UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA ELECTRÓNICA

Memoria Laboral

“Diseño e Implementación del Esquema de Seguridad Perimetral para la Red de Datos de la Dirección de Registro, Control y Administración de Bienes Incautados”

Postulante: Juan Carlos Quelca Velasquez

Tutor: Ing. Juan Carlos Duchen

La Paz, Mayo 2019.

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

Mis mayores agradecimientos a:

A Dios por la vida y salud que me da, para realizar esta memoria laboral, es el quien ha estado en las etapas buenas y malas de la vida, que a pesar de mis errores siempre me da una nueva oportunidad.

A todos los docentes, de la carrera de Ingeniería Electrónica, que con su sabiduría, conocimiento y apoyo, motivaron a desarrollarme como persona y profesional en la Universidad Mayor de San Andrés.

A mis docentes Ing. Juan Carlos Duchen, Ing. Marcelo Ramírez, Ing. Víctor Laredo e Ing. Edwin Carrazana, por la orientación, el seguimiento y la supervisión continúa de la memoria laboral, pero sobre todo por la motivación y el apoyo recibido a lo largo de este tiempo.

A mis padres por haberme apoyado al dar todo su esfuerzo para que ahora este culminando esta etapa más en mi vida, a mis hermanos y hermanas que siempre pusieron su confianza en mí y por ayudarme incondicionalmente a cumplir mi sueño y volverlo realidad.

Juan Carlos Quelca.

INDICE DE CONTENIDO

1. INTRODUCCIÓN

Resumen de la actividad laboral. 1

2. CASO DE ESTUDIO 12

2.1 Sección diagnostica. 12

2.1.1 Objetivo. 15

2.1.1.1. Objetivo principal. 15

2.1.1.2. Objetivos secundarios. 15

2.1.2. Justificación. 15

2.1.3. Alcances y límites. 17

2.1.3.1. Alcances. 17

2.1.3.2. Límites. 18

2.1.4. Marco referencial. 19

2.1.4.1 Definiciones. 20

2.2 Desarrollo. 30

2.2.1 Relevamiento infraestructura tecnológica. 31

2.2.1.1 Hardware e infraestructura. 33

2.2.1.2 Instalaciones eléctricas. 34

2.2.1.3 Equipamiento informático. 35

2.2.1.4 Software y licencias. 36

2.2.1.5 Comunicación y redes. 36

2.2.1.6 Recursos humanos encargados de los sistemas. 36

2.2.2. Diseño De Red De Seguridad Perimetral. 37

2.2.2.1. Capa Central (Core o Núcleo). 39

2.2.2.2. Capa de Distribución. 40

2.2.2.3. Capa de Acceso. 40

2.2.2.4. Esquema de la Arquitectura Propuesta e Implementada 41

2.2.3. Elección de la Solución. 47

2.2.4. Adquisición de Equipos, Mantenimiento preventivo y correctivo

del hardware e infraestructura tecnológica. 48

2.2.4.1. Infraestructura Centro de Procesamiento de Datos. 48

2.2.4.2. Instalaciones Eléctricas. 50

2.2.4.3. Equipamiento Informático. 54

2.2.4.4 Software y Licencias. 58

2.2.4.5. Comunicación y redes. 62

2.2.4.5.1. Servicio de Internet. 62

2.2.4.5.2. Red LAN. 63

2.2.5. Implementación de la Red de Seguridad Perimetral. 65

Etapa 1 – Capacitación en la Administración de los equipos de seguridad adquiridos.

Etapa 2 – Instalación de equipos.

