CAPÍTULO III

ANÁLISIS DE LA RED IP Y SEGURIDAD PERIMETRAL DE PETROCOMERCIAL QUITO

3.1- Introducción

El objetivo principal de este capítulo es el desarrollo de los dos primeros pasos sistemáticos detallados en la metodología en la cual se fundamenta el presente proyecto (Metodología de diseño de redes área local descrita por Cisco Systems). Es entonces primordial para este efecto realizar la documentantación de los requisitos y expectativas de cada uno de los temas y subtemas que conciernan al proyecto, para posteriormente realizar el análisis de la información recolectada.

3.2- Topología Básica de la Red IP

La red actual de PETROCOMERCIAL Quito, que conforman los edificios El Rocio y Ex-Salesianos, está compuesta por un backbone de fibra óptica multimodo, con una topología tipo estrella extendida y enlaces de cable UTP de 10 Mbps y 100Mbps a switches y a los servidores de red. Los principales accesos son a Internet, al SRI, al Ministerio de Energía y Minas (DNH), a las filiales de Petroecuador, Petroindustrial, y al Sistema de Oleoducto Trans-Ecuatoriano

(SOTE); además a Sucursales como: Riobamba, Cuenca, Guayaquil; a Terminales como: Corazón y Chalpi; y a la red WAN de PETROCOMERCIAL.

A continuación se muestra la topología actual de la red:

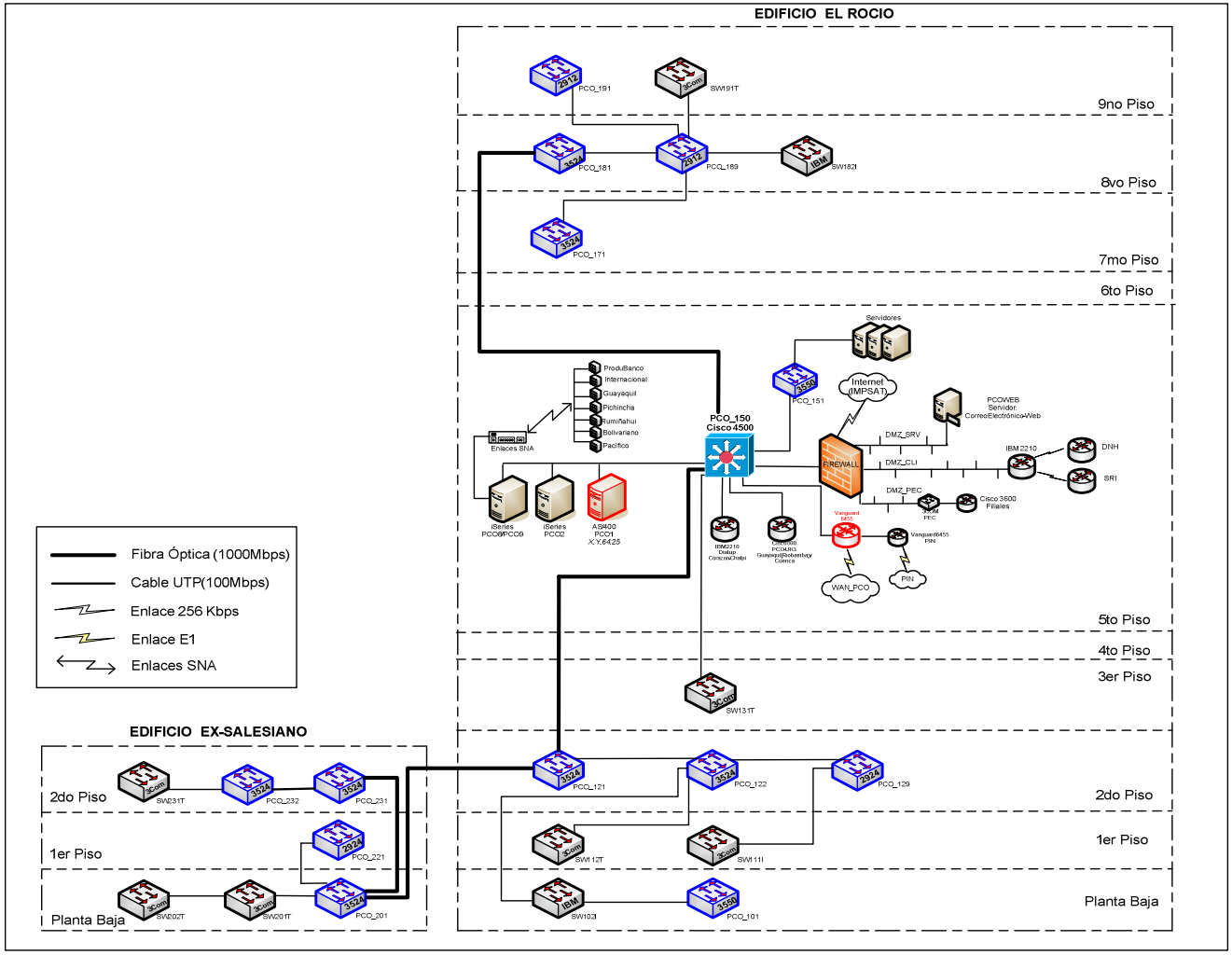

Figura 3.1: Topología actual de LAN de PETROCOMERCIAL Quito.

Este diseño presenta los siguientes inconvenientes:

- ✓ Bajas velocidades en el tráfico de datos por la presencia de switches capa 2, los cuales limitan su capacidad a 10Mbps.
- ✓ La topología de la red vertical es inadecuada
- ✓ Infraestructura inadecuada para la ubicación de los switchs por piso.
- ✓ Utilización de switchs no configurables, los cuales limitan el control de la red local.
- ✓ Altos tiempos de respuesta en el tráfico de datos, esta información se la visualizó mediante gráficos estadísticos realizados mediante un monitoreo a la red IP, como se muestra en el Anexo A.
- ✓ Falta de cableado adecuado.
- ✓ Sub utilización de los equipos de conmutación.

3.3- Direccionamiento IP

La red de PETROCOMERCIAL, tanto la Regional Norte como la Regional Sur, tiene asignada la dirección: X.Y.0.0[1] , es decir es una red clase B; y a su vez esta red esta divida en sub-redes (subneteada). Es así que PETROCOMERCIAL Quito tiene asignada la dirección X.Y.64.0, con máscara de subred 255.255.248.0. La dirección de red X.Y.0.0 permite establecer 30 subredes de 2046 usuarios cada una, teniendo entonces la subred X.Y.64.0 capacidad para 2046 usuarios, y su rango va desde la dirección X.Y.64.1 hasta la dirección X.Y.71.254, como se explica en el siguiente cuadro:

[1] Por motivos de confidencialidad de la empresa se representaran los dos primeros octetos de la dirección IP con las letras “X” y “Y”.

Tabla 3.1: Subneteo de la red X.Y.0.0 para la mascara 255.255.248.0

No. Subred	Dirección de la Subred	1ero Host de la Subred	Último Host de la Subred	Dirección de Broadcast
1	X.Y.0.0	X.Y.0.1	X.Y.7.254	X.Y.7.255
2	X.Y.8.0	X.Y.8.1	X.Y.15.254	X.Y.15.255
3	X.Y.16.0	X.Y.16.1	X.Y.23.254	X.Y.23.255
4	X.Y.24.0	X.Y.24.1	X.Y.31.254	X.Y.31.255
5	X.Y.32.0	X.Y.32.1	X.Y.39.254	X.Y.39.255
6	X.Y.40.0	X.Y.40.1	X.Y.47.254	X.Y.47.255
7	X.Y.48.0	X.Y.48.1	X.Y.55.254	X.Y.55.255
8	X.Y.56.0	X.Y.56.1	X.Y.63.254	X.Y.63.255
9	**X.Y.64.0**	**X.Y.64.1**	**X.Y.71.254**	**X.Y.71.255**
10	X.Y.72.0	X.Y.72.1	X.Y.79.254	X.Y.79.255
11	X.Y.80.0	X.Y.80.1	X.Y.87.254	X.Y.87.255
12	X.Y.88.0	X.Y.88.1	X.Y.95.254	X.Y.95.255
13	X.Y.96.0	X.Y.96.1	X.Y.103.254	X.Y.103.255
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
32	X.Y.248.0	X.Y.248.1	X.Y.255.254	X.Y.255.255

La máscara de subred 255.255.248.0 representa lo siguiente:

2^5 Subredes= 32

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 **0 0 0. 0 0 0 0 0 0 0 0**

2^{11}Host=2048

Es esencial además conocer el direcciónamiento de todas las sucursales y terminales de PETROCOMERCIAL, tanto regional norte como regional sur.

El direccionamiento IP de la red de PETROCOMERCIAL es el siguiente:

Cuadro 3.1 : DIRECCIONES IP DE PETROCOMERCIAL

PETROCOMERCIAL - REGIONAL NORTE			
Nombre	**Ubicación**	**Dirección IP**	**Dirección WAN**
El Rocio	Quito	X.Y.64.11	X.Y.36.25
BeaterioA	Beaterio	X.Y.129.11	X.Y.36.14/36.29
Gasolinera	Gasolinera	X.Y.134.11	X.Y.36.18
Aeropuerto	Aeropuerto	X.Y.75.11	X.Y.36.22
Ambato	Ambato	X.Y.130.11	X.Y.36.6
Riobamba	Riobamba	X.Y.131.11	X.Y.39.34
StoDomingo	StoDomingo	X.Y.161.11	X.Y.36.10/32.94
EsmeraldasPCO	Esmeraldas	X.Y.40.1/50.5	X.Y.36.130
EsmeraldasCab	Esmeraldas	X.Y.163.11	X.Y.36.134
EsmeraldasSuc	Esmeraldas	X.Y.164.11/ 40.5	X.Y.36.138
EsmeraldasPIN	Esmeraldas	X.17.Y..22/ Y.40.6	X.Y.36.142
Oyambaro	Oyambaro	X.Y.76.10	X.Y.36.170
Condijua	Condijua		X.Y.36.154
Osayacu	Osayacu	X.Y.136.10	X.Y.36.158
ShushufindiCab	Shushufindi	X.Y.137.11	X.Y.36.162
ShushufindiSuc	Shushufindi	X.Y.138.11	X.Y.36.166
ShushufindiPIN	Shushufindi	X.Y.24.22	X.Y.36.150
Gaspetsa	Gaspetsa	X.Y.166.11/ 40.3	X.Y.36.174
Corazon	Corazon	X.Y.77.10	X.Y.32.5
Quijos	Quijos	X.Y.140.10	X.Y.32.13
Chalpi	Chalpi	X.Y.139.10	X.Y.32.17
Faisanes	Faisanes	X.Y.141.10	X.Y.32.21
PETROCOMERCIAL - REGIONAL SUR			
Nombre	**Ubicación**	**Dirección IP**	**Dirección WAN**
Regional	Regional	X.Y.97.11	X.Y.36.26
Tres Bocas	Tres Bocas	X.Y.170.131	X.Y.36.58
CABECERA_LIB	Libertad	X.Y.165.11	X.Y.36.66
Lib_Pin_Cabecera	Libertad	X.Z.28.254	X.Y.36.146
Lib_Pin_Sistemas	Libertad	X.Z.28.251	
Sucursal_Lib	Sucursal Libertad	X.Y.165.71	X.Y.39.250

El direccionamiento de los dispositivos de red de la PETROCOMERCIAL Quito se encuentra planteado de la siguiente manera:

Cuadro 3.2 : RANGO DE DIRECCIONES IP DE PETROCOMERCIAL QUITO

X.Y.64.0	**DIRECCIÓN DE RED**
X.Y.64.1 … X.Y.64.19	**Comunicaciones(Routers,Firewall,RAS)**
X.Y.64.20 … X.Y.64.29	**I-Series (AS-400's)**
X.Y.64.30 … X.Y.64.49	**Direcciones para usuarios de Servicios Especiales**
X.Y.64.50 … X.Y.64.69	**Servidores**
X.Y.64.70 … X.Y.64.99	**Impresoras de Red**
X.Y.64.101 … X.Y.64.232	**Switches**
X.Y.64.254	
X.Y.65.255	
X.Y.65.0	
X.Y.65.1 … X.Y.65.255	**Rango de direcciones para el Servidor de DHCP de datos**
X.Y.67.0 X.Y.67.255	
X.Y.68.0 … X.Y.68.254	
X.Y.68.255	
X.Y.69.0	
X.Y.69.1	**Dirección Estática-Central Telefónica IP**
X.Y.69.30 … X.Y.69.240	**Rango de direcciones para el DHCP de la central telefónica IP**
X.Y.69.242	**Dirección estática E2T(Central Telefónica)**
… X.Y.69.255	
…	
X.Y.71.0	
…	
X.Y.71.21	**Dirección estática PCORED1(Servidor)**
…	
X.Y.71.255	**Dirección de broadcast**

Esta distribución del direccionamiento IP se estableció con el fin de manejar un orden coherente que facilite el manejo de los equipos a través de su direccionamiento, sin embargo este direccionamiento presenta algunos inconvenientes, como son:

- ✓ Los rangos de las direcciones IP de los diversos dispositivos de red no se encuentran agrupados en su totalidad de acuerdo al tipo de dispositivo o de acuerdo a su utilización.
- ✓ No se toma en cuenta el crecimiento de la organización, por lo que no se asignan rangos de direcciones disponibles para nuevos equipos.
- ✓ Existen rangos sobreestimados y subestimados en los grupos de dispositivos.
- ✓ Desperdicio de direcciones IP
- ✓ El orden del direccionamiento IP no se encuentra bien establecido en su totalidad.

