CAPÍTULO IV

REDISEÑO DE LA RED IP Y POLÍTICAS DE SEGURIDAD PERIMETRAL DE PETROCOMERCIAL QUITO

4.1- Introducción

El presente capítulo concierne a los pasos sistemáticos tercero y cuarto, señalados en la metodología a la cual corresponde este proyecto. Para este efecto se documentan y analizan propuestas para el rediseño de la red IP. Esto se lo realiza analizando características, ventajas y desventajas de posibles alternativas, para así determinar las mejores opciones y plantear un rediseño adecuado respaldado por la documentación correspondiente.

PETROCOMERCIAL Quito realizó una renovación tecnológica de los equipos de conmutación lo que permitió la remodelación del cableado horizontal de varias áreas de los edificios El Rocio y Ex-Salesiano. Esta renovación tecnológica se aprovecho para proponer el rediseño para la red IP de la empresa. Con este capítulo se plantea asimismo, la optimización de las políticas de seguridad de la organización mediante su equipo de seguridad perimetral Firewall, con el fin de proponer mejores y eficaces propuestas en cuanto a las definiciones de las políticas de seguridad , que permitan alcanzar un alto nivel de protección a nivel perimetral para PETROCOMERCIAL Quito.

4.2- Disposición de Equipos

Los equipos adicionales a los actualmente instalados y que se utilizarán para la realización del rediseño de la red IP se enfocan básicamente en el incremento de switches administrables capa 3 a la red vertical de la empresa. Con el fin de mantener una estandarización de marca, en los equipos de conmutación, la renovación tecnológica de PETROCOMERCIAL Quito consiste en switches marca Cisco.

Los switches que se añadirán para el diseño de la red IP son:

Cuadro 4.1 : Renovación tecnológica de equipos de conmutación de PETROCOMERCIAL Quito.

Cantidad	Switch	Modelo
4	Cisco Catalyst	WS-C3560-48PS
5	Cisco Catalyst	WS-C3560-48PS

Los nuevos equipos adquiridos por PETROCOMERCIAL Quito, son de mejores características y capacidades a los instalados actualmente, sin embargo sus puertos gigabit ethernet son puertos SFP[1](Small Form-Factor Pluggable), por lo que estos equipos requieren de tarjetas diseñadas para dichos puertos. En el cuadro 4.2 se detallan las tarjetas Gigabit Ethernet adquiridas por PETROCOMERCIAL Quito para los switches Cisco 3560:

[1] **SFP Small Form-Factor Pluggable (**pequeños y fácilmente conectables**).-** son puertos gigabit de fibra óptica. El uso de puertos SFP es un beneficio para infraestructuras más pequeñas; los módulos SFP no sólo cuestan mucho menos que los convertidores de interface estándar gigabit, sino que también soportan fibra simple y multimodo.

Cuadro 4.2 : Tarjetas Gigabit Ethernet para switches Cisco 3560

Cantidad	Modelo	Descripción
10	Cisco 30-1301-01 1000 BASE-SX	Tarjeta 850NM 21CRF

La información técnica sobre el equipo Cisco Catalyst 3560 se la puede visualizar en el Anexo C.

Como parte del proceso de renovación tecnológica, se retirarán los equipos de menores capacidades, estos recibirán su adecuado mantenimiento para poder ser utilizados en otras sucursales o terminales de PETROCOMERCIAL, donde la empresa lo crea conveniente.

Los equipos administrables retirados son los siguientes:

Cuadro 4.3 : Switches Cisco retirados de PETROCOMERCIAL Quito.

Nombre	Dirección IP	Etiqueta	Switch	Modelo
PCO_101	X.Y.64.101	SW101C	Cisco Catalyst	WS-C3550-PWR-XL-EN
PCO_121	X.Y.64.121	SW121C	Cisco Catalyst	WS-C3524-PWR-XL-EN
PCO_122	X.Y.64.122	SW122C	Cisco Catalyst	WS-C3524-PWR-XL-EN
PCO_201	X.Y.64.201	SW201C	Cisco Catalyst	WS-C3524-PWR-XL-EN
PCO_171	X.Y.64.171	SW171C	Cisco Catalyst	WS-C3524-PWR-XL-EN
PCO_181	X.Y.64.181	SW181C	Cisco Catalyst	WS-C3524-PWR-XL-EN
PCO_189	X.Y.64.189	SW189C	Cisco Catalyst	WS-C2924-PWR-XL-EN
PCO_191	X.Y.64.191	SW199C	Cisco Catalyst	WS-C2912-PWR-XL-EN

Asimismo todos los equipos de conmutación no administrables serán retirados de producción. Estos son:

Cuadro 4.4 : Switches no administrables retirados de PETROCOMERCIAL Quito.

Nombre	SWITCH	Modelo
SW102I	IBM	8271-E24
SW111I	IBM	8271-E24
SW182I	IBM	8271-E24
SW112T	3COM	3C16791
SW131T	3COM	3C16791
SW191T	3COM	3C16791
SW201T	3COM	3C16791
SW202T	3COM	3C16791
SW231T	3COM	3C16791

En resumen el rediseño de la red IP contará con los siguientes switches:

Cuadro 4.5 : Lista de switches para el rediseño de la red IP de PETROCOMERCIAL Quito.

Cantidad	Switch	Modelo
4	Cisco Catalyst	WS-C3560-48PS
5	Cisco Catalyst	WS-C3560-24PS
3	Cisco Catalyst	WS-C3550-PWR-XL-EN
2	Cisco Catalyst	WS-C2924-PWR-XL-EN
1	Cisco Catalyst	WS-C4507R

En cuanto a la central telefónica IP se modificará exclusivamente su direccionamiento IP, mientras que los teléfonos IP se mantendrán bajo su misma configuración actual. De igual manera, en los computadores personales únicamente cambiará su direccionamiento IP, el cual dependerá de la VLAN a la que pertenezca el equipo.

En cuanto a los equipos necesarios para la red vertical de fibra óptica, no se necesitarán dispositivos extras, puesto que únicamente se procederá a reconectorizar los patch panel de fibra óptica ya instalados en ambos edificios de PETROCOMERCIAL Quito.

4.2.1- Nueva nomenclatura de switches

La nomenclatura que se detalla a continuación fue determinada por recomendaciones del personal de la empresa de modo que permita facilitar y agilitar la identificación de los equipos de conmutación.

La nomenclatura de los switches será redefinida de la siguiente manera:

Los switches manejarán el formato **PCO_EDIFICIO_PAB** donde: PCO es constante, 'EDIFICIO' indica el edificio puede ser el El Rocio **ROC** o Ex-Salesiano **SAL**, 'P' es constante, 'A' indica el número de piso dentro del correspondiente edificio y 'B el número de orden del switch ese el piso.

Las direcciones IP que se designarán a los equipos están consideradas desde la dirección X.Y.64.130 a la dirección X.Y.64.179. Se reservaran grupos de cinco direcciones IP para cada piso del edificio El Rocio a partir de la dirección de inicio para un posible crecimiento en la red. Así los switches de planta baja irán desde X.Y.64.130 a X.Y.64.134, los switches del primer piso desde X.Y.64.135 a X.Y.64.139, y así sucesivamente. En el caso de los switches del edificio Ex-Salesiano el direccionamiento se lo hará solo a partir de la dirección X.Y.64.170 iniciando desde la planta baja, se designarán grupos de 3 direcciones por piso. El rango de direcciones IP para este segundo edificio se lo considera de un rango mucho menor puesto que el número de puntos de red necesarios para esa área

es relativamente bajo. Este direccionamiento de switches esta predispuesto a cambios debido al direccionamiento de las vlans que se hará posteriormente.

Sin embargo la dirección X.Y.160 se encuentra ocupada para el equipo de monitoreo de la red WAN, Packeteer[1], este equipo debe conservarse con su actual direccionamiento IP por fines de monitoreo, por lo que se mantendrá dentro del rango destinado para los switches.

De acuerdo a lo planteado, los switches de PETROCOMERCIAL Quito tendrán designados la nomenclatura y direccionamiento IP que se muestra en el cuadro 4.6, tomando en cuenta que las direcciones se detallarán únicamente de manera general para que posteriormente sean ubicadas en la VLAN donde se designe a los equipos de administración, lo que se proyecta es plantear la distribución y separación en cuanto al direccionamiento de los equipos.

Cuadro 4.6 : Nomenclatura y direccionamiento de switches para el rediseño de la Red IP de PETROCOMERCIAL Quito.

Dirección IP		Nomenclatura	Modelo	No. Serie
VLAN de Administración	**.X0**[2]	**Pco_Roc_P01**	WS-C3560-48PS-S	CAT1046ZJDE
	.X1	**Pco_Roc_P02**	WS-C3560-24PS-S	CAT1027RHC7
	.X2	Libre		
	.X3	Libre		
	.X4	Libre		
	.X5	Libre		
	.X6	Libre		
	.X7	Libre		
	.X8	Libre		
	.X9	Libre		
	.X10	**Pco_Roc_P20**	WS-C3560-48PS-S	CAT1046ZJBR

[1] **Packeteer**.- es un equipo Hardware con su respectivo Software asociado, fabricado por Packeteer Inc., y cuya función es la de administrador de ancho de banda.

[2] Por motivos de generalización se representaran los primeros dígitos de la dirección IP con las letras “X” , “Y” y “Z”

VLAN de Administración	**.X11**	**Pco_Roc_P21**	WS-C3560-24PS-S	CAT1021N369
	.X12	**Pco_Roc_P22**	WS-C3560-24PS-S	CAT1027RH81
	.X13	Libre		
	.X14	Libre		
	.X15	Libre		
	.X16	Libre		
	.X17	Libre		
	.X18	Libre		
	.X19	Libre		
	.Y10	**Pco_Roc_P50**	WS-C4507R	varias series
	.Y11	**Pco_Roc_P51**	WS-C3524-PWR-XL-EN	CHK0630W0WN
	.Y12	Libre		
	.Y13	Libre		
	.Y14 - .Y19	Libre		
	.Y10	Equipo de Monitoreo de WAN (Packeteer)		
	.Y11	**Pco_Roc_P80**	WS-C3560-48PS-S	CAT1046ZJD7
	.Y12	**Pco_Roc_P81**	WS-C3560-48PS-S	CAT1046ZJCC
	.Y13	**Pco_Roc_P82**	WS-C2924-XL-EN	FAB0502V3P7
	.Y14	Libre		
	.Y15	Libre		
	.Y16	Libre		
	.Y17	Libre		
	.Y18	Libre		
	.Y19	Libre		
	.Z10	**Pco_Sal_P10**	WS-C3560-24PS-S	CAT1021N49Z
	.Z11	**Pco_Sal_P11**	WS-C3560-24PS-S	CAT1024Z3SK
	.Z12	Libre		
	.Z13	**Pco_Sal_P20**	WS-C2924-XL-EN	FAB0502V3QK
	.Z14	Libre		
	.Z15	Libre		
	.Z16	**Pco_Sal_P30**	WS-C3524-PWR-XL-EN	CHK0644W03A
	.Z17	**Pco_Sal_P31**	WS-C3524-PWR-XL-EN	CHK0630W0N1
	.Z18	Libre		
	.Z19	Libre		

Este esquema de nomenclatura y direccionamiento IP para switches presenta las siguientes ventajas:

- ✓ La nomenclatura asignada es breve y concisa, permitiendo identificar fácilmente la ubicación del equipo mediante la misma.
- ✓ El direccionamiento brinda disponibilidad exacta para los equipos, es decir toma en consideración el crecimiento anual de la red sin embargo no provoca el desperdicio de direcciones IP.
- ✓ El direccionamiento no tiene relación con la nomenclatura de los equipos, lo cual favorece a los administradores pues solo ellos deben manejar ese tipo de información.