2.3. Conclusiones y recomendaciones. 73

2.3.1. Resultados principales. 73

2.3.2. Recomendaciones. 75

3. ANALISIS DE LA ACTIVIDAD. 77

3.1. Desempeño Laboral. 77

3.2. Formación Recibida en la UMSA. 78

ABREVIATURAS UTILIZADAS 79

BIBLIOGRAFÍA 81

ANEXOS Y DEFINICIONES 82

CONFIDENCIALIDAD 82

AUTENTICIDAD 82

SOFTWARE ANTIVIRUS 82

SISTEMAS DE DETECCIÓN DE INTRUSOS 82

INTEGRIDAD 82

DISPONIBILIDAD 82

PERÍMETRO 83

NO REPUDIO 83

DoS 83

CHOKE 83

PROXI 83

DIRECCIONES BROADCAST 83

DIRECCIONES MULTICAST 84

BASTION 84

ROUTER 84

SWITCH 84

TIPOS DE REDES. 85

TIPOS DE ATAQUES INFORMÁTICOS. 88

VPN – Red Privada Virtual. 91

MODELO OSI. 100

TIPOS DE FIREWALL. 106

MODELO DE DISEÑO JERÁRQUICO. 108

VLAN (VIRTUAL LOCAL AREA NETWORK). 112

IDS / IPS (SISTEMAS DE DETECCIÓN DE INTRUSOS). 114

CARACTERISTICAS EQUIPOS CISCO. 121

CONFIGURACIÓN EQUIPOS. 126

INDICE DE FIGURAS

Figura 1: Estructura de la red de distritales departamentales DIRCABI**.** 12
Figura 2: Flujo de información SIREBI v1. 13
Figura 3: Flujo de información SIREBI v2. 14
Figura 4: Esquema básico de seguridad con Firewall. 25
Figura 5: Cortafuegos de filtrado de paquetes. 26
Figura 6: Arquitectura Dual-Homed Host. 27
Figura 7: Arquitectura Screened Host. 28
Figura 8: Arquitectura Screened Subnet. 29
Figura 9: Modelo de Diseño Jerárquico. 39
Figura 10: Esquema de seguridad perimetral de la dirección nacional, distrital La Paz, Cochabamba, Santa Cruz de DIRCABI. 44
Figura 11: Esquema de seguridad perimetral de las direcciones departamentales de Tarija, Oruro, Beni y Pando. 45
Figura 12: Esquema De Seguridad Perimetral Global. 46
Figura 13: Esquema Implementado de la Dirección Nacional. 66
Figura 14: Esquema Implementado Dirección Departamental Cochabamba y Santa Cruz. 69
Figura 15: Esquema Implementado Direcciones Departamentales de Tarija, Oruro, Beni y Pando. 71
Figura 16: PANDA Businessecure – Gatedefender. 72
Figura 17: Red LAN. 85
Figura 18: Red WAN. 86
Figura 19: Red CAN. 87
Figura 20: Acceso VPN Red Privada Virtual. 91
Figura 21: VPN peer to peer. 93
Figura 22: VPN peer to client. 94
Figura 23: Diagrama de configuración IPs públicas. 96
Figura 24: Modelo OSI. 100
Figura 25: VLAN. 112

Figura 26: Router CISCO 2600. 121
Figura 27: Firewall PIX 515E-R. 122
Figura 28: Switch CISCO 3560. 123
Figura 29: Switch CISCO 2950. 123
Figura 30: Firewall PIX 501. 124

MEMORIA LABORAL

1. INTRODUCCIÓN.

Resumen de la Actividad Laboral.

La presente memoria laboral deriva de la realización de mis prácticas profesionales en el área de redes, comunicaciones, bases de datos, sistemas operativos y otros relacionados con tecnologías de la información y comunicación.

La seguridad perimetral de la red de datos de la Dirección y Registro de Bienes Incautados del Narcotráfico (DIRCABI) fue uno de los casos de estudio, diseño e implementación que se tuvo a cargo. Este proyecto fue realizado para la implantación del Sistema de Registro de Bienes Incautados (SIREBI) versión 2 en las 7 distritales departamentales.

En cada dirección departamental existe un servidor de base de datos, los mismos que se comunican con un servidor de base de datos centralizado en la dirección nacional localizada en la ciudad de La Paz. La confidencialidad, la integridad y la disponibilidad de la información son los objetivos de este proyecto para lo cual se analizaron y evaluaron equipos diseñados para la seguridad de datos y comunicación de servidores.

La implementación de Centro de Procesamiento de Datos en las prefecturas de La Paz, Oruro, Potosí, Santa Cruz, Sucre en el marco del apoyo de USAID a la modernización administrativa mediante la instalación de Tecnologías de la Información y Comunicación "Tics" apoyaron a la implantación del Sistema Integrado de Gestión y Modernización Administrativa (SIGMA). Estos proyectos ampliaron los conocimientos en el área comunicaciones, ya que fueron diseñados y supervisados de manera conjunta con personal técnico de amplia experiencia del Ministerio de Hacienda.

Es oportuno mencionar que estas experiencias profesionales fueron de gran contribución para el desarrollo profesional, ya que enriqueció y consolido los conocimientos adquiridos a lo largo de la licenciatura en ingeniería electrónica de nuestra prestigiosa Universidad Mayor de San Andrés.

1.1. Dirección de Registro, Control y Administración de Bienes Incautados del Narcotráfico.

1.1.1. Periodo de trabajo.

Se desarrollaron desde agosto/2004 a agosto/2006.

1.1.2. Supervisado por.

Responsable Nacional de Registro y Sistemas, Lic. Vladimir Duran Chavez.

1.1.3. Dependientes.

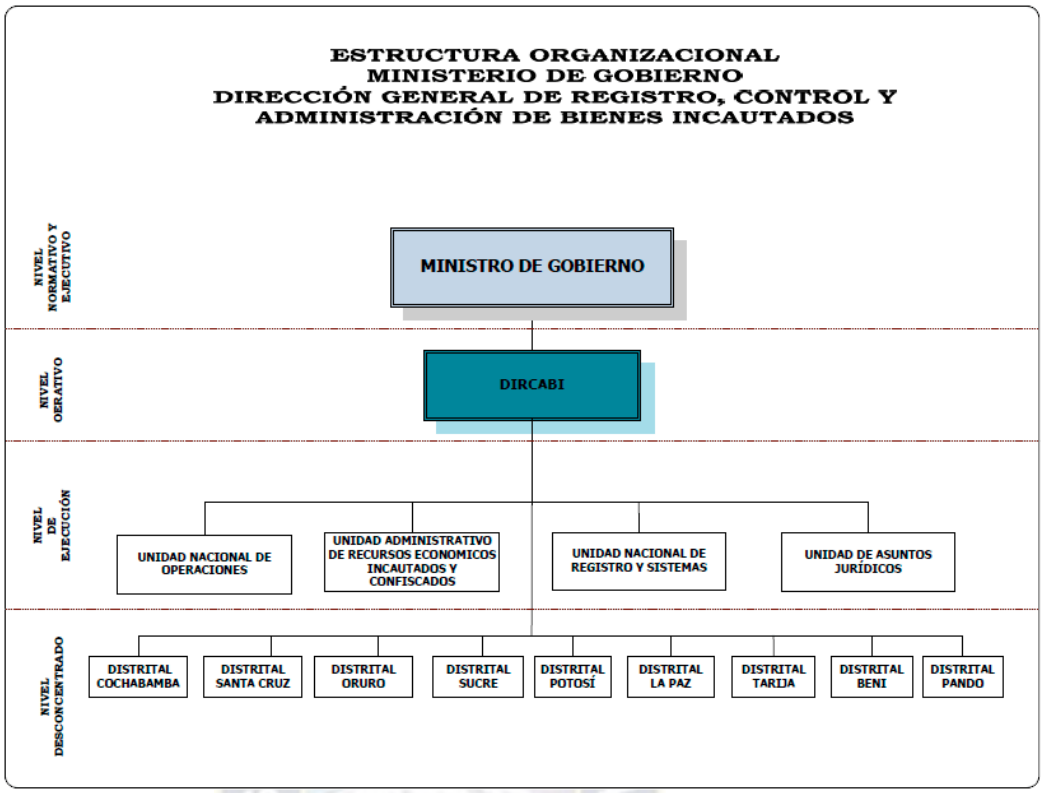
La supervisión y coordinación de trabajo de los 7 encargados de sistemas y registro departamentales, (La Paz, Cochabamba, Santa Cruz, Tarija, Oruro, Pando y Beni) fue una de las principales responsabilidades del cargo ocupado.