3.4- Equipos de PETROCOMERCIAL Quito

Los equipos que forman parte de la red local de PETROCOMERCIAL Quito son:

- ✓ Switchs
- ✓ Servidores
- ✓ I-Series (AS/400)[1]
- ✓ Computadores personales
- ✓ Impresoras de red
- ✓ Teléfonos IP

[1] **i-series:** Es un ordenador empresarial, servidor eServer de IBM. Es un servidor *midrange*.

- ✓ Central telefónica IP Mitel

Es importante detallar la cantidad y el detalle de los principales dispositivos para poder realizar el rediseño de la red IP.

3.4.1- Switches

PETROCOMERCIAL Quito, cuenta con un total de 23 switches, 14 de ellos switches configurables de marca Cisco, equipos de capa dos y tres; y el resto de switches son de capa 2 no administrables, marcas IBM y 3Com

3.4.1.1- Nomenclatura de Switches

Los switches tienen el formato **Pco_XYZ** donde Pco es constante, 'X' Indica el edificio (Edificio El Rocio. / Edificio Ex-Salesiano), 'Y' Indica el número de piso dentro del correspondiente edificio y 'Z' el número de orden del switch. Si es ascendente comenzando desde 1 corresponde a la Serie Cisco Catalyst 3500 y 3550. Si es descendente comenzando desde 9 corresponde a la Serie Cisco Catalyst 2900.

Las direcciones IP que en este momento están ocupadas por los switchs, se encuentran en la numeración: **X.Y.64.N**, donde N corresponde al nombre XYZ del switch respectivo, por ejemplo Pco_153 tiene como dirección IP 172.20.64.153.

3.4.1.2- Etiquetado

Los switches están etiquetados con el formato **SWXYZM** donde 'W' es constante, 'X' indica el edificio, 'Y' es el número de piso dentro del correspondiente edificio y 'Z' indica el número de orden del switch. Si es ascendente comenzando desde 1 corresponde a la Serie Cisco Catalyst 3500 y

3550.Si es descendente comenzando desde 9 corresponde a la Serie Cisco Catalyst 2900.

3.4.1.3- Descripción de los Switches

Los switches existentes en la empresa en la actualidad son:

Cuadro 3.3 : Switches Marca Cisco de PETROCOMERCIAL Quito

Nombre	Dirección IP	Etiqueta	Switch	Modelo
PCO_101	X.Y.64.101	SW101C	Cisco Catalyst 3550	3550
PCO_231	X.Y.64.231	SW221C	Cisco Catalyst 3500	3524
PCO_232	X.Y.64.232	SW222C	Cisco Catalyst 3500	3524
PCO_121	X.Y.64.121	SW121C	Cisco Catalyst 3500	3524
PCO_122	X.Y.64.122	SW122C	Cisco Catalyst 3500	3524
PCO_129	X.Y.64.129	SW129C	Cisco Catalyst 2900	2924
PCO_201	X.Y.64.201	SW201C	Cisco Catalyst 3500	3524
PCO_221	X.Y.64.221	SW219C	Cisco Catalyst 2900	2924
PCO_150	X.Y.64.150	SW150C	Cisco Catalyst 4500	4507
PCO_151	X.Y.64.151	SW151C	Cisco Catalyst 3550	3550
PCO_171	X.Y.64.171	SW171C	Cisco Catalyst 3500	3524
PCO_181	X.Y.64.181	SW181C	Cisco Catalyst 3500	3524
PCO_189	X.Y.64.189	SW189C	Cisco Catalyst 2900	2924
PCO_191	X.Y.64.191	SW199C	Cisco Catalyst 2900	2912

Cuadro 3.4 : Switches IBM y 3COM de PETROCOMERCIAL Quito

Nombre	SWITCH	Modelo
SW102I	IBM 10/100	8271-E24
SW111I	IBM 10/100	8271-E24
SW182I	IBM 10/100	8271-E24
SW112T	3COM 10/100	8 puertos
SW131T	3COM 10/100	8 puertos
SW191T	3COM 10/100	8 puertos
SW201T	3COM 10/100	8 puertos
SW202T	3COM 10/100	8 puertos
SW231T	3COM 10/100	8 puertos

Como se detalla anteriormente, se trata de un considerable número de equipos de conmutación por lo que es esencial en el rediseño de la red local se plantee un modelo que logre obtener el mayor rendimiento posible de los recursos existentes en la empresa para plantear un diseño óptimo y efectivo.

3.4.2- i-Series y Servidores

Los i-Series existentes en la empresa en la actualidad son:

Cuadro 3.5 : i-Series de PETROCOMERCIAL Quito

Nombre	Capacidad Procesamiento (CPW)	Capacidad Memoria (Gb)	Capacidad Almacenamiento (Gb)	% Uso Alm.	Observaciones
PCO1	2800	6	211.692	58	
PCO2	750	2	140.660	74	
PCO3	1.000	2	140.660	34	Equipo de Respaldo

PCO8	1.250	4	352.586	65	Partición I
PCO9	220	2	211.692	20	Partición II

Los servidores existentes en la empresa en la actualidad son:

Cuadro 3.6 : Servidores de PETROCOMERCIAL Quito

Nombre	Aplicación	Software Instalado	Sistema Operativo	Modelo
PCOWEB	Servidor de Correo Externo	DB2 Conect Server, Internet Information Server	Windows 2003 Server	Compaq Proliant ML350
PCORED	Servidor de Correo interno	Internet Information Server	Windows 2000 Server	Compaq Proliant ML350
PCORED1	Aplicación SRI, Sistema de Oferentes, Auditoria	DB2 Conect Server, Office profesional, Internet information Server(Intranet)	Windows 2000 Server	IBM Netfinity 3500
PCORED4	TSM Client	Trivoli Storage Manager Server para Windows	Windows 2000 Server	IBM Netfinity 3500
PCORED7	Lotus Domino 6.5	Domino	Red Hat Enterprise Linux WS r3.1	Compaq Proliant ML350
PCORED11	Lotus Workflow, Lotus notes 7, I-Series Navigator	DB2 Connect Enterprise, Symantec Antivirus,Domino	Windows 2003 Enterprise Server R2 SP1	IBM HS21 Type 8853

PCORED12	Servidor de Impresión	Windows Server Update Services, Antivirus Symantec	Windows 2003 Enterprise Server R2 SP1	IBM HS21 Type 8853
PCORED13	IBM Websphere Aplication, Portal y Process Server V6	IBM DS400 FastStorage, Java,Symantec,VNC	Windows 2003 Enterprise Server R2 SP1	IBM HS21 Type 8853
PCORED14	IBM Rational Portofolio Manager	DB2 Enterprise Edition	Windows 2003 Enterprise Server R2 SP1	IBM HS21 Type 8853
PCORED16	Ambiente de pruebas de desarrollo de IBM Websphere Portal	IBM Websphere Portal versión 6.0	Windows 2003 Enterprise Server R2 SP1	IBM HS21 Type 8853
PCORED01	DNS, DHCP, Silecpro	DB2 Connect,Active Directory,Internet Information Server	Windows 2003 R2 Server Standard Edition SP1	Dell Power Edge 2850
PCORED02	IBM HTTP Server Rational Clear Case	IBM DB2 Enterprise Edition Websphere, VNC	Windows Server 2003 SP1	Dell Power Edge 2850
PCORED03	PcoRed03V1, PcoRed03V2, PcoRed03V3	ESX (Virtualización)	Red Hat Enterprise Linux ES R3	Dell Power Edge 2850

PCORED04	PcoRed04V1,PcoRed 04V2,PcoRed04V3	ESX (Virtualización): LinuxRHE3.0, LinuxRH4.0	Windows Server 2003 SP1	Dell Power Edge 2850
PCORED05	Symantec System Center	Symantec Antivirus, Easy CD Creator, VNC	Windows 2003 R2 Server Standard Edition SP1	Dell Power Edge 2850

Al igual que en el caso anterior respecto a los equipos de conmutación, se trata de una considerable cantidad de servidores en la organización, por lo que será necesario plantear un diseño que facilite el acceso cada uno de los servidores por parte de los usuarios autorizados respectivamente, conservando ante todo la protección de la información.

3.4.3- Central Telefónica IP MITEL

La Plataforma Integrada de Comunicaciones (ICP) 3300 de Mitel es una solución Voz sobre IP de alta capacidad con características superiores en cuanto a la calidad de voz, siendo una solución ideal para el sistema de comunicaciones de las medianas y grandes empresas.

El sistema 3300 ICP está compuesto de un controlador, una Unidad de Servicios Analógica (ASU) y una Unidad Universal de Servicios de Red (NSU).

El controlador es el núcleo de la central telefónica, este brinda voz, señalización, procesamiento central y los recursos de comunicaciones para el sistema 3300 ICP.

La Unidad de Servicios de Red (NSU) provee de conectividad a troncales [1]digitales para redes públicas o privadas.

La Unidad de Servicios Analógica (ASU) proporciona conectividad para troncales y teléfonos analógicos. Cada ASU tiene capacidad para cuatro troncales y 16 extensiones y se pueden conectar hasta 4 ASUs en el controlador.

La siguiente figura muestra el sistema 3300 ICP completo con todos los elementos antes indicados.

Figura 3.2: Sistema 3300 ICP

3.4.4- Computadores personales y Teléfonos IP

La red local de PETROCOMERCIAL Quito trabaja en base a dos servidores de DHCP, el primero es PCORED01 el cual es el servidor DHCP para los computadores personales de los usuarios, y el segundo es el servidor DHCP perteneciente a la Central Telefónica IP Mitel, el cual se encarga de asignar direcciones a los teléfonos IP.

La Central Telefónica se encuentra directamente conectada a la red local, es así que la transmisión de datos y de voz se la realiza mediante un solo punto de

[1] Troncal.- **Una troncal es** una línea telefónica que puede usarse para realizar llamadas al exterior del sistema de comunicaciones de la organización.

red. Es decir, los teléfono IP MITEL poseen un puerto dual[1] el cual le permite actuar como un switch, el teléfono IP al conectarse al switch de core por su primer puerto se identifica ante la central telefónica IP conectada al mismo, y se le asigna su respectiva dirección IP, luego por su segundo puerto deja pasar los datos hacia el computador pues este se encuentra conectado al teléfono IP y recibe la dirección IP que el servidor DHCP le asigne, como se explica en la siguiente figura:

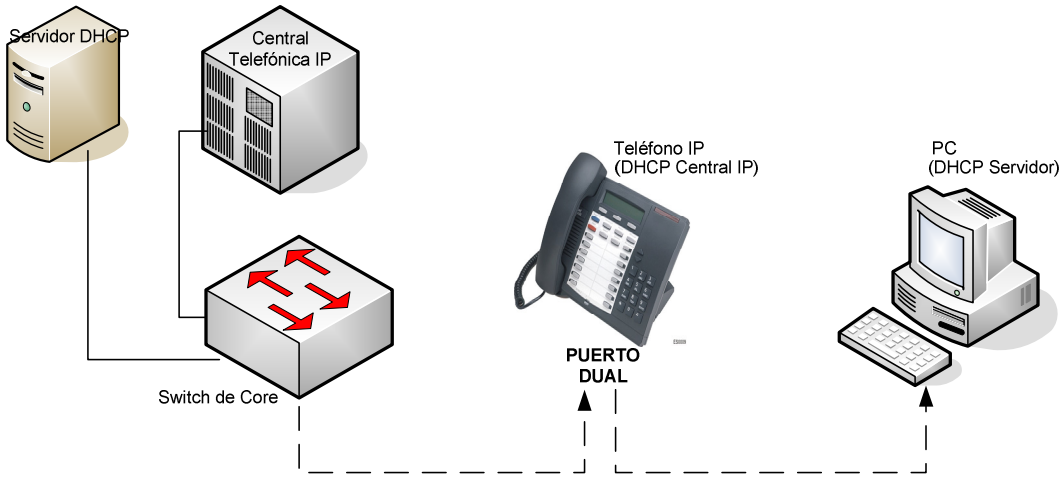

Figura 3.3: Funcionamiento de los computadores personales y teléfonos IP

Los computadores personales existentes en la empresa, por departamento son:

Cuadro 3.7 : Teléfonos IP de PETROCOMERCIAL Quito por departamentos

Departamento	No. PC's
Cuentas por pagar	4
Administración Financiera	10

[1] Puerto Dual.- El puerto dual de estos teléfonos IP son NICs fast ethernet duales, es decir que comprenden dos puertos y por lo tanto funcionan como un switch interno.