4.3- Cableado y distribución de MDF[1] e IDFs[2]

Mediante la readecuación de algunos de las áreas físicas de los Edificios El Rocio y Ex-Salesiano, y con el fin de alcanzar un diseño óptimo para el cableado vertical y horizontal de PETROCOMERCIAL Quito, se establece la distribución de los armarios de distribución intermedia y de distribución principal de la siguiente manera, como se muestra en la figura 4.1:

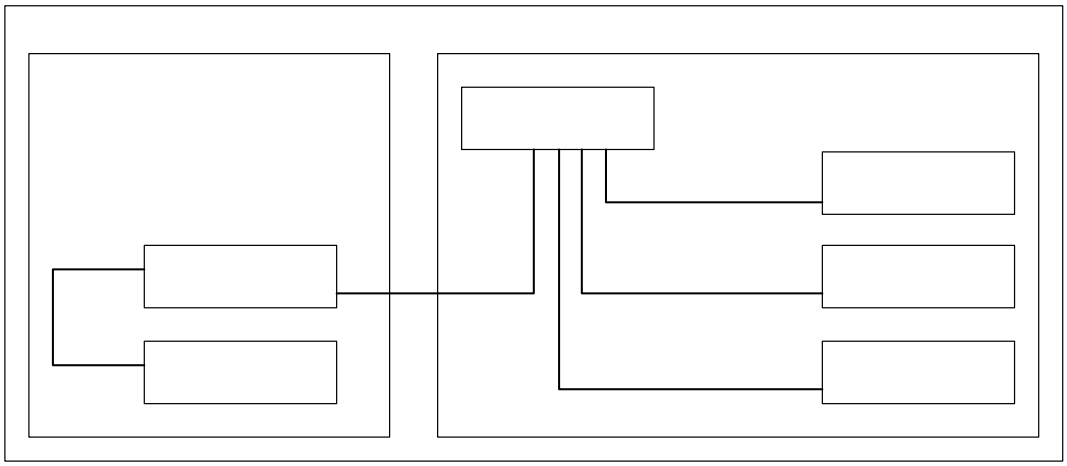

Figura 4.1: Distribución de MDF e IDFs en PETROCOMERCIAL Quito

[1] **MDF(Main Distribution Frame):** Instalación principal de distribución. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión.

[2] **IDF(Intermedia Distribution Frame):** Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

4.3.1- Cableado Vertical

Para el cableado desde cada uno de los IDF hacia el MDF se empleará la fibra óptica multimodo de seis hilos existente en la empresa, la cual se encuentra tendida en ambos edificios, sin embargo no todos los hilos de las fibras instaladas se encuentran activos, debido que al ser tendida la fibra óptica se conectorizó exclusivamente un par de hilos dado que se requería únicamente de un enlace, y no se determinó la necesidad de activar el resto de hilos.

A lo largo del rediseño de la red se reactivarán los hilos de la fibra óptica que sean necesarios, como se expondrá en el rediseño de la topología de la red. Es importante mencionar que los IDF ya designados dan solución al problema de cableado vertical existente, puesto que se establece como IDF solamente a los armarios de cableado que cuentan con la infraestructura física adecuada para la distribución de equipos y cableado.

4.3.2- Cableado Horizontal

En cuanto al cableado horizontal que tiene PETROCOMERCIAL Quito, no se realizaron cambios relevantes, puesto que algunas de las áreas físicas de los edificios están en proceso de readecuación de su cableado horizontal y por lo tanto se encuentra en buenas condiciones, sin embargo en otras áreas a pesar de ser necesaria la reinstalación de cableado horizontal no se lo ha realizado por cuestiones administrativas de la empresa.

En cuanto a la capacidad de puertos disponibles en los switches para el acceso a la red por parte de los usuarios de los edificios El Rocio y Ex-Salesiano, el incremento se lo ha realizado tomando en cuenta las proyecciones de crecimiento de la empresa así como el límite de puntos de red por área, es así

que la siguiente tabla muestra la propuesta de redistribución de puertos disponibles en referencia a la distribución actual.

Tabla 4.1: Propuesta y porcentaje de crecimiento para el cableado vertical de PETROCOMERCIAL Quito.

Situación Actual		Rediseño		No.puntos de red/rack	% Crecimiento
Ubicación de los Switches	No.Puertos Disponibles	Rack	No. Nuevos Puertos Disponibles		
El Rocio		**El Rocio**			
Planta Baja	48	Planta Baja	72	72	
1er Piso	32	-	-	-	
2do Piso	72	2do Piso	96	106	
3er Piso	8	-	-	-	
4to-5to-6toPiso	96	5toPiso(MDF)	96	104	
7mo Piso	24	-	-	-	
8vo Piso	36	8vo Piso	108	107	
9no Piso	20	-	-	-	
Total El Rocio	**336**	**Total El Rocio**	**372**	389	
ExSalesiano		**ExSalesiano**			
Planta Baja	40	Planta Baja	48	60	
1er Piso	24	1er Piso	24	-	
2do Piso	56	2do Piso	48	60	
Total Ex Salesiano	**120**	**Total ExSalesiano**	**120**	120	
Total Puertos Actuales	**456**	**Total Puertos Rediseño**	**492**	509	**7,895**

Como se muestra en la tabla anterior, en el edificio ExSalesiano no existe un incremento de puertos disponibles puesto que para el rediseño se ha tomado en cuenta que en este edificio el número de puertos es ya superior al necesario, sin embargo existen en su mayoria switches no administrables 3Com de ocho puertos, los cuales al ser reemplazados por switches Cisco y reubicados, indudablemente mejorarán la productividad de la red, sin provocar el desperdicio de equipos.

4.4- Rediseño de la Topología de la Red IP

De acuerdo a la metodología utilizada para este proyecto, el proceso de rediseño de la topología de la Red IP se fundamenta en determinar un diseño LAN para PETROCOMERCIAL Quito que satisfaga los requisitos del usuario. Por lo tanto el rediseño de la topología de la red IP busca dar solución a los inconvenientes de la topología actual basándose para esto en la sustitución de equipos de bajo rendimiento, el uso eficiente de la infraestructura física existente de acuerdo a sus condiciones, la reconfiguración de los equipos de conmutación y el planteo de un diseño eficiente de la red vertical que permita alcanzar excelentes tiempos de respuesta en las transmisiones de voz y datos a nivel local.

La topología física (en referencia a la capa física del modelo OSI) diseñada para PETROCOMERCIAL Quito es la siguiente:

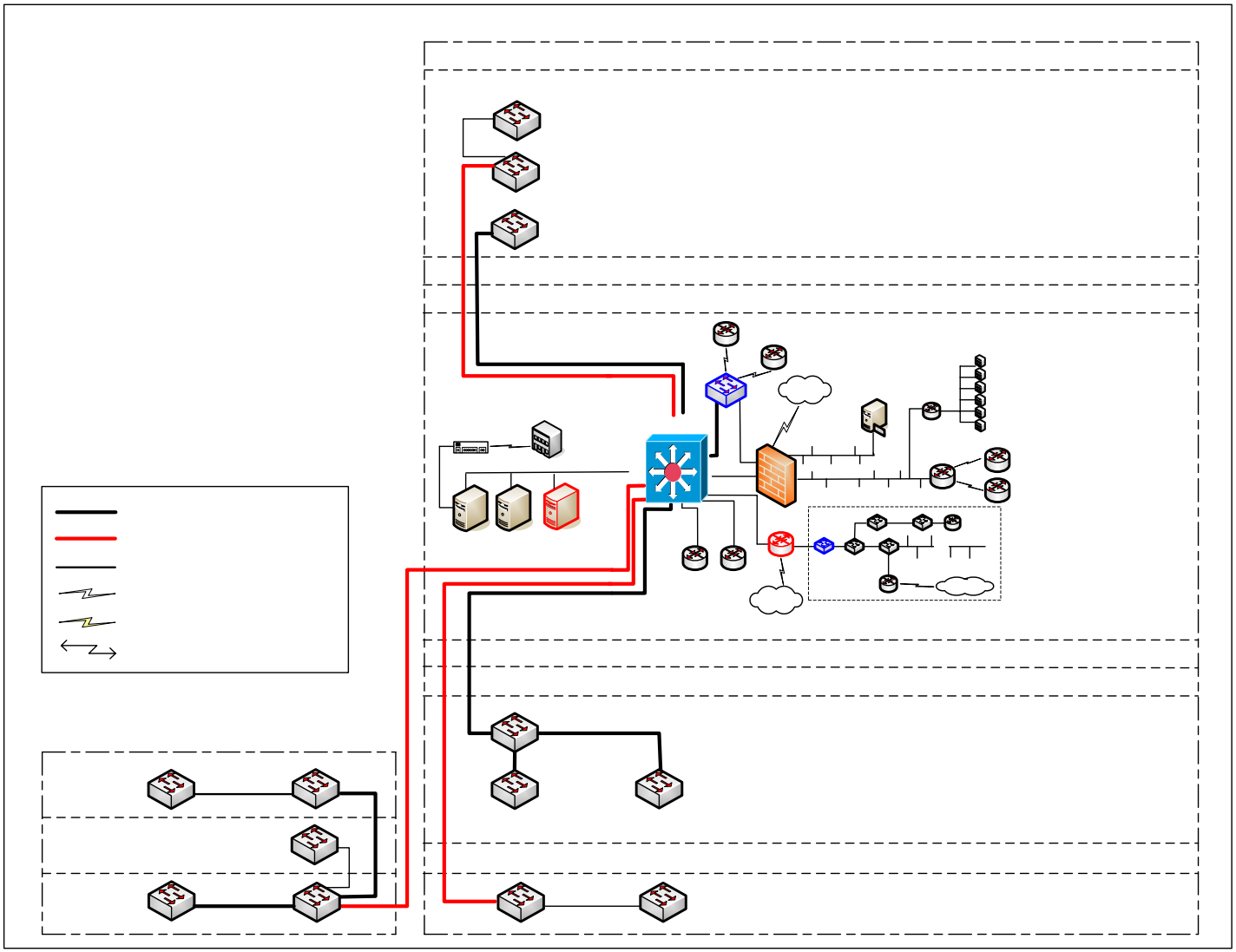

Figura 4.2: Rediseño de la Topología de la red IP de PETROCOMERCIAL Quito

La topología propuesta en la figura 4.2 presentará las siguientes ventajas:

