.30.49	contraloria01	00:08:0d:b3:7f:f7	10.3.30.52
pccbohorquez	00:04:AC:25:4A:9	10.3.30.57	pcpacheco	00:0d:60:a5:c5:cf	10.3.30.58

Equipo	Dirección MAC	IP	Equipo	Dirección MAC	IP
	7				
imp-ingenieria	08:00:37:2b:7e:2a	10.3.30.59	pcesolis	00:0d:60:41:59:46	10.3.30.60
imp_concesion	08:00:37:27:4C:A6	10.3.30.61			

Tabla 4: Direcciones IP Configuradas en Enrutador

Nombre	IP	Descripción
Admin1	10.3.40.34	Dirección Obsoleta
Admin2	10.3.40.35	Administrador de Bases de Datos
Admin3	10.3.40.45	Dirección Obsoleta
Admin4	10.3.40.37	Administrador de Redes
Admin5	10.3.40.41	Dirección Obsoleta
Admin6	10.3.40.39	Dirección Obsoleta
Admin7	10.3.40.40	Dirección Obsoleta
Aix	10.1.0.233	Servidor Bases de Datos
Aix2	10.3.20.58	Servidor de Desarrollo
Aixdes	10.3.20.58	Servidor de Desarrollo
Atenbio	10.3.61.47	Equipo Programacion de Biométricos
Basepsion	10.3.10.205	Equipo de Comunicaciones
Bio1	10.3.10.22	Equipo Biométrico
Bio2	10.3.10.24	Equipo Biométrico
Bio3	10.3.10.25	Equipo Biométrico
Bio4	10.3.10.26	Equipo Biométrico
Bio5	10.3.10.27	Equipo Biométrico
Bio6	10.3.10.28	Equipo Biométrico
Bio7	10.3.61.44	Equipo Biométrico
Christian	10.3.20.38	Dirección Obsoleta
Cobra	10.101.0.1	Servidor Tarja
Comunic	10.1.0.249	Servidor de Archivos
Digit	10.1.0.247	Servidor de Digitalización
Dominio	10.1.0.237	Controlador de Dominio
Drivers	10.1.0.244	Servidor de Archivos
Drweb	10.1.0.245	Dirección Obsoleta
Dwh	10.1.0.230	Dirección Obsoleta
Eikon	10.3.20.53	Servidor de Pruebas WebService
Equipo	10.1.0.191	Servidor de Pruebas
Fiel	10.1.0.250	Servidor de Aplicación
Instalacion	10.3.10.60	Dirección Obsoleta
Jsanlucas	10.3.10.189	Jefe de Producción
Lexmark	10.3.20.48	Impresora de Sistemas
Lnieves	10.3.20.49	Asistente de Sistemas
Mail	10.1.0.229	Servidor de Correos
Mail2	10.3.10.252	Dirección Obsoleta
Malvarado	10.3.10.146	Recursos Humanos
Oper	10.3.20.40	Dirección Obsoleta
Pcamoreno	10.3.20.52	Jefe de Desarrollo
Pcantinar	10.3.10.199	Dirección Obsoleta
Pccgarcia	10.3.10.195	Seguridad Física
Pcdanielg	10.3.10.139	Control de Tráfico de Buques
Pcdrueda	10.3.20.47	Dirección Obsoleta
Pcebonilla	10.3.63.4	Control de Tráfico de Buques
Pcjgellibert	10.3.20.54	Dirección Obsoleta
Pcjjimenez	10.3.10.158	Seguridad Física
Pcjjimenez1	10.3.63.20	Control de Tráfico de Buques
Pcjsanlucas	10.3.20.42	Dirección Obsoleta
Pcnpluas	10.3.63.7	Control de Tráfico de Buques
Pcocastillo	10.3.20.34	Dirección Obsoleta
Pcopip	10.3.63.44	Control de Tráfico de Buques
Pcpbarreiro	10.3.10.133	Control de Gestión
Pcpcarrion	10.3.63.1	Control de Tráfico de Buques
Pcracines	10.3.10.168	Seguridad Física

Nombre	IP	Descripción
Pcrquiroz	10.3.20.35	Operador de Sistemas
Pcrrosero	10.3.10.115	Control de Gestión
Portal	10.1.0.241	Portal Empresarial
Portal_B	10.1.0.100	Dirección Obsoleta
Portaldes	10.1.0.243	Dirección Obsoleta
Presidente	10.3.30.51	Presidente APG
Procla	10.1.0.246	Dirección Obsoleta
Proxy	10.3.10.210	Servidor Proxy Telconet
Psion	10.1.0.248	Equipo de Comunicaciones
Respaldodigital	10.3.62.23	Dirección Obsoleta
Sapg05	10.3.20.51	Servidor de Desarrollo
Sapg08	10.1.0.250	Dirección Redundante
Sapgbkup	10.1.0.239	Dirección Obsoleta
Satur	10.3.20.59	Dirección Obsoleta
Sharepoint	10.1.0.190	Dirección Obsoleta
Sqlprod	10.1.0.232	Servidor Bases de Datos
Sus	10.1.0.242	Controlador de Dominio