1.1.4. Organización.

La Dirección General de Registro, Control y Administración de Bienes Incautados (DIRCABI) tiene la misión institucional de administrar los bienes incautados, decomisados y confiscados del narcotráfico de acuerdo a la legislación vigente, en todo el territorio boliviano. (Art. 11. del D.S. 26143). La DIRCABI realiza el saneamiento legal y administración física de los bienes e inmuebles incautados a nivel nacional para lo cual realiza transferencia de información diariamente a la dirección nacional mediante el sistema SIREBI. Así también recibe el apoyo de la Oficina de Asuntos de Narcóticos (NAS) de la Embajada Americana.

1.1.5. Posiciones.

La estructura de la Dirección de Registro, Control y Administración de Bienes Incautados del Narcotráfico es la siguiente:



El cargo ocupado fue de Supervisor de Sistemas Nacional.

1.1.6. Actividad.

- Diseño e implementación del esquema de Seguridad Perimetral para la Red de Datos de la DIRCABI.
- Implementación y configuración del sistema SIREBI v2 en las distritales departamentales.
- Administración de servidores bajo plataforma Windows 2000 Server y bases de datos SQL Server.
- Mantenimiento preventivo y correctivo de servidores y la red física.
- Envío de reportes diarios de la información registrada en el SIREBI v2 a la Dirección General de DIRCABI, Ministerio de Gobierno y Oficina NAS de la Embajada Americana.

1.1.7. Resultados.

- Implementación de la seguridad perimetral de la red DIRCABI.
- Implantación del sistema SIREBI v2 a nivel nacional.
- Cumplimiento de los objetivos del proyecto en cuanto a la seguridad de la información.
- Protocolos y reglamentos de uso de equipos informáticos dentro de DIRCABI a nivel nacional.

1.2. USAID – Iniciativas Democráticas Bolivia.

1.2.1. Periodo de trabajo.

Se desarrollaron desde febrero / 2007 a noviembre / 2007.

1.2.2. Supervisado por.

Director de Sistemas, Ing. Gonzalo Gutiérrez Mollard.

1.2.3. Dependientes.

La principal responsabilidad fue la supervisión y apoyo técnico en los proyectos y convenios que USAID -IDB participa. Estas tareas fueron realizadas de manera conjunta con el personal técnico de cada gobernación o ministerios involucrados. Así también se tuvo la supervisión y coordinación de empresas y consultores externos.

1.2.4. Organización.

USAID – Iniciativas Democráticas Bolivia (IDB) apoya a la modernización administrativa mediante la instalación e implantación de Tecnologías de la información y Comunicación “Tics” en las Gobernaciones Departamentales de Bolivia.

1.2.5. Posiciones.

El cargo ocupado fue de Asistente en Sistemas.

1.2.6. Actividad.

- Relevamiento de información de la situación tecnológica en la que se encuentra las gobernaciones y SEDUCA de los departamentos donde USAID-IDB apoya.
- Elaboración de términos de referencia para la contratación, adquisición de productos y servicios en el área de tecnología y comunicación.
- Supervisión y apoyo técnico en la implementación de centros de procesamiento de datos.
- Mantenimiento preventivo y correctivo equipos informáticos.

1.2.7. Resultados.

- Implementación de centros de procesamiento de datos en las prefecturas de La Paz, Oruro, Potosí, Santa Cruz y Sucre.
- Supervisión en la verificación de la certificación de cableado estructurado.

1.3. Seguro Social Universitario.

1.3.1. Periodo de trabajo.

Se desarrollaron desde enero / 2008 a diciembre / 2008.

1.3.2. Supervisado por.

Jefe de Sistemas, Ing. Marco Antonio Monzón.

1.3.3. Dependientes.

No existía dependientes. El cargo ocupado tenía la responsabilidad de atender de forma directa y personal todas las solicitudes de la institución. Así también apoyar al técnico encargado de desarrollo de software de acuerdo a los requerimientos.

1.3.4. Organización.

Seguro Social Universitario, hospital de 3º nivel de la Universidad Mayor de San Andrés.