Secretaria General	8
Activos	7
Materiales	16
Seguros	5
Crédito y Cobranzas	8
Negocios propios	4
Abastecedora	20
Finanzas	5
Presupuesto	4
Gerencia	9
Subgerencia Comercia.	4
Comercializadora	14
Programación	6
Sistemas	29
lanificación Financiera	8
Redes y Telecomunicaciones	5
Vicepresidencia	15
Subgerencia de Transporte	12
Contabilidad	13
Subgerencia Administrativa	3
Recursos Humanos	9
Unidad Administrativa	2
Servicios Administrativos	11
Legal	17

Seguridad Física	4
Mantenimiento Eléctrico	1
Bodega-Materiales	2
Proyectos	11
Mantenimiento de Sistemas	9
Contratos	10
Bienestar Laboral	5
Relaciones Públicas	5
Control de Gestión	15
Recepción	1
TOTAL PC's	**311**

Es importante mencionar que los computadores personales de los usuarios de PETROCOMERCIAL Quito requieren del acceso a cualquiera de los servidores mencionados en los cuadros 3.5 y 3.6 , y de igual manera solicitan la comunicación con cualquier otro computador personal, dependiendo de los requerimientos específicos y de las funciones definidas de cada uno de los empleados, es decir que el flujo de datos no se limita a transmitirse entre usuarios de un mismo departamento, cualquier usuario debe ingresar a cualquier otro equipo de ser necesario, siempre y cuando este sea autorizado a hacerlo.

En cuanto a los teléfonos IP PETROCOMERCIAL Quito, maneja equipos marca MITEL, al igual que su central telefónica. Existen cinco diferentes tipos de versiones de teléfonos IP MITEL en la empresa, cada uno de ellos necesita de una licencia para ponerlos en producción. Menos del 10% de los equipos son de linea simple, lo que representa que no tienen un puerto dual y por tanto trabajan

independientemente y no tienen la capacidad de funcionar con un computador personal. Los tipos de teléfonos IP MITEL existentes en PETROCOMERCIAL Quito son:

Cuadro 3.8 : Tipos de teléfonos IP MITEL de PETROCOMERCIAL Quito

Versión	Tipo	No. Teléfonos IP
5001 IP	Single Line	16
5010 IP	Multi Line	85
5215 IP	Multi Line	62
5020 IP	Multi Line	50
5220 IP	Multi Line	3
TOTAL		**216**

Los teléfonos IP existentes en la empresa por departamento, en la actualidad son:

Cuadro 3.9 : Número de teléfonos IP MITEL de PETROCOMERCIAL Quito

Departamento	No.TeléfonosIP
Cuentas por pagar	4
Administración Financiera	8
Secretaria General	4
Activos	3
Materiales	12
Seguros	4
Crédito y Cobranzas	4
Negocios propios	2
Abastecedora	15

Finanzas	4
Presupuesto	3
Gerencia	4
Subgerencia Comercia.	2
Comercializadora	10
Programación	4
Sistemas	20
Planificación Financiera	5
Redes y Telecomunicaciones	5
Vicepresidencia	11
Subgerencia de Transporte	10
Contabilidad	8
Subgerencia Administrativa	3
Recursos Humanos	8
Unidad Administrativa	2
Servicios Administrativos	6
Legal	10
Seguridad Física	2
Mantenimiento Eléctrico	1
Bodega-Materiales	2
Proyectos	8
Mantenimiento de Sistemas	6
Contratos	9
Bienestar Laboral	3

Relaciones Públicas	3
Control de Gestión	10
Recepción	1
TOTAL TELEFONOS IP	**216**

La telefonía es un ente primordial para la organización y al ser una transmisión en tiempo real, es esencial que la transmisión de voz reciba prioridades ante la transmisión de datos.

Uno de los inconvenientes del diseño actual de la red es justamente la falta de priorización de la voz sobre los datos, puesto que actualmente el teléfono IP no identifica que señales pertenecen al mismo, en otras palabras el teléfono IP recibe un paquete de datos completo y posteriormente identifica su paquete de voz y el resto lo deja pasar, lo que provoca problemas en la transmisión de voz, como interferencias en las llamadas y baja calidad en la transmisión. El nuevo diseño debe plantear un modelo de la red que permita separar las señales de voz sobre las de datos, brindando alta calidad a la transmisión tanto de voz como de datos.

3.5- Proyeccion de Usuarios para PETROCOMERCIAL Quito

Actualmente la empresa no maneja un registro definido en cuanto al crecimiento anual de usuarios en la empresa. Es por ello que el análisis a continuación se lo ha realizado en base a valores aproximados dados por el área de Ingeniería y Procesamiento de la organización.

Es importante mencionar que el crecimiento anual es considerado de incremento normal, puesto que al tratarse de una entidad pública el número de empleados no presenta un amplio crecimiento.

El crecimiento anual de los últimos cinco años en PETROCOMERCIAL Quito es de un promedio aproximado del 3%, como se visualiza a continuación:

Tabla 3.2: Crecimiento anual de usuarios en los últimos cinco años en PETROCOMERCIAL Quito

AÑO	No.Usuarios	%Crecimiento
2003	469	
2004	481	2,495
2005	495	2,828
2006	512	3,320
2007	530	3,396
Promedio		**3,010**

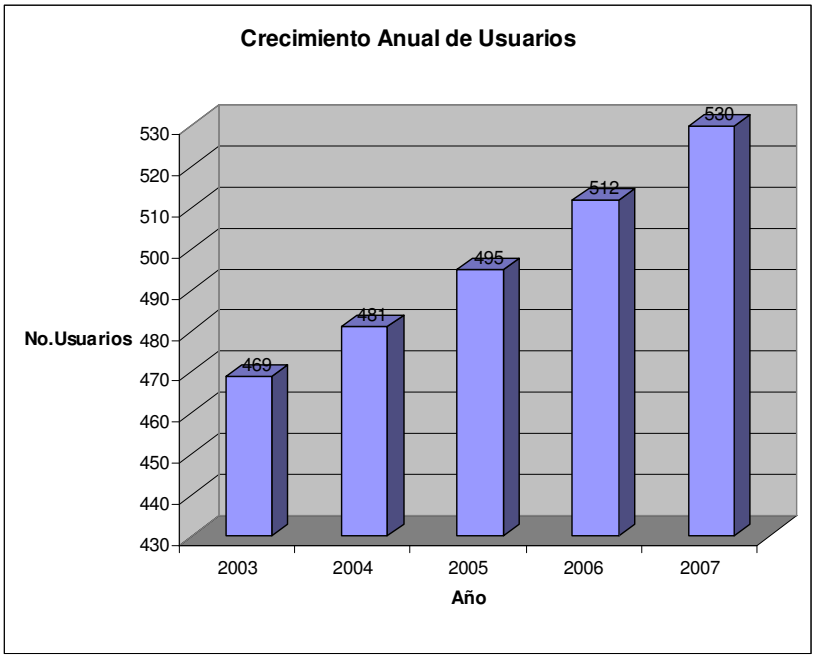

Figura 3.4: Crecimiento anual de Usuarios en los últimos cinco años en PETROCOMERCIAL Quito

Para la proyección de los próximos cinco años en PETROCOMERCIAL Quito se ha tomado un rango de crecimiento de solamente el 5%, más no del 10%, como se recomienda por las metodologías de diseño, puesto que por la situación específica de la empresa su crecimiento es limitado.

Es así que el número de usuarios que se espera en los proximos 5 años es el siguiente:

Tabla 3.3: Crecimiento anual de usuarios en los próximos cinco años en PETROCOMERCIAL Quito

AÑO	No. Usuarios
2008	557
2009	583
2010	610
2011	636
2012	663

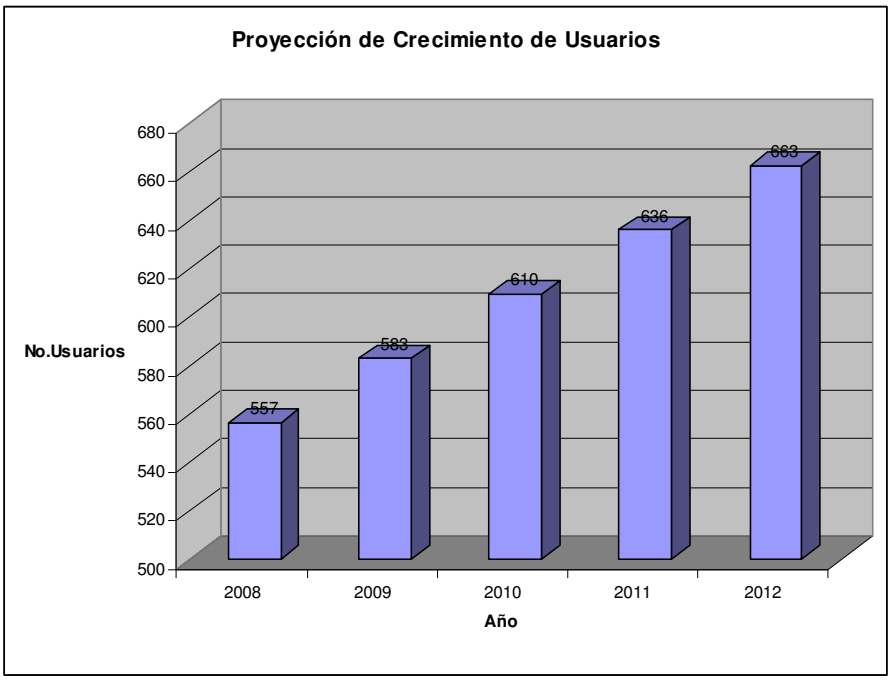

Figura 3.5: Crecimiento anual de Usuarios en los próximos cinco años en PETROCOMERCIAL Quito

Podemos concluir entonces que la red IP de PETROCOMERCIAL Quito debe diseñarse para responder a las futuras necesidades de la empresa como es el incremento de usuarios internos, que para este caso particular se restringe a un 5%.

3.6- Opiniones de los Usuarios de la Red IP

Con el fin de analizar el estado de la Red IP de PETROCOMERCIAL Quito desde la perspectiva del usuario final se diseño una encuesta, cuyo objetivo fue el de investigar el nivel de efectividad actual en la empresa tanto en la red de datos como en la red de voz. La encuesta planteada se muestra en el anexo B.

Esta encuesta fue aplicada al 10% del número de usuarios actuales de PETROCOMERCIAL Quito, siendo el número total 530 usuarios, se efectuó entonces 50 encuestas.