Tabla 5: Redes Configuradas en Equipo Enrutador

Nombre	Red/Prefijo CIDR	Descripción
Red Ccomputo	10.3.10.0/24	Red de Usuarios
Red Sistemas	10.3.20.0/27	Red de Sistemas
Red Presidencia	10.3.30.0/27	Red de Presidencia/Ingeniería
Red Administradores	10.3.40.0/26	Red de Administradores
Red Ingenieria	10.3.50.64/29	Red Obsoleta
Red Ausuario	10.3.61.32/27	Red de Atención al Usuario
Red Inventarios	10.3.62.16/28	Red Obsoleta
Red Operaciones	10.3.63.0/26	Red Obsoleta
Red Corporativa	10.100.0.0/24	Red Obsoleta
Red Servidores	10.1.0.0/24	Red de Servidores
Red Cae1	192.168.100.0/24	Red Obsoleta
Red Cae2	157.100.115.0/24	Red Obsoleta
Red Cae3	10.3.50.0/24	Red Obsoleta
Red Pol	192.168.0.0/28	Red Obsoleta

Tabla 6: Puertos Configurados en Equipo Enrutador

Nombre	Puerto	Descripción
HTTP	80	Hypertext Transfer Protocol
SSH	22222	Uso desconocido
FTP1	21	File Transfer Protocol (Control)
FTP2	20	File Transfer Protocol (Data)
KERBEROS	88	Kerberos
HTTPS	443	HTTP sobre TSL/SSL
SMB	135:139	RPC Endpoint mapper, Profile Naming System, NetBIOS Name Service, NetBIOS Datagram Service
NETBIOS	139	NetBIOS Session Service
GPO	4319	Uso desconocido
GPO1	2725	Microsoft SQL 2000 Analysis Services
WINS	445	SMB sobre TCP/IP
SMTP	25	Simple Mail Transfer Protocol
POP	110	Post-Office Protocol v3
IMAP	143	Internet Message Access Protocol
DNS	53	Domain Name System
LDAP	389	Lightweight Directory Access Protocol
LDAP1	636	LDAP sobre TSL/SSL
MSQL	1433	Microsoft SQL Server

Nombre	Puerto	Descripción
PROXY	3128	Conexión Proxy
NTP	123	Network Time Protocol
DCOM	1024:1030	Distributed COM
NESSUSD	1241	Nessus
ANALYSIS	2725	Microsoft SQL 2000 Analysis Services
LIVESERVER	8888	Conexión Proclarity
DIGIT	3234	Conexión Alchemy
DRWEB	2371	Conexión Antivirus Dr. Web
BIO	3001	Conexión Equipos Biométricos
PSION	16101	Conexión Equipo Teklogix
RT	16102	Conexión Equipo Teklogix
LEXMARK	515	Conexión Impresora Lexmark

Tabla 7: Políticas de Acceso Configuradas en Enrutador

Origen	Destino	Tipo	Puerto
Dominio	Admin4	Tcp	Gpo Smb
Instalacion	Aix	Tcp	
Cualquiera	Aix2	Tcp	23
Psion 10.3.20.39	Basepsion	Tcp	Psion
Atenbio Drivers	Bio1 Bio2 Bio3 Bio4 Bio5 Bio6	Tcp	Bio
Drivers	Bio7	Tcp	Bio
Red Ccomputo	Christian	Tcp	Wins
Instalacion Pcantinar Pccgarcia Pcdanielg Pcdrueda Pcebonilla Pcjjimenez1 Pcocastillo Pcopip Pcpcarrion Pcracines Pcrquiroz	Cobra	Tcp	Msql
Red Ausuario Red Ccomputo Red Operaciones Red Sistemas	Comunic	Tcp	Wins
Red Inventarios	Digit	Tcp	Digit Wins
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Dominio	Tcp	Dcom Dns Kerberos Ldap Ldap1 Ntp Smb Wins
Admin4	Dominio	Tcp	Smb

