2.2. ENTREVISTAS AL PERSONAL DE AREA DE NETWORKING VP DE ANDINATEL. S.A.

La realización de entrevistas y encuestas permitirán determinar un reflejo del nivel de aceptación y calidad de los servicios tecnológicos actuales, así como las tendencias en la seguridad informática.

2.2.1 ENTREVISTAS A LOS JEFES DEPARTAMENTALES DE LAS ÁREAS DE SERVIDORES, COMUNICACIONES Y PC`S.

La entrevista con sus respectivas preguntas, realizadas a cada jefe departamental de esta área, se detallan en el anexo #3.

2.2.2 ENCUESTAS AL PERSONAL DE LAS AREAS DE SERVIDORES COMUNICACIONES Y PC´S.

El esquema de las encuestas realizadas al personal antes mencionado se encuentra en el anexo #4.

2.2.3 ANÁLISIS ENTREVISTAS A LOS JEFES DEPARTAMENTALES DE LAS ÁREAS DE SERVIDORES, COMUNICACIONES Y PC`S.

Interpretación de resultados de las entrevistas realizadas en el área de Networking de ANDINATEL S.A. a los tres Jefes de los Departamentos de PC`s, Servidores y Cominucaciones.

1. **Conclusión:** No existe un Comité de Informática integrado por representantes de las áreas funcionales claves (Gerencia Administrativa, Responsables de las Áreas de Informática y Operaciones PC`s, servidores y comunicaciones).

2. **Conclusión:** Si se cuenta con planificaciones de proyectos pero el apoyo de la alta gerencia no es suficiente para una consecución y puesta en marcha de los mismos.

3. **Conclusión:** Actualmente así lo son ya que las soluciones que se presenta a problemas dados se los realiza para arreglarlos al momento.

4. **Conclusión:** La escasez de personal debidamente capacitado, aumenta el nivel de riesgo de errores al disminuir la posibilidad de los controles internos en el procesamiento de la información; y limita la cantidad de soluciones que pueden implementarse en tiempo y forma oportuna a los efectos de satisfacer los requerimientos de las áreas funcionales.

5. **Conclusión:** Existe una adolescencia por los que se requiere se establezca un manual de funciones para cada uno de los cargos funcionales en que se sub-divida el Área de Networking.

6. **Conclusión:** Carencia de un estudio actualizado de vulnerabilidad de la Corporación, frente a las riesgos físicos o no físicos, incluyendo el riesgo Informático.

7. **Conclusión:** Establecer convenios bilaterales con empresas o proveedores a los efectos de asegurar los equipos necesarios para sustentar la continuidad del procesamiento

8. **Conclusión:** Posibilidad de que adulteraciones voluntarias o involuntarias sean realizadas a los elementos componentes del procesamiento de datos (programas, archivos de datos, definiciones

de seguridad de acceso, etc) o bien accesos a datos confidenciales por personas no autorizadas que no sean detectadas oportunamente

9. **Conclusión:** Implementar normas y/o procedimientos que aseguren la eficaz administración de los recursos informáticos, y permitan el crecimiento coherente del área conforme a la implementación de las soluciones que se desarrollen y/o se requieran.

10. **Conclusión:** Se tiene para servidores Intel se tiene, Windows 2000 Advance Server, Windows 2000 server, Windows 2000 Professional, Windows NT Server 4.0 y para servidores RS/6000 el sistema AIX, para Pc's windows 95, 98, 2000.

11. **Conclusión:** La escasa documentación técnica a dificultado llevar un buen inventario de equipos.

2.2.4 ANÁLISIS ENCUESTAS AL PERSONAL DE LAS AREAS DE SERVIDORES, COMUNICACIONES Y PC´S.

Análisis de las encuestas realizadas al personal de Networking de la Vicepresidencia de Sistemas de ANDINATEL S.A. Área de PC´s, Área de Servidores, así como, las del Área de Comunicaciones se localiza en el anexo #5.

2.3 DEFINICIÒN DEL ESTADO DE REFERENCIA.

En este punto se dará a conocer la situación actual en la que se encuentra la red de datos, red eléctrica, servidores de dominio, servidores de aplicaciones, base de datos, computadores, y demás aplicaciones; todo esto en base a encuestas previamente realizadas y tomas de muestras iniciales.

2.3.1 INSPECCIÓN FÍSICA DE LOS COMPONENTES DE EQUIPAMIENTO E INFRAESTRUCTURA (CENTRO DE COMPUTO).

Los trabajos de inspección en el sitio, recopilación de datos, ejecución de programas informáticos especializados y la obtención de

información, se han realizado con la finalidad de presentar un diagnostico inicial de su situación actual, identificando puntos críticos con alto potencial de incidencia sobre fallas y deficiencias en la seguridad informática actividades que serán detalladas adelante.

2.3.1.1 SISTEMAS DE ALIMENTACIÓN Y DISTRIBUCIÓN ELECTRICA.

Es uno de los sistemas importantes a tomar en consideración dentro de la seguridad física, el contar con una buena infraestructura de distribución eléctrica.

Actualmente las adecuaciones y modificaciones a este sistema se han realizado de acuerdo a las necesidades de cada ubicación física, que ANDINATEL S. A., así lo a requerido.

Los servidores se encuentran ubicados en el Centro de Cómputo del Edificio de Tecnología (planta baja). Actualmente esta en marcha un proyecto de profunda remodelación de las instalaciones mencionadas; con énfasis en los sistemas de alimentación eléctrica, suministro continuo de energía eléctrica, aires acondicionados y cableado estructurado.

Se ha incluido una capacidad de crecimiento futuro, considerando los planes de crecimiento de ANDINATEL S. A., de acuerdo a sus planes estratégicos.

Al momento no existe una documentación completa del sistema eléctrico de cada ubicación, solo se tiene información parcial, no actualizada. A medida que se realizan nuevos trabajos, el personal de mantenimiento documenta su labor, de acuerdo a su visión de las situaciones debido a que no cuentan con un conjunto de especificaciones técnicas para el desarrollo de los trabajos eléctricos.

Falta por definir las directrices que se deben seguir para la realización de los trabajos eléctricos en las nuevas instalaciones y en las adecuaciones a las ya existentes; no se especifican las normas y estándares de referencia, marca y características de materiales a utilizar, criterios de pruebas y aceptación, contenido de las documentaciones tanto gráfica, como texto, formato de recepción y responsable de las actualizaciones.

Por otro lado el detalle de los contenidos y rutas de las canaletas del sistema eléctrico, en el área del Centro de Informática no esta claro, existe tuberías y canaletas que no están marcadas ni pintadas

exteriormente y podrían en algún momento ser utilizadas para la transportación de otros tipos de cables.

2.3.1.2 SISTEMA DE CABLEADO DE DATOS.

Este punto especifica la estructura o sistema de cableado de la red de la Empresa.

Originalmente existían redes en los departamentos que no estaban conectadas entre sí. Se utilizaba cable coaxial (en algunos sitios aún permanece instalado sin uso). Gradualmente se cambió este esquema, hasta sustituir el cable inicial por cable de par trenzado sin blindaje de 4-pares (UTP = Unshielded Twisted Pair), en su gran mayoría marca Belden categoría 5 (100 Mbps - 100 Mhz) para distribución a puestos de trabajo.

El crecimiento del sistema de cableado de datos se dio de acuerdo a las necesidades diarias que han sido atendidas. No ha existido una planificación a mediano o largo plazo por lo que al momento se encuentra colapsado.

De la inspección física de los recorridos de cables de datos, tanto internos como externos del Edificio de Tecnología de la Corporación, se constato que a la fecha, los trabajos de instalación de nuevos puntos de cableado, se realizan utilizando todos los materiales recomendados por las normas respectivas, tanto en marca, modelo y calidad de los productos. Lamentablemente, los métodos de instalación, recorrido y documentación no son los que las normas especifican.

No disponen de la suficiente documentación, que permita identificar y certificar todos los puntos de red actuales (TP y fibra óptica). Para de esta manera estimar la cantidad de recursos necesarios para normalizar el sistema de cableado actual.

2.3.1.3 TOPOLOGIA DE RED.

Antiguamente ANDINATEL S. A se conectaba con redes de teleprocesos, que básicamente constaban de Hosts (Servidores), terminales tontos, emuladores de terminal, módems, equipos multipuertos y enlaces de baja velocidad.

A partir del año 1998 se procede a la actualización de la red. Para el efecto se migra hacia una red TCP/IP, con tecnología ethernet, que sirve de soporte para las estaciones de trabajo y fastethernet para los enlaces troncales, mejorando sustancialmente el desempeño y calidad de los servicios de red.

En la actualidad, la mayor parte de los hosts se conectan por medio de fastethernet (100Mbps) y los enlaces troncales se migraron a Gigabit Ethernet (1000Mbps) para alcanzar niveles superiores de confiabilidad y disponibilidad de la red.

ANDINATEL S. A. tiene interconectadas sus redes de área local de datos de la ciudad de Quito, por medio de una red de área metropolitana que consta de varios anillos de fibra óptica. La conexión con sus oficinas de provincia es por medio de enlaces de datos del tipo dedicados E1 ("leased line").