Los resultados obtenidos fueron los siguientes:

En cuanto a la velocidad del acceso al Internet un alto porcentaje de los usuarios considera al servicio como bueno simplemente, otro grupo de similar tamaño califica al servicio como muy bueno, seguido de una minoria que lo califica de excelente y finalmente menos del 12% cree que el servicio es malo y pésimo, como se visualiza a continuación:

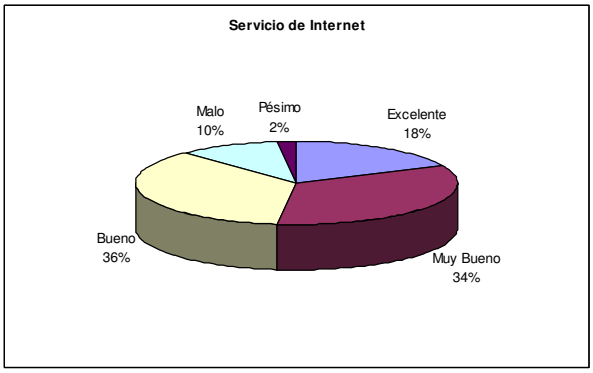

Figura 3.6: Eficiencia del servicio de Internet en la Empresa

El servicio de correo eléctrónico es calificado como muy bueno por la mayoria de los usuarios, otro porcentaje cercano lo considera como excelente y bueno. Menos de la décima parte piensa que el servicio es malo y pésimo. Estos datos se visualizan en la siguiente figura:

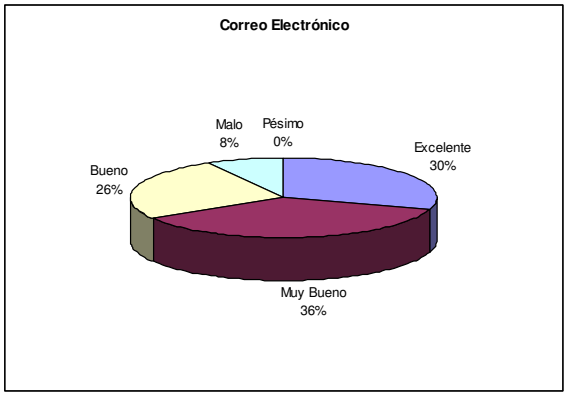

Figura 3.7: Eficiencia del servicio de correo electrónico en la Empresa

En relación al acceso a los Sistemas internos de PETROCOMERCIAL Quito (servidores e I-Series), casi la mitad de los usuarios considera al servicio como muy bueno, seguido de una cuarta parte que lo califica de bueno solamente. Menos de la cuarta parte cree que el acceso es excelente y menos del 10% lo estima como malo y pésimo, como se muestra en la siguiente figura:

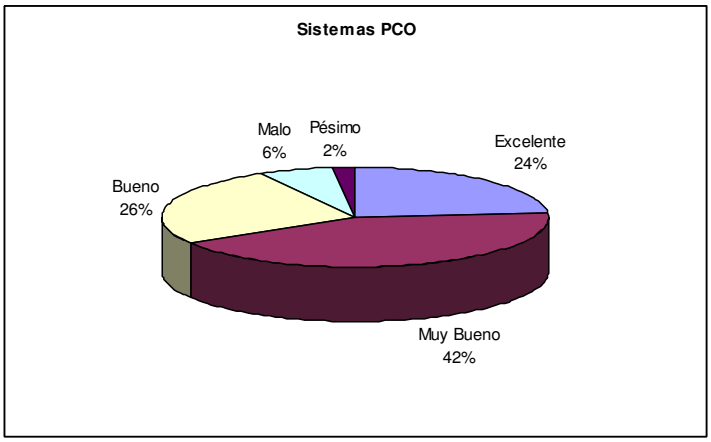

Figura 3.8: Eficiencia del los sistemas internos de PETROCOMERCIAL

Una mayoria de los usuarios considera como bueno al nivel de calidad de voz en las llamadas telefónicas IP, una cuarta parte lo califica de excelente y muy bueno. Una minoria del 10% lo considera malo y pésimo. A continuación se muestran los datos mencionados:

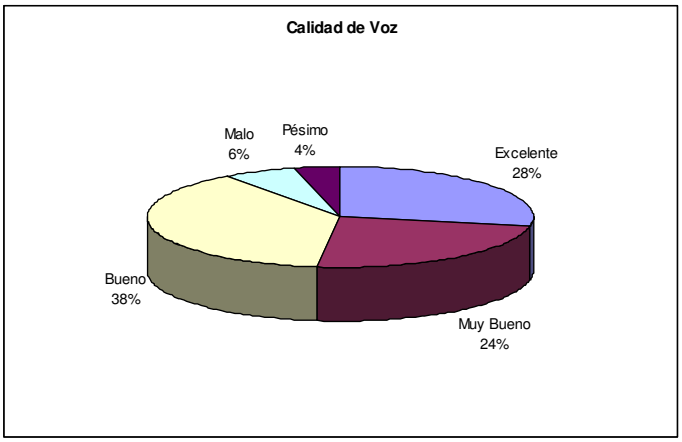

Figura 3.9: Nivel de la calidad de Voz

La periodicidad de problemas ocurridos en la red de datos es considerablemente alta puesto que casi la mitad de los usuarios cree que los inconvenientes en la red ocurren ocasionalmente. Una cuarta parte cree que existen problemas nunca y casi nunca, mientras que una minoria estima que suceden frecuentemente. La siguiente figura muestra lo explicado:

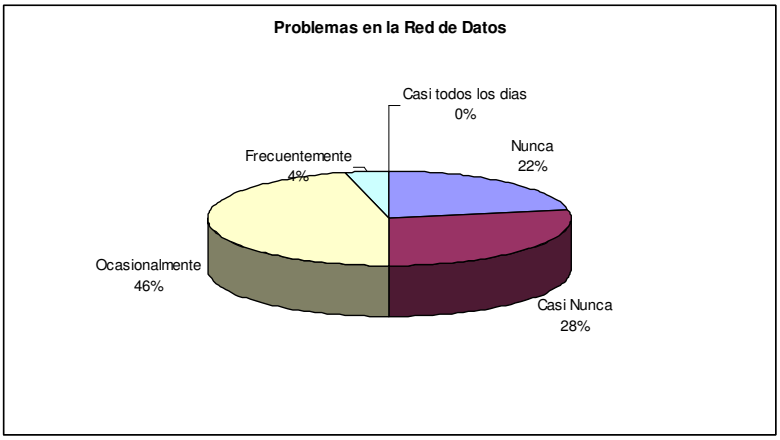

Figura 3.10: Periodicidad de Problemas en la red de datos

La periodicidad de problemas en la red de voz se da de manera similar al caso anterior. La mitad de los usuarios piensan que se sucitan problemas ocasionalmente, más de una cuarta parte considera que suceden casi nunca, una

minoría piensa que nunca ocurren estos problemas, y el 6% lo considera frecuente o de casi todos los días, como se muestra en la figura a continuación:

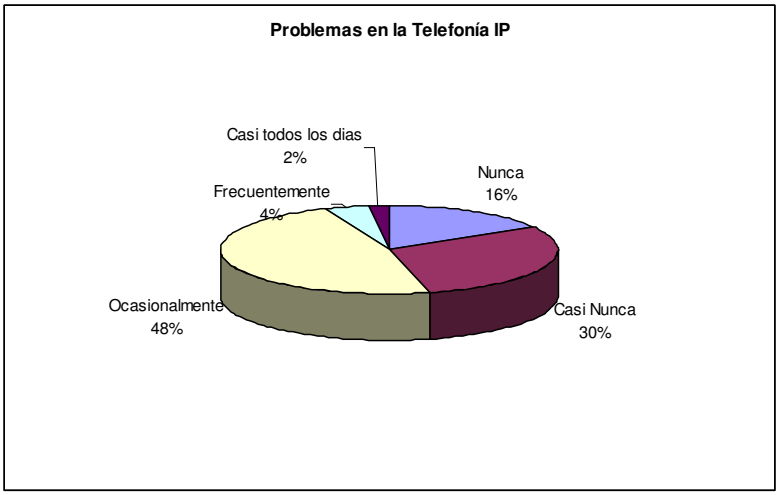

Figura 3.11: Periodicidad de problemas en la red de Voz

En base a la información analizada se deducen las siguientes conclusiones:

- ✓ Ninguno de los servicios prestados a través de la red IP es considerado de nivel excelente para los usuarios de la red.
- ✓ Una décima parte de los usuarios considera a todos los servicios como deficientes.
- ✓ Si bien la gran mayoria considera que los servicios son buenos no los califica como excelentes puesto que cree que existen problemas ocasionalmente y por tanto la red IP necesita mejoras.

3.7- Seguridad Perimetral de PETROCOMERCIAL Quito

La seguridad a nivel perimetral de PETROCOMERCIAL Quito comprende las siguientes conexiones:

ENLACE PCO-IMPSAT: Acceso a Internet (ISP Impsat)

ENLACE DMZ_PEC: Filiales de PetroEcuador (SOTE, PetroIndustrial)

ENLACE DMZ_Cli: Servicio de Rentas Internas (SRI) y Ministerio de Energia y Minas (DNH)

Clientes (Bancos)

ENLACE DMZ_SRV: Servidores PCO

La siguiente figura muestra las conexiones mencionadas:

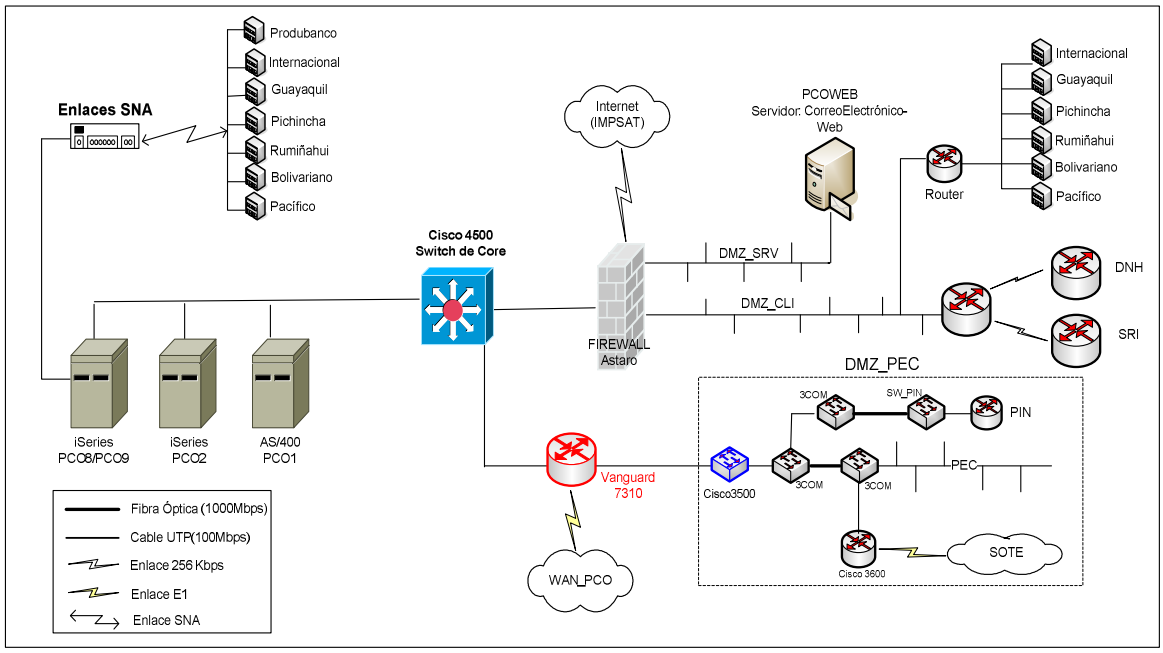

Figura 3.12: Seguridad Perimetral de PETROCOMERCIAL Quito

ENLACE PCO-IMPSAT

IMPSAT es el proveedor del acceso a Internet para PETROCOMERCIAL Quito. Este enlace consiste en la conexión a este ISP[1].

ENLACE DMZ_PEC

Este enlace corresponde a la conexión hacia el resto de filiales de PETROECUADOR. La conexión comprende el acceso a PETROINDUSTRIAL, y al Sistema de Oleoducto Trans-Ecuatoriano (SOTE).

[1] **ISP (Internet Service Provider):** Es un proveedor de servicios de Internet es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes, y brindar mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

ENLACE DMZ_Cli

Este enlace consiste en dos conexiones. La primera conexión es hacia el Servicio de Rentas Internas SRI y al Ministerio de Energía y Minas DNH. La otra conexión corresponde a los enlaces hacia las instituciones bancarias, quienes proveen su propio equipo para realizar la comunicación. La conexión hacia los bancos es esencial pues a través de ellos se realizan los servicios de facturación de la comercialización de combustibles.

Los bancos pertenecientes al enlace son:

- ✓ Banco Internacional
- ✓ Banco de Guayaquil
- ✓ Banco de Pichincha
- ✓ Banco Rumiñahui
- ✓ Banco del Pacífico
- ✓ Banco Bolivariano
- ✓ ProduBanco

Todas las instituciones bancarias anteriormente mencionadas poseen una comunicación SNA[1] con el servidor i-Series PCO8 para el proceso de facturación de combustibles.