1.3.5. Posiciones.

El cargo ocupado fue de Técnico Encargado de Hardware y Soporte de Red.

1.3.6. Actividad.

- Implantación del Sistema de Gestión Hospitalario adquirido por la institución.
- Administración de Servidores bajo plataforma Windows Server y Motor de Base de Datos SQL Server.
- Mantenimiento preventivo y correctivo en equipos informáticos.

1.3.7. Resultados.

- Implantación del Sistema de Gestión Hospitalario en todas las dependencias del Seguro Social Universitario.
- Implementación de cableado estructurado en las oficinas administrativas de la institución.

1.4. Solidar Suiza – Apoyo a la Democracia Municipal.

1.4.1. Periodo de trabajo.

Se desarrollaron desde abril / 2009 a diciembre / 2016.

1.4.2. Supervisado por.

Director Responsable para Bolivia, Lic. Martin Perez Bustamante y Administradora, Eliana Argote Franulic.

1.4.3. Dependientes.

Se tenía la responsabilidad de supervisión de consultores externos en el área de tecnología que prestan servicios en los diferentes proyectos que la institución apoya y financia.

1.4.4. Organización.

Organización no Gubernamental Suiza que apoya en el área de educación, ciudadanía y salud.

1.4.5. Posiciones.

El cargo ocupado fue de Encargado de Sistemas.

1.4.6. Actividad.

- Administración de servidores Web de los diferentes dominios y subdominios.
- Administración de servidores Web mail.
- Administración de servidores FTP y base de datos.
- Soporte técnico en equipo informático.
- Diseño, desarrollo e implementación de sistemas de datos Web.

- Diseño, desarrollo e implementación de páginas Web.

- Uso de herramientas TIC.

1.4.7. Resultados.

- Servidores Web, Web mail, FTP y bases de datos en producción y monitoreados para la prevención de posibles ataques cibernéticos.

1.5. Fundación ACEQUIA

1.5.1. Periodo de trabajo.

Se desarrollaron en enero / 2017 a enero / 2018.

1.5.2. Supervisado por.

Director académico, Dr. Guery Zabala Gumucio.

1.5.3. Dependientes.

No existían dependientes. Responsabilidad directa de todas las tareas encomendadas dentro de los términos de referencia.

1.5.4. Organización

Institución que realiza capacitación e investigación en Grafología, Psicología y Programación Neurolingüística.

1.5.5. Posiciones.

Consultor en Sistemas.

1.5.6. Actividad.

- Implementación de servidor Web.

- Administración de servidores Web mail.

- Soporte técnico en equipo informático.
- Diseño, desarrollo e implementación de la página Web.
- Implementación de plataformas E-Learning (aulas virtuales).
- Uso de herramientas TIC.

1.5.7. Resultados.

- Servidores Web, Web mail, FTP y bases de datos en producción y monitoreados para la prevención de posibles ataques cibernéticos.

1.6. HELVETAS Swiss Intercooperation.

1.6.1. Periodo de trabajo.

Se desarrollaron del 01/ ago. / 2017 al 31 / ago. / 2017.

1.6.2. Supervisado por.

Responsables técnicos Helvetas PRRD, Ing. Marco Loma e Ing. Javier Quispe.

1.6.3. Dependientes.

No existían dependientes. Responsabilidad directa de todas las tareas encomendadas dentro de los términos de referencia.

1.6.4. Organización.

Organización No Gubernamental que tiene como uno de sus objetivos el apoyo y la modernización tecnológica a diferentes instituciones públicas.

1.6.5. Posiciones.

Consultor en Sistemas.

1.6.6. Actividad.

- Implementación de servidor Web para la Unidad de Contingencia Rural del Viceministerio de Desarrollo Rural y Tierras.
- Diseño, desarrollo, implementación y capacitación de la página web del Sistema de Alerta Temprana de la Unidad de Contingencia Rural.
- Implementación de reportes de estaciones agro meteorológicas.
- Uso de herramientas TIC.

1.6.7. Resultados.

- Servidores Web, FTP y bases de datos en producción y monitoreados para la prevención de posibles ataques cibernéticos.

1.7. Organización de las Naciones Unidas para la Alimentación y la Agricultura - FAO

1.7.1. Periodo de trabajo.

Se desarrollaron en agosto / 2017 a noviembre / 2017.

1.7.2. Supervisado por.

Coordinador responsable de proyectos FAO, Ing. Oscar Mendoza , Director de la Unidad de Contingencia Rural dependiente del Viceministerio de Desarrollo Rural y Tierras , Franklin Condori y Encargado de sistemas del Viceministerio de Defensa Civil, Ing. Carlos Mariaca.

1.7.3. Dependientes.

No existían dependientes. Responsabilidad directa de todas las tareas encomendadas dentro de los términos de referencia.

1.7.4. Organización.

Organización No Gubernamental que tiene como uno de sus objetivos el apoyo y la modernización tecnológica a diferentes instituciones públicas.

1.7.5. Posiciones.

Consultor en Sistemas.

1.7.6. Actividad.

- Diseño, desarrollo, implementación y capacitación de la página web del Sistema de Índice de Estrés Agrícola (ASIS).
- Implementación de servidor web en el Viceministerio de Defensa Civil.
- Diseño e implementación de plataforma E-Learning (aulas virtuales) en el Viceministerio de Defensa Civil.
- Evaluación y diseño de la seguridad perimetral del Viceministerio de Defensa Civil.
- Uso de herramientas TIC.