- ✓ Existe concentración directa de todo el tráfico de voz y datos al switch de core de la empresa (Cisco Catalyst 4500).
- ✓ Se hace uso útil del backbone físico de fibra óptica que ya se encuentra tendido.
- ✓ Transmisión a 1000Mbps al 80 por ciento de la red vertical, permitiendo una transmisión efectiva entre los equipos de conmutación lo que permitiría incrementar la velocidad de transferencia de voz y datos a los usuarios.
- ✓ Existe redundancia en el backbone de la red, puesto que quedan todavía hilos de fibra óptica multimodo ya tendidos pero sin conectorizar.
- ✓ El switch Cisco Catalyst 4500, trabajará en la capa de core, distribución y de acceso de la red ; por su alta capacidad de procesamiento y su disponibilidad de módulos.
- ✓ Evita cuellos de botella de tráfico para acceder hacia los Servidores e i-series desde cualquier lugar dentro de la red local, pues tanto estos equipos como los switches están conectándolos directamente al core de la red local IP con Gigabit Ethernet, proveendo un rápido manejo del tráfico IP.
- ✓ Al concentrar el tráfico en el switch de core (Cisco 4500) por ser el equipo de conmutación de mejores características y rendimiento, se facilita y centraliza la administración de la red.

4.5- Diseño de VLANs para PETROCOMERCIAL Quito

Luego de analizar el comportamiento de la red IP de PETROCOMERCIAL Quito, características y necesidades, este proyecto propone un esquema práctico para la creación de VLANs con el fin de hacer uso efectivo de los beneficios que brindan este tipo de redes virtuales para beneficio de la organización. Para esto es necesario seleccionar a los grupos de usuarios o equipos a partir de los cuales se realizará la asignación para las VLANs.

4.5.1- Grupos de usuarios y equipos

Los grupos más importantes son:

4.5.1.1- Servidores

PETROCOMERCIAL Quito posee clasificado a los servidores en tres diferentes tipos:

- ✓ i-Series[1]
- ✓ Servidores Blade [2]
- ✓ Servidores de aplicaciones

Esta clasificación es importante puesto que el tipo de servicios que brindan cada uno de los grupos de equipos mencionados es diferente, siendo estos accesados para diversos tipos de necesidades y por usuarios de distintos departamentos a nivel local y/o nacional, es así que los equipos deben asociarse por aplicaciones.

El tamaño estimado tomando en cuenta el crecimiento de la empresa para los servidores dependerá de cada uno de los grupos.

[1] i-series: Es un ordenador empresarial, servidor eServer de IBM. Es un servidor *midrange*.
[2] Servidor blade**:** Es un tipo de servidor para los centros de proceso de datos específicamente diseñada para aprovechar el espacio, reducir el consumo y simplificar su explotación.

4.5.1.2- Telefonía IP

Este grupo incluiría:

- ✓ Central Telefónica IP
- ✓ Teléfonos IP

A pesar de que el tamaño proyectado para la telefonía IP es de 256 direcciones IP, a este grupo se le asignará 512, puesto que la empresa ha iniciado ya las gestiones respectivas para la creación de un proyecto de implementación de videoconferencia sobre IP.

4.5.1.3- Administración

Este grupo comprende:

- ✓ Equipos de telecomunicaciones
- ✓ Switches
- ✓ Controladores S.A.N.[1]

Posteriormente este grupo podría ser subdivido puesto que el cambio de direccionamiento IP en cuanto a los equipos de telecomunicaciones sería un cambio crítico que provocaría profundos inconvenientes en el acceso a los sistemas de PETROCOMERCIAL Quito a nivel nacional, es por ello que una subclasificación permitirá al grupo de telecomunicaciones manejar un mismo direccionamiento IP que el actual, sin embargo eso se analizará en cada una de las propuestas del direccionamiento para VLANs. El tamaño para el direccionamiento de telecomunicaciones se estima en 16 direcciones IP mientras el resto de equipos de administración se considerará en 128 direcciones IP.

[1] **S.A.N. (Storage Area Network**) Red de área de almacenamiento, aplica un modelo de red a los ambientes de almacenamiento en los centros de datos. Los SANs operan detrás de los servidores para proveer una ruta común entre los servidores y los dispositivos de almacenamiento.

4.5.1.4- Industrial

Esto grupo no tiene ningún equipo asignado por el momento pues se trata de un proyecto para realizar el monitoreo de la producción de combustible en las terminales de PETROCOMERCIAL sobre todo en la Terminal El Beaterio, este proyecto permitiría controlar y monitorear los movimientos industriales diarios.

El tamaño estimado de este grupo es de 128 direcciones IP.

4.5.1.5- Usuarios de Servicios Especiales

Esta clasificación se refiere a un grupo de usuarios de distintos departamentos de PETROCOMERCIAL Quito, que actualmente manejan direcciones estáticas para poder acceder y ser accedidas hacia y desde PETROECUADOR respectivamente, esto por la necesidad de acceder a las aplicaciones desarrolladas en Petroecuador como son:

- ✓ Sistema de Oferentes
- ✓ Sistema de Auditoria
- ✓ Sistema de Seguros y
- ✓ Conexión al Banco Central del Ecuador

En la actualidad existen 25 computadores personales que pertenecen a este grupo. Es necesario considerar un crecimiento adecuado para direccionamiento IP.

4.5.1.6- Usuarios de Sistemas y Telecomunicaciones

Este grupo comprende a los usuarios de la Unidad de Sistemas y Telecomunicaciones de PETROCOMERCIAL Quito y a los servidores empresariales cuyas aplicaciones son únicamente accedidas por los usuarios

de esta unidad. El tamaño considerado para estos usuarios es de 128 direcciones IP a pesar de el número de usuarios no es mayor a 50, sin embargo se debe tomar en cuenta un rango de direccionamiento extra necesario para realizar pruebas relacionadas las áreas de sistemas y telecomunicaciones.

4.5.1.7- Usuarios Finales

Para el caso particular de PETROCOMERCIAL, de existir una subdivisión de grupos de usuarios de acuerdo a los departamentos a los que pertenecen, no sería conveniente pues no existen servidores con aplicaciones específicas dedicadas a un solo grupo de usuarios. Los equipos i-series de la empresa brindan servicios a nivel local y nacional, estos soportan varias aplicaciones y son dedicados para varios grupos de usuarios en la empresa. Es por ello que la única clasificación conveniente para dividir a los usuarios existiría de acuerdo a las aplicaciones que utilizan. Para esto se ha realizado un análisis del uso de los i-Series de acuerdo a los departamentos existentes en PETROCOMERCIAL Quito, el cual se muestra a continuación:

Cuadro 4.7 : Uso de i-Series por departamento en PETROCOMERCIAL Quito

Departamento	PCO1	PCO2	PCO8	PCO9
Cuentas por pagar	X	X		
Administración Financiera	X	X		
Secretaria General				
Activos	X	X		
Materiales	X	X		
Seguros	X	X		
Crédito y Cobranzas			X	
Negocios propios			X	

Abastecedora			X	
Finanzas	X	X		
Presupuesto	X	X		
Gerencia				
Subgerencia Comercia.			X	
Comercializadora			X	
Programación			X	
Sistemas	X	X	X	X
Planificación Financiera	X	X		
Vicepresidencia				
Subgerencia de Transporte			X	
Contabilidad	X	X		
Subgerencia Administrativa	X	X		
Recursos Humanos	X	X		
Unidad Administrativa	X	X		
Servicios Administrativos	X	X		
Legal				
Seguridad Física				
Mantenimiento Eléctrico				
Bodega-Materiales	X	X		
Proyectos	X	X		
Contratos	X	X		
Bienestar Laboral	X	X		
Relaciones Públicas				
Control de Gestión	X	X		
Recepción				

Nota: Únicamente los equipos de las secretarías de todos los departamentos ingresan al sistema de viáticos de la empresa, el mismo que se conecta a los i-series PCO1 y PCO2, por lo que las secretarias formarán parte del grupo “Administrativo”.

La tabla muestra departamentos que no constan en ningún i-Series, sin embargo hacen uso de las aplicaciones de algunos de los equipos ocasionalmente. En cuanto al resto de usuarios se pudo analizar la existencia

de cuatro tipos de usuarios de acuerdo al uso de las aplicaciones en los servidores empresariales y equipos i-Series, estos son:

1. **Grupo "General"**

Este grupo hace uso no frecuente de las aplicaciones en los equipos i-Series, y consta de los siguientes departamentos:

Cuadro 4.8 : Cuadro 4.8: Departamentos del Grupo General de usuarios

Departamento	No. PC's
Secretaria General	8
Vicepresidencia	15
Legal	17
Seguridad Física	4
Mantenimiento Eléctrico	1
Relaciones Públicas	5
Recepción	1
TOTAL	**51**

2. **Grupo "Administrativo"**

Este grupo, denominado administrativo por las funciones de los departamentos con los que cuenta, acceden principalmente a los equipos PCO1 y PCO2. En este grupo se incluye a los equipos de las secretarías de todos los departamentos. Este grupo posee los siguientes grupos

Cuadro 4.9 : Departamentos del Grupo Administrativo de usuarios

Departamento	No. PC's
Cuentas por pagar	4
Administración Financiera	10
Activos	7
Materiales	16
Seguros	5
Finanzas	5
Presupuesto	4

Planificación Financiera	8
Contabilidad	13
Subgerencia Administrativa	3
Recursos Humanos	9
Unidad Administrativa	2
Servicios Administrativos	11
Bodega-Materiales	2
Proyectos	11
Contratos	10
Bienestar Laboral	5
Control de Gestión	15
Secretarias del resto de departamentos	14
TOTAL	**154**

3. Grupo “Comercialización”

Los departamentos pertenecientes a este grupo acceden al i-Series PCO8 y estos son:

Cuadro 4.10 : Departamentos del Grupo Comercialización de usuarios

Departamento	No. PC’s
Gerencia	9
Crédito y Cobranzas	8
Negocios propios	4
Abastecedora	20
Subgerencia Comercia.	4
Comercializadora	14
Programación	6
Subgerencia de Transporte	12
TOTAL	**77**

4. Grupo “Sistemas”

Este grupo por su función en la empresa accede hacia todos los equipos empresariales y como se determinó anteriormente se lo considerará como un grupo especial de usuarios.