ENLACE DMZ_SRV

Este enlace se refiere a la conexión hacia el servidor PCOWEB, el cual provee de correo electrónico externo y acceso a la página web de

[1] **SNA (Systems Network Architecture):** Es una arquitectura de red diseñada y utilizada por IBM para la conectividad con sus hosts o mainframe.Los bancos aún lo siguen utilizando por considerarlo más seguro que TCP/IP, es común que las redes de cajeros automáticos estén conectadas bajo SNA. SNA define los estándares, protocolos y funciones usadas por los dispositivos para permitirles la comunicación entre ellos en las redes SNA.

PETROCOMERCIAL. Esta página brinda información de los servicios de la empresa a nivel nacional e internacional.

3.7.1- Firewall ASTARO

Astaro Security Gateway, versión 6.0, es una solución completa de software y hardware para seguridad de redes, este provee varias aplicaciones de seguridad integradas en una sola plataforma de administración para así cumplir con las políticas empresariales de seguridad aumentando de esta manera la productividad general.

Las aplicaciones ya mencionadas permiten una mejor protección perimetral y control de acceso a la red, estas son:

- ✓ Firewall o cortafuegos
- ✓ Antivirus
- ✓ Filtrado de contenidos
- ✓ Protección contra Spyware
- ✓ Filtrado de Spam
- ✓ Protección contra Phishing
- ✓ Gateway de VPN
- ✓ IPS e IDS
- ✓ Surf Protection (Filtro URL)

La siguiente figura muestra las principales funcionalidades del equipo y su relación con los recursos de una empresa:

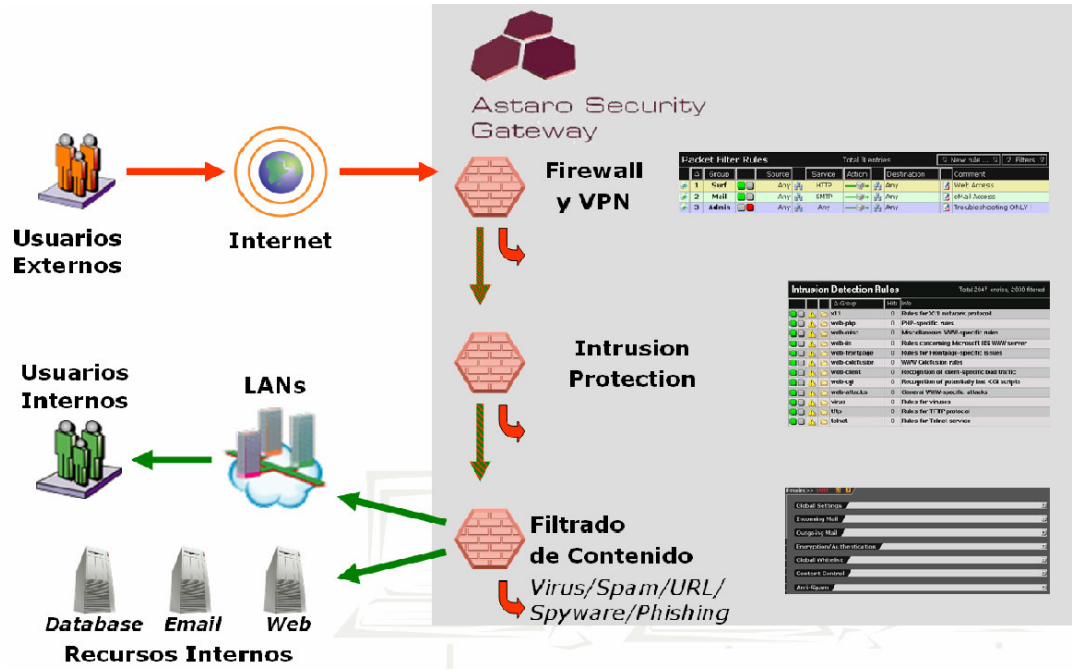

Figura 3.13: Seguridad Perimetral Astaro Security Gateway

Astaro Security Gateway provee de una herramienta de definición de políticas que permite a los usuarios configurar de manera sencilla al equipo en locaciones remotas. Esta configuración se la realiza mediante una interfaz web bastante amigable que permite realizar la administración y navegación mediante menús, botones y ayuda en línea. Astaro posee el servicio UP2DATE el cual proporciona de forma automática un mecanismo simple de actualización para toda la plataforma de seguridad. Las actualizaciones son descargadas automáticamente.

La configuración básica del sistema permite establecer el nombre del equipo y definir al o los administradores del equipo, los cuales serán continuamente notificados de cualquier inconveniente o de información relevante a través de sus correos electrónicos personales.

La configuración básica de red permite la creación de varios tipos de interfaces, definición de calidad de servicio sobre las interfaces del equipo, ruteo básico y dinámico, configuración de VLANs y servicio DHCP, entre las principales opciones.

Permite además la configuración de sesiones de administrador, puertos de conexión, autentificación de usuarios, NAT[1], recuperación de configuraciones mediante respaldos automáticos y acceso remoto.

Astaro cuenta también con un generador de reportes gráficos y estadísticos. Funciona en base a un motor de reportes de seguridad centralizado que recopila, correlaciona y analiza la información de seguridad.

Astaro brinda considerables beneficios de seguridad en relación al resto de soluciones de disponibles en el mercado, las principales ventajas de Astaro Securitu Gateway son:

- ✓ Capacidad de usuarios tras el firewall ilimitada.
- ✓ Capacidad para definición de políticas de seguridad y recursos ilimitada.
- ✓ Rendimiento de 1000 Mbps y hasta 265Mbps en VPNs.
- ✓ Brinda actualización automática de todos los sistemas de seguridad.
- ✓ Es de fácil administración a pesar de pertenecer a una plataforma Unix.
- ✓ Incluye sistema operativo.
- ✓ Alto número de aplicaciones de seguridad.

[1] **NAT** (**Network Address Translation**): Traducción de dirección de red es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. Su uso más común es permitir utilizar direcciones privadas y aún así proveer conectividad con el resto de Internet.

- ✓ Disponible como software para ser instalado en una PC, o preinstalado en equipos dedicados listos para operar.
- ✓ Permite respaldos automáticos en caso de fallas de red o de hardware.
- ✓ Balanceo de carga incrementado.
- ✓ Es un miembro activo de la comunidad de código abierto.
- ✓ Es una solución de seguridad de alta calidad y de bajo presupuesto.
- ✓ Ofrece entre sus aplicaciones de seguridad todas las soluciones de mayor importancia ante los riesgos informáticos de cualquier empresa.

3.7.2- Políticas de Seguridad de PETROCOMERCIAL Quito

Las políticas de seguridad de PETROCOMERCIAL Quito están definidas en base a su equipo de seguridad perimetral ASTARO, mencionado anteriormente.

Antes de esta plantear las políticas de seguridad existentes, es necesario establecer los recursos que se administran a a través del equipo de seguridad, el cual cuenta con cuatro tipos de recursos, detallados a continuación:

- ✓ **Redes**

  Estos recursos definen rangos de direccionamiento IP que incluyen al host, grupo o grupos que se requieran, para que posteriomente este pueda ser utilizado en la determinación de una política de seguridad.

- ✓ **Servicios**

  En la determinación de servicios se establecen los puertos de acceso y el protocolo a través de los cuales se permitirá o negará el acceso a una red,

ya sea de origen o de destino. El equipo cuenta ya con los principales puertos ya registrados como son: **FTP**, puerto 20-21; **DNS**, puerto 53, **HTTP**, puerto 80; entre otros. Sin embargo se pueden definir nuevos servicios de acuerdo a los requerimientos que surjan en la empresa, permitiendo crear inclusive un servicio que conste de multiples puertos en el caso de ser necesario.

- ✓ **Usuarios**

  La designación de usuarios se refiere a quienes serán los administradores del equipo de seguridad. Se definen los atributos de los administradores, estableciendo los permisos de acceso para cada uno de ellos.

- ✓ **Eventos**

  Los eventos o también denominados eventos de tiempo, permiten establecer permisos a cualquiera de las redes definidas para realizar alguna actividad y esto se lo establece por rangos de tiempo. Este tipo de recurso es opcional para la definición de una política de seguridad.

3.7.2.1- Recurso Redes

A continuación se definiden las redes establecidas en el Firewall ASTARO de PETROCOMERCIAL Quito, las cuales fueron creadas en base a las necesidades de la empresa:

Cuadro 3.10 : Redes definidas en el firewall de PETROCOMERCIAL Quito

Nomenclatura	Contenido	Descripción
Acc_Grp_PcoRed01	BCO_Bol_Net	Acceso al Servidor de Producción WEB Services
	BCO_Pch_Net1	
Acc_Grp_PcoRed13	BCO_Gye_Hst _Des	Acceso al Servidor de Desarrollo WEB Services
	BCO_Pch_Net1	
BCE_GRP_Hst	BCE_Srv_A.B.254.19	Grupo de Servidores del Banco Central del Ecuador
	BCE_Srv_A.B.254.20	
BCE_Net_192.168.254.16	A.B.254.16/29	Red del Banco Central del Ecuador
BCE_Srv_192.168.254.19	A.B.254.19	Servidor del Banco Central del Ecuador
BCE_Srv_192.168.254.20	A.B.254.20	Servidor del Banco Central del Ecuador
BCO_Bol_Net	A.B.28.14	Banco Bolivariano
BCO_Bol_Net1	A.B.28.0/27	Red de Banco Bolivariano
BCO_Gye_Grup	BCO_Gye_Hst	Grupo de Servidores del Banco de Guayaquil
BCO_Gye_Hst	X.Z.64.118	Banco de Guayaquil Host Producción
BCO_Gye_Hst _Des	A.B.102.54	Banco de Guayaquil Host Desarrollo
BCO_Gye_Net	A.B.102.0/26	Banco de Guayaquil Red Desarrollo
BCO_Pac_Grup	BCO_Pac_Hst_189	Banco del Pacifico Grupo de monitoreo ICMP
	BCO_Pac_Hst_242	
	BCO_Pac_Hst_39	
	BCO_Pac_Hst_40	

	BCO_Pac_Hst_70		
	BCO_Pac_Net		
BCO_Pac_Hst_189	n.1.218.189		Banco del Pacifico Servidor de Producción
BCO_Pac_Hst_242	n.1.231.242		Banco del Pacifico Monitoreo ICMP
BCO_Pac_Hst_39	n.1.213.39		Banco del Pacifico Desarrollo
BCO_Pac_Hst_40	n.1.213.40		Banco del Pacifico Desarrollo
BCO_Pac_Hst_70	n.5.218.70		Banco de Pacifico Monitoreo ICMP
BCO_Pac_Net	n.1.0.0/16		Banco del Pacifico
BCO_Pch_Grup	BCO_Pch_Hst_190		Grupo de host del Banco del Pichincha
	BCo_Pch_Hst_239		
	BCO_Pch_Net1		
BCO_Pch_Hst_190	n.0.151.190		Host del Banco del Pichincha
BCo_Pch_Hst_239	n.0.92.239		
BCO_Pch_Net1	200.31.27.32/27		Red del Banco del Pichincha
Broadcast_Group	**DMZ_Cli (Broadcast)**		**Grupo de Interfaces**
	DMZ_Pec (Broadcast)		
	DMZ_SRV (Broadcast)		
	External (Broadcast)		
	Internal (Broadcast)		
DMZ_Cli (Address)	BCO_Bol_Net	*X.Y.15.1*	Dirección de la interface 'DMZ_Cli'
DMZ_Cli (Broadcast)		*X.Y.15.31*	Dirección de Broadcast de la interface 'DMZ_Cli'
DMZ_Cli (Network)		*X.Y.15.0/27*	Dirección de Red de la interface 'DMZ_Cli'
DMZ_Cli_WEB_COM (Address)		*X.Y.15.3*	Dirección de la interface 'DMZ_Cli_WEB_COM'
DMZ_Cli_WEB_COM (Broadcast)		*X.Y.15.31*	Dirección de Broadcast de la interface 'DMZ_Cli_WEB_COM'
DMZ_Cli_WEB_COM (Network)		*X.Y.15.0/27*	Dirección de red de la interface 'DMZ_Cli_WEB_COM'
DMZ_Cli_WEB_COM1 (Address)		*X.Y.15.4*	Dirección de la interface 'DMZ_Cli_WEB_COM1'