Origen	Destino	Tipo	Puerto
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Drivers	Tcp	Wins
Red Ccomputo Red Operaciones Red Sistemas	Drweb	Tcp	Drweb
Red Ccomputo Red Operaciones Red Sistemas	Equipo	Tcp	Http
Red Ausuario Red Inventarios Red Operaciones Red Sistemas	Fiel	Tcp	Wins
Red Ccomputo Red Presidencia	Fiel	Tcp	Cualquiera
Aix	Lexmark	Tcp	Lexmark
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Mail	Tcp	Http Netbios Pop Smtp Wins
Cualquiera	Mail2	Tcp	25
Pcjjimenez	Pcnpluas	Tcp	Wins
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Portal	Tcp	Http Https
Pcpbarreiro Pcrrosero	Portal Portal	Tcp Tcp	Wins Wins
Red Sistemas Red Sistemas	Portal_B	Tcp	Http Https
Red Ccomputo	Procla	Tcp	Http Liveserver Wins
Red Presidencia	Procla	Tcp	Http
Red Sistemas	Procla	Tcp	Wins
Red Ausuario Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Proxy	Tcp	Proxy
Red Presidencia	Sapgbkup	Tcp	Cualquiera
Red Ccomputo Red Sistemas	Sharepoint Sharepoint	Tcp Tcp	Http Http
Instalacion	Sqlprod	Tcp	Msql
Red Ccomputo Red Operaciones Red Presidencia	Red Servidores Red Servidores Red Servidores	Tcp Tcp Tcp	Analysis Analysis Analysis
Red Operaciones	Red Servidores	Tcp	Liveserver
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia	Red Servidores	Tcp	Msql
Pcrquiroz	Cualquiera	Tcp	Ftp1 Ftp2
Dominio	Admin4	Udp	Gpo1

Origen	Destino	Tipo	Puerto
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Dominio	Udp	Dcom Dns Kerberos Ldap Ldap1 Ntp Smb Wins
Admin4	Dominio	Udp	Wins
Red Sistemas	Mail	Udp	Pop
Red Presidencia	Sapgbkup	Udp	Cualquiera
Red Ccomputo Red Inventarios Red Operaciones Red Sistemas	Red Servidores	Udp	Nessusd
Cualquiera	Admin4	Cualquiera	Cualquiera
Lnieves	Aix	Cualquiera	Cualquiera
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia	Aix	Cualquiera	Cualquiera
Cualquiera	Aix2	Cualquiera	Cualquiera
Red Presidencia	Aixdes	Cualquiera	Cualquiera
Rt	Basepsion	Cualquiera	Cualquiera
Jsanlucas	Cobra	Cualquiera	Cualquiera
Cualquiera	Eikon	Cualquiera	Cualquiera
Pcamoreno	Mail	Cualquiera	Cualquiera
Cualquiera	Mail2	Cualquiera	Cualquiera
Satur Red Operaciones	Procla	Cualquiera	Cualquiera
Flanker Foxbat Kfir Sapgbkup Red Pol	Proxy	Cualquiera	Cualquiera
Digit	Respaldodigital	Cualquiera	Cualquiera
Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia Red Sistemas	Sus	Cualquiera	Cualquiera
Dominio Sus	Red Administradores	Cualquiera	Cualquiera
Red Ccomputo	Red Ausuario	Cualquiera	Cualquiera
Dominio Red Ausuario	Red Ccomputo	Cualquiera	Cualquiera
Aix Sus	Red Ausuario Red Ccomputo Red Inventarios Red Operaciones Red Presidencia	Cualquiera	Cualquiera
Proxy	Red Pol	Cualquiera	Cualquiera
Sus	Red Sistemas	Cualquiera	Cualquiera
10.1.0.200	10.3.40.37	Cualquiera	Cualquiera

Origen	Destino	Tipo	Puerto
Admin1 Admin2 Admin3 Admin4 Admin5 Admin6 Admin7 Aix2 Eikon Jsanlucas Mail2 Oper Pcdrueda Presidente Proxy Satur Red Cae1 Red Cae2 Red Cae3 10.3.10.119	Cualquiera	Cualquiera	Cualquiera

Tabla 8: Configuración IP de Interfases de Equipo Fortigate

Puerto	Asignado a	Dirección	Máscara de Red
1	Acceso a Internet	200.110.76.195	255.255.255.248
2	Red de Clientes	10.100.0.26	255.255.255.248
3	Inhabilitado		
4	Calle H	10.2.0.225	255.255.255.0
5	Administradores	192.168.50.3	255.255.255.0
6	Servidores	10.1.0.225	255.255.255.0
LAN	Asotarja	10.10.10.60	255.255.255.0