4.5.2- Propuestas para el diseño de VLANs en PETROCOMERCIAL Quito

Tomando en consideración la información analizada en cuanto a los grupos de usuarios y equipos existentes en la empresa, se plantearán tres propuestas factibles para el diseño e implementación de VLANs para PETROCOMERCIAL Quito, analizando sus características, ventajas y desventajas para posteriormente optar por la mejor alternativa y desarrollarla.

4.5.2.1- Primera Propuesta

La primera propuesta plantea el siguiente diseño de VLANs:

Cuadro 4.11 : Primera propuesta de diseño de VLANs

No.	Nombre	ID	Dirección IP	Máscara	Rango	Tamaño
1	Comunicaciones	VLAN 10	X.Y.64.0	/28	64.1 - 64.15	16
2	i-Series	VLAN 20	X.Y.64.16	/28	64.17- 64.31	16
3	Servidores Blade	VLAN 30	X.Y.64.32	/27	64.33 - 64.63	32
4	Servidores	VLAN 40	X.Y.64.64	/27	64.65 - 64.95	32
5	Pruebas	VLAN 50	X.Y.64.96	/27	64.97 - 64.127	32
6	Administración de Equipos	VLAN 60	X.Y.64.128	/26	64.129 - 64.191	64
7	Usuarios Especiales	VLAN 70	X.Y.64.192	/26	64.193 - 64.255	64
8	Usuarios Sistemas	VLAN 80	X.Y.65.0	/25	65.1 - 65.127	128
9	Industrial	VLAN 90	X.Y.65.128	/25	65.129 - 65.255	128
10	General	VLAN 1	X.Y.66.0	/24	66.1 - 66.255	256
11	Comercialización	VLAN 110	X.Y.67.0	/24	67.0 - 67.255	256
12	Administrativa	VLAN 120	X.Y.68.0	/23	68.0 - 69.255	512
13	VOIP	VLAN 1001	X.Y.70.0	/23	70.1 - 71.255	512

Características:

- ✓ Designa una VLAN a cada uno de los grupos de servidores e i-Series, es decir de acuerdo a sus aplicaciones, tal como se explico anteriormente en el grupo “Servidores”.
- ✓ Asigna rangos limitados de 16 y 32 direcciones IP a las VLANs de servidores con el fin de mantener el direccionamiento IP actual de los equipos.

- ✓ Asigna una VLAN libre, denominada de pruebas, de 32 direcciones IP con el fin de utilizarla para pruebas o para futuras aplicaciones que se implanten en la empresa.
- ✓ Sobrevalora el tamaño para las VLANs designadas a la administración de equipos y a los usuarios especiales con 128 direcciones IP cada una.
- ✓ Asigna 1024 direcciones IP en total para los usuarios, divididos en los grupos: General, Administrativa y Comercialización.
- ✓ Asigna 512 direcciones IP a la VLAN de telefonía IP.

La siguiente figura muestra la propuesta analizada:

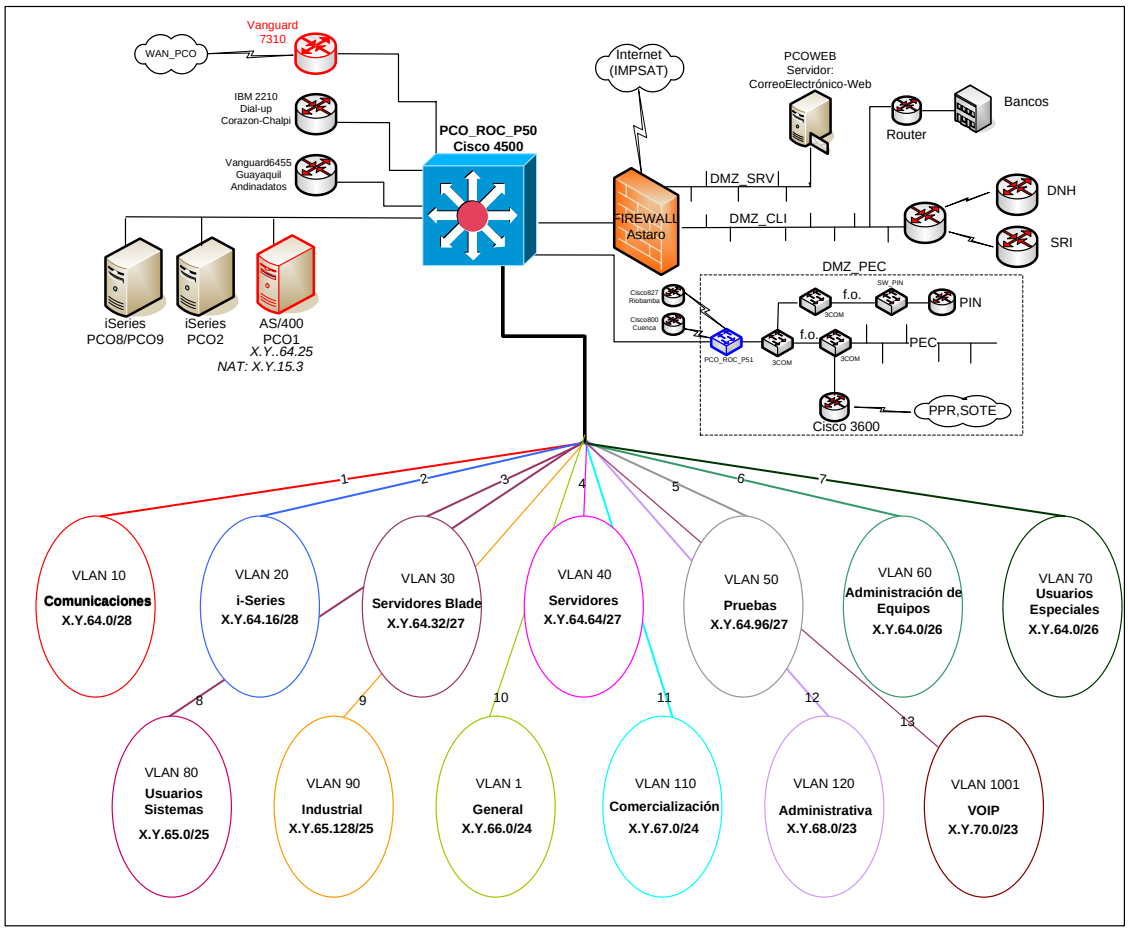

Figura 4.3: Primera propuesta para el Diseño de VLANs de PETROCOMERCIAL Quito

Ventajas:

- ✓ La implementación de esta propuesta no implicaría cambios críticos a nivel nacional en cuanto al direccionamiento IP de los principales servidores de la empresa.
- ✓ El direccionamiento IP propuesto permitiría que más del 50% de los equipos se mantengan con su dirección IP actual.
- ✓ Se crean todos los grupos de equipos y usuarios necesarios, asociados de acuerdo a sus aplicaciones, e inclusive se crea una VLAN libre.
- ✓ Las VLANs establecidas a excepción de las VLANs de servidores brindan considerables rangos de direccionamiento IP respecto a su tamaño actual concediendo escalabilidad al diseño de VLANs.
- ✓ La nomenclatura de las VLANs permite de igual manera escalabilidad a las VLANs, utilizando multiplos de 10 para identificación.

Desventajas:

- ✓ Los rangos de direccionamiento IP para las VLANs de servidores y la VLAN de comunicaciones son muy limitados, no existen suficientes direcciones IP disponibles.
- ✓ En relación a la organización se separa a los equipos de comunicación con los de administración por conveniencia del uso del direccionamiento IP actual.

Nota: El identificador de la **VLAN de Voz** se determinó como **1001** debido a que esta es la identificación que PETROCOMERCIAL Quito mantenía configurada manualmente en los teléfonos IP, razón por la cual este valor no se modificará por sugerencia del personal de la empresa.

4.5.2.2- Segunda Propuesta

La segunda propuesta dispone a las VLANs de la siguiente manera:

Cuadro 4.12 : Segunda propuesta de diseño de VLANs

No	ID	Nombre	Dirección IP	Máscara	Rango	Tamaño
1	Equipos Empresariales	VLAN 10	X.Y.64.0	/27	64.1 - 64.31	32
2	Servidores Blade	VLAN 20	X.Y.64.32	/27	64.32 - 64.63	32
3	Servidores	VLAN 30	X.Y.64.64	/26	64.65 - 64.127	64
4	Administración de Equipos	VLAN 40	X.Y.64.128	/25	64.129 - 64.255	128
5	Usuarios Especiales	VLAN 50	X.Y.65.0	/25	65.1 - 65.127	128
6	Pruebas	VLAN 60	X.Y.65.128	/25	65.129 - 65.255	128
7	Industrial	VLAN 70	X.Y.66.0	/24	66.1 - 66.255	256
8	Usuarios Sistemas	VLAN 80	X.Y.67.0	/24	67.1 - 67.255	256
9	General	VLAN 1	X.Y.68.0	/25	68.1 - 68.255	128
10	Comercialización	VLAN 90	X.Y.68.128	/25	68.129 - 68.255	128
11	Administrativa	VLAN 100	X.Y.69.0	/24	69.1 - 69.255	256
12	VOIP	VLAN 1001	X.Y.70.0	/23	70.1 - 71.255	512

Características:

- ✓ Crea una VLAN con equipos de comunicación y servidores empresariales que brindan servicios a nivel nacional, denominada “Equipos Empresariales”, con el fin de manipular un grupo cuyo direccionamiento IP se mantenga igual al actual evitando cambios críticos en la red nacional y local. Existiría un rango de 32 direcciones IP.
- ✓ Se designan dos VLANs mas para servidores, distribuidos de acuerdo a sus aplicaciones, de 32 y 64 direcciones IP respectivamente.
- ✓ Se crea una VLAN libre de 128 direcciones IP, con el objetivo de efectuar pruebas o para utilizar este rango para aplicaciones que se presenten en el futuro.
- ✓ Se sobrevaloran las VLAN para usuarios de sistemas y la VLAN industrial, determinando 256 direcciones IP cada una.