1.7.7. Resultados.

- Servidores Web, FTP y bases de datos en producción.
- Propuesta de diseño de la seguridad perimetral.

2. CASO DE ESTUDIO

En la presente memoria laboral se describirá el Diseño e Implementación del Esquema de Seguridad Perimetral para la Red de Datos de la Dirección de Registro, Control y Administración de Bienes Incautados del Narcotráfico. Red que comprende las 7 distritales departamentales (La Paz, Cochabamba, Santa Cruz, Tarija, Oruro, Beni y Pando) y la dirección nacional, localizada en la ciudad de La Paz.

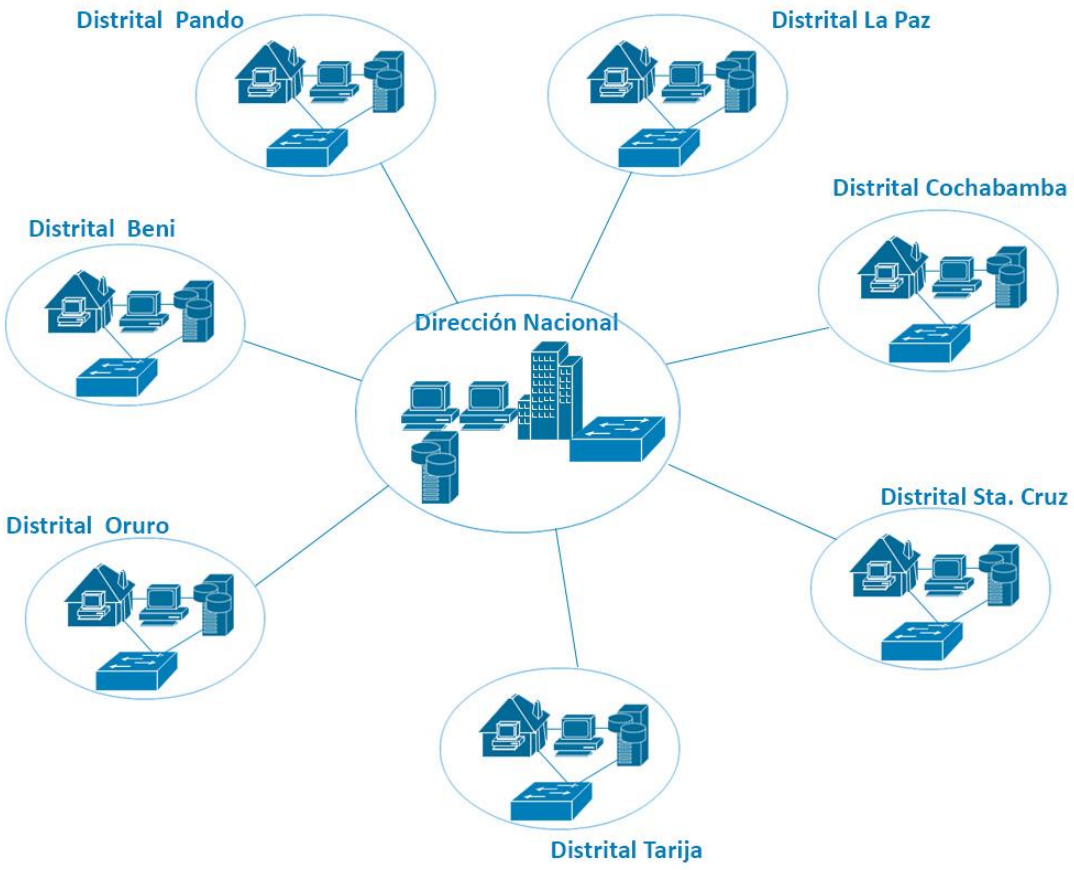


Figura 1: Estructura de la red de distritales departamentales DIRCABI**.**
Fuente: Elaboración propia**.**

2.1. Sección diagnostica

La Dirección General de Registro, Control y Administración de Bienes Incautados (DIRCABI), hasta antes de la implementación de la red de seguridad perimetral, administraba la información generada mediante el sistema de registro "SIREBI v1", la cual tenía las siguientes características de funcionamiento y proceso de datos:

Figura 2
Fuente: Elaboración propia**.**

- El "SIREBI v1" funcionaba de manera local en la LAN de cada distrital departamental. Este sistema era implantado en un servidor local de base de datos (motor de base de datos access), el cual no tenía comunicación directa con otros servidores de DIRCABI.

- Los reportes del SIREBI v1 (reportes diarios del movimiento de bienes incautados), eran enviados mediante FAX a la Dirección Nacional.

- Dentro del protocolo de comunicaciones entre distritales departamentales y la dirección nacional, indicaba que cada 15 días cada distrital departamental tenía que enviar un backup de la base de datos, a la dirección nacional en medio magnético.

- Los reportes mensuales del sistema SIREBI v1 que se emitía cada 10 días del siguiente mes, eran enviados por la dirección nacional a las diferentes instituciones socias. Este reporte era enviado previa verificación de la información, con la respectiva documentación legal y bancaria existente en los archivos de la dirección nacional.

Todo este proceso tenía los siguientes problemas:

- Se demoraba mucho tiempo en la verificación mensual del SIREBI v1, con la documentación enviada por las distritales departamentales.