Tabla 9: Direcciones IP configuradas en Equipo Fortigate

Nombre	IP	Descripción
AIX	10.1.0.233	Servidor Bases de Datos
Base de Datos	10.1.0.232	Servidor SQL
Base-Psion	10.3.10.205	Equipo de Comunicaciones
Bio-1	10.3.10.22	Equipo Biométrico
Bio-2	10.3.10.24	Equipo Biométrico
Bio-3	10.3.10.25	Equipo Biométrico
Bio-4	10.3.10.26	Equipo Biométrico
Bio-5	10.3.10.27	Equipo Biométrico
Bio-6	10.3.10.28	Equipo Biométrico
Bio-7	10.3.61.44	Equipo Biométrico
Corp-194	200.110.76.194	IP Pública 1
Corp-195	200.110.76.195	IP Pública 2
Corp-196	200.110.76.196	IP Pública 3
Corp-197	200.110.76.197	IP Pública 4
Corp-198	200.110.76.198	IP Pública 5
Corp-199	200.110.76.199	IP Pública 6
Dominio	10.1.0.237	Controlador de Dominio
Dr. Web	10.1.0.245	Dirección Obsoleta
Fiel	10.1.0.250	Servidor de Aplicación
Hand Held	10.1.0.248	Equipo de Comunicaciones
Int-194	10.4.76.194	
Int-195	10.4.76.195	
Int-196	10.4.76.196	

Nombre	IP	Descripción
Int-197	10.4.76.197	
Int-198	10.4.76.198	
Int-199	10.4.76.199	
Jefe-Produccion	10.3.40.34	Jefe de División Producción
Mail Server	10.1.0.229	Servidor de Correos
Operador-1	10.3.20.40	Dirección Obsoleta
Pc Cobra	10.101.0.1	Servidor de Tarja
Portal Empresarial	10.1.0.241	Portal Empresarial
Proclarity	10.1.0.246	Dirección Obsoleta
Red Cae-Capitania	10.102.1.4	Dirección Obsoleta
Redes	10.3.40.37	Administrador de Redes
San Lucas	10.3.10.160	Jefe de División Producción
Seguridades	10.3.40.35	Administrador Bases de Datos
Servidor Biometricos	10.1.0.244	Servidor de Archivos
Servidor Tarja	10.10.10.52	
Symantec-SUS	10.1.0.242	

Tabla 10: Mapeo de Direcciones IP externas a Internas en Equipo Fortigate

Nombre	IP Externa	Interfaz	IP Interna
194	200.110.76.194	Acceso a Internet	10.4.76.194
195	200.110.76.195	Acceso a Internet	10.1.0.229
196	200.110.76.196	Acceso a Internet	10.3.40.37
197	200.110.76.197	Acceso a Internet	10.4.76.197
198	200.110.76.198	Acceso a Internet	10.4.76.198
199	200.110.76.199	Acceso a Internet	10.4.76.199

Tabla 11: Servicios Configurados en Equipo Fortigate

Servicio	Tipo	Puertos	Rangos
echo-replay	icmp		
echo-request	icmp	Tipo 8	
ad-microsoft	tcp		1024-1030, 1024-65535
biometrico	tcp	3001	1024-65535
digitalizacion	tcp	3234	1024-65535
drweb	tcp	2371	1024-65535
informix	tcp	1525	1024-65535
loc-srv	tcp	135	1024-65535
mail	tcp	25	1024-65535
microsoft-ds	tcp	445	1024-65535
netbios-ssn	tcp	139	1024-65535
psion	tcp	16101	1024-65535
remote-desktop	tcp	3389	1024-65535
sql	tcp	1433	1024-65535
kerberos	udp	88	1024-65535
ldap-udp	udp	389	1024-65535
netbios-ns	udp	137	

Tabla 12: Políticas de Acceso Configuradas en Equipo Fortigate

Interfaz Origen	Interfaz Destino	Dirección Origen	Dirección Destino	Puerto
Acceso a Internet	Servidores	Cualquiera	195	mail
Antinarcoticos	Acceso a Internet	Cualquiera	Cualquiera	Cualquiera
Antinarcoticos	Acceso a Internet	Cualquiera	Cualquiera	Cualquiera