- ✓ Se establecen 512 direcciones IP en total para usuarios, divididos en los grupos: General, Administrativa y Comercialización.
- ✓ Sobrevalora el tamaño para las VLANs designadas a la administración de equipos y a los usuarios especiales con 128 direcciones IP cada una.
- ✓ Se asigna 512 direcciones IP a la VLAN de telefonía IP.

La figura a continuación modela la segunda propuesta:

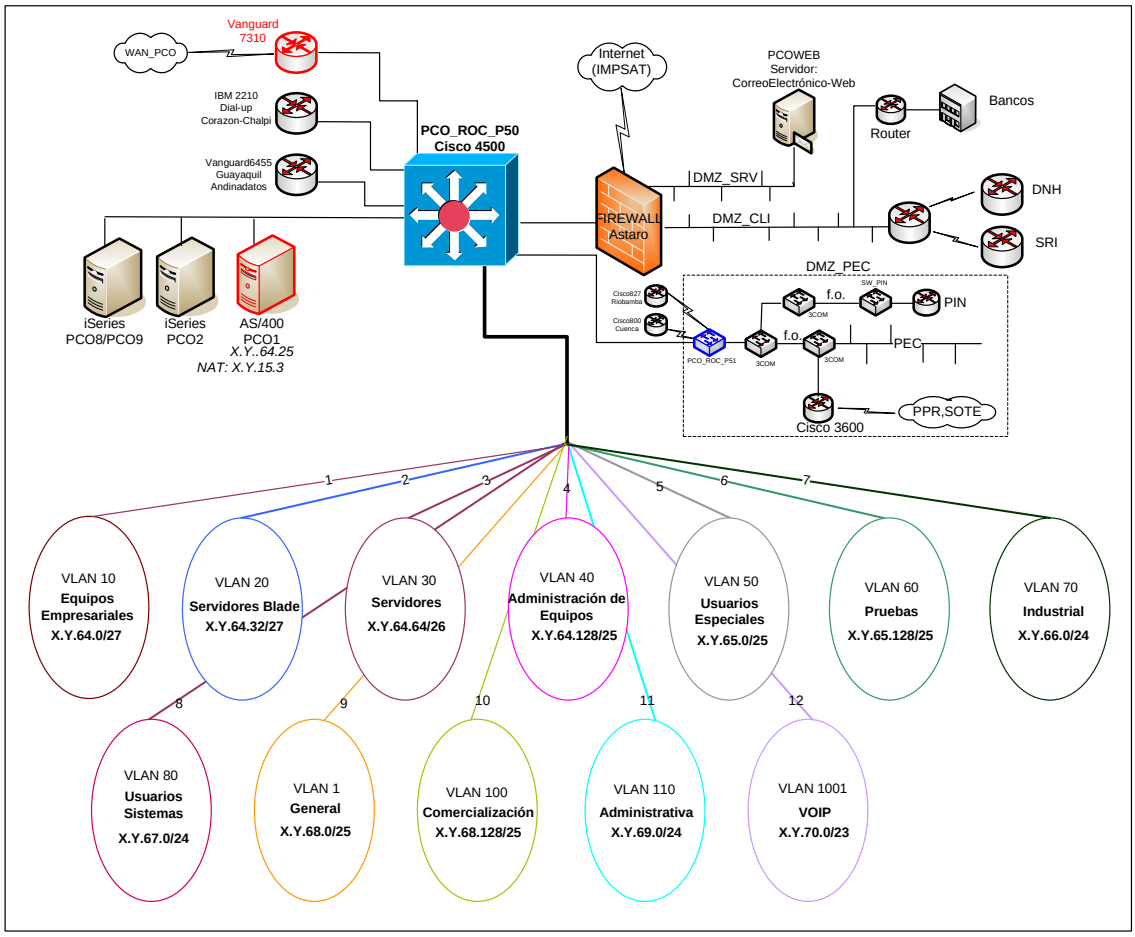

Figura 4.4: Segunda propuesta para el Diseño de VLANs de PETROCOMERCIAL Quito

Ventajas:

- ✓ Se ubica a los equipos empresariales en una sola VLAN, evitando el cambio de direccionamiento IP y por tanto evitando cambios críticos a nivel de la red nacional de PETROCOMERCIAL.

- ✓ Se designan un considerable rango de direcciones IP disponibles para el resto de servidores.
- ✓ Se crea una VLAN libre con 128 direcciones IP disponibles.
- ✓ Se asigna un vasto rango de 256 direcciones IP para la VLAN de usuarios de sistemas.
- ✓ La nomenclatura de las VLANs permite brinda escalabilidad a las mismas, utilizando multiplos de 10 para identificación.

Desventajas:

- ✓ Se determinan solo 512 direcciones a los usuarios de los grupos General, Administrativo y Comercialización, este rango soporta el tamaño actual de estos usuarios y hasta un 50% de crecimiento, sin embargo es aconsejable utilizar un rango mayor.
- ✓ La asignación de estas VLANs implican múltiples cambios en la red local, a pesar de que estos cambios no tienen trascendencia a nivel nacional.
- ✓ Se sobrevaloriza el rango de la VLAN Industrial la cual por el momento no maneja ningún equipo.

4.5.2.3- Tercera Propuesta

Esta propuesta, expone el diseño de VLANs de la siguiente forma:

Cuadro 4.13 : Tercera propuesta de diseño de VLANs

No	Nombre	ID	Dirección IP	Rango	Rango	Tamaño
1	Equipos Empresariales	VLAN 10	X.Y.64.0	/25	64.1 - 64.127	128
2	Administración de Equipos	VLAN 20	X.Y.64.128	/26	64.129 - 64.255	64
3	Usuarios Especiales	VLAN 30	X.Y.64.192	/26	65.1 - 65.127	64
4	Usuarios Sistemas	VLAN 40	X.Y.65.0	/25	65.129 - 65.255	128
5	Industrial	VLAN 50	X.Y.65.128	/25	66.1 - 66.255	128
6	Administrativa	VLAN 60	X.Y.66.0	/23	67.1 - 67.255	512
7	Comercialización	VLAN 70	X.Y.68.0	/24	68.1 - 68.255	256
8	General	VLAN 1	X.Y.69.0	/24	68.129 - 68.255	256
9	VoIP	VLAN 1001	X.Y.70.0	/23	69.1 - 69.255	512

Características:

- ✓ Crea una VLAN con los principales equipos de comunicación y todos los servidores, empresariales y locales. Este VLAN se denomina “Equipos Empresariales” y posee 126 direcciones disponibles, esto con el fin de manipular un grupo cuyo direccionamiento IP se mantenga igual al actual evitando así cambios críticos en la red nacional y local por cuanto contiene a los principales equipos de la empresa.
- ✓ No se crea ninguna VLAN libre.
- ✓ Se reducen los rangos de direccionamiento IP para las VLANs de Administración de equipos y usuarios especiales, asignando solamente 64 direcciones IP, las cuales soportan sin problema el tamaño actual y un 50% de crecimiento, para ambos casos.
- ✓ Asigna 1024 direcciones IP en total para los usuarios, divididos en los grupos: General, Administrativa y Comercialización.
- ✓ Asigna 512 direcciones IP a la VLAN de telefonía IP.

A continuación se visualiza la tercera propuesta:

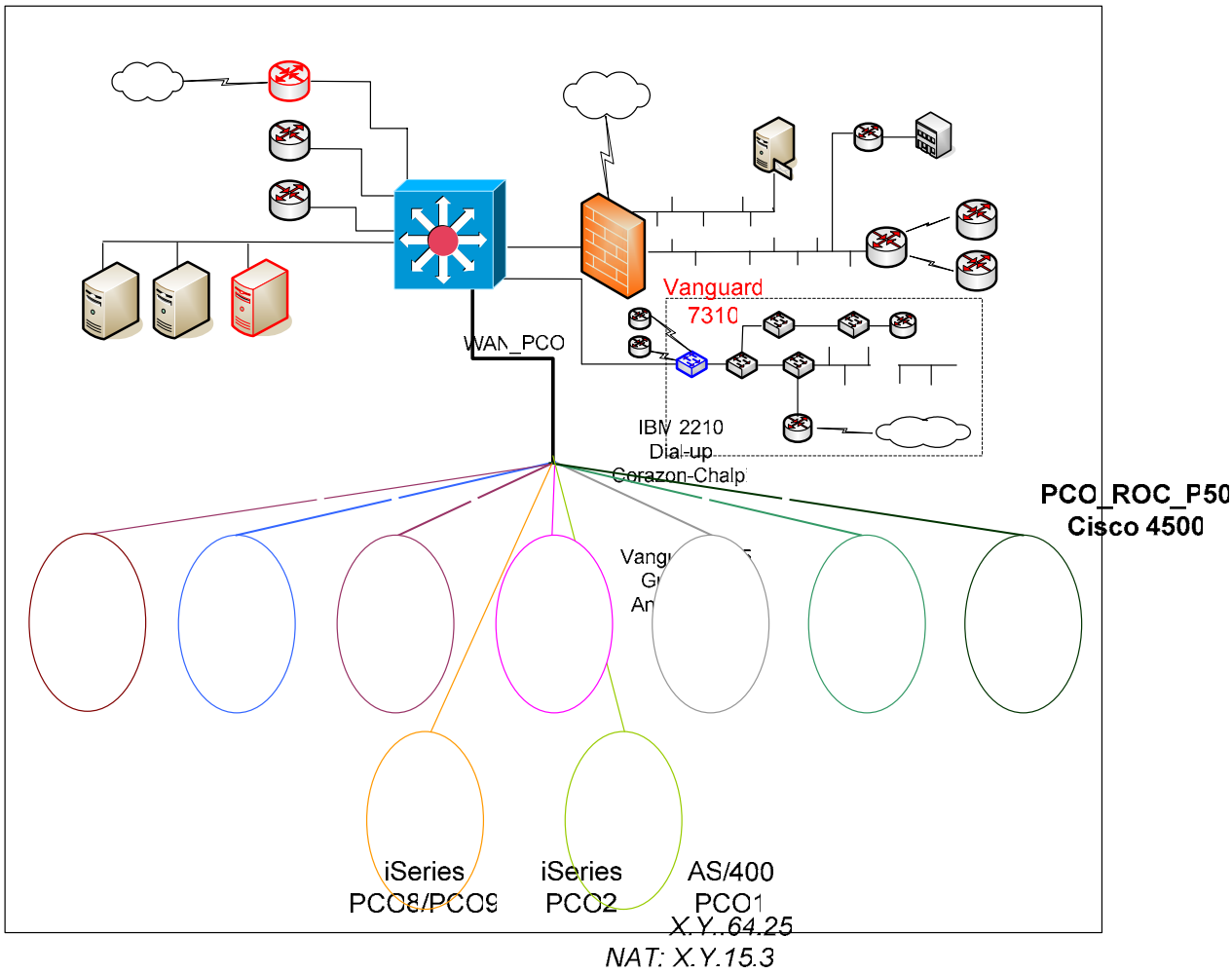

Figura 4.5: Tercera propuesta para el Diseño de VLANs de PETROCOMERCIAL Quito

Ventajas:

- ✓ Se ubica a todos los servidores en una sola VLAN, evitando el cambio de direccionamiento IP y por tanto evitando cambios críticos a nivel de la red nacional de PETROCOMERCIAL.
- ✓ Se provee de un considerable rango de direcciones IP disponibles en la VLAN de servidores, dando un soporte de más del 200% de crecimiento.
- ✓ Se asignan mesuradamente los rangos de direcciones IP tanto para la VLAN de Administración de equipos, usuarios especiales, usuarios de

sistemas, e Industrial, brindando un espacio suficiente para el número de equipos actuales y para su posible crecimiento.