No cuenta con un inventario detallado de todos los equipos activos de redes, en primer lugar, para validar lo que está instalado (marca, modelo, número de parte, número de serie, tipo y número de puertos, identificación de los puertos y cables de interconexión

entre dispositivos). Por tanto, no están etiquetados de manera visible, codificada y unificada, cada uno de los dispositivos de red.

Existen equipos que aún no han sido estandarizados de acuerdo a la comunidad que utiliza ANDINATEL S. A. Representan un riesgo alto de seguridad. Su configuración de la comunidad SNMP seleccionada, tiene levantado algunos privilegios.

Los equipos de red (en especial en los Switch, Ruteadores, Bridge, Ras y Modem) no utilizan clave de acceso.

2.3.1.4 SERVIDORES – EQUIPOS.

ANDINATEL S. A. ha normalizado la utilización de una sola marca de servidores, utiliza equipos marca IBM (aunque aún existen equipos Compaq, varios modelos y configuraciones).

Las configuraciones no son robustas y estables, dado que no existen procedimientos de recopilación y análisis de las estadísticas de utilización de los recursos de los servidores (procesador, memoria, disco duro, entrada / salida a la red, entre otros servicios), no ha sido posible establecer la idoneidad de las mismas.

2.3.1.5 SERVIDORES – SISTEMA OPERATIVO.

No se encontró un procedimiento formal de instalación del sistema operativo de los servidores que ejecutan Microsoft Windows 2000, que incluya todos los pasos y procedimientos necesarios para su instalación.

La instalación del sistema operativo de servidores de misión crítica es una tarea altamente especializada y de precisión, pero la misma se lo realiza, siguiendo las instrucciones del CD de instalación. No se realizan trabajos de optimización de recursos y minimización de errores de seguridad por seguir procedimiento por defecto.

Existen servicios asociados al sistema operativo que se ejecutan en los servidores, la mayoría de ellos levantados para su ejecución constante de acuerdo a la configuración que incluye el CD de instalación y que estos no son necesarios para el rol que están desempeñando. Se encontró por ejemplo levantadas: facilidades de Lan Manager, acceso remoto (RAS), Alerter, Messenger, acceso Remoto al archivo de configuraciones (Remote Registry), acceso Remoto (Remote Access), telefonía (TapiSrv), y otros.

2.3.2 ARQUITECTURA TECNOLOGICA DE ANDINATEL S.A

2.3.2.1 SERVIDORES.

Andinatel posee 2 plataformas de servidores:

- RISC RS/6000
- Intel con sistema operativo Windows 2000.

2.3.2.1.1 Servidores RISC6000.

Actualmente ANDINATEL S.A. posee 10 servidores RISC6000, de los cuales 4 son nodos del sistema SP y 1 es el Control Workstation del SP. Sobre esta plataforma trabajan las bases de datos Oracle del sistema Openflexis y SIGAC.

2.3.2.1.2 Servidores Intel.

Los servidores Intel brindan los siguientes servicios:

- Active Directory para el manejo de las estaciones de trabajo de la red.
- Correo electrónico con Microsoft Exchange Server

- Lotus Domino para manejo de aplicaciones colaborativas
- Impresión en red.
- DNS
- DHCP
- Publicación de sitios Web (Internet Information Server 5.0 y Lotus Domino)
- Servicio de Internet a través del servidor Proxy (Microsoft ISA Server)
- Bases de datos SQL Server 7.0
- Servidor de archivos
- Firewall de la empresa

2.3.2.1.3 Plano del Centro de Computo de ANDINATEL S.A..

El plano del Centro de Computo se observa en el anexo # 6.

2.3.2.1.4 Estructura de los Rack.

La estructura de los rack se encuentra en el anexo # 7.

CPU		DISCO DURO		MEMORIA	PROCESADOR		SISTEMA	ROL
MARCA	MODELO	TAMAÑO	CONTROLADORA	RAM	TIPO	VELOCIDAD	OPERATIVO	PRINCIPAL
IBM	NETFINITY 3500	2 * 4 GB	NO	256 MB	PII	266 MHZ	WINDOWS NT 4.0	SQL SERVER
COMPAQ	PROLIANT DL380	4*36 GB	SI	1 GB	PIII	2 * 1.4 GHZ	WINDOWS 2000 AS	LOTUS
COMPAQ	PROLIANT 1600	2 * 4 / 18 GB	NO	260 MB	PII	300 MHZ	WINDOWS NT 4.0	SERVIDOR SQL
COMPAQ	PROLIANT 1600	4 GB	NO	256 MB	PII	300 MHZ	WINDOWS 2000 AS	SERVIDOR ISA
COMPAQ	PROLIANT 800	8 / 4 GB	NO	327 MB	PII	400 MHZ	WINDOWS 2000 AS	SERVIDOR IMPRESORAS
COMPAQ	PROLIANT 1600	4 GB	NO	196 MB	PII	300 MHZ	WINDOWS NT 4.0	SERVIDOR SQL
COMPAQ	PROLIANT ML370	3 * 18 GB	NO	1 GB	PIII	1000MHZ	WINDOWS 2000 AS	EXCHANGE 2000
IBM	NETFINITY 3500	4 GB	NO	196 MB	PII	266 MHZ	WINDOWS 2000 AS	ACTIVE DIRECTORY
COMPAQ	PROLIANT 1600	2 * 4 GB	NO	256 MB	PII	300 MHZ	WINDOWS NT 4.0	F OPEN
AVANTECH	IC 610	9 GB	NO	128 MB			WINDOWS NT 40 WS	APLICACIONES 114
COMM LOGIK	TELECOM SERVER	2 * 19 GB	NO	256 MB	PIII	700 MHZ	WINDOWS NT 40 WS	APLICACIONES 114
COMPAQ	PROLIANT 1600	4 GB	NO	512 MB	PII	300 MHZ	WINDOWS NT 4.0	SERVIDOR IMPRESORAS
DELL	POWER EDGE 4400	10 * 19 GB	SI	1 GB	PIII	2 * 1 GHZ	WINDOWS 2000 AS	INTRANET
COMPAQ	PROLIANT 1600	4 GB	NO	128 MB	PII	300 MHZ	WINDOWS 2000 S	INFOMAP SELINA
COMPAQ	PROLIANT 800	4 GB / 2 * 18 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	SERVIDOR IMPRESORAS
COMPAQ	PROLIANT ML370	3 * 18 GB	NO	1 GB	PIII	1000MHZ	WINDOWS 2000 AS	FIREWALL
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS 2000 AS	DHCP / F OPEN
COMPAQ	PROSIGNIA	1.5 GB	NO	46 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN
COMPAQ	PROLIANT 800	8 GB	NO	256 MB	PII	400 MHZ	WINDOWS NT 4.0	DHCP / F OPEN

Tabla 9: Características de los Servidores Intel de ANDINATEL S.A.

2.3.2.2 SOFTWARE.

A continuación se detalla el software utilizado por ANDINATEL S.A.

2.3.2.2.1 Sistemas Operativos.

Software	Descripción
Unix AIX 4.3.3	Sistema operativo de servidores RISC 6000
Windows 2000 Advance Server	Sistema operativo para servidores Intel
Windows 2000 server	Sistema operativo para servidores Intel
Windows 2000 Professional	Sistema operativo para estaciones de trabajo
Windows NT Server 4.0	Sistema operativo para servidores Intel
Windows 98	Sistema operativo para estaciones de trabajo
Windows 95	Sistema operativo para estaciones de trabajo

Tabla 10: Descripción Sistemas Operativos

2.3.2.2.2 Herramientas de Oficina.

Software	Descripción
Microsoft Office 2000 professional	Suite de herramientas para trabajo en oficina (Word, Excel, PowerPoint, Access)
Microsoft Project 2000	Programa para la planeación de proyectos
Lotus Notes Desktop 5.0 con colaboración	Cliente para aplicaciones colaborativas
Microsoft Project Central 2000	Programa para la planeación de proyectos en grupo
Oracle Discoverer	Programa para la obtención de reportes

Tabla 11: Descripción Herramientas de Oficina

2.3.2.2.3 Graficadores.

Software	Descripción
Visio 2000 Standard	Graficador con plantillas predefinidas
Corel Draw 9 for Windows	Graficador para diseño
Autocad 2000	Graficador técnico
Autocad LT	Graficador técnico

Tabla 12: Descripción Graficadores

2.3.2.2.4 Aplicaciones Servidores.

Software	Descripción
Exchage Server 2000	Servidor de Correo de Andinatel
SQL Server 7.0	Base de datos para diferentes aplicaciones
Lotus Domino Server 6.0	Utilizado para aplicaciones colaborativas y páginas Web
Oracle 8.0.4 Enterprise Server	Base de datos para sistema Sigac y Spyral
Oracle 8i para Unix con Parallel Server y Particionamiento.	Base de datos en la que funciona el sistema Openflexis
Microsoft ISA Server Check Point	Sistema Proxy para la salida a Internet Firewall para la protección de la red
Tivoli storage manager	Software para la obtención de respaldos.
Tivoli Data Protection for Exchange	Herramienta para obtención de respaldos con Tivoli Storage Manager
PSSP 3.2.	Software que maneja el paralelismo y la administración de los nodos RISC 6000.
Oracle Enterprise Manager;	Suite de herramientas de Oracle para la administración, mantenimiento y monitoreo de bases de datos Oracle

Tabla 13: Descripción Aplicación de Servidores

2.3.2.2.5 Herramientas de Desarrollo de Aplicaciones.

Software	Descripción
Visual Basic Professional 6.0	Herramienta de desarrollo de sistemas de Microsoft
Visual Interdev Professional 6.0	Herramienta de desarrollo de sistemas en el Web de Microsoft
Oracle Internet Developer Suite (incluye Oracle Designer, Oracle Forms, Oracle Reports, Oracle Discoverer Administrator Edition)	Herramientas de desarrollo de Oracle
Lotus Notes 5.0 para desarrollo con colaboración	Herramienta para el desarrollo de aplicaciones colaborativas.
Visual.net	Ultima versión de la herramienta de desarrollo de Microsoft

Tabla 14: Descripción Herramientas de Desarrollo de Aplicaciones

2.3.2.2.6 Antivirus.

Software	Descripción
Active Virus Defense	Suite de programas antivirus que protegen estaciones, servidores, servidor proxy, correo electrónico y tiene una herramienta para la actualización remota del antivirus.
Virex	Antivirus para equipos Macintosh

Tabla 15: Descripción Antivirus

2.3.2.2.7 Otras Aplicaciones.

Software	Descripción
Silec Pro	Sistema Legal de la empresa.