Interfaz Origen	Interfaz Destino	Dirección Origen	Dirección Destino	Puerto
Antinarcoticos	Calle H	Cualquiera	Cualquiera	Cualquiera
Antinarcoticos	Cobra	Cualquiera	Cualquiera	Cualquiera
Antinarcoticos	Servidores	Cualquiera	Cualquiera	Cualquiera
Asotarja	Calle H	Tarja	Cualquiera	Cualquiera
Asotarja	Cobra	Servidor Tarja	Pc Cobra	Cualquiera
Calle H	Antinarcoticos	Cualquiera	Cualquiera	Cualquiera
Calle H	Asotarja	Cualquiera	Tarja	Cualquiera
Calle H	Servidores	Cualquiera	Cualquiera	Cualquiera
Cobra	Asotarja	Cualquiera	Cualquiera	Cualquiera
Red de Clientes	Acceso a Internet	Cualquiera	Cualquiera	Cualquiera
Red de Clientes	Asotarja	Cualquiera	Cualquiera	Cualquiera
Red de Clientes	Cobra	Cualquiera	Cualquiera	Cualquiera
Red de Clientes	lan	Cualquiera	Cualquiera	Cualquiera
Red de Clientes	Servidores	Cualquiera	Cualquiera	Cualquiera
Servidores	Acceso a Internet	Cualquiera	Cualquiera	Cualquiera
Servidores	Antinarcoticos	Cualquiera	Cualquiera	Cualquiera
Servidores	Red de Clientes	Cualquiera	Cualquiera	Cualquiera

Tabla 13: Equipos usados para Enlaces hacia Edificios Adjuntos

Enlace	Ubicación	Marca	Modelo	IOS	Fecha IOS	Interfases
Atención al Usuario	Edificio Central	Cisco	805	12.2(8)T5	21/06/2002	1 Ethernet, 1 Serial
Atención al Usuario	Atención al Usuario	Cisco	805	12.2(8)T5	21/06/2002	1 Ethernet, 1 Serial
Operaciones/Inventario	Edificio Central	Cisco	1760	12.2(15)T10	11/12/2003	1 Fast Ethernet, 2 SHDSL
Operaciones/Inventario	Inventario	Cisco	828	12.3(6c)	20/07/2004	1 Ethernet, 1 G.SHDSL
Operaciones/Inventario	Operaciones	Cisco	828	12.3(4)T1	25/11/2003	1 Ethernet, 1 G.SHDSL

Tabla 14: Configuración de las Interfases de los Equipos usados en los Enlaces

Enlace	Ubicación	Interfaz	Dirección	Máscara
Atención al Usuario	Edificio Central	Eth0	10.3.60.6	255.255.255.252
		Serial0	10.3.200.5	255.255.255.252
Atención al Usuario	Atención al Usuario	Eth0	10.6.61.33	255.255.255.224
		Serial0	10.3.200.6	255.255.255.252
Operaciones/Inventario	Edificio Central	FastEth0	10.3.60.10	255.255.255.252
		ATM1/PVC8	10.3.200.9	255.255.255.252
		ATM1/PVC9	10.3.200.13	255.255.255.252
Operaciones/Inventario	Inventario	Eth0	10.3.62.17	255.255.255.240
		ATM1/PVC8	10.3.200.10	255.255.255.252
Operaciones/Inventario	Operaciones	Eth0	10.3.63.33	255.255.255.192
		ATM1/PVC9	10.3.200.14	255.255.255.252

Tabla 15: Configuración DHCP en Equipos

Equipo	Subred	Máscara de Red	Puerta de Enlace	DNS	NBNS
Atención al Usuario	10.3.61.32	255.255.255.224	10.3.61.33	10.1.0.237	10.1.0.237
Inventario	10.3.62.16	255.255.255.240	10.3.62.17	10.1.0.237	10.1.0.237
Operaciones	10.3.63.0	255.255.255.192	10.3.63.33	10.1.0.237	10.1.0.237

Tabla 16: Conmutadores del Centro de Cómputo

Objetivo	Subred	Marca	Modelo	Puertos	Velocidad	Administrable
Usuarios	10.3.10.0	3Com	3C16471	24	100Mbps	No
Usuarios	10.3.10.0	3Com	3C16471	24	100Mbps	No
Sistemas	10.3.20.32	3Com	3C16471	24	100Mbps	No
Presidencia/Ingeniería	10.3.30.32	3Com	3C16471	24	100Mbps	No
Administradores	10.3.40.32	Cnet	CNSH-800	8	100Mbps	No
Servidores	10.1.0.0	Dlink	DES-3226	24	100Mbps	Sí

Configuraciones Implementadas

Tabla 17: Nuevas VLANs

VLAN	Identificador
Red de Administradores	1
Red de Sistemas - Producción	2
Red de Sistemas - Desarrollo	3
Presidencia	4
Departamento Administrativo	5
Recursos Humanos	6
Contabilidad y Facturación	7
Jurídico, Gerencia, Procesos y Servicios Varios	8
Tesorería	9
Adquisiciones	11
Auditoría	12
Atención al Usuario y Servicios Generales	13
Presupuestos	14
Seguridad Industrial	15
Secretaria General y Digitalización	16
Control de Gestión	17
Departamento Técnico	18
Monitoreo	19
Telefonía	21