- Se tenían que realizar las solicitudes de actualización de datos vía teléfono y FAX a las diferentes distritales departamentales, en caso de error.

- No se tenía comunicación directa con servidores de bases de datos de cada distrital departamental.

Por esta problemática, se inició en el año 2003 el diseño y programación del sistema "SIREBI v2", con el apoyo del Programa de las Naciones Unidas para el Desarrollo "PNUD". Este sistema funcionaba con base de datos centralizada y con un flujo de información en tiempo real.

El SIREBI v2 fue implantado a inicios del año 2005 a nivel nacional, por lo cual inicialmente como prioridad, se tenía que implementar toda la infraestructura de red necesaria para la comunicación segura de los servidores a nivel nacional.

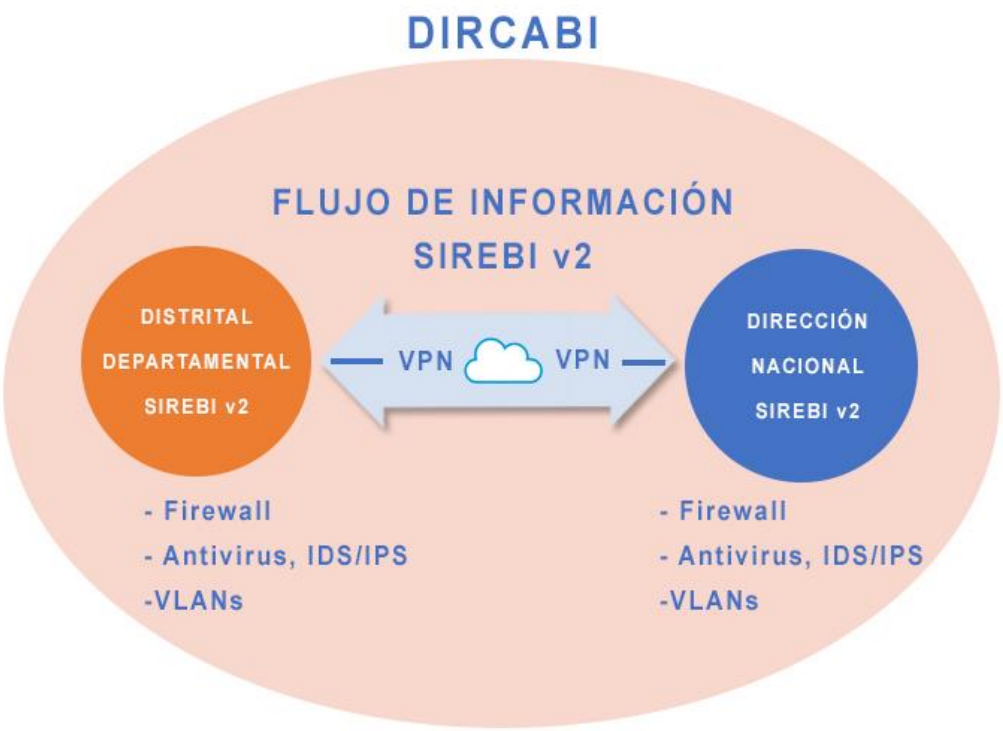


Figura 3
Fuente: Elaboración propia**.**

2.1.1. Objetivo

2.1.1.1. Objetivo Principal

- Diseño del Esquema de Seguridad Perimetral y su implementación para la red de datos de la Dirección de Registro, Control y Administración de Bienes Incautados del Narcotráfico, con el fin de que la confidencialidad, integridad y disponibilidad de la información que administra DIRCABI fueran preservadas.

2.1.1.2. Objetivos Secundarios

- Relevamiento de información de la situación actual de la red lógica y física de la DIRCABI a nivel nacional.
- Configuración de políticas en los firewalls, en el nivel de red, con el adecuado diseño de segmentación con políticas de acceso a las VLANs.
- Estudio de costos para la adquisición de los equipos, para la implementación de la solución integrada.
- Servidores de bases de datos instalados en las 7 distritales departamentales y la dirección nacional.
- Sistema de Registro de Bienes Incautados "SIREBI v2" implantado en las 7 distritales departamentales y la dirección nacional.

2.1.2. Justificación.

La utilización de servicios informáticos, redes e Internet como medios para transferir, procesar y almacenar información en los últimos años; ha incrementado y transformado la información digital a un activo de altísimo valor[1] , por lo cual se debe proteger y asegurar.

La seguridad de las redes es una parte integral de las redes informática que incluye protocolos, tecnologías, dispositivos, herramientas y

[1] "La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente." (Carlos Andrés Gil, Jonathan Martínez, Julieth Veloza & Ray Alejandro Mora, ISO/IEC 27001)

técnicas, que aseguran los datos y reducen las amenazas. Así también está directamente relacionada con la confidencialidad, integridad y disponibilidad de la información que administra.

Una brecha en la seguridad de la red puede causar la pérdida de datos, amenazar la privacidad de los usuarios (con potenciales consecuencias legales y económicas), comprometer la integridad y confiablidad de la información que administra DIRCABI, a través del sistema SIREBI v2.

El sistema SIREBI v2, administraba lo siguiente:

- Información general a nivel nacional de todos los casos abiertos, en proceso y concluidos provenientes del narcotráfico.
- Información legal: relacionado con el monitoreo, desde la apertura del caso con la incautación de los bienes del narcotráfico, hasta la conclusión del mismo, lo cual significa que el caso tiene una sentencia ejecutoriada.
- Información económica: realiza un monitoreo de las cuentas en banco y el movimiento de dinero incautado del narcotráfico. Así también realiza un control de movimiento de dinero proveniente de la monetización de los bienes incautados.