Tabla 16: Descripción Otras Aplicaciones

2.3.2.3 COMUNICACIONES.

La red de datos de ANDINATEL S.A, administrada por el Departamento de Redes de la Vicepresidencia de Sistemas, se forma por distintos tipos de redes, entre los cuales se distinguen:

2.3.2.3.1 Red de Área Local (LAN).

En cada edificio de ANDINATEL S.A. existe una infraestructura de red compuesta por cableado estructurado y dispositivos activos de red –hubs y suites, aunque los primeros dejaron de utilizarse cuando se migro la red de ethernet a fastethernet. A los switches se conectan las estaciones de trabajo formando así la red de área local.

2.3.2.3.2 Red de Área Metropolitana (MAN).

La red MAN une los principales edificios de ANDINATEL S.A. considerados así por la cantidad de usuarios existentes, o por el volumen de tráfico generado. Para conectar los edificios y formar la red MAN de la Vicepresidencia de Tecnología se utiliza parte de la Red Metropolitana de Fibra Óptica, la cual es administrada por la Vicepresidencia de Operaciones, lo que permite alcanzar velocidades de hasta 1Gbps en cada uno de los enlaces.

Los edificios de ANDINATEL S.A. que forman la red MAN son: Estudio Z, Droira, Mariscal, Quito Centro, Cotocollao, La Luz, Carcelen, San Rafael, Sangolquí, Tumbaco, Villaflora, El Pintado. Todos estos enlaces se centralizan en el centro de computo de la VP de Tecnología ubicado en Iñaquito.

Diagrama de la Red MAN de Datos de ANDINATEL S.A se localiza en el anexo # 8.

2.3.2.3.3 Red de Área Extendida (WAN).

La red WAN enlaza los sitios más remotos del País, donde ANDINATEL S.A. tiene cobertura. Las tecnologías utilizadas van desde enlaces satelitales por medio del sistema COMSAT, hasta la red SDH que utiliza la red troncal de fibra óptica, enlaces que son provistos por la Gerencia de Transmisiones.

La red WAN llega a todas las provincias en las que ANDINATEL S.A. tiene cobertura y esta formada aproximadamente por 50 E1's. Mediante esta red los usuarios tienen acceso a consultar información y pagar sus cuentas localmente, evitando así que se queden sin servicio telefónico por no ser actualizada a tiempo la información en el sistema informático.

Dentro de la WAN, también se mantiene la interconexión con las diversas entidades financieras. Así se facilita el pago de los servicios a los usuarios de ANDINATEL S.A., estos podrán utilizar la infraestructura de cajeros y de Internet, dando así una vía alternativa para realizar sus operaciones, pagos y consultas.

Diagrama de la Red WAN de Datos de ANDINATEL S.A se sitúa en el anexo # 9.

En la siguiente tabla se presenta los canales E1 de la red de datos que se encuentran actualmente en operación.

#	LOCALIDAD	CANAL	#	LOCALIDAD	CANAL
1	STA. ROSA SANGOLQUI	E1	15	GUAJALO	E1
2	SAN RAFAEL	E1	16	GUAMANI	E1
3	CARCELEN	E1	17	STO DOMINGO	E1
4	CARAPUNGO	E1	18	ESMERALDAS	E1
5	GUAYLLABAMBA	E1	19	QUININDE	E1
6	CAYAMBE	E1	20	ATACAMES	E1
7	OTAVALO	E1	21	LATACUNGA	E1
8	IBARRA	E1	22	AMBATO	E1
9	TULCÁN	E1	23	BAÑOS	E1
10	LA LUZ	E1	24	RIOBAMBA	E1
11	COTOCOLLAO	E1	25	GUARANDA	E1
12	TUMBACO	E1	26	CONOCOTO	E1
13	TENA	E1	27	PUYO	E1
14	LAGO AGRIO	E1	28	COCA	E1

Tabla 17: Canales E1 de la red de datos

2.3.2.3.4 Direccionamiento IP de la Red de Datos de ANDINATEL S.A.

Sitio	ID Red	Mascara	Rango Valido	Broadcast	
Esmeraldas	172.22.1.0	255.255.255.0	172.22.1.1 – 172.22.1.254	172.22.1.255	254
Quininde	172.22.2.0	255.255.255.0	172.22.2.1 – 172.22.2.254	172.22.2.255	254
Atacames	172.22.3.0	255.255.255.0	172.22.3.1 – 172.22.3.255	172.22.3.255	254
La Concordia	172.22.4.0	255.255.255.0	172.22.4.1 – 172.22.4.255	172.22.4.255	254
Esmeraldas 3	172.22.5.0	255.255.255.0	172.22.5.1 – 172.22.5.256	172.22.5.255	254
Las Golondrinas					

Tabla 18 a: Direcciones IP de la Red de Datos

Sitio	ID Red	Mascara	Rango Valido	Broadcast	
Ambato	172.25.1.0	255.255.255.0	172.25.1.1 – 172.25.1.254	172.25.1.255	254
Riobamba	172.25.2.0	255.255.255.0	172.25.2.1 – 172.25.2.254	172.25.2.255	254
Latacunga	172.25.3.0	255.255.255.0	172.25.3.1 – 172.25.3.254	172.25.3.255	254
Guaranda	172.25.4.0	255.255.255.0	172.25.4.1 – 172.25.4.254	172.25.4.255	254
Puyo	172.25.5.0	255.255.255.0	172.25.5.1 – 172.25.5.254	172.25.5.255	254
Alausi	172.25.6.0	255.255.255.0	172.25.6.1 – 172.25.6.254	172.25.6.255	254
Lasso	172.25.7.0	255.255.255.0	172.25.7.1 – 172.25.7.254	172.25.7.255	254
Pujili	172.25.8.0	255.255.255.0	172.25.8.1 – 172.25.8.254	172.25.8.255	254
Salcedo	172.25.9.0	255.255.255.0	172.25.9.1 – 172.25.9.254	172.25.9.255	254
Baños	172.25.10.0	255.255.255.0	172.25.10.1 – 172.25.10.254	172.25.10.255	254
La Mana	172.25.11.0	255.255.255.0	172.25.11.1 – 172.25.11.254	172.25.11.255	254
					2794

Tabla 18 b: Direcciones IP de la Red de Datos

Sitio	ID Red	Mascara	Rango Valido	Broadcast	
Ibarra	172.23.1.0	255.255.255.0	172.23.1.1 - 172.23.1.254	172.23.1.255	254
Tulcan	172.23.2.0	255.255.255.0	172.23.2.1 - 172.23.2.254	172.23.2.255	254
San Gabriel	172.23.3.0	255.255.255.0	172.23.3.1 - 172.23.3.254	172.23.3.255	254
Otavalo	172.23.4.0	255.255.255.0	172.23.4.1 - 172.23.4.254	172.23.4.255	254
Atuntaqui	172.23.5.0	255.255.255.0	172.23.5.1 - 172.23.5.254	172.23.5.255	254
Salinas					

Tabla 18 c: Direcciones IP de la Red de Datos

Sitio	ID Red	Mascara	Rango Valido	Broadcast	
Santo Domingo	172.21.1.0	255.255.255.0	172.21.1.1 - 172.21.1.254	172.21.1.255	254
Santa Martha	172.21.2.0	255.255.255.0	172.21.2.1 - 172.21.2.254	172.21.2.255	254
					508