DMZ_Cli_WEB_COM1 (Broadcast)		*X.Y.15.31*	Dirección de broadcast de la interface 'DMZ_Cli_WEB_COM1'
DMZ_Cli_WEB_COM1 (Network)		*X.Y.15.0/27*	Dirección de red de la interface 'DMZ_Cli_WEB_COM1'
DMZ_Pec (Address)		*X.Z.230.12*	Dirección de la interface 'DMZ_Pec'
DMZ_Pec (Broadcast)		*X.Z.230.255*	Dirección de Broadcast de la interface 'DMZ_Pec'
DMZ_Pec (Network)		*X.Z.230.0/24*	Dirección de red de la interface 'DMZ_Pec'
DMZ_SRV (Address)		*X.Y.10.1*	Dirección de la interface 'DMZ_SRV'
DMZ_SRV (Broadcast)		*X.Y.10.255*	Dirección de Broadcast en la interface 'DMZ_SRV'
DMZ_SRV (Network)		*X.Y.10.0/24*	Dirección de red en la interface 'DMZ_SRV'
External (Address)		*201.234.84.66*	Dirección de la interface Externa
External (Broadcast)		*201.234.84.79*	Dirección de Broadcast de la interface Externa
External (Network)		*201.234.84.64/28*	Dirección de red de la interface Externa
External_Mail_Web (Address)		*201.234.84.67*	Dirección de la interface 'External_Mail_Web'
External_Mail_Web (Broadcast)		*201.234.84.79*	Dirección de Broadcast de la interface 'External_Mail_Web'
External_Mail_Web (Network)		*201.234.84.64/28*	Dirección de red en la interface 'External_Mail_Web'
Internal (Address)		*X.Y.64.6*	Dirección de la interface Interna
Internal (Broadcast)		*X.Y.71.255*	Dirección de Broadcast de la interface Interna
Internal (Network)		*X.Y.64.0/21*	Dirección de red de la interface Interna
Internal_7 (Address)		*X.Y.64.7*	Dirección de segunda interface Interna
Internal_7 (Broadcast)		*X.Y.71.255*	Dirección de Broadcast de la interface 'Internal_7'
Internal_7 (Network)		*X.Y.64.0/21*	Dirección de red de la interface 'Internal_7'

IPSEC-Pool	n.160.145.0/24	Autogenerado randomicamente IPSEC-Pool network.
MEM_Grp_Hst	MEM_Hst_X.Z.2.12	Grupo Host UIO-MEM, grupo de usuarios del Ministerio de Energía y Minas para el acceso al AS_400 PETROINDUSTRIAL (I-Series)
	MEM_Hst_X.Z.3.177	
	MEM_Hst_X.Z.3.185	
	MEM_Hst_X.Z.3.240	
	MEM_Hst_X.Z.Z.23	
	MEM_Hst_X.Z.4.6	
MEM_Grp_Net	MEM_Net_X.Z.2.0	
	MEM_Net_X.Z.16.0	
	MEM_Net_X.Z.4.0	
MEM_GRP_SRV	MEM_Srv_X.Z.1.1	Grupo de Servidores de Mail
	MEM_Srv_X.Z.1.20	
	MEM_Srv_X.Z.1.5	
	MEM_Srv_X.Z.1.8	
	MEM_Srv_X.Z.1.9	
	MEM_Srv_X.Z.3.218	
MEM_Hst_X.Z.2.12	X.Z.2.12	Host UIO-MEM para el acceso al AS_400 PETROINDUSTRIAL
MEM_Hst_X.Z.3.177	X.Z.3.177	Host UIO-MEM para el acceso al AS_400 PETROINDUSTRIAL
MEM_Hst_X.Z.3.185	X.Z.3.185	Host UIO-MEM para el acceso al AS_400 PETROINDUSTRIAL
MEM_Hst_X.Z.3.240	X.Z.3.240	Host UIO-MEM para el acceso al AS_400 PETROINDUSTRIAL
MEM_Hst_X.Z.Z.23	X.Z.16.23	Host de Libertad
MEM_Hst_X.Z.20.25	X.Z.20.25	Host Desde MEM GYQ A AS_400(20070223 Guido)
MEM_Hst_X.Z.20.46	X.Z.20.46	Host Desde MEM GYQ A AS_400(20070223 Guido)
MEM_Hst_X.Z.20.49	X.Z.20.49	Host Desde MEM GYQ A AS_400(20070223 Guido)
MEM_Hst_X.Z.20.6	X.Z.20.6	Host Desde MEM GYQ A AS_400(20070223 Guido)

MEM_Hst_X.Z.4.6	X.Z.4.6	Host de Refineria Esmeraldas (20070119 MPCJ)
MEM_Hst_X.20.167.99	X.Y.167.99	Host de Pascuales MEM(20070528 MPCJ)
MEM_Net_X.Z.1.0	X.Z.1.0/24	Red del Ministerio para el acceso al AS_400 PCO8
MEM_Net_X.Z.2.0	X.Z.2.0/24	Red del Ministerio para el acceso al AS_400 PCO8
MEM_Net_X.Z.3.0	X.Z.3.0/24	Red del Ministerio para el acceso a los AS_400 PETROINDUSTRIAL
MEM_Net_X.Z.16.0	X.Z.16.0/24	Red de Libertad
MEM_Net_X.Z.20.0	X.Z.20.0/26	Red del MEM GYE
MEM_Net_X.Z.4.0	X.Z.4.0/24	Red de Refineria Esmeraldas
MEM_Net_X.22.1.0	X.22.1.0/24	Red del Ministerio para el acceso al AS_400 PCO8
MEM_Rt_X.Y.15.30	X.Y.15.30	Router para conectarce al MEM
MEM_Srv_X.Z.1.1	X.Z.1.1	Servidor Linux Proxy MEM
MEM_Srv_X.Z.1.20	X.Z.1.20	MEM Servidor Oracle
MEM_Srv_X.Z.1.5	X.Z.1.5	MEM Servidor Oracle
MEM_Srv_X.Z.1.8	X.Z.1.8	MEM Servidor DOMINO
MEM_Srv_X.Z.1.9	X.Z.1.9	MEM Servidor Oracle
MEM_Srv_X.Z.3.218	X.Z.3.218	MEM Host Fran Cedeno
Net_Bco_Int	A.B.16.0/24	Red Banco Internacional
Net_Ptrs_BCE_Grp	PCO_Hst_GRN_130.24	
	PCO_Hst_GRN_134.72	
	PCO_Hst_GRN_134.81	
	PCO_Hst_GRS_132.34	
	PCO_Hst_GRS_132.37	
	PCO_Net_Gye_Grace	
	PCO_Net_Host_UIO-PCO	
	PIN_Net_X.Z.Z.0	
PCO_Grp_Cli_Bcos	PCO_Hst_Cli_Bol	Bancos Aplicación WEB Comercialización
	PCO_Hst_Cli_Gua	

	PCO_Hst_Cli_Int	
	PCO_Hst_Cli_Pac	
	PCO_Hst_Cli_Pic	
	PCO_Hst_Cli_Pro	
	PCO_Hst_Cli_Rum	
PCO_Grp_Srv_AS_400	PCO_Srv_As_PCO1	Servidores AS/400 de PETROCOMERCIAL
	PCO_Srv_As_PCO2	
	PCO_Srv_As_PCO3	
	PCO_Srv_As_PCO8	
	PCO_Srv_As_PCO9	
PCO_Grp_Srv_Audit	PCO_Srv_Pcored1	Servidores de UIO y GYE que tienen la aplicacion audit.
	PCO_Srv_Pcored11	
	PCO_Srv_PCOSUR	
	PCO_Srv_PCOSUR1	
PCO_Grp_Srv_Web_COM	PCO_Srv_As_PCO1	Servidores Web de Comercializacion (Websphere)
	PCO_Srv_Pcored13	
PCO_Hst_Cli_Bol	X.Y.15.15	Banco Bolivariano
PCO_Hst_Cli_Gua	X.Y.15.11	Banco de Guayaquil
PCO_Hst_Cli_Int	X.Y.15.10	Banco Internacional
PCO_Hst_Cli_Pac	X.Y.15.16	Banco Pacifico
PCO_Hst_Cli_Pic	X.Y.15.13	Banco Pichincha
PCO_Hst_Cli_Pro	X.Y.15.12	Produbanco
PCO_Hst_Cli_Rum	X.Y.15.14	Banco Rumiñahui
PCO_Hst_GRN_130.24	X.Y.130.34	Host de la GRN-AMB Acceso BCE
PCO_Hst_GRN_134.32	X.Y.134.32	Host de la Gasolinera GRN-UIO Acceso Autotrac

PCO_Hst_GRN_134.72	X.Y.134.72	Host de la Gasolinera GRN-UIO Acceso BCE
PCO_Hst_GRN_134.81	X.Y.134.81	Host de la Gasolinera GRN-UIO Acceso BCE
PCO_Hst_GRN_15.25	X.Y.15.25	
PCO_Hst_GRN_SIP_11.Y	X.Y.11.Y	Pruebas F. Tapia
PCO_Hst_GRN_SIP_127	X.Y.64.127	Ingenieria y Procesamiento Pruebas
PCO_Hst_GRN_SIP_128	X.Y.64.128	Ingenieria y Procesamiento Pruebas
PCO_Hst_GRN_SIP_129	X.Y.64.129	Ingenieria y Procesamiento
PCO_Hst_GRN_SSTJR	X.Y.64.246	Soporte Técnico
PCO_Hst_GRN_SSTJR1	X.Y.64.Y9	Soporte Técnico - Actualizaciones
PCO_Hst_GRS_132.34	X.Y.132.34	Host de Cuenca para ingresar al BCE
PCO_Hst_GRS_132.37	X.Y.132.37	Host de Cuenca para ingresar al BCE
PCO_Hst_GRS_GSI	X.Y.97.40	Sistemas
PCO_Net_Ambato	X.Y.130.0/24	Red de Ambato
PCO_Net_Beaterio	X.Y.129.0/24	Red del Beaterio
PCO_Net_Chalpi	X.Y.139.0/24	Red de Chalpi
PCO_Net_ChalpiV	X.Y.135.0/24	Red de chalpi por Vanguard
PCO_Net_Corazon	X.Y.77.0/24	Red de Corazon
PCO_Net_Corazon1	X.Y.160.0/24	Red de Corazon Provisional en SEDE PETROECUADOR
PCO_Net_Cuenca	X.Y.132.0/24	Red de Cuenca
PCO_Net_EC	X.Y.0.0/16	Red de Petrocomercial
PCO_Net_Ecuafuel GYE	X.Y.170.0/24	Red de Ecuafuel Guayaquil
PCO_Net_Ecuafuel UIO	X.Y.75.0/24	Red de Ecuafuel Quito
PCO_Net_EsmCab	X.Y.163.0/24	Red de Esmeraldas Cabecera
PCO_Net_EsmSuc	X.Y.164.0/24	Red de Esmeraldas Sucursal
PCO_Net_Faisanes	X.Y.141.0/24	Red de Faisanes
PCO_Net_Gal_Btr	X.Y.171.128/26	Red de Galapagos Baltra
PCO_Net_Gal_PtoAyr	X.Y.171.0/26	Red de Galapagos Pto. Ayora
PCO_Net_Gye_Grace	X.Y.97.0/24	Red de Guayaquil Ed. Grace
PCO_Net_Gyq_Ecuafuel	X.Y.171.64/26	Red de Ecuafuel
PCO_Net_Host_GYE-PEC	X.Y.97.0/25	Red de Host Especiales para Aplicaciones PETROECUADOR

PCO_Net_Host_UIO-PCO	X.Y.64.64/26	Red de Host Especiales para Aplicaciones PETROECUADOR
PCO_Net_Libertad	X.Y.165.0/24	Red de Libertad
PCO_Net_Loja	X.Y.133.0/24	Red de Loja
PCO_Net_Manta	X.Y.169.0/24	Red de Manta
PCO_Net_Osayacu	X.Y.136.0/24	Red de Osayacu
PCO_Net_Oyamboro	X.Y.76.0/24	Red de Oyambaro
PCO_Net_Pascuales	X.Y.167.0/24	Red de Pascuales
PCO_Net_Quijos	X.Y.140.0/24	Red de Quijos
PCO_Net_Riobamba	X.Y.131.0/24	Red de Riobamba
PCO_Net_Shushu_Sucursal	X.Y.138.0/24	Red de Shushufindi Sucursal
PCO_Net_Shushufindi_Cabecera	X.Y.137.0/24	Red de Shushufindi Cabecera
PCO_Net_Srv_Sis	X.Y.64.0/27	Red de Servidores del Rocio
PCO_Net_SST	X.Y.64.252/30	Maquinas para download de Software
PCO_Net_StoDgo	X.Y.161.0/24	
PCO_Net_UIO	X.Y.64.0/21	Red Quito
PCO_Net_UIO_Esp	X.Y.68.0/29	IP's limitar acceso HTTP
PCO_Net_UIO_Gasolinera	X.Y.134.0/24	Red de Gasolinera
PCO_Net_XXX	X.Y.11.0/24	Red pruebas aplicaciones software
PCO_Rout_64.11	X.Y.64.11	Router UIO
PCO_Rout_64.3	X.Y.64.3	Router UIO-Andinatel
PCO_Srv_As_PCO1	X.Y.64.25	iSeires PCO1
PCO_Srv_As_PCO2	X.Y.64.26	iSeires PCO2
PCO_Srv_As_PCO3	X.Y.170.145	iSeires PCO3
PCO_Srv_As_PCO8	X.Y.64.28	iSeires PCO8
PCO_Srv_As_PCO9	X.Y.64.29	iSeires PCO9
PCO_Srv_Mail_Int	PCO_Srv_PCOSUR1	Servidores de Mail
	PCO_Srv_UIO_Mail	
PCO_Srv_Pcored01	X.Y.64.21	Servidor DHCP-DNS Interno
PCO_Srv_Pcored02	X.Y.64.25	
PCO_Srv_Pcored03V1	X.Y.64.66	Servidor SUCO S.O. Linux R.H.
PCO_Srv_Pcored05	X.Y.64.35	Servidor Symantec AV