Toda la información que administra el sistema es respaldada con documentación digitalizada, la misma que es almacenada en los diferentes servidores.

El aprendizaje de los usuarios es una parte importante en éste modelo de seguridad, ya que por lo general, el desconocimiento de la importancia de llevar la información con responsabilidad, puede llevar consigo varios riesgos. Es por eso, que la creación de un manual de políticas y procedimientos en base a la norma ISO 27001[2] apoyo en la seguridad de

[2] ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. (https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/)

la información que cursa por la red, protegiéndola de posibles ataques externos e internos. Por lo tanto, mantener la red segura, evita que la seguridad de los usuarios y de la red sea vulnerable; y de esta manera proteger los intereses de DIRCABI.

Así también, el modelo de seguridad implementado, requiere vigilancia de parte de los profesionales encargados de sistema de DIRCABI, quienes deberían estar constantemente actualizados, en las nuevas y evolucionadas amenazas y ataques a las redes, así como de las vulnerabilidades de los dispositivos y aplicaciones en uso.

2.1.3. Alcances y límites.

2.1.3.1. Alcances

Para determinar el alcance del proyecto, se debió delimitar de manera adecuada el campo de acción de la investigación, considerando la información obtenida en el estudio realizado de la situación en la que se encontraba la red DIRCABI. En base a ello se hizo lo siguiente:

- Se realizó el relevamiento de información de la situación actual de la red de datos de DIRCABI, tanto de la red física como lógica y se determinaron las vulnerabilidades y amenazas a las que estaba expuesta. En base a estos aspectos, se establecieron los requerimientos de seguridad, lo que permitió diseñar un esquema que se adaptara a las necesidades de DIRCABI.

- Se adecuaron los ambientes físicos para el centro de procesamiento de datos, de cada distrital departamental, tomando en cuenta los requerimientos mínimos y necesarios en cuanto el sistema eléctrico (energía regulada y unidades UPS), sistema de climatización (refrigeración para regular las condiciones ambientales).

- El proyecto implementó una plataforma segura para el control de accesos y protección de los servicios informáticos, garantizando un

correcto aprovechamiento de la infraestructura; garantizando la integridad y confidencialidad de la información que administra DIRCABI, en sus diferentes distritales departamentales. El modelo diseñado resaltó la importancia de instalar routers, firewalls, IDS/IPS, así como la reorganización de los servidores, sin dejar de analizar los fundamentos necesarios que nos permitirán realizar la segmentación de la red mediante VLANs con políticas de acceso a las mismas.

- El proyecto permitió la implementación de la red de servidores de bases de datos del SIREBI v2 en las 7 distritales departamentales y la dirección nacional. Los servidores permitieron el flujo de procesos de información en tiempo real mediante el uso de VPNs.

2.1.3.2. Limites

- El proyecto no contempla medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, robo de activos.
- El proyecto tuvo como prioridad precautelar la integridad del centro de procesamiento de datos en cuanto al sistema eléctrico y sistema de climatización. Actividades que fueron gestionadas y supervisadas por las direcciones departamentales y el director de sistemas de la dirección nacional.
- La red de seguridad perimetral no cuenta con sistemas de redundancia en caso de que los firewalls fallen, lo cual involucra una constante supervisión y monitoreo por los encargados de sistema de las distritales departamentales.
- El proyecto no contempla una zona DMZ (desmilitarizada), debido a que no existen recursos públicos, como servidores de correo electrónico, web y DNS (servidor de nombres de dominio). La conexión es privada, entre servidores de las distritales departamentales y el servidor central, mediante el uso de VPNs.

- La limitación económica, fue uno de los factores preponderantes para el no cumplimiento de la norma ISO 270001 sobre la seguridad de la información y el estándar TIA-942 (recomendaciones y directrices para la instalación de Centros de Procesamiento de Datos). Se tuvo que priorizar la implementación de servidores y equipos de seguridad, en aquellas distritales donde la transacción de datos era alta por día y ver otras soluciones más económicas para algunas distritales departamentales.

2.1.4. Marco Referencial.

El proyecto se encuentra dentro de los lineamientos básicos de seguridad informática que se detallan dentro del Reglamento de Sistemas Informáticos con los que contaba la institución. Pero se tuvo la necesidad de una revisión y actualización de las políticas de organización, políticas sobre centralización de actividades, políticas sobre datos y políticas de costos de informática.

El proyecto cumplió:

- Con los fundamentos de comunicación en redes de datos.
- Con bloqueo de accesos no autorizados con el menor riesgo de caída de los servidores de datos.
- Con un análisis de costos del equipamiento informático y licencias necesarias para la implementación.

Al implementar el SIREBI v2 a nivel nacional teniendo como medio de comunicación el Internet, el mismo se encuentran abierto a posibles riesgos de accesos no autorizados y/o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios autorizados. Por lo tanto se incluyó medidas necesarias para detectar, documentar y contrarrestar dichas amenazas.

La seguridad de la tecnología de la información, se orienta a la protección de la infraestructura de red y todo lo relacionado a esta, de tal forma que garantice la confidencialidad, disponibilidad e integridad de datos mediante la protección, clasificación y conocimiento de impactos o daños

de las potenciales amenazas o intenciones perjudiciales de forma indirecta o directa para minimizar riesgos.