Tabla 18 d: Direcciones IP de la Red de Datos

Sitio	ID Red	Mascara	Rango Valido	Broadcast	
Guayaquil	172.18.1.0	255.255.255.0	172.18.1.1 - 172.18.1.254	172.18.1.255	254
Tena	172.18.2.0	255.255.255.0	172.18.2.1 - 172.18.2.254	172.18.2.255	254
Shushufindi	172.18.3.0	255.255.255.0	172.18.3.1 - 172.18.3.254	172.18.3.255	254
Lago Agrio	172.18.4.0	255.255.255.0	172.18.4.1 - 172.18.4.254	172.18.4.255	254
Coca	172.18.5.0	255.255.255.0	172.18.5.1 - 172.18.5.254	172.18.5.255	254
Guajalo	172.18.6.0	255.255.255.0	172.18.6.1 - 172.18.6.254	172.18.6.255	254
Guayllabamba	172.18.7.0	255.255.255.0	172.18.7.1 - 172.18.7.254	172.18.7.255	254
Cayambe	172.18.8.0	255.255.255.0	172.18.8.1 - 172.18.8.254	172.18.8.255	254
Solanda	172.18.9.0	255.255.255.0	172.18.9.1 - 172.18.9.254	172.18.9.255	254
Monjas	172.18.10.0	255.255.255.0	172.18.10.1 - 172.18.10.254	172.18.10.255	254
Machachi	172.18.11.0	255.255.255.0	172.18.11.1 - 172.18.11.254	172.18.11.255	254
Guamani	172.18.12.0	255.255.255.0	172.18.12.1 - 172.18.12.254	172.18.12.255	254
Estación Terrena	172.18.13.0	255.255.255.0	172.18.13.1 - 172.18.13.254	172.18.13.255	254

Tabla 18 e: Direcciones IP de la Red de Datos

2.4 INSTALACIÓN DE RECURSOS DE MEDICIÓN Y MONITOREO.

Con la finalidad de aumentar la productividad de las empresas de toda índole, resulta de gran valía contar con la capacidad de medir y monitorear procesos en sus redes y sistemas de datos, así como, obtener resultados de problemas y falencias por las que se este atravesando, logrando esto con de la implementación de Software, existiendo varias alternativas.

2.4.2 INSTALACION DE GFI LANGUARD N.S.S .

GFI LANguard Network Security Scanner (N.S.S.), es una herramienta de monitoreo utilizada para detectar fallas o irregularidades en la Red. Maximiza la disponibilidad de monitoreo en todos los aspectos de los Servidores (incluyendo UNÍS/LINUX),estaciones de trabajo y dispositivos (routers, etc.), cuando detecta una falla este puede alertar por email, sms o mensajes net send y a su vez permite tomar una acción correctiva como por ejemplo reiniciar automáticamente servicios, correr un scrip o reiniciar el equipo. También presenta un modulo para poder aplicar reglas y personalizarlas.

Este producto permite monitorear en línea base de datos están pueden ser (SQL, Oracle, etc.). En SQL puede monitorearlas a través de una interfaz ADO y Oracle vía TNS ping que permite chequear los procesos de

Logon/logoff en otras bases como Access, FoxPro, Parados, SyBase, Informix, IBM DB2 pueden ser monitorizadas vía ODBC.

A nivel de servidores de Internet permite monitorear FTP, ICMP ping, http, DNS, SMTP, POP3, TNP, SNMP, TCP, UDP, NTP.

El generador de informes de GFI LANguard permite identificar tendencias de seguridad, como entradas al sistema (logon) fallidas, Todas las cuentas bloqueadas durante un período de tiempo, Usuarios que no pudieron entrar debido a un nombre de usuario o contraseña erróneos, posible manipulación de registros de seguridad durante un período de tiempo, permitiendo controlar quien está intentando acceder a dichos archivos, permitiéndole preveer "ataques" más amplios en la red o intentos de hacking.

Detecta intrusos y de seguridad, actuando como un sistema de detección de intrusos basado en host mediante el análisis de sucesos de seguridad en tiempo real. Determina todas las posibles brechas de seguridad en la red y alerta de las debilidades antes de que un hacker pueda encontrarlas, permitiendo tratarlas antes de que este las aproveche.

GFI LANguard escanea, proporciona información como el nivel de service pack de la máquina, parches de seguridad no instalados, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la máquina, entrada de claves de registro, contraseñas débiles, usuarios/grupos, y más.

Los reportes nos permite generarlos en formato html o csv para ser exportado a Excel, que puede personalizarse, permitiéndole asegurar su red proactivamente - por ejemplo, cerrando puertos innecesarios, eliminando recursos compartidos, instalando servic e packs y parches de seguridad, etc.

Figura 12 a: Pantalla de Instalación de GFI LANguard N.S.S

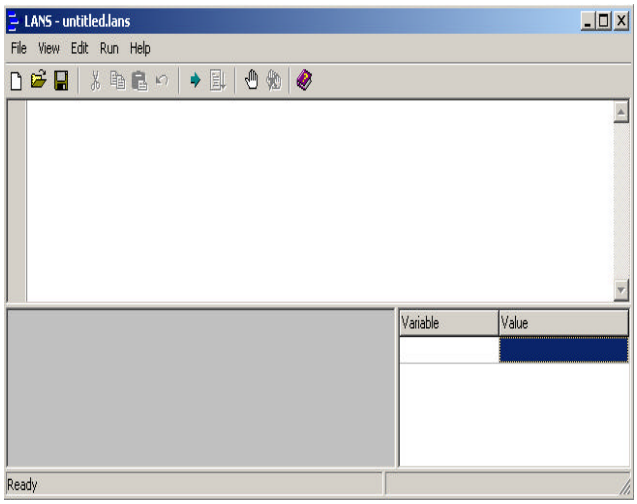

Figura 12 b: Pantalla Principal de GFI LANguard N.S.S

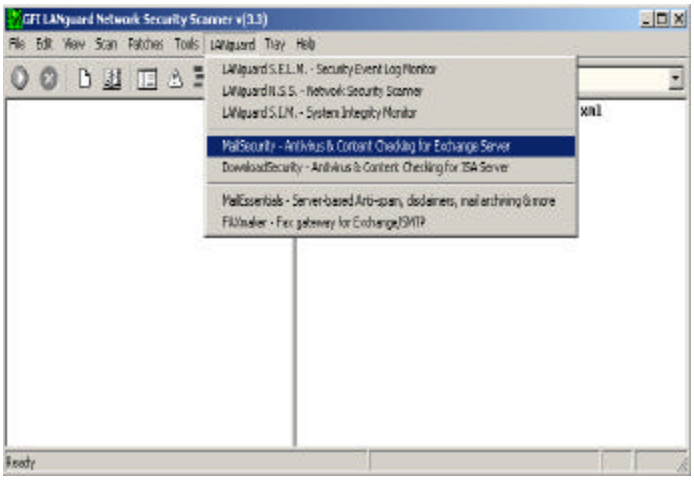

Figura 12 c: Submenú de GFI LANguard N.S.S

2.4.3 INSTALACION DE RETINA.

Retina Network Security Scanner, es un sofisticado analizador de vulnerabilidades que incorpora tecnología avanzada de Inteligencia Artificial (AI). De fácil manejo e interface amigable con Retina es posible detectar todas las vulnerabilidades de seguridad proponiendo las reparaciones oportunas, facilita correcciones automáticas y genera informes a medida. Retina sobresale además por ser el escáner más rápido del mercado ventaja que se amplía en grandes redes.

Funciona con las plataformas Windows NT, Windows 2000 y Windows XP, analiza todos los tipos de sistemas operativos para buscar vulnerabilidades,

incluidos los sistemas basados en UNIX (como las plataformas Solaris, Linux y *BSD). Analiza equipos host, servidores y dispositivos de red como ruteadores y cortafuegos. Comprueba sistemas y servicios como NetBIOS, HTTP, CGI y WinCGI, FTP, DNS, vulnerabilidades de DoS, POP3, SMTP, LDAP, TCP/IP, UDP, registro, servicios, usuarios y cuentas, vulnerabilidades de contraseñas, extensiones de publicación, etc.

Admite la auditoría de redes inalámbricas. Analiza una red completa de clase C en aproximadamente 15 minutos.