Tabla 18: Nuevas Subredes

Nombre	Red	Máscara	Máx. # de Equipos
Red de Administradores	172.16.1.0	255.255.255.248	6
Red de Sistemas - Producción	172.16.2.0	255.255.255.240	14
Red de Sistemas - Desarrollo	172.16.3.0	255.255.255.240	14
Presidencia	172.16.4.0	255.255.255.224	30
Departamento Administrativo	172.16.5.0	255.255.255.248	6
Recursos Humanos	172.16.6.0	255.255.255.240	14
Contabilidad y Facturación	172.16.7.0	255.255.255.224	30
Jurídico, Gerencia, Procesos y Servicios Varios	172.16.8.0	255.255.255.224	30
Tesorería	172.16.9.0	255.255.255.248	6
Adquisiciones	172.16.11.0	255.255.255.248	6
Auditoría	172.16.12.0	255.255.255.224	30
Atención al Usuario y Servicios Generales	172.16.13.0	255.255.255.224	30
Presupuestos	172.16.14.0	255.255.255.248	6
Seguridad Industrial	172.16.15.0	255.255.255.240	14

Nombre	Red	Máscara	Máx. # de Equipos
Secretaria General y Digitalización	172.16.16.0	255.255.255.240	14
Control de Gestión	172.16.17.0	255.255.255.224	30
Departamento Técnico	172.16.18.0	255.255.255.192	62
Monitoreo	172.16.19.0	255.255.255.240	14
Telefonía	172.16.21.0	255.255.255.240	14

Tabla 19: Nuevos Servidores DHCP

Nombre	Puerta de Enlace	Márcara de Red	IP Inicio	IP Fin
Red de Administradores	172.16.1.1	255.255.255.248	172.16.1.2	172.16.1.6
Red de Sistemas - Producción	172.16.2.1	255.255.255.240	172.16.2.2	172.16.2.14
Red de Sistemas - Desarrollo	172.16.3.1	255.255.255.240	172.16.3.2	172.16.3.14
Presidencia	172.16.4.1	255.255.255.224	172.16.4.2	172.16.4.30
Departamento Administrativo	172.16.5.1	255.255.255.248	172.16.5.2	172.16.5.6
Recursos Humanos	172.16.6.1	255.255.255.240	172.16.6.2	172.16.6.14
Contabilidad y Facturación	172.16.7.1	255.255.255.224	172.16.7.2	172.16.7.30
Jurídico, Gerencia, Procesos y Servicios Varios	172.16.8.1	255.255.255.224	172.16.8.2	172.16.8.30
Tesorería	172.16.9.1	255.255.255.248	172.16.9.2	172.16.9.6
Adquisiciones	172.16.11.1	255.255.255.248	172.16.11.2	172.16.11.6
Auditoría	172.16.12.1	255.255.255.224	172.16.12.2	172.16.12.30
Atención al Usuario y Servicios Generales	172.16.13.1	255.255.255.224	172.16.13.2	172.16.13.30
Presupuestos	172.16.14.1	255.255.255.248	172.16.14.2	172.16.14.6
Seguridad Industrial	172.16.15.1	255.255.255.240	172.16.15.2	172.16.15.14
Secretaria General y Digitalización	172.16.16.1	255.255.255.240	172.16.16.2	172.16.16.14
Control de Gestión	172.16.17.1	255.255.255.224	172.16.17.2	172.16.17.30
Departamento Técnico	172.16.18.1	255.255.255.192	172.16.18.2	172.16.18.62
Monitoreo	172.16.19.1	255.255.255.240	172.16.19.2	172.16.19.14
Telefonía	172.16.21.1	255.255.255.240	172.16.21.2	172.16.21.14