- ✓ La nomenclatura de las VLANs brinda escalabilidad a las mismas, utilizando múltiplos de 10 para identificación.
- ✓ Se establecen menor cantidad de VLANs en relación a las propuestas anteriores.

Desventajas:

- ✓ El rango de direccionamiento para la VLAN de Equipos Empresariales es amplio, lo que resta efectividad a la reducción de dominios de broadcast.
- ✓ No existe ninguna VLAN libre, puesto que no quedan direcciones IP disponibles fuera de los rangos detallados.
- ✓ La asignación de estas VLANs implican múltiples cambios en la red local, a pesar de que estos cambios no tienen trascendencia a nivel nacional.

Nota: Para esta propuesta no se ha considerado la subdivisión de los equipos principales de comunicación y de los distintos tipos de servidores, puesto que por recomendaciones del personal de la Unidad de Sistemas y Telecomunicaciones, señalan la predilección de iniciar con un grupo amplio de administración para evitar la modificación de direccionamiento IP en los equipos servidores.

Es también importante mencionar que en ninguna de las alternativas presentadas se ha tomado como inconveniente en el diseño la cantidad de

VLANs planteadas ni la frecuente convergencia de algunas de las VLANs hacia las principales como son las VLANs de servidores o equipos empresariales, puesto que el equipo de conmutación de Core (Cisco Catalyst 4500) presenta características técnicas de alto rendimiento que hacen del proceso de enruteo entre VLANs no permita la presencia de latencia, realizando este paso de manera tan ágil como la conmutación.

4.5.3- Desarrollo del mejor diseño de VLANs propuesto para PETROCOMERCIAL Quito.

Para seleccionar la mejor alternativa para el diseño de VLANs se realizará una comparación entre las alternativas disponibles, para esto en el siguiente cuadro se considerarán las principales características que debe cumplir el diseño de VLANs para el caso particular de PETROCOMERCIAL Quito, y su relación con las propuestas existes:

Cuadro 4.14 : Comparación entre las propuestas de VLANs

Propuesta / Factores	PROPUESTA1	PROPUESTA2	PROPUESTA3
Fácilidad de Implementación	2	1	3
Rangos mínimos de crecimiento	1	2	2
Organización adecuada	2	3	3
Grupos apropiadamente definidos	2	3	3
Escalabilidad	1	2	2
Espacio libre disponible	1	3	2
Rangos IP adecuados	2	2	3
Cantidad mínima de desventajas	3	2	2
TOTAL	**14**	**18**	**20**

Valorización		
	ALTO	**3**
	MEDIO	**2**
	BAJO	**1**
	NULO	**0**

Podemos concluir entonces mediante el cuadro 4.14 que la propuesta 3 brinda mayor cantidad de beneficios en cuanto a su diseño y por tanto será la alternativa a desarrollarse.

4.6- Desarrollo del Mejor Diseño Propuesto

Luego de haber seleccionado a la propuesta 3 como la mejor alternativa se debe plantear detalladamente como se ejecutará a la misma. Los aspectos que se deben tomar en consideración son los siguientes:

4.6.1- Nuevo direccionamiento IP para PETROCOMERCIAL Quito

La propuesta 3 detalla la distribución de direcciones IP por cada una de las VLANs, sin embargo es necesario puntualizar la puerta de acceso para cada una de ellas, así como el direccionamiento para las impresoras de red, respectivamente. Es así que para cada una de las VLANs se seleccionará a la primera dirección válida de cada VLAN como su puerta de acceso, y se asignará un rango de doce a treinta direcciones IP para impresoras dependiendo del tamaño de la VLAN y tomando en cuenta solamente a los grupos que soportan usuarios. Conjuntamente se describe el tipo de direccionamiento IP con el que funcionará cada grupo (estático o DHCP), tal como se explica en el siguiente cuadro:

Cuadro 4.15 : Nuevo Direccionamiento IP PETROCOMERCIAL Quito

VLAN ID	DirecciónIP	Descripción	Tipo de Direccionamiento
VLAN 10	X.Y.64.0	DIRECCION DE RED	Estático
	X.Y.64.1	Gateway VLAN 10	
	…	**Equipos Empresariales**	
	X.Y.64.127	Dirección de broadcast	
VLAN 20	X.Y.64.128	Dirección de Subred	Estático
	X.Y.64.129	Gateway VLAN 40	
	…	**Administración de Equipos**	
	X.Y.64.191	Dirección de broadcast	
VLAN 30	X.Y.64.192	Dirección de Subred	Estático
	X.Y.64.193	Gateway VLAN 50	
	…	**Usuarios Especiales**	
	X.Y.64.255	Dirección de broadcast	
VLAN 40	X.Y.65.0	Dirección de Subred	DHCP (scope)
	X.Y.65.1	Gateway VLAN 60	
	…	**Usuarios de Sistemas**	
	X.Y.65.115	Impresoras de Red Sistemas	
	…		
	X.Y.65.127	Dirección de broadcast	
VLAN 50	X.Y.65.128	Dirección de Subred	DHCP (scope)
	X.Y.65.129	Gateway VLAN 70	
	…	**Industrial**	
	X.Y.65.255	Dirección de broadcast	
VLAN 60	X.Y.66.0	Dirección de Subred	DHCP (scope)
	X.Y.66.1	Gateway VLAN 80	
	…	**Administrativa**	
	…		
	X.Y.67.225	Impresoras de Red Administrativa	
	…		
	X.Y.67.255	Dirección de broadcast	
VLAN 70	X.Y.68.0	Dirección de Subred	DHCP (scope)
	X.Y.68.1	Gateway VLAN 90	
	…	**Comercialización**	
	X.Y.68.240	Impresoras de Red Comercialización	
	…		
	X.Y.68.255	Dirección de broadcast	
VLAN 1	X.Y.69.0	Dirección de Subred	DHCP (scope)
	X.Y.69.1	Gateway VLAN 1	
	…	**General**	
	X.Y.69.240	Impresoras de Red General	
	…		
	X.Y.69.255	Dirección de broadcast	
VLAN 1001	X.Y.70.0	Dirección de Subred	DHCP (Central Telefónica)
	X.Y.70.1	Gateway VLAN 1001	
	…	**VOIP**	
	…		
	X.Y.71.255	Dirección de broadcast	

La siguiente tabla resume las VLANs que serán establecidas, con su respectivo detalle:

Cuadro 4.16 : Resumen de VLANs para PETROCOMERCIAL Quito

No	Nombre	ID	Dirección IP	Rango	Rango	Tamaño
1	Equipos Empresariales	VLAN 10	X.Y.64.0	/25	64.1 - 64.127	128
2	Administración de Equipos	VLAN 20	X.Y.64.128	/26	64.129 - 64.255	64
3	Usuarios Especiales	VLAN 30	X.Y.64.192	/26	65.1 - 65.127	64
4	Usuarios Sistemas	VLAN 40	X.Y.65.0	/25	65.129 - 65.255	128
5	Industrial	VLAN 50	X.Y.65.128	/25	66.1 - 66.255	128
6	Administrativa	VLAN 60	X.Y.66.0	/23	67.1 - 67.255	512
7	Comercialización	VLAN 70	X.Y.68.0	/24	68.1 - 68.255	256
8	General	VLAN 1	X.Y.69.0	/24	68.129 - 68.255	256
9	VoIP	VLAN 1001	X.Y.70.0	/23	69.1 - 69.255	512

Es importante indicar que el cambio de direccionamiento IP para esta propuesta implica que aproximadamente el 20% de los servidores, computadores y otros de equipos en funcionamiento de PETROCOMERCIAL Quito deban modificar exclusivamente su direccionamiento IP, por lo que al ser implementada esta solución se deben tomar todas las medidas posibles para precautelar posibles inconvenientes, sobre todo evitando perturbar el desenvolvimiento de los usuarios.

4.6.2- Tipo de asignación para las VLANs

Dadas las circunstancias específicas para PETROCOMERCIAL Quito, la mejor alternativa para la implementación de VLANs sobre los equipos de conmutación Cisco Catalyst, es la asignación estática de VLANs en base a puertos, esto debido a que los métodos de asignación de VLANs en base a direcciones MAC y el método de VLANs basadas en direcciones de red no son convenientes para este caso. El método de VLANs basadas en direcciones de

red no es adecuado puesto que las VLANs propuestas utilizarían el servidor DHCP existente en PETROCOMERCIAL Quito.

En cuanto al direccionamiento basado en direcciones MAC, se presentan algunas inconvenientes. El principal problema se refiere al requerimiento de un equipo que cumpla las funciones de servidor de configuración de VLANs o también denominado VMPS[1] debido a que en este método se utiliza una base de datos de software que contiene un mapeo de direcciones MAC a VLAN que el administrador debe configurar primero. Conjuntamente este método afecta el desempeño, escalabilidad y administración de la red, por cuanto consume recursos al gestionar una base de datos de direcciones MAC. Es importante mencionar también que no se cuenta con un registro actualizado de las direcciones MAC de los PCs de la empresa, y en el caso de tenerla esta recopilación no sería completamente útil puesto que los equipos tienden a cambiar periódicamente debido a circunstancias particulares de la organización. Teóricamente con este hecho el método facilitaría la administración al realizarse desplazamientos de usuarios, sin embargo para PETROCOMERCIAL Quito, el constante cambio de usuarios se lo realiza entre distintos departamentos organizacionales, lo que inevitablemente implicaría la reconfiguración manual de los switches por cada desplazamiento de usuarios, en el caso de aplicar el método de direccionamiento basado en direcciones MAC

Por lo tanto, la asignación estática de VLANs en base a puertos se adapta mejor a las condiciones físicas de los edificios de PETROCOMERCIAL Quito, puesto que a pesar de que los equipos sean cambiados periódicamente,

[1] **VMPS** (VLAN Management Policy Server): Es un servidor de políticas de administración de VLANs que maneja la base de datos de todas las direcciones MAC

el nuevo equipo que ocupara la misma ubicación pertenecerá al mismo grupo lógico (misma VLAN), por lo que no necesitaría cambios frecuentes en la configuración de los equipos. La asignación de VLANs en base a puertos no requiere de tablas de búsqueda complejas para la segmentación de VLANs, evitando el gasto adicional de recursos, provee además de seguridad, facilidad de configuración y facilidad de monitoreo.