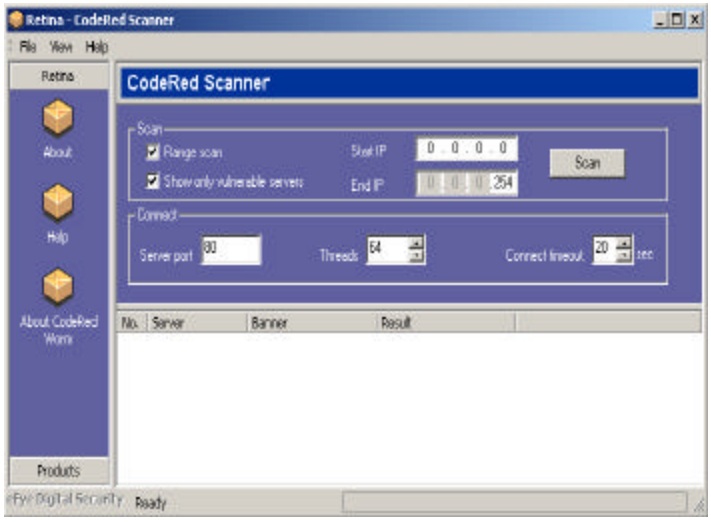

Figura 13 a: CodeRed Scanner de Retina

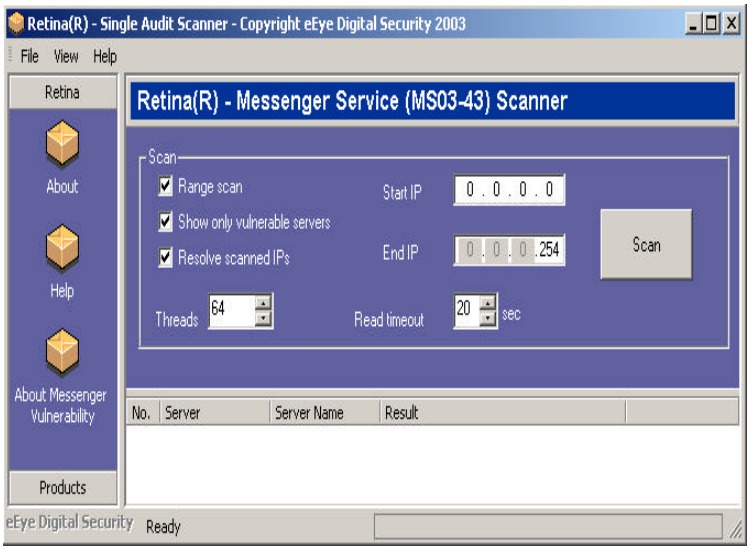

Figura 13 b: Messenger Service Scanner de Retina

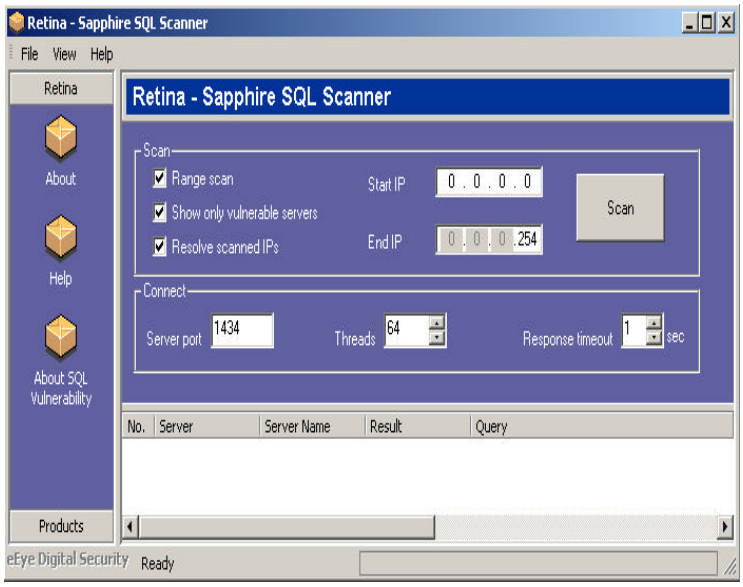

Figura 13 c: Sapphire SQL Scanner de Retina

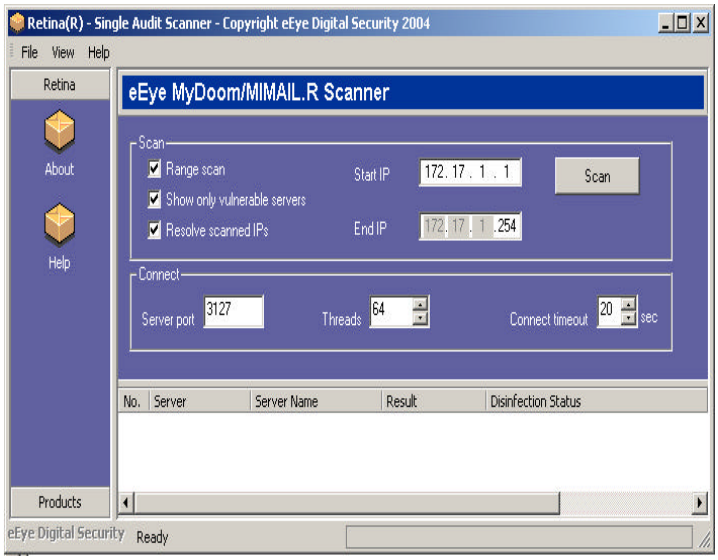

Figura 13 d: eEye MyDoom/MIMAIL Scanner de Retina

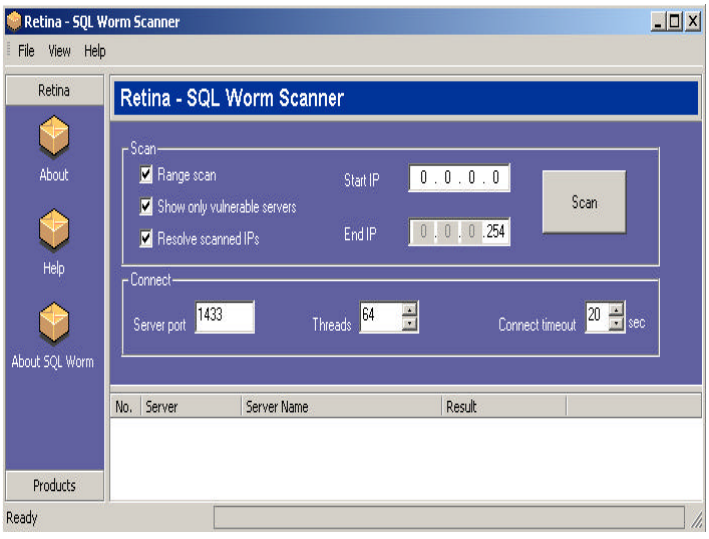

Figura 13 e: SQL Worm Scanner de Retina

2.4.4 INSTALACION DE MICROSOFT BASELINE SECURITY ANALYZER (MBSA).

Realiza búsquedas centrales de errores comunes de configuración de la seguridad en equipos basados en Windows con Microsoft Baseline Security Analyzer. Ésta herramienta se ejecuta en equipos basados en Windows 2000 y Windows XP, y busca revisiones que faltan y vulnerabilidades de la seguridad en equipos basados en Windows NT 4.0, Windows 2000 y Windows XP.

Figura 14 a: Pantalla Principal de Baseline Security Analyzer

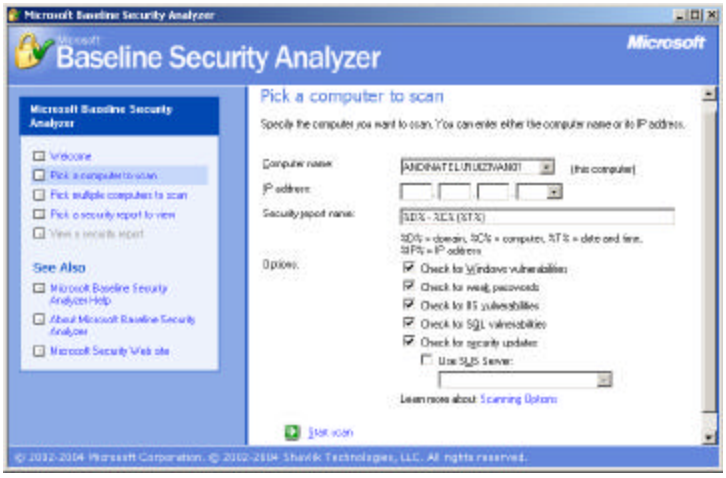

Figura 14 b: Pick a Computer to Scan

2.5 IDENTIFICACIÒN DE VULNERABILIDADES Y DE CONGESTIÓN.

2.5.2 SERVIDORES – VULNERABILIDADES (PARCHES).

Todo programa de computación es susceptible a incluir errores, por omisiones de diseño, por falta de compatibilidad con otros programas y quipos, por detección de problemas de seguridad.

En revisión realizada a los servidores de ANDINATEL S. A. Se encontró que no estaban instalados los últimos parches disponibles a la fecha.

En ciertos servidores no están completamente parchados, como es el caso de equipos de misión crítica para la ANDINATEL S. A., como por ejemplo,

servidores de dominio, de archivos, de impresión, base de datos, etc. Mismos que por su rol, criticidad y acuerdo de confidencialidad han llevado a reportar solo una muestra de algunos de estos equipos:

Se presenta a continuación un ejemplo del análisis de los Parches no instalados/ detectados / confirmados en los servidores obtenido con GFI LANguard. El analisis completo se observa en el anexo # 10.

UIOINT01 (172.17.1.43)

---

* WINDOWS 2000 ADVANCED SERVER SP3

Patch NOT Found	MS02-042	Q326886
Patch NOT Found	MS02-045	Q326830
Patch NOT Found	MS02-048	Q323172
Patch NOT Found	MS02-050	Q329115
Patch NOT Found	MS02-051	Q324380
Patch NOT Found	MS02-055	Q323255
Patch NOT Found	MS02-063	Q329834

* INTERNET EXPLORER 6 GOLD

Warning
The latest service pack for this product is not installed.
Currently Gold is installed. The latest service pack is Internet

Explorer 6 SP1.

Patch NOT Found	MS02-009	Q318089
Patch NOT Found	MS02-068	324929

* SQL SERVER 7.0 GOLD

Warning
The latest service pack for this product is not installed.
Currently SQL Server 7.0 Gold is installed. The latest service pack is SQL Server 7.0 SP4.

Observación: Una vez que se instalen los parches en referencia, aumentará el nivel de seguridad en los Servidores. Esta tarea debe ser realizada de manera periódica (por ejemplo, cada 15 días), de lo contrario la situación de seguridad obtenida se perderá.