Tabla 20: Direcciones IP Configuradas en Equipo Fortigate

Nombre	IP	Descripción
EB Biometrico 1	172.16.6.11	Equipo Biométrico
EB Biometrico 2	172.16.6.12	Equipo Biométrico
EB Biometrico 3	172.16.6.13	Equipo Biométrico
EB Biometrico 4	172.16.6.14	Equipo Biométrico
UP DAD Jefe Administrativo	172.16.5.6	Jefe Administrativo
UN US Cevallos Grace	172.16.3.14	Desarrollador
UP US Jefe Producción	172.16.2.13	Jefe de Division
UP US Jefe Producción - Laptop	172.16.2.14	Jefe de Division
OS IP Descargas	172.16.2.12	Operador
SD SAPG05	10.1.0.228	SQL Server
SD SAPG21	10.1.0.226	SQL Server
SP AIX	10.1.0.233	Informix
SP PCHANDHELP	10.1.0.248	Aplicaciones
SP PORTALWAPG	10.1.0.241	Portal Empresarial
SP SAPG03	10.1.0.229	Correo Electrónico
SP SAPG04	10.1.0.191	SQL Server
SP SAPG10	10.1.0.232	SQL Server
SP SAPG13	10.1.0.247	Digitalización
SP SAPGAXIS	10.1.0.194	File Server
SP SAPGBIO	10.1.0.236	Biométricos
SP SAPGDC01	10.1.0.237	Controlador de Dominio
SP SAPGDC02	10.1.0.238	Controlador de Dominio
SP SAPGFIEL	10.1.0.235	Fiel Magister
SP SAPGFS	10.1.0.198	File Server
SP SAPGISA	10.1.0.239	Proxy Server
SP SAPGWS	10.1.0.253	Web Service

Nombre	IP	Descripción
SP SharePoint	10.1.0.234	SharePoint

Tabla 21: Grupos de Direcciones

Grupo	Direcciones
Controladores de Dominio	SP SAPGDC01 SP SAPGDC02
E Biométricos	EB Biometrico 1 EB Biometrico 2 EB Biometrico 3 EB Biometrico 4

Tabla 22: Mapeo de Direcciones IP externas a Internas en Equipo Fortigate

Nombre	IP Externa	Interfaz	IP Interna
Ecuanet 1	157.100.167.6	Acceso a Internet	10.1.0.193
Ecuanet 2	157.100.167.7	Acceso a Internet	10.1.0.229
Ecuanet 3	157.100.167.8	Acceso a Internet	10.1.0.241
Ecuanet 4	157.100.167.9	Acceso a Internet	10.1.0.253

Tabla 23: Servicios Configurados en Equipo Fortigate

Servicio	Tipo	Puertos	Rangos
Global Catalog Server	TCP	3269 3268	
LDAP Server	TCP UDP	389 389	
LDAP SSL	TCP UDP	636 636	
IPsec ISAKMP	UDP	500	
NAT-T	UDP	4500	
RPC	TCP	135	
NTDS	TCP	781	
Netlogon	TCP	782	
NTFRS	TCP	783	
RPC Dinámico	TCP		49152 -49652
Kerberos	TCP UDP	88 88	
NetBIOS Datagram Service	UDP	138	
NetBIOS Name Resolution	UDP	137	
NetBIOS Session Service	TCP	139	
SMB	TCP	445	
DNS	UDP TCP	53 53	
PING	ICMP		
HTTP	TCP	80	
HTTPS	TCP	443	

Servicio	Tipo	Puertos	Rangos
SMTP	TCP	25	
POP3	TCP	110	
LPD	TCP	515	
NTP	UDP	123	
TELNET	TCP	23	
WebProxy	TCP	8080	
Alchemy	TCP	3234	
Informix	TCP	1525	
Biométricos	TCP	3001	
Fiel Magister	TCP	7921	

Tabla 24: Grupos de Servicios

Grupo	Servicios
Navegacion	HTTP HTTPS FTP
Lotus	HTTP POP3 SMTP NetBIOS Session Service SMB
PORTAL	HTTP HTTPS
FileSharing	NetBIOS Session Service SMB HTTP
ActiveDirectory	Global Catalog Server LDAP Server LDAP SSL IPsec ISAKMP NAT-T RPC NTDS Netlogon NTFRS RPC Dinámico Kerberos NTP

Tabla 25: Políticas de Acceso Configuradas en Equipo Fortigate

Red Origen	Red Destino	Dirección Origen	Dirección Destino	Servicio
Departamento Administrativo	Internet	UP DAD Jefe Administrativo	Cualquiera	Cualquiera
Sistemas - Desarrollo	Servidores	Cualquiera	SP SAPGAXIS	FileSharing
Sistemas - Desarrollo	Servidores	Cualquiera	SD SAPG15	SQL
Sistemas - Desarrollo	Servidores	UN US Cevallos Grace	SP SharePoint SP PORTALWAPG	FileSharing
Sistemas - Producción	Internet	UP US Jefe Producción UP US Jefe Producción - Laptop	Cualquiera	Cualquiera
Sistemas - Producción	Internet	OS IP Descargas	Cualquiera	HTTP HTTPS FTP
Secretaria General y Digitalización	Servidores	Cualquiera	SP SAPG13	Alchemy FileSharing
Servidores	Recursos Humanos	SP SAPGBIO	E Biométricos	Biométricos
Administradores Sistemas - Producción Sistemas - Desarrollo	Servidores	Cualquiera	Controladores Dominio	ActiveDirectory DNS FileSharing
Presidencia Departamento Administrativo Recursos Humanos			SP AIX	Informix Telnet
Contabilidad y Facturación			SP SAPG03	Lotus
Jurídico, Gerencia, Procesos y Servicios Varios			SP SAPG10 SD SAPG21	SQL
Tesorería Adquisiciones Auditoría			SP SAPGFS	FileSharing
Atención al Usuario y Servicios Generales Presupuestos			SP SAPGISA	WebProxy
Seguridad Industrial Secretaria General y Digitalización Control de Gestión			SP SharePoint SP PORTALWAPG	HTTP HTTPS
Departamento Técnico Monitoreo Telefonía			SP SAPGFIEL	Fiel Magister FileSharing