PCO_Srv_Pcored1	X.Y.64.21	
PCO_Srv_Pcored11	X.Y.64.41	Servidor SUCO S.O.Windows
PCO_Srv_Pcored12		Actualizaciones Microsoft
PCO_Srv_Pcored13	X.Y.64.43	Servidor Web Comercializacion Desarrollo
PCO_Srv_Pcored15	X.Y.64.15	Servidor de Base de Datos
PCO_Srv_PCOSUR	X.Y.97.21	Servidor PCOSUR
PCO_Srv_PCOSUR1	X.Y.97.Y	Servidor de Mail-Aplicaciones
PCO_Srv_UIO_Mail	X.Y.64.Y	Servidor de Mail Interno
PCO_Srv_Web	X.Y.10.2	Servidor Web direccion de la DMZ
PEC_Grp_Host_Sistemas	PEC_Hst_X.Z.144.145	PETROECUADOR Grupo de Host Sistemas
	PEC_Hst_X.Z.144.150	
	PEC_Hst_X.Z.144.182	
	PEC_Hst_X.Z.144.231	
	PEC_Hst_X.Z.144.245	
PEC_Grp_Net	PEC_Net_n.n.n.0	
	PEC_Net_X.Z.226.0	
PEC_Grp_Srv_SMTP	PEC_Srv_X.Z.226.16	
	PEC_Srv_X.Z.226.4	
PEC_Grp_Srv_Web	PEC_Srv_X.Z.226.21	PETROECUADOR Grupo de servidores WEB
	PEC_Srv_X.Z.226.22	
	PEC_Srv_X.Z.226.6	
PEC_Hst_n.n.n.15	n.n.n.15	PETROECUADOR Firewall
PEC_Hst_X.Z.144.145	X.Z.144.145	PETROECUADOR Host de Sistemas
PEC_Hst_X.Z.144.150	X.Z.144.150	
PEC_Hst_X.Z.144.182	X.Z.144.182	PETROECUADOR Host de Sistemas
PEC_Hst_X.Z.144.231	X.Z.144.231	PETROECUADOR Host de Sistemas
PEC_Hst_X.Z.144.245	X.Z.144.245	PETROECUADOR Host de Sistemas
PEC_Hst_226.4	X.Z.226.4	PETROECUADOR SPECLnx2

PEC_Hst_226.5	X.Z.226.5	PETROECUADOR dblinux
PEC_Net_n.n.n.0	n.n.n.0/24	PETROECUADOR Red para Servidores de las direc n.n.n.0
PEC_Net_X.Z.144.0	X.Z.0.0/16	PETROECUADOR Red para Host de Sistemas
PEC_Net_X.Z.226.0	X.Z.226.0/24	PETROECUADOR Red para Servidores
PEC_Rt_X.Z.230.10	X.Z.230.10	PETROECUADOR Router 36Y
PEC_Srv_X.Z.226.16	X.Z.226.16	PETROECUADOR Srv mail2
PEC_Srv_X.Z.226.17	X.Z.226.17	PETROECUADOR petroecuador.com.ec
PEC_Srv_X.Z.226.Z	X.Z.226.Z	PETROECUADOR Srv ORACLE
PEC_Srv_X.Z.226.21	X.Z.226.21	PETROECUADOR Srv Intranet
PEC_Srv_X.Z.226.22	X.Z.226.22	PETROECUADOR Srv Intranet
PEC_Srv_X.Z.226.4	X.Z.226.4	PETROECUADOR Srv Mail3
PEC_Srv_X.Z.226.5	X.Z.226.5	PETROECUADOR Srv SPETROECUADORInX3
PEC_Srv_X.Z.226.6	X.Z.226.6	PETROECUADOR Srv SPETROECUADORWin1
PEC_Srv_As_X.Z.226.24	X.Z.226.24	PETROECUADOR Srv Intranet
PEC_Srv_Base_Datos	PEC_Hst_226.5	PETROECUADOR Servidores de Base de Datos (MPCJ)
	PEC_Srv_X.Z.226.Z	
PIN_GRP_Hst	PIN_Hst_X.Z.24.103	PETROINDUSTRIAL Grupo Host que ingresan al MEM SICHOI
	PIN_Hst_X.Z.24.142	
	PIN_Hst_X.Z.24.148	
	PIN_Hst_X.Z.24.44	
PIN_Grp_Srv_AS	PIN_Srv_AS_Esm	Grupo de Servidores AS_400 PETROINDUSTRIAL
	PIN_Srv_AS_Lib	
	PIN_Srv_AS_Shu	
PIN_Hst_X.Z.24.103	X.Z.24.103	PETROINDUSTRIAL Host DNH
PIN_Hst_X.Z.24.142	X.Z.24.142	PETROINDUSTRIAL Host DNH, a pedido de N. Guzman 19-12-06

PIN_Hst_X.Z.24.148	X.Z.24.148		PETROINDUSTRIAL Host DNH, a pedido de N. Guzman 19-12-06
PIN_Hst_X.Z.24.44	X.Z.24.44		PETROINDUSTRIAL Host DNH
PIN_Net_X.Z.Z.0	X.Z.Z.0/24		
PIN_Net_X.Z.20.0	X.Z.20.0/24		PETROINDUSTRIAL-MEM (MPCJ 20061113)
PIN_Net_X.Z.24.0	X.Z.24.0/24		
PIN_Net_X.Z.28.0	X.Z.28.0/24		PETROINDUSTRIAL-MEM (MPCJ 20061113)
PIN_Net_Shushufindi	X.Z.16.0/24		
PIN_Rt_X.Z.230.14	X.Z.230.14		
PIN_Srv_AS_Esm	X.Z.20.12		Servidor AS_400 de Esmeraldas PETROINDUSTRIAL X.Z.20.12
PIN_Srv_AS_Lib	X.Z.28.11		Servidor AS_400 de PETROINDUSTRIAL Libertad
PIN_Srv_AS_Shu	X.Z.24.11		Servidor AS_400 de PETROINDUSTRIAL Shushufindi
PPTP-Pool	n.81.197.0/29		Autogenerado randomicamente PPTP-Pool network.
Soporte GMS	200.41.80.0/24		
SRI_GRP_SRV	SRI_Srv_n.1.7.n		
	SRI_Srv_n.1.7.8		
SRI_Net_n.1.7.0	n.1.7.0/28		
SRI_Srv_n.1.7.n	n.1.7.n		SRI Srv ORACLE
SRI_Srv_n.1.7.8	n.1.7.8		SRI Srv ORACLE
supportGMS (L2TP user)	Inactive		Autogenerado
supportGMS (PPTP user)	Inactive		Autogenerado
VPN_PCO_Bco_Pich_Ext	X.Y.15.13		VPN Petrocomercial Bco. Pichincha
VPN_PCO_Bco_Pich_Int	BCO_Pch_Net1		VPN Petrocomercial Bco. Pichincha
VPN_PCO_GMS_Ext	X.Y.15.2		
VPN_PCO_GMS_Int	192.168.2.51		
Web_Mail (Address)	Interface up	*201.234.84.78*	Dirección de la interface 'Web_Mail'
Web_Mail (Broadcast)	Interface up	*201.234.84.79*	Dirección de Broadcast de la interface 'Web_Mail'

Web_Mail (Network)	Interface up	*201.234.84.64/28*	Dirección de red de la interface 'Web_Mail'

3.7.2.2- Recurso Servicios

Una vez ya definidas las redes existentes en el equipo de seguridad, se muestran en el siguiente cuadro los servicios programados existentes en la actualidad:

Cuadro 3.11 : Servicios definidos en el firewall de PETROCOMERCIAL Quito

No.	Nombre	Protocolo	Puerto de origen	Puerto de Salida	Observaciones
1	**10000**	TCP/UDP	1:65535	**10000**	
2	**79**	TCP/UDP	1:65535	**79**	
3	**AUS**	TCP	1:65535	**222**	
4	**BD**	TCP	1:65535	**3050**	Base de Datos SUCO
5	**BGP**	TCP	1024:65535	**179**	
6	**CITRIX**	TCP	1024:65535	**1494**	
7	**DNS**	TCP/UDP	1:65535	**53**	
8	**EUDORA**	TCP	1024:65535	**106**	
9	**FTP**	TCP	1024:65535	**20:21**	
10	**FTP-CONTROL**	TCP	1024:65535	**21**	
11	**HBCI**	TCP	1024:65535	**3000**	
12	**http**	TCP	1024:65535	**80**	
13	**http-FTP**		FTP		
			HTTP		

14	**http-HTTPS**		HTTP		
			HTTP_9040		
			HTTPS		
			HTTPS_9446		
15	**http_8080**	TCP/UDP	1:65535	**8080**	
16	**http_8500**	TCP/UDP	1:65535	**8500**	
17	**http_9040**	TCP	1024:65535	**9040**	WEB Comercializacion
18	**http_9080**	TCP	1024:65535	**9080**	Businessobjects
19	**http_Mail**	TCP	1:65535	**8000**	Web Mail PCO
20	**http_WSUS**	TCP	8530	**1:65535**	WSUS
21	**HTTPS**	TCP	1024:65535	**443**	
22	**HTTPS_9446**	TCP	1024:65535	**9446**	WEB oferentes
23	**HTTPS_MEM**	TCP	442	**442**	HTTS Ministerio de Energia y Minas
24	**IDENT**	TCP	1024:65535	**113**	
25	**CITRIX**	TCP	1024:65535	**143**	
26	**IRC**	TCP	1024:65535	**6667:6668**	
27	**ISAKMP**	UDP	500	**500**	
28	**LDAP_TCP**	TCP	1024:65535	**389**	
29	**LDAP_UDP**	UDP	1024:65535	**389**	
30	**LOCAL_ALL**	TCP/UDP	1:65535	**1:65535**	
31	**LOTUSNOTES**	TCP	1024:65535	**1352**	
32	**Microsoft-SMB**	TCP/UDP	1:65535	**445**	
33	**Microsoft-SQL_Monitor**	TCP/UDP	1:65535	**1434**	
34	**Microsoft-SQL_Server**	TCP/UDP	1:65535	**1433**	
35	**Monitoreo_PCO_SRV**		ping-reply		
			ping-request		
			traceroute-udp		