2.5.3 SERVIDORES – OTRAS VULNERABILIDADES.

Como trabajo complementario, a continuación se presenta los servicios instalados y levantados por defecto, detectados en los servidores por GFI LANguard en el anexo # 11. Aquí un ejemplo:

Nombre computador:	**UIODNS01**
Dirección IP:	**172.17.1.10**

A. **Servicios a ser detenidos y deshabilitados** (Startup DISABLED, Service Status STOP):

Servicio	**Descripción**
Alerter	Notifies selected users and computers of administrative alerts.
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service

B. Servicios levantados potencialmente innecesarios (Evaluar y bajar sí fuera necesario):

Servicio	Estado
FTP Publishing Service	Detenido
“220 UIODNS01 Microsoft FTP Service (Version 5.0)”	
Simple Mail Transport Protocol (SMTP)	Detenido
“220 UIODNS01.andinatel.int Microsoft ESMTP MAIL	
Service, Version 5.0.2195.5329 ready” Telnet	Detenido
World Wide Web Publishing Service	Detenido

C. Internet Information Service (IIS):

Se encuentran instaladas aplicaciones de ejemplo del producto. Pueden ser utilizadas con fines de acceso no autorizado.

Ejecutar IIS Lockdown Tool para eliminar y desactivar servicios, directorios y archivos no necesarios.

D. Políticas Manejo Contraseñas:

Longitud Mínima = 0 caracteres
Longitud Máxima = 0 caracteres
Vigencia Mínima (en días) = No Controlar
Forzar historial de contraseñas = Deshabilitada

Definir y aplicar políticas de uso general en el dominio y los servidores correspondientes.

E. Otras vulnerabilidades encontradas:

1) No está deshabilitada cuenta GUEST **?**

Deshabilitar y renombrar cuenta GUEST.

No está restringido acceso Anónimo **?**

Configurar RestrictAnonymous = **1** (dado que es PDC).

2) No está restringido acceso GUEST a las bitácoras (Logs) **?**

Crear nombre clave DWORD llamado RestrictGuestAccess con valor=1, en las siguientes entradas del REGEDIT (Registry Editor):

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLo g/System

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLo g/Securit y

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLo g/Application.

3) Revisar uso de servicio en Puerto UDP 1167 (phone=> Conference Calling) Deshabilitar en caso de no ser necesario.

4) Revisar uso de servicio en Puerto UDP 1167 (phone=> Conference Calling) Deshabilitar en caso de no ser necesario.

2.5.4 ESTACIONES DE TRABAJO VULNERABILIDADES PARCHES.

Las Estaciones de Trabajo, no han sido actualizadas. Falta la instalación de parches de: Sistema Operativo, Navegador (Internet Explorer), Base de Datos (SQL Server), Cliente de Correo (Outlook / Exchange), entre otras deficiencias. Encontramos equipos ejecutando Windows 2000 con el Service Pack 1 y Windows XP sin ningún Service Pack, Windows 9x sin parches actualizados.

Del análisis de parches NO instalados detectados con baseline security analyzer, se presenta una parte del detalle de los equipos, que necesitan ser actualizados con la última versión disponible de los Service Pack de cada producto Microsoft instalados en estos, su totalidad se encuentra en el anexo#12:

ESTACIONES DE TRABAJO				
Relativo	Nombre de equipo Direccion IP	MS Windows	MS Internet Explorer	MS SQL Server
1	172.17.20.146 (172.17.20.146)	2000 SP2 Ultimo:SP3		
2	172.17.25.28 (172.17.25.28)	2000 Gold Ultimo:SP3	5.01 Gold Ultimo:SP3	
3	172.17.26.32 (172.17.26.32)	2000 SP2 Ultimo:SP3	6 Gold Ultimo:SP1	
4	172.17.27.110 (172.17.27.110)	XP Gold Ultimo:SP1	6 Gold Ultimo:SP1	
5	AGUILARCESAR (172.17.26.50)	2000 SP2 Ultimo:SP3		

Tabla 19: Estaciones de Trabajo

2.5.5 SERVIDORES – CONTROL DE CUENTAS DE USUARIOS RED.

Se realiza una minuciosa evaluación de la estructura de claves del dominio ANDINATEL. Encontradas 1933 cuentas creadas para ingreso a la Red, de las cuales 726 (38%) no cumplen con los niveles mínimos de seguridad. Es posible obtener su estructura con un programa especializado en menos de 10 segundos.

Con la finalidad de validar la idoneidad de la estructura de las claves que utilizan los usuarios para acceso a la Red, se desarrollo un análisis al respecto.

Existen:

- **348 cuentas**, con palabra clave (password) = número; por ejemplo: 123, 321, 123456, 654321, 12345678, 1313).
- **210 cuenta**s, con nombre del usuario = palabra clave (password); por ejemplo: cquiroz = cquiroz).
- **168 cuenta**s, con palabra clave (password) simple; por ejemplo: nombre propios como ANA, ANDREA, CARLOS, PABLO, palabras como HOLA ECUADOR, PASSWORD.

Detallamos en el anexo # 13 el análisis de la estructura de claves que no cumplen los niveles mínimos de seguridad de ingreso a Red, a continuación una muestra:

USUARIOS CON CLAVE = 123456							
Relativo	Usuario	Relativo	Usuario	Relativo	Usuario	Relativo	Usuario
1	aalvear	88	evelastegui	175	Llevoyer	262	ofalconi
2	aandino	89	fcabrera	176	Llopez	263	oojeda
3	aarauz	90	fcorrea	177	lmachado	264	oromero
4	abahamonde	91	fdelcastillo	178	lmmartinez	265	osantana
5	aburbano	92	fflores	179	lmontenegro	266	palegria
6	acparedes	93	fjaramillo	180	Lnuniez	267	paperez

Tabla 20 a: Usuarios con Claves 123456

USUARIOS = CLAVE					
Relativo	Usuario	Clave	Relativo	Usuario	Clave
1	1-800excavar	1-800excavar	106	guest	guest
2	aaguilar	aaguilar	107	hron	Hron
3	aarias	aarias	108	htroya	Htroya
4	acalero	acalero	109	humana	Humana
5	acobo	acobo	110	hzuniga	Zúñiga
6	aegas	aegas	111	ialbuja	Ialbuja

Tabla 20 b: Usuarios con Claves Iguales

USUARIOS CON CLAVE SIMPLE (o fácil de descubrir)					
Relativo	Usuario	Clave	Relativo	Usuario	Clave
1	aacosta	anita	85	jehidalgo	Jhidalgo
2	acajas	caviar	86	jgalvez	Jose
3	acamacho	ac123	87	jobando	Jorge
4	acgallegos	jorge	88	jpuente	Carlos
5	achicaiza	david	89	jromero	Juan
6	adminoracle	oracle	90	jsalazar1	Rabel

Tabla 20 c: Usuarios con Claves Fáciles de Descubrir

2.5.6 BASE DE DATOS – USUARIOS Y SEGURIDADES.

Encontramos que existen cuentas para acceso a Bases de Datos, que no tienen clave ó el nombre del usuario es el mismo que la clave.

Los roles y derechos sobre la base no están definidos claramente, por lo que la puesta en práctica de una situación ideal no es posible.

Se utilizan para la instalación del MS SQL Server, el puerto que por omisión busca un virus que aprovecha los errores de configuración de los equipos correspondientes.

En la siguiente muestra se encuentran usuarios con clave impropia en MS SQL, explorados con Retina, el detalle se observa en el anexo # 14.

(172.17.1.43)

Logins
****
Name = fvillacis NUEVO
WARNING: No Password has been set for this account!
Name = consulta NUEVO
WARNING: No Password has been set for this account!
Name = fcastillo NUEVO
WARNING: fcastillo's password is fcastillo
Name = calidad
WARNING: calidad's password is calidad
Name = flor
WARNING: flor's password is flor
Name = intranet
WARNING: intranet's password is intranet
Name = rlandeta
WARNING: rlandeta's password is rlandeta
Audit of Server Roles
****
sysadmin BUILTIN\Administrators
sysadmin calidad
sysadmin fcastillo
sysadmin flor
sysadmin intranet
sysadmin rlandeta
sysadmin sa
securityadmin fcastillo
securityadmin rlandeta

DATABASES
****
There are 11 databases defined.
Audit of db_trafico's database roles
---
db_owner dbo
db_owner rlandeta
Audit of db_traficoint's database roles
---
db_owner dbo

db_owner rlandeta
Audit of DB_GESTEL's database roles
---
db_owner dbo
db_owner rlandeta
Audit of Intranet's database roles
---
db_owner dbo
db_owner fcastillo
db_owner intranet
Audit of DB_Calidad's database roles
---
db_accessadmin fvillacis
db_owner calidad
db_owner dbo
db_owner flor
db_owner florflor
db_owner fvillacis

En las Base de Datos ORACLE, se encontró los siguientes mensajes de seguridad en 2 servidores que ejecutan el producto mencionado:

172.17.1.19

Oracle Security Checks

Server is vulnerable to PLSExtProc vulnerability. This allows an attacker to run arbitrary commands on the server without having to authenticate.
Listener Security
Services:
PLSExtProc
SIGACP
Version:
TNSLSNR for 32-bit Windows: Version 8.1.7.4.0 - Production
Security:
OFF
Last Started:
27-OCT-2002 20:07:16
Trace Level:
off

172.17.1.26

Oracle Security Checks

Server is vulnerable to PLSExtProc vulnerability. This allows an attacker to run arbitrary commands on the server without having to authenticate.
Listener Security
Services:
PLSExtProc
iasdb.uioweb01.andinatel.int
Version:
TNSLSNR for 32-bit Windows: Version 9.0.1.3.1 – Production
Security:
OFF
Last Started:
22-OCT-2002 15:17:53
Trace Level:
off

2.5.7 SERVIDOR APACHE.

Este es un Servidor Web, que interactúa con aplicaciones web, especialmente con programas CGI y bases de datos. En un ambiente no seguro, Apache deja pasar accesos no autorizados CGI sin validar los controles de acceso a la base de datos.