Mediante este método no se proveerá seguridad a nivel de la capa 2, la cual administra los equipos en base al direccionamiento MAC, en su lugar se incorporará seguridad a nivel de capa 3, es decir en base al direccionamiento IP. Esto se logrará mediante el direccionamiento IP de las puertas de enlace de cada una de las VLANs. Dado que todos los usuarios de la empresa requieren fundamentalmente de los servicios de la VLAN de Equipos empresariales (VLAN 10), es primordial establecer en cada una de las tarjetas de red de los PCs de la empresa, la puerta de enlace de su respectiva VLAN para que de esta manera puedan acceder al resto de grupos. El direccionamiento IP establecido como puerta de enlace para cada VLAN será de conocimiento exclusivo de los administradores de red, por lo que el movimiento de usuarios dentro de la red sería controlado, ya que obligatoriamente los usuarios debiesen informar al personal correspondiente para realizar cualquier desplazamiento.

Por lo demás en el caso de que se ingrese un equipo no autorizado a la red local, este no podría funcionar adecuadamente.

Mediante el análisis realizado anteriormente podemos concluir asimismo que será necesario la configuración de VTP[1] en la red, con el fin de que las

[1] VLAN Trunking Protocol (VTP): Protocolo usado para configurar y administrar VLANs en equipos Cisco

VLANs sean propagadas hacia todos los switches sin necesidad de aplicar la configuración independientemente a cada uno de los equipos, lo que también permite que los equipos sean actualizados automáticamente en el caso de que existan cambios en cuanto a VTP. El tráfico de las VLANs solo se transmitirá a través de enlaces troncales de tal manera que no se consumirá el ancho de banda del resto de paquetes.

Finalmente se configurará el protocolo spanning-tree, con el fin de evitar lazos lógicos en la red vertical, además de brindar mayor rapidez en cuanto a la convergencia de red.

4.6.3- Asignación de usuarios para VLANs por ubicación

El siguiente cuadro resume la asignación de VLANs de acuerdo a la posición física de los usuarios y de los equipos, relacionándola al piso y al departamento al que pertenecen, respectivamente, sin embargo el cuadro cuenta solamente con las VLANs de acceso por parte de usuarios, a excepción de la VLAN para usuarios especiales, la cual se aplica únicamente para un pequeño grupo de usuarios pertenecientes a distintos departamentos de la empresa, como se explicó con anterioridad.

Cuadro 4.17 : Asignación de VLANs por ubicación

Edificio	PISO	DEPARTAMENTO	IDF	VLAN 60 Sistemas	VLAN 80 Administrativa	VLAN 90 Comercialización	VLAN 1 General	VLAN 1001 VOIP
EL ROCIO	Subsuelo	Mantenimiento Eléctrico	1				X	X
		Cajita de PCO	1		X			X
	PB	Secretaria General	1				X	X
		Administración de Activos	1		X			X
		Administración Financiera	1		X			X
		Cuentas por pagar	1		X			X
		Recepción(Servicios Administrativos)	1				X	X
	1	Negocios Propios	1					X
		Credito y Cobranzas	1					X
		Seguros	1		X			X
		Materiales	1		X			X
	2	Abastecedora	2			X		X
		Finanzas	2		X			X
		Presupuesto	2		X			X
	3	Subgerencia de Comercialización	2			X		X
		Gerencia	2				X	X
		Comercializadora	2			X		X
	4	Programación	MDF			X		X
		Planificación y Finanzas	MDF		X			X
		Soporte de Aplicaciones	MDF	X				X
	5	Sistemas y Telecomunicaciones	MDF	X				X
	6	Vicepresidencia	MDF				X	X
	7	Subgerencia de Transporte	3			X		X
		Contabilidad	3		X			X
	8	Servicios Administrativos	3		X			X
		Recursos Humanos	3		X			X
		Subgerencia Administrativa	3				X	X
	9	Seguridad Física	3				X	X
		Legal	3				X	X
EX-SALESIANO	PB	Soporte Técnico y Mantenimiento	4	X				X
		Proyectos	4		X			X
		Fondo de Jubilación	4				X	X
	1	Contratos	5		X			X
		Bienestar Laboral	5		X			X
	2	Control de Gestión	5		X			X
		Relaciones Públicas	5				X	X

4.7- Consideraciones para el control de la seguridad perimetral

Previo a la búsqueda de una propuesta que alcance la optimización de la seguridad perimetral de PETROCOMERCIAL Quito, es necesario realizar un análisis detallado de las políticas de seguridad existentes.

Tal como se indicó en el capítulo anterior, se han encontrado inconvenientes en algunas de las políticas planteadas, a continuación se puntualiza un estudio minucioso para cada una de ellas.

4.7.1- Políticas de seguridad incorrectamente definidas

4.7.1.1- Políticas con rangos inadecuados

Cuadro 4.18 : Política 1 con rangos inadecuados

Recurso	Origen	Servicio	Política	Destino	Descripción
Serv_Externos	**Internal**	Oracle_SQL_NET	Permitir	MEM_GRP_SRV	Política para acceso desde la red interna hacia el servidor de M.E.M. que contiene la aplicación para que se guarde la información en su base de datos a través del puerto 1521

La política mostrada en el cuadro 4.18 determina claramente un tipo de servicio específico, sin embargo su rango de origen es considerablemente amplio, lo cual indiscutiblemente pondría en riesgo la seguridad de la red de PETROCOMERCIAL Quito, así como la integridad de los datos del Ministerio de Energía y Minas. Es entonces conveniente realizar un nuevo grupo de origen limitado, para el acceso a estos servidores.

PROPUESTA

Luego de determinar el grupo de usuarios que actualmente requieren el acceso hacia el Ministerio de Energía y Minas, se han determinado únicamente dos equipos, un servidor y un equipo perteneciente a un usuario de la Unidad de Sistemas de la empresa, estos son:

Cuadro 4.19 : Lista de equipos para la creación de una red para la política 1

Nombre del Equipo	Tipo de Equipo	Dirección IP
PCORED01	Servidor	X.Y.64.21
SSABH	PC	X.Y.71.5

Mediante esta información se creará un nuevo recurso, una red, la cual dado su contenido, se lo denominará **PCO_Grp_MEM,** y contendrá las direcciones IP de los equipos mencionados. Este recurso se definiría de la siguiente manera:

Cuadro 4.20 : Nuevo recurso de red para la política 1.

Nomenclatura	Contenido	Descripción
PCO_Grp_MEM	X.Y.64.21	Grupo de hosts que acceden al Servidor del M.E.M.
	X.Y.71.5	

Con la definición de este grupo la política se establecería como se muestra a continuación:

Cuadro 4.21 : Propuesta para la Política 1 con rangos inadecuados

Recurso	Origen	Servicio	Política	Destino	Descripción
Serv_Externos	**PCO_Grp_MEM**	Oracle_SQL_NET	Permitir	MEM_GRP_SRV	Política para acceso desde la red interna hacia el servidor de M.E.M. que contiene la aplicación para que se guarde la información en su base de datos a través del puerto 1521

En el caso de que otro equipo deba ingresar al recurso ya definido simplemente se procederá a ingresar la dirección IP del equipo en la definición del recurso.

4.7.1.2- Políticas con tipos de servicio inexactos

Política 1

Cuadro 4.22 : Política 1 con tipos de servicio inexactos

Recurso	Origen	Servicio	Política	Destino	Descripción
PetroEcuador	PCO_Net_UIO	**Todos los servicios**	Permitir	PEC_Grp_Net	Política para el acceso desde la red de PCO hacia los servidores de PetroEcuador

Esta política expuesta en el cuadro 4.22, permite la ejecución de cualquier servicio y por tanto el acceso completo desde la red de PETROCOMERCIAL Quito hacia la red de servidores de PETROECUADOR. Esta política se determinó dado que en lugar de utilizar el acceso a Internet para el ingreso a la página web de Petroecuador, se utiliza el enlace directo existente con la institución. Además Petroecuador presta servicios al grupo de usuarios especiales los cuales requieren de información de esta institución , no obstante, al autorizar esta política, contrariamente a lo que se desea obtener, se pone en riesgo la seguridad de la red interna, puesto que cualquier tipo de ataque informático o intromisión no autorizada podría ingresar tanto a través del rango de origen, el cual es considerablemente extenso, como mediante el grupo de destino, aunque con menor probabilidad, dejando en claro la necesidad de establecer como permitidos exclusivamente a los servicios que se consideren indispensables y de acuerdo a los requerimientos de cada grupo de usuarios.

Por lo demás, como se mencionó recientemente en relación a los rangos del grupo de origen, se lo debe redefinir puesto que únicamente es conveniente habilitar esta política con el servicio HTTP para todos los usuarios, y crear una segunda política para quienes requieran otro tipo de servicios a estos servidores, evitando así cualquier tipo de inconveniente que pudiese darse desde o hacia los usuarios internos de ambas instituciones.

PROPUESTA

Para esta política se propone la creación de dos políticas en su lugar. La primera será la encargada de permitir el acceso al sitio Web, para esto se permitirá a toda la red de PETROCOMERCIAL Quito el servicio HTTP hacia los

servidores de Petroecuador. Es así que la política quedaría establecida de la siguiente manera:

Cuadro 4.23 : Primera parte de la propuesta para la Política 1 con tipos de servicio inexactos.

Recurso	Origen	Servicio	Política	Destino	Descripción
PetroEcuador	PCO_Net_UIO	**HTTP**	Permitir	PEC_Grp_Net	Política para el acceso al sitio Web de Petroecuador desde la red de PCO.

Para establecer la segunda política se necesita determinar adecuadamente el grupo de origen y la clase de servicios que deben ser permitidos, especificando así el tipo de comunicación requerida con los servidores de Petroecuador.

El grupo de usuarios que necesitan acceder a los servidores para trabajar en las aplicaciones de Petroecuador, es el grupo de usuarios especiales, citado anteriormente al realizar el análisis de VLANs, es así que para esta segunda política, se creará una red correspondiente a la VLAN de estos usuarios, de esta manera este nuevo recurso se denominará **Pco_Grp_UsEspeciales**, y permanecería definido así:

Cuadro 4.24 : Recurso de red agregado para la segunda parte de la propuesta para la Política 1 con tipos de servicio inexactos.