Red Origen	Red Destino	Dirección Origen	Dirección Destino	Servicio
Servidores	Administradores Sistemas - Producción Sistemas - Desarrollo Presidencia Departamento Administrativo Recursos Humanos Contabilidad y Facturación Jurídico, Gerencia, Procesos y Servicios Varios Tesorería Adquisiciones Auditoría Atención al Usuario y Servicios Generales Presupuestos Seguridad Industrial Secretaria General y Digitalización Control de Gestión Departamento Técnico Monitoreo Telefonía	SP AIX	Cualquiera	LPD
Administradores	Sistemas - Producción Sistemas - Desarrollo Presidencia Departamento Administrativo Recursos Humanos Contabilidad y Facturación Jurídico, Gerencia, Procesos y Servicios Varios Tesorería Adquisiciones Auditoría Atención al Usuario y Servicios Generales Presupuestos Seguridad Industrial Secretaria General y Digitalización Control de Gestión Departamento Técnico Monitoreo Telefonía Servidores	UP NetAdm	Cualquiera	PING

Tabla 26: Monitoreo de Enlace de Internet

Dirección	Protocolo	Puerto/Tipo	Descripción
www.google.com	TCP	80	Sitio Web de Google
www.cisco.com	TCP	80	Sitio Web de Cisco Systems
199.5.247.1	ICMP	8	Core de Ecuanet/Megadatos

Tabla 27: Servicios Críticos a Monitorear

Equipo	Dirección	Protocolo	Puerto/Tipo	Descripción
APG15	10.1.0.200	TCP	1433	Servidor Tarja
SAPG10	10.1.0.232	TCP	1433	Servidor Monitoreo Naves
SAPG03	10.1.0.229	TCP	25	Servidor de Correo
SAPGDC01	10.1.0.237	TCP	53	Controlador de Dominio
SAPGDC02	10.1.0.238	TCP	53	Controlador de Dominio
SAPGSPPS	10.1.0.234	TCP	80	Sharepoint Portal Server
PORTALWAPG	10.1.0.241	TCP	80	Servidor de Portal Empresarial
SAPGWS	10.1.0.253	TCP	80	Web Service
SAPGESX01	10.1.0.111	ICMP	8	Servidor de Virtualización 1
SAPGESX02	10.1.0.112	ICMP	8	Servidor de Virtualización 2
SAPGESX05	10.1.0.115	ICMP	8	Servidor de Virtualización 5
SAPGAXIS	10.1.0.194	ICMP	8	Servidor de Accesos
SAPGFS	10.1.0.198	ICMP	8	Servidor de Archivos
SAPGEVE	10.1.0.199	ICMP	8	Servidor de Eventos
APG	10.1.0.233	ICMP	8	AIX
SAPGBIO	10.1.0.236	ICMP	8	Administración de Biometricos
SAPGISA	10.1.0.239	ICMP	8	Servidor Proxy
SAPG13	10.1.0.247	ICMP	8	Servidor Alchemy
Biometrico 1	172.16.6.11	ICMP	8	Equipo Biométrico
Biometrico 2	172.16.6.12	ICMP	8	Puerta 1 Entrada
Biometrico 3	172.16.6.13	ICMP	8	Puerta 1 Salida Izquierda
Biometrico 4	172.16.6.14	ICMP	8	Puerta 2 Entrada
Fortigate	172.16.1.1	ICMP	8	Segmentador de Red

BIBLIOGRAFÍA

[1] Cisco Systems Inc., Unified Access Network Design and Considerations, http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/Unified_Access_Book.pdf

[2] International Standards Organization, ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management

[3] Cisco Systems Inc, Virtual LAN, http://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html, fecha de consulta: 4 de Febrero de 2015

[4] Cisco Systems Inc, Inter-Switch Link and IEEE 802.1Q Frame Format, http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html, fecha de consulta: 4 de Febrero de 2015.