Es necesario actualizar la versión de Apache, para incorporar las mejoras y protecciones de seguridad necesarias para una instalación crítica como ANDINATEL S.A.

La versión instalada es Apache 1.3.7, la recomendada es 1.3.27. A continuación como ejemplo, se incluye un anuncio de seguridad, publicado en Hispasec el 15 de Octubre 2003, que claramente indica los peligros de las versiones no parchadas, especialmente en el caso de usuarios locales (caso ANDINATEL S.A).

15/10/2003 NUEVAS VERSIONES DE APACHE

Se acaban de publicar dos actualizaciones de Apache, para las ramas 1.3. y 2 .0.*. Estas actualizaciones solucionan varios problemas de seguridad.Apache es el servidor web más popular del mundo, disponible en código fuente y para infinidad de plataformas, incluyendo UNIX, Microsoft Windows y Novel NetWare.*

Las versiones no actualizadas de Apache contienen varios problemas de seguridad. La recomendación es actualizar cuanto antes a Apache 1.3.27 o 2.0.43.

En concreto, los problemas de seguridad solucionados son:

** 1.3.27:*

*- Un problema en la gestión de la memoria compartida permite que cualquier usuario *LOCAL* en la máquina, que pueda ejecutar código con el UID de Apache (típicamente "nobody"), pueda enviar cualquier señal UNIX a cualquier proceso del sistema, como "root". También puede provocar un DoS*

(Ataque de Denegación de Servicio) sobre la máquina local, en particular el propio proceso Apache.

Esta vulnerabilidad solo es explotable para usuarios locales.

- Apache permite explotar vulnerabilidades CSS (Cross Site Scripting) en la página web por defecto cuando se muestra un error 404 (página inexistente), en dominios que admitan comodines en el DNS.

- Varios desbordamientos de búfer en el código de "ab.c", herramienta incluida en el sistema para realizar pruebas de carga de un servidor web. Las vulnerabilidades son explotables cuando se utiliza "ab" contra un servidor web malicioso."[1]

2.5.8 SERVICIOS PROTOCOLO SNMP.

Se observó que se encuentra levantado en servidores y otros equipos de networking el protocolo SNMP (Simple Network Management Protocol). Esto es un potencial incidente de seguridad.

La situación indicada se convierte en problema activo de seguridad, dado que el nombre de la comunidad definida es "public". Durante una exploración de vulnerabilidades esta es una de las mejoras formas de obtener de manera no autorizada información de una red, o de un equipo en particular

[1] Publicación Hispasec 15 de octubre del 2003

SNMP es ampliamente utilizado para monitorear y administrar todo tipo de dispositivos listos para TCP/IP. Se enconto que el servicio SNMP esta levantado en varios de los equipos RS/6000, configurado con la comunidad por omisión "public". Facilitando la exploración no autorizada del equipo y los servicios que se están ejecutándose en este.

A continuación como ejemplo, se incluye un anuncio de seguridad, publicado en Hispasec el 12 de febrero 2003, que claramente indica los peligros de las versiones no adecuadamente configuradas, como utilizando la comunidad "public" (caso ANDINATEL S.A).

"GRAVE VULNERABILIDAD EN EL PROTOCOLO SNMP

El mundo de la seguridad se vio sobresaltado ayer por la tarde por una importante noticia, el descubrimiento de una serie de vulnerabilidades en la mayoría de implementaciones del protocolo SNMP. El problema es tal, que cientos de dispositivos, sistemas y fabricantes se ven afectados. SNMP (Simple Network Management Protocol) es un protocolo estándar para la administración de red en Internet. Prácticamente todos los sistemas operativos, routers, switches, modems cable o ADSL modem, firewalls, etc. se ofrecen con el servicio SNMP.

En general cualquier fabricante o producto que soporte el protocolo SNMP puede verse afectado por estos problemas (ordenadores, sistemas operativos,

routers, switches, nodos de acceso, etc.). Estas vulnerabilidades pueden permitir el acceso a privilegios no autorizados, ataques de denegación de servicio o provocar comportamientos inestables. La versión 1 del protocolo SNMP (SNMPv1) define múltiples tipos de mensajes SNMP que se emplean para petición de información o cambios de configuración, respuestas de las peticiones, enumeración de objetos SNMP y envío de alertas. El OUSPG, Grupo de Programación Segura de la Universidad de Oulu (Finlandia), ha reportado numerosas vulnerabilidades en las implementaciones SNMPv1 de diferentes dispositivos de un gran número de fabricantes.

Existe una herramienta diseñada para enviar cientos de eventos de prueba a los demonios SNMP desde un sistema remoto para descubrir fallos de programación o vulnerabilidades explotables. Esta herramienta tiene capacidades para provocar la caída de demonios SNMP y dispositivos hardware que ejecuten SNMP.

El OUSPG ha desarrollado una suite de aplicaciones bajo el nombre de PROTOS, diseñada para enviar cientos de pruebas a los demonios SNMP desde un sistema remoto con el objetivo de descubrir fallos de configuración o vulnerabilidades explotables. Esta herramienta tiene la capacidad de provocar la caída de demonios SNMP y dispositivos de hardware con SNMP.

Si se emplea un sistema con SNMP se recomienda revisar su configuración y proceder a una correcta configuración del sistema. Estas vulnerabilidades pueden causar problemas de denegación de servicios, interrupciones de

servicio e incluso permitir al atacante conseguir acceso sobre el dispositivo afectado.

Como medidas para evitar los problemas se recomienda:

Aplicar el parche correspondiente del vendedor del producto afectado. Por otra parte se recomienda deshabilitar el servicio SNMP. Si bien en algunos casos los productos afectados pueden presentar un comportamiento inesperado o denegaciones de servicio incluso si SNMP no se encuentra activo.[2]

2.5.9 SERVICIOS FTP (FILE TRANSFER PROTOCOL).

El dominio FTP es utilizado para distribuir archivos a usuarios autenticados o anónimos (por medio de nombre de usuario y palabra clave). Los datos ingresados son enviados por la red en forma texto, claro, sin ninguna medida que permita que estos no sean interceptados en su ruta. Esto es posible con cualquier herramienta de husmeo (sniffer). Esto se complica si se acostumbra realizar accesos remotos a los servidores que ejecutan FTP /tftp

2.5.10 SERVICIO SENDMAIL.

Sendmail es el programa que envía, recibe y reenvía procesos de mensajería en ambientes Unix. Históricamente es uno de los programas más atacados.

[2] Publicación Hispasec 12 de febrero del 2003

Por eso, debe estar siempre actualizado al último parche válido y configurado adecuadamente. Un atacante podría escalar privilegios ó un desbordamiento de buffers, por medio de este programa Sendmail.

La versión actualmente instalada es 8.9.3. Se sugiere actualizar a la versión segura.

Un anuncio que dio a conocer Hispasec, habla referente a una nueva vulnerabilidad en Sendmail.

NUEVA VULNERABILIDAD EN SENDMAIL

Se anuncia una nueva vulnerabilidad en Sendmail, presente en todas las versiones anteriores a la 8.12.8 (inclusive).

Sendmail es el MTA (Mail Transfer Agent) más veterano y popular en Internet, con una cuota de bastante más del 50% de los servidores de correo.

Las versiones 8.12.8 y anteriores de Sendmail tienen una vulnerabilidad como consecuencia de que el analizador de direcciones realiza, en determinadas circunstancias, unas comprobaciones de límite insuficientes debido a una conversión de tipo char a int. Esto puede ser utilizado por un atacante para conseguir el control de la aplicación.

El impacto de esta vulnerabilidad puede estimarse en la obtención de privilegios de root por parte del atacante. Se ha verificado que la vulnerabilidad es explotable en local y aunque no se ha podido verificar la

posibilidad de que también se pueda explotar remotamente, tampoco se ha podido descartar esta posibilidad. Aquellas instalaciones de Sendmail configuradas con separación de privilegios también son vulnerables, dada la posibilidad de comprometer la cuenta de smmsp y controlar la cola de mensajes.

El problema se encuentra en la función prescan(), del archivo parseaddr.c que, bajo ciertas circunstancias, sobrepasa los límites del búfer asignado y sobrescribe las variables de la pila, alcanzando y sobrepasando el puntero de la instrucción almacenada. La función prescan() se utiliza ampliamente en todo el código de Sendmail durante el proceso de las direcciones de correo."

El consorcio Sendmail ha publicado una nueva versión de Sendmail, que elimina esta vulnerabilidad. También facilita indicaciones de como parchear las versiones anteriores para evitar esta vulnerabilidad.[3]

2.5.11 SAMBA.

Es un producto utilizado para la gestión de impresoras en ANDINATEL S.A. Crítico para la operación diaria de la Empresa. Debe minimizarse la posibilidad de una falla o puerta abierta en este producto.