Nomenclatura	Contenido	Descripción
Pco_Grp_UsEspeciales	X.Y.64.192/26 (VLAN 30)	Grupo de usuarios especiales que accesan a PetroEcuador

En cuanto a la redefinición de servicios, se determinó que las aplicaciones de Petroecuador que son utilizadas por PETROCOMERCIAL son las siguientes:

- ✓ Sistema contable de Petroecuador. Este sistema requiere el rango del puerto 137 al puerto 139, a través del protocolo TCP.
- ✓ Acceso a la base de datos "SUCO"[1]. Esta es una base de datos perteneciente a PetroEcuador, a la cual el equipo PCORED11 de PETROCOMERCIAL replica con el fin de que sus usuarios accedan más ágilmente a la información almacenada en esta base. Para que el servidor de PETROCOMERCIAL acceda a la base Interbase[2] de Petroecuador se utiliza del puerto 3050 a través del protocolo TCP.

  Este servicio actualmente si se encuentra definido como recurso en el equipo de seguridad.

Con esta información se procederá a determinar un nuevo servicio que incluya los puertos ya especificados, el nuevo servicio resultaría establecido de la siguiente manera:

Cuadro 4.25 : Recurso de servicio agregado para la segunda parte de la propuesta para la Política 1 con tipos de servicio inexactos.

No.	Nombre	Protocolo	Puerto de origen	Puerto de Salida	Observaciones
1	**Aplicaciones PEC**	TCP	1:65535	**3050**	Base de Datos SUCO
		TCP	1:65535	**137:139**	Aplicaciones Contables

Mediante los dos nuevos recursos planteados se determina la segunda parte de la propuesta, la misma que se establecería así:

[1] SUCO: Sistema Unificado de Calificación de Oferentes de Petroecuador.
[2] Tipo de motor de base de datos.

Cuadro 4.26 : Segunda parte de la propuesta para la Política 1 con tipos de servicio inexactos

Recurso	Origen	Servicio	Política	Destino	Descripción
PetroEcuador	Pco_Grp_UsEspeciales	**AplicacionesPEC**	Permitir	PEC_Grp_Net	Política para el acceso de usuarios autorizados hacia los servidores de las aplicaciones de PetroEcuador

Estas dos nuevas políticas brindan seguridad y un funcionamiento adecuado en cuando a los accesos solicitados por los usuarios.

Política 2

Cuadro 4.27 : Política 2 con tipos de servicio inexactos

Recurso	Origen	Servicio	Política	Destino	Descripción
SRV_Web_Correo	PCO_Srv_Web	Todos los servicios	Permitir	0.0.0.0/0	Política para el acceso desde el servidor Web y de correo hacia todos los destinos.

La política indicada en el cuadro 4.26 permite al servidor Web y al servidor de correo externo acceder hacia todos los destinos mediante el Internet , sin embargo si bien el destino debe ser indefinido debido a la necesidad de navegación por parte de ambos servidores, el tipo de servicio asignado no es adecuado, puesto que actualmente se tiene autorizado todo tipo de servicio siendo factible y necesario redefinir únicamente a el o los servicios que se indispensables para el manejo y la navegación en la red pública por parte de estos dos servidores.

PROPUESTA

La propuesta para esta política consiste en el establecimiento de los servicios específicos que sean imprescindibles para el correcto funcionamiento

del servidor Web y el servidor de correo externo de PETROCOMERCIAL Quito. Ante esta necesidad se han determinado dos servicios para esta nueva política, HTTP y SMTP respectivamente. Sin embargo PETROCOMERCIAL Quito recurre para su acceso a Internet de los servicios prestados por Impsat (ISP), de manera que se requiere del servicio de DNS externo, el cual toma del ISP, siendo este otro servicio que debe ser añadido a esta política. Finalmente esta política sería establecida de la siguiente manera:

Cuadro 4.28 : Propuesta para la política 2 con tipos de servicio inexactos

Recurso	Origen	Servicio	Política	Destino	Descripción
SRV_Web_Correo	PCO_Srv_Web	HTTP, SMTP,DNS	Permitir	0.0.0.0/0	Política para el acceso desde el servidor Web y de correo hacia todos los destinos.

Es importante mencionar que esta política se complementa con la restricción de acceso a páginas de contenidos no autorizados por la empresa, lo cual ya se encuentra establecido en el equipo de seguridad perimetral de la empresa, en la actualidad.

Política 3

Cuadro 4.29 : Política 3 con tipos de servicio inexactos

Recurso	Origen	Servicio	Política	Destino	Descripción
Usuarios	PCO_Net_EC	Todos los servicios	Permitir	BCE_GRP_Hst	Política para el acceso de la red interna de PCO hacia el grupo de host del Banco Central de PCO

La política definida en el cuadro 4.28, presenta inconvenientes en cuanto a la dimensión del grupo de origen y al delimite de sus servicios

permitidos, es entonces conveniente redefinir un restringido grupo de inicio y únicamente los servicios que sean esenciales. Si bien la apertura a todo tipo de servicios hacia los usuarios externos, en este caso del Banco Central del Ecuador, esta política puede dar lugar a varios inconvenientes por posibles intromisiones no autorizadas por parte de grupos de usuarios de PETROCOMERCIAL.

PROPUESTA

Como paso inicial se establecerá la posibilidad de crear un grupo limitado de usuarios para el acceso a los servidores mencionados para posteriormente analizar el servicio que sea necesario.

Para esto se realizó un levantamiento de información, determinando a doce usuarios que requieren del acceso a los servidores del Banco Central del Ecuador para realizar consultas o descargas en línea. A este grupo se lo denominará Pco_Grp_HostBC, y estaría establecido de la siguiente forma:

Cuadro 4.30 : Nuevo recurso para la política 3 con tipos de servicio inexactos

Nomenclatura	Contenido	Descripción
Pco_Grp_HostBC	X.Y.134.81	Grupo de usuarios que accesan a los servidores del Banco Central del Ecuador
	X.Y.132.34	
	X.Y.132.37	
	X.Y.134.72	
	X.Y.134.88	
	X.Y.134.35	
	X.Y.64.96	
	X.Y.64.97	
	X.Y.64.98	
	X.Y.97.39	
	X.Y.97.37	

Dado que estos usuarios acceden a la información mediante la página web del Banco, se ha determinado que únicamente necesitarán el servicio

HTTP_HTTPS, ya definido en los servicios del equipo de seguridad anteriormente y que contiene a los puertos 80, 9040,443 Y 9446 a través del protocolo TCP, siendo este grupo de puertos los necesarios para el acceso que requieren estos usuarios. Mediante esta información se puede definir una nueva política de seguridad que limitará el acceso a información requerida desde el Banco Central del Ecuador por parte de los usuarios de PETROCOMERCIAL.

La política se redefiniría de la siguiente manera:

Cuadro 4.31 : Propuesta para la política 3 con tipos de servicio inexactos.

Recurso	Origen	Servicio	Política	Destino	Descripción
Usuarios	Pco_Grp_HostBC	HTTP_HTTPS	Permitir	BCE_GRP_Hst	Política para el acceso de un grupo de usuarios autorizados hacia el grupo de servidores del Banco Central de PCO

De esta manera exclusivamente los usuarios autorizados cuya dirección IP consta en el recurso definido podrán acceder a la información privada del Banco Central del Ecuador.

4.7.1.3- Políticas de carácter temporal (no deshabilitadas)

Cuadro 4.32 : Política 1 y 2 de carácter temporal

Recurso	Origen	Servicio	Política	Destino	Descripción
Admin_Serv	gpalacios (PPTP user)	Telnet	Permitir	PCO_Net_UIO	Politica para el acceso a ASTARO via dial-up para el usuario especificado

Recurso	Origen	Servicio	Política	Destino	Descripción
Admin_Serv	PCO_Net_UIO	Telnet	Permitir	gpalacios (PPTP user)	Politica para el acceso a ASTARO via dial-up para el usuario especificado

Estas dos políticas definidas, básicamente permiten a un administrador el acceso mediante telnet hacia la red de PETROCOMERCIAL Quito y viceversa. Si bien esta política fue ejecutada por motivos específicos del administrador, no es favorable mantener este tipo de políticas para un rango tan amplio, es así que para que se mantenga activa y adecuadamente definida esta política, es necesario ajustar el grupo de origen a un grupo o grupos limitados y que requieran ser monitoreados, como son los grupos de equipos empresariales, servidores, etc.

PROPUESTA

Mediante la definición de VLANs realizada anteriormente se establecerá un recurso que contenga todos los equipos de administración. El recurso se denominará **PCO_Grp_Adm** y se delimitaría de esta forma:

Cuadro 4.33 : Nuevo recurso para la política 1 y 2 de carácter temporal

Nomenclatura	Contenido	Descripción
PCO_Grp_Adm	X.Y.64.0/25(Vlan 10)	Grupo de equipos de administración para PETROCOMERCIAL Quito
	X.Y.64.128/26 (Vlan 20)	

Mediante este nuevo recurso señalado se redefinirá a las políticas anteriormente mencionadas como se muestra a continuación:

Cuadro 4.34 : Propuesta para las políticas 1 y 2 de carácter temporal

Recurso	Origen	Servicio	Política	Destino	Descripción
Admin_Serv	gpalacios (PPTP user)	Telnet	Permitir	PCO_Grp_Adm	Politica para el acceso a ASTARO via dial-up para el usuario especificado

Recurso	Origen	Servicio	Política	Destino	Descripción
Admin_Serv	PCO_Grp_Adm	Telnet	Permitir	gpalacios (PPTP user)	Politica para el acceso a ASTARO via dial-up para el usuario especificado

De esta manera se mantendrá permitido el servicio con fines de monitoreo exclusivamente a los equipos empresariales y demás servidores.

4.7.1.4- Políticas des actualizadas

Cuadro 4.35 : Política 1 des actualizada

Recurso	Origen	Servicio	Política	Destino	Descripción
Serv_GasPco_Pto1723	PCO_Hst_GRN_134.32	PPTP	Permitir	Todos los destinos	Política para el ingreso mediante PPTP desde los host de la estación de Servicio hacia todos los destinos

Esta política fue establecida puesto que un usuario de la estación de servicio requirió temporalmente otro tipo de acceso, especificado anteriormente, por lo que la solución ante esta política es la exclusión de la misma.

PROPUESTA

La propuesta consiste en la eliminación de esta política, pues no es de carácter primordial para la empresa, poniendo en inseguridad a la red de PETROCOMERCIAL.

En el siguiente capítulo se aplicarán las propuestas anteriormente analizadas.