36	**netbios-dgm**	TCP/UDP	138	**138**	
37	**netbios-ns**	TCP/UDP	137	**137**	
38	**netbios-ssn**	TCP/UDP	1024:65535	**139**	
39	**NEWS**	TCP	1024:65535	**139**	
40	**NNTP**	TCP	1024:65535	**119**	
41	**NTP**	UDP	123	**123**	
42	**NTP-Async**	UDP	1024:65535	**123**	
43	**Oracle**	TCP	1024:65535	**1522**	
44	**Oracle_SQL_NET**	TCP	1:65535	**1521**	
45	**Ping**		ping-reply		
			ping-request		
46	**ping-reply**	ICMP	[T00/C00] Ping: Echo reply		
47	**ping-request**	ICMP	[T00/C00] Ping: Echo reply		
48	**Platts**	TCP/UDP	1:65535	**1838**	
49	**POP3**	TCP	1:65535	**110**	
50	**POP3_MEM**	TCP	81	**81**	POP3 habilitado para el Ministerio de Energia y Minas
51	**PPTP**	TCP	1:65535	**1723**	
52	**RIP**	UDP	520	**520**	
53	**Servcio_MEM**		HTTPS_MEM		Servicios utilizados por el Ministerio de Energía y Minas
			LOTUSNOTES		
			Oracle_SQL_NET		
			ping-reply		
			ping-request		
			POP3_MEM		
			SMTP		

			traceroute-udp		
54	**Servicio_WEB_PEC**		HTTP-HTTPS		Servicios de HTTP para Petroecuador
			HTTP_8500		
			SQUID		
55	**Servicios Admin**		FTP		
			PPTP		
			Telnet		
56	**SMTP**	TCP	1:65535	**25**	
57	**SNMP**	UDP	1024:65535	**161**	
58	**SQUID**	TCP	1024:65535	**8080**	
59	**SSH**	TCP	1:65535	**22**	
60	**Sybase-SQL**	TCP/UDP	1:65535	**1498**	
61	**SYSLOG**	UDP	1024:65535	**514**	
62	**TCP_UDP_ALL**	TCP/UDP	1024:65535	**1:65535**	
63	**Telnet**	TCP	1024:65535	**23**	
64	**traceroute-udp**	UDP	1024:65535	**33000:34000**	
65	**TTL-exceeded**	ICMP	[T11/C00] TTL: TTL exceeded		
66	**VPN_GMS**	TCP/UDP	1:65535	**1723**	Acceso VPN A la Red GMS
67	**WHOIS**	TCP	1024:65535	**43**	
68	**WHOIS_PP**	TCP	1024:65535	**63**	
69	**XDMCP**	TCP	1024:65535	**177**	

3.7.2.3- Estado actual de las políticas de seguridad

Una vez establecidos todos los recursos primordiales, se pueden detallar las políticas de seguridad de PETROCOMERCIAL Quito. Se debe recalcar que las mencionadas políticas han sido determinadas en base a las necesidades de comunicación en la empresa pero tomando en cuenta los parámetros de seguridad que se han considerado apropiados.

Las políticas de seguridad de PETROCOMERCIAL Quito se detallan a continuación en el cuadro 3.12

Cuadro 3.12 : Políticas de Seguridad de PETROCOMERCIAL Quito

No.	Descripción del Recurso	Origen	Servicio	Política	Destino	Descripción
1	SRV_Web_Comercializ	PCO_Srv_As_PCO1	Todos los servicios	Permitir	X.Y.15.0/27 DMZ_Cli (Network)	Politica de Monitoreo
2	SRV_Web_Comercializ	Net_Bco_Int	http_9040	Permitir	PCO_Grp_Srv_Web_COM	Politica para el Acceso de los servidores del Banco Internacional hacia los servidores de aplicaciones de PCO
3	SRV_Web_Comercializ	BCO_Gye_Grup	http_9040	Permitir	PCO_Grp_Srv_Web_COM	Politica para el Acceso de los Servidores del Banco Guayaquil hacia los servidores de aplicaciones de PCO
4	SRV_Web_Comercializ	BCO_Bol_Net1	http_9040	Permitir	PCO_Grp_Srv_Web_COM	Politica para el Acceso de los servidores del Banco Bolivariano hacia los servidores de aplicaciones de PCO
5	SRV_Web_Comercializ	BCO_Pac_Grup	http_9040	Permitir	PCO_Grp_Srv_Web_COM	Politica para el Acceso de los servidores del Banco Pacifico hacia los servidores de aplicaciones de PCO
6	SRV_Web_Comercializ	BCO_Pch_Grup	http_9040	Permitir	PCO_Grp_Srv_Web_COM	Politica para el Acceso de los servidores del Banco Pichincha hacia los servidores de aplicaciones de PCO
7	SRV_Web_Comercializ	PCO_Srv_Pcored13	Todos los servicios	Permitir	DMZ_Cli	Politica desde el Servidor WAS de desarrollo hacia la rede DMZ CLIENTES BANCOS
8	SRV_Web_Comercializ	Acc_Grp_PcoRed13	http_9040	Permitir	PCO_Srv_Pcored13	Politica para el acceso de los servidores del Banco del Pichincha hacia el Servidor de Desarrollo WAS
9	Monitoreo Banco Pacifico	BCO_Pac_Grup	Ping	Permitir	DMZ_Cli	Politica para el monitoreo de los servidores del Banco del Pacifico hacia la interface asignada

10	Serv_Externos	Net_Ptrs_BCE_Grp	HTTP-HTTPS	Permitir	BCE_GRP_Hst	Politica para el acceso de los host de PCO hacia el Banco Central del Ecuador
11	Serv_Externos	BCE_GRP_Hst	Todos los servicios	Permitir	Net_Ptrs_BCE_Grp	Política para el acceso de los servidores del Banco Central hacia los hosts de servicios especiales de PCO
12	Petroecuador	PEC_Net_X.Z.144.0	Todos los servicios	Permitir	PCO_Net_UIO	Politica para el acceso de los servidore de PEC hacia los host especiales de PCO (SEGUROS, CONTRATOS, AUDITORIA)
13	Petroecuador	PEC_Srv_As_X.Z.226.24	Todos los servicios	Permitir	PCO_Grp_Srv_AS_400	Politica para el acceso desde el servidor I-Series de PetroEcuador hacia el el grupo de servidores iSeries de PCO
14	Petroecuador	PCO_Net_EC	Servicio_WEB_PEC	Permitir	PEC_Grp_Srv_Web	Politica para el acceso de la red de PCO hacia el servidor WEB DE PetroEcuador (INTRANET)
15	Petroecuador	PCO_Net_Ecuafuel GYE	Todos los servicios	Permitir	PEC_Net_X.Z.226.0	Politica para el acceso desde Ecuafuel PCO hacia los servidores de PetroEcuador
16	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
17	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.
18	SRV_Web_Correo	Todos los origenes	HTTP	Permitir	PCO_Srv_Web	Politica para el acceso desde el mundo hacia el servidor web de PCO
19	SRV_Web_Correo	PCO_Srv_Mail_Int	Todos los servicios	Permitir	PCO_Srv_Web	Politica para el acceso desde los servidores internos de correo hacia el servidor de correo externo(Réplica de Correo Electrónico)
20	Usuarios	PCO_Net_EC	FTP	Denegar	Todos los destinos	Politica para evitar FTP desde la red interna de PCO hacia el mundo

21	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
22	Sistemas	PCO_Srv_Pcored01	DNS	Permitir	Todos los destinos	Politica para que el servidor de DNS pueda ver a los servidores externos de impsat
23	Sistemas	PCO_Srv_Pcored15	Todos los servicios	Permitir	PCO_Srv_Web	Polìtica para el acceso hacia el servidor web desde el servidor Pcored15
24	Petroecuador	PEC_Grp_Srv_SMTP	SMTP	Permitir	PCO_Srv_Web	Política de acceso SMTP desde los servidores SMTP de PetroEcuador hacia el servidor web de PCO
25	Petroecuador	PEC_Grp_Host_Sistemas	Todos los servicios	Permitir	PCO_Grp_Srv_Audit	Politica de acceso de los usuarios de sistemas hacia los servidores de UIO y GYE que tienen la aplicación Audit.
26	Petroecuador	PEC_Hst_226.4	BD	Permitir	PCO_Srv_Pcored11	Politica para el acceso del servidor de base de datos de PetroEcuador hacia el Servidor PCO11 donde reside la base de datos SUCO
27	Petroecuador	PCO_Srv_Pcored11	BD	Permitir	PEC_Srv_X.Z.226.5	Politica de acceso del servidor PCORED11 (Base de Datos SUCO) hacia el servidro de base de datos de PetroEcuador
28	Petroecuador	PEC_Grp_Host_Sistemas	Todos los servicios	Permitir	PCO_Grp_Srv_AS_400	Politica de acceso desde los host de sistemas hacia los servidores iSeries de PetroEcuador
29	Petroecuador	PEC_Srv_X.Z.226.5	DNS	Permitir	PCO_Srv_Pcored01	Politica de acceso desde el servidor de DNS de PetroEcuador hacia el servidor de DNS de PCO
30	Petroecuador	PCO_Srv_Pcored1	Todos los servicios	Permitir	PEC_Srv_Base_Datos	Politica de acceso desde el servidor PCORED1 hacia los servidores de Bases de Datos de PEC

31	Petroecuador	PCO_Net_Host_GYE-PEC	Todos los servicios	Permitir	PEC_Grp_Net	Politica para el acceso de los host especiales de SISTEMAS, SEGUROS, CONTRATOS de PCO-Guayaquil hacia los servidores de PetroEcuador
32	Serv_Externos	PIN_GRP_Hst	Servcio_MEM	Permitir	MEM_GRP_SRV	Politica para acceso desde los host de PetroIndustrial y DNH hacia los servidores de MEM donde reside la aplicación SICOHI
33	Serv_Externos	MEM_Grp_Hst	Telnet	Permitir	PIN_Grp_Srv_AS	Politica para el acceso de los host de MEM hacia los servidores iSeries de PetroIndustrial
34	Serv_Externos	MEM_Grp_Hst	Telnet	Permitir	PCO_Srv_As_PCO8	Política para el acceso de los host de MEM hacia el servidor iSeries de PCO
35	Serv_Externos	Internal	Oracle_SQL_NET	Permitir	MEM_GRP_SRV	Politica para acceso desde la red interna hacia el servidor de MEM que contine la aplicación para que se guarde la información en su base de datos a través del puerto 1521
36	Serv_Externos	PCO_Srv_Pcored01	Oracle_SQL_NET	Permitir	SRI_GRP_SRV	Política para el acceso desde el servidor que tiene la aplicación desarrollada en java de PCO para que se guarde la información en la base de datos del servidor del SRI a través de el puerto 1521
37	Servicio FTP	PCO_Srv_Pcored05	FTP	Permitir	Todos los destinos	Politica para que el servidor de Antivirus pueda realizar sus actualizaciones utilizando FTP
38	Admin_Serv	gpalacios (PPTP user)	Telnet	Permitir	PCO_Net_UIO	Politica para el acceso a ASTARO via dial-up para el usuario especificado
39	Admin_Serv	PCO_Net_UIO	Telnet	Permitir	gpalacios (PPTP user)	Politica para el acceso a ASTARO via dial-up para el usuario especificado
40	WEB_Com_World	Todos los origenes	Todos los servicios	Permitir	PCO_Srv_As_PCO1	Política para el acceso de todos los destinos hacia el i-Series de PCO

41	WEB_Mail_World	Todos los origenes	HTTP_Mail	Permitir	PCO_Srv_UIO_Mail	Politica para el ingreso al correo electrónico desde Internet
42	WEB_Mail_World	PCO_Srv_UIO_Mail	HTTP_Mail	Permitir	Todos los destinos	Politica para el ingreso al correo electrónico desde Internet
43	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.

Luego de analizar las políticas de seguridad para PETROCOMERCIAL Quito podemos concluir los siguientes inconvenientes:

- ✓ Existen políticas que contemplan rangos bastante amplios en relación a su rango de origen o destino, es decir de acuerdo al tamaño del grupo definido por su direccionamiento IP. Las políticas que presentan este inconveniente son:

Cuadro 3.13 : Políticas de Seguridad con inconvenientes relacionados a rangos de direccionamiento IP

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

- ✓ Existen políticas cuyas limitaciones del tipo de servicio no estan adecuadamente definidas de acuerdo a las exigencias de cada una de ellas, estas son:

Cuadro 3.14 : Políticas de Seguridad con inconvenientes relacionados a limitaciones de tipos de servicios

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
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.
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

- ✓ Existe políticas que fueron de carácter temporal y no se las ha deshabilitado, como se muestra en el siguiente cuadro:

Cuadro 3.15 : Políticas de Seguridad con inconvenientes relacionados a definiciones 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

Admin_Serv	PCO_Net_UIO	Telnet	Permitir	gpalacios (PPTP user)	Politica para el acceso a ASTARO via dial-up para el usuario especificado

- ✓ Existen políticas desactualizadas. Las políticas que pertenecen a este caso son:

Cuadro 3.16 : Políticas de Seguridad con inconvenientes relacionados a desactualizaciones

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

Algunas de las políticas mencionadas presentan también otros tipos de inconvenientes, sin embargo los problemas planteados anteriormente han sido analizados desde una perspectiva general, de manera que en el siguiente capítulo se hará un estudio minucioso de cada una de las políticas para plantear soluciones a cada una de ellas, en el caso de que sea pertinente hacerlo, o se eliminará o agregará políticas que se consideren importantes para mantener un alto nivel de seguridad perimetral en la empresa.