La versión instalada es insegura. Es necesario que se actualice a la última versión estable.

[3] Publicación Hispasec

A continuación dos avisos de Hispasec al respecto.

Aviso 1: VULNERABILIDAD EN SAMBA

Las versiones no actualizadas de SAMBA contienen un desbordamiento de búfer que permite que un atacante remoto ejecute código arbitrario en el servidor, con privilegios de administrador o "root". Samba es una implementación Unix "Open Source" del protocolo SMB/NetBIOS, utilizada para la compartición de archivos e impresora en entornos Windows. Gracias a este programa, se puede lograr que máquinas Unix y Windows convivan amigablemente en una red local, compartiendo recursos comunes. Incluso es factible utilizar un servidor Samba para, por ejemplo, actuar como controlador de un dominio Windows.

Las versiones de Samba anteriores a la 2.2.8 contienen un desbordamiento de búfer que permite que un atacante remoto ejecute código arbitrario en el servidor, típicamente con privilegios de administrador o "root".

La vulnerabilidad reside en el demonio "smbd", concretamente en el re-ensamblado de fragmentos "SMB/CIFS". Si un atacante envía datagramas convenientemente formateados, puede producir sobreescritura de memoria y, potencialmente, la ejecución de código arbitrario. El ataque puede explotarse de forma remota y anónima.

La recomendación es que todos los administradores de sistemas SAMBA actualicen con la mayor urgencia a la versión 2.2.8 del servidor, disponible desde hace días. Adicionalmente, los puertos SMB (UDP/137, UDP/138,

TCP/139 y TCP/445) deberían ser accesibles, exclusivamente, a los usuarios y redes que lo necesiten. En particular, no deberían ser accesibles desde Internet."

Aviso 2: VULNERABILIDAD EN SAMBA

Las versiones no actualizadas de Samba contienen un problema de seguridad que permite que un atacante obtenga privilegios de superusuario o root. Samba es una implementación Unix "Open Source" del protocolo SMB/NetBIOS utilizada para la compartición de archivos e impresora en entornos Windows. Gracias a este programa, se puede lograr que máquinas Unix y Windows convivan amigablemente en una red local, compartiendo recursos comunes. Incluso es factible utilizar un servidor Samba para, por ejemplo, actuar como controlador de un dominio Windows.

Las versiones de Samba previas a la 2.0.10 o a la 2.2.0a contienen un problema de seguridad que posibilita que un atacante obtenga privilegios de superusuario, mediante la sobreescritura de archivos de forma casi arbitraria.

La recomendación es actualizar cuanto antes a Samba 2.0.10, 2.2.0a o superior. En caso de no ser posible, debe planificarse una migración en un plazo breve y, mientras tanto, eliminar todas las apariciones del macro "%m" en el fichero de configuración "smb.conf".

El problema reside en el tratamiento del macro "%m", que contiene la información sobre identidad del cliente Samba que realiza una petición determinada. Un atacante puede introducir en dicha identidad caracteres considerados especiales por el sistema de ficheros unix, como ".." o "/", y sobre escribir así archivos en el servidor."[4]

Se concluye diciendo que el estado actual de la seguridad en el ambiente RS/6000 AIX es baja. Debe ser revisado e instalado el conjunto completo de parches y mejoras en los programas / productos / servicios. Es necesario recordar que actualmente las seguridades son basadas en los Servidores (Host), por lo que estos deben ser SEGUROS.

2.5.12 REVISIÓN SERVIDOR LOTUS DOMINIO (172.17.1.17).

Aún no han sido aplicados los últimos parches del producto Lotus Domino en los servidores que lo ejecutan.

Una sugerencia seria que los especialistas del producto, realicen a la brevedad posible la actualización.

[4] Los dos avisos fueron tomados de Hispasec

2.5.13 PUNTO DE RUPTURA DE LA SEGURIDAD PERIMETRAL.

2.5.13.1 IDENTIFICACION DE MODEM`S.

Se identifico equipos que tienen instalados servicios de comunicación telefónica (dial-up), por medio de módems. Esto constituye un potencial problema de seguridad, dado que, ANDINATEL S.A utiliza un esquema de protección basado en seguridad perimetral por medio de un firewall y, seguridad basada en servidores.

Los módems están ubicados en el interior del perímetro protegido, por lo que al ser utilizados abren una "puerta posterior".

A continuación se enumera unos pocos moden`s encontrados, la lista completa se encuentra en el anexo # 15.

Relativo	Equipo	(Dirección IP)	Observación
1	ALBANF	(172.17.25.37)	Modem
2	ARELLANOJUAN	(172.17.26.171)	Modem
3	ARGUELLOMARIA	(172.17.20.59)	Modem
4	AVARELLOC	(172.17.26.205)	Modem
5	AVILESCARLOS	(172.17.20.46)	Modem

Tabla 21: Equipos con módems instalado

2.5.13.2 REVISION DE CUENTAS DE USUARIO.

Se realizo un seguimiento de las cuentas definidas dentro de los dominios de ANDINATEL S.A., tomando como muestra 250 cuentas, de las cuales 30 de estas no reportan haber sido utilizadas.

El tener cuentas creadas y no utilizadas, constituye un riesgo de seguridad Informática. Además es un recargo de trabajo administrativo para los técnicos encargados del manejo de cuentas.

Existen varias explicaciones para la existencia de este estado de las cuentas indicadas:

a) Las cuentas fueron asignadas a personas que trabajaban en ANDINATEL S.A., pero no llegaron a utilizarlas.
b) Las cuentas fueron asignadas a personas que realizaron trabajos temporales en ANDINATEL S.A., pero no llegaron a utilizarlas.
c) Las cuentas fueron asignadas a personas que trabajan en ANDINATEL S.A., pero que utilizan cuentas de terceros (de sus compañeros de área) en su trabajo diario.

De las 250 cuentas, tomadas como muestra, se detallan las 30 cuentas en el anexo #16 creadas y no utilizadas que fueron identificadas, a continuación una pequeña muestra.

Alias de Enchange	Nombre cuenta	Descripción	Dirección de correo electrónico
Abaldeon	NEG Baldeón Aída	Gerencia de Call Center	abaldeon@andinatel.com
Aburbano	OTR Burbano Alberto	Siemens Red Troncal Fibra Optica	aburbano@andinatel.com
Acamacho	NEG Camacho Alicia	Gerencia Comercial Centro Sur	acamacho@andinatel.com
Achavez	FIN Chávez Andréz	Gerencia Financiera	achavez@andinatel.com
Acparedes	NEG Paredes Ana	Gerencia de Call Center	acparedes@andinatel.com

Tabla 22: Cuentas Creadas y no Utilizadas

2.5.14 FIREWALL.

Debido a la criticidad de la información que encierra este tema, con referencia a la empresa ANDINATEL S.A., se lo tratara de una forma global.

Lo referente a las políticas de accesos en un firewalls, deben diseñarse poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, debido a que las medidas diferirán notablemente en función de esos usuarios.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger?. Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse?. De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques internos que puedan preverse y prevenir.

Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

El como protegerse, esta es una pregunta muy difícil y se orienta a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

a. Paradigmas de seguridad.

- Se permite cualquier servicio excepto aquellos expresamente prohibidos.
- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontento.

b. Estrategias de seguridad.

- Paranoica: se controla todo no se permite nada.
- Prudente: se controla y se conoce todo lo que sucede.
- Permisiva: se controla pero se permite demasiado.
- Promiscua: no se controla (o se hace poco) y se permite todo.

Lo que costara esta en función de lo que se desea proteger y se debe decidir cuanto es conveniente invertir.

La parte más importante de las tareas que realizan los Firewalls, la de permitir o negar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1. **Usuarios internos con permiso de salida para servicios restringidos:** permite especificar una serie de redes y direcciones a los que denomina Trusted (validados). Estos usuarios, cuando prevengan del interior, van a poder acceder a determinados servicios externos que se han definido.
2. **Usuarios externos con permiso de entrada desde el exterior:** este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interno de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

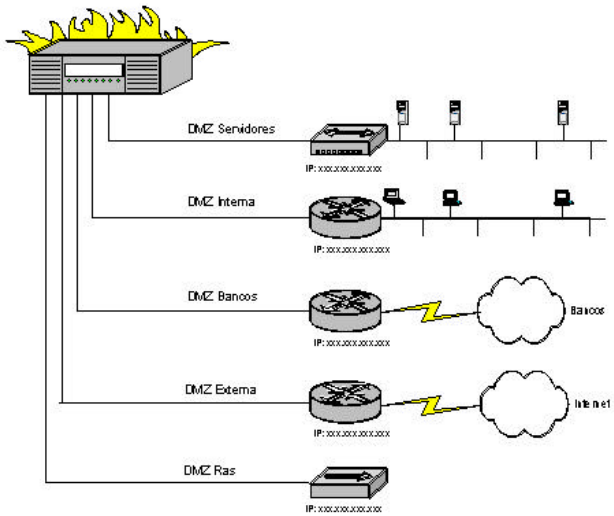

Figura 15: Configuración de Interfaces del Firewall