2.1.4.1. Definiciones.

Vulnerabilidades [3]

Las vulnerabilidades constituyen el otro factor que pone en peligro la seguridad de un sistema, generalmente se cree que una vulnerabilidad es un punto débil de un sistema y aunque no es una definición incorrecta, tampoco expresa en su totalidad lo que es una vulnerabilidad.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

Tipos de Vulnerabilidades

Las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes.

Para esta investigación, se clasifican las vulnerabilidades en seis tipos: Físicas, naturales, de hardware, de software, de red y de factor humano.

i. Física: Está relacionada con el acceso físico al sistema.

ii. Natural: Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.

iii. Hardware: Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable.

iv. Software: Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación.

[3] http://itroduc.blogspot.com/2015/08/vulnerabilidad-y-seguridad-de-redes-en.html

v. Red: Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

vi. Factor humano: Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema.

Amenazas [4]

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado).

Ataques [5]

Un ataque a una Red de datos es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar a otro sistema informático constituido como una Red de comunicación privada.

Tipos de ataques informáticos[6]

Entre los distintos tipos de ataques informáticos, se podría diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

[4] Instituto Nacional de Ciberseguridad de España

[5] https://www.slideshare.net/martinjosepomatolentino/ataque-a-la-red-de-datos-diapositivas

[6] Alvaro Gomez Vieites - https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

Los principales tipos de ataques son:

i. Actividades de reconocimiento de sistemas.

ii. Detección de vulnerabilidades en los sistemas.

iii. Robo de información mediante la interceptación de mensajes.

iv. Análisis del tráfico.

v. Ataques de suplantación de la identidad.

vi. Conexión no autorizada a equipos y servidores.

vii. Consecuencias de las conexiones no autorizadas a los sistemas informáticos.

viii. Ataques de Inyección de Código SQL: SQL, "Structured Query Language" (Lenguaje de Consulta Estructurado), es un lenguaje textual utilizado para interactuar con bases de datos relacionales.

ix. Ataques contra los sistemas criptográficos.

x. Denegación del Servicio (Ataques DoS – Denial of Service).

Mecanismos de seguridad.[7]

Los mecanismos de seguridad son técnicas que se utiliza para implantar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad.

Mecanismos de prevención: En esta etapa se toman las acciones necesarias para prevenir una posible intrusión o la violación de la seguridad, permitiendo aumentar la fiabilidad del sistema. Dentro del grupo de mecanismos de prevención tenemos:

Mecanismos de identificación y autenticación: Este sistema es el más utilizado permitiendo identificar de forma única al sistema.

Mecanismos de control de acceso: Mediante los mecanismos de control de acceso controlan los tipos de acceso al objeto por parte de cualquier entidad del sistema.

[7] Seguridad Informática, Aguilera Lopez

Mecanismos de separación: Si el sistema dispone de diferentes niveles de seguridad se deben implantar mecanismos que permitan separar los objetos dentro de cada nivel.

Mecanismos de seguridad en las comunicaciones: Se utiliza para garantizar la privacidad e integridad de los datos cuando viajan por la red.

Mecanismos de detección: Son aquellos que se utilizan para detectar violaciones a la seguridad o intentos de violaciones ya que si no se da cuenta del ataque el daño va a ser mayor.

Mecanismos de respuesta: Son aquellos que se aplican cuando una violación del sistema se ha detectado, ya que busca minimizar los efectos de un ataque o problema y finalmente retomar al sistema a su modo de trabajo normal.

Mecanismo de análisis forense: Permite determinar las acciones que ha realizado el atacante desde ver que agujeros de seguridad han utilizado para entrar al equipo, hasta ver las acciones que ha realizado en el sistema, de esta forma prevenir y detectar posteriores ataques al sistema.

Seguridad Perimetral [8]

La seguridad perimetral es un método de defensa de red, que se basa en el establecimiento de recursos de seguridad en el perímetro de la red y a diferentes niveles, permitiendo definir niveles de confianza, el acceso de usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de suportación (auto soportados, soportados, enterrados, detección visual, etc.).

[8] https://www.monografias.com/trabajos106/elementos-basicos-seguridad-perimetral/elementos-basicos-seguridad-perimetral.shtml

Existen varias tecnologías muy utilizadas como son: Firewalls, IDS, VPNs[9], DMZ[10] que permiten una administración centralizada de la red con niveles de protección.

Firewall [11]

Es un dispositivo de seguridad de red basado en hardware o software que supervisa el tráfico de red entrante y saliente, actuando como un intermediario entre la red local (o la computadora local) y una o varias redes externas (VPN site – site, Internet, etc), decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Un sistema firewall contiene un conjunto de reglas predefinidas que permiten: autorizar una conexión (allow), bloquear una conexión (deny), re direccionar un pedido de conexión sin avisar al emisor (drop).

El conjunto de estas reglas permite instalar un método de filtración dependiente de la política de seguridad adoptada por la organización. Se distinguen habitualmente dos tipos de políticas de seguridad que permiten:

– Permitir únicamente las comunicaciones autorizadas explícitamente: "Todo lo que no es autorizado explícitamente está prohibido".

– Impedir cualquier comunicación que fue explícitamente prohibida.

[9] VPN (Virtual Private Network): Red privada virtual es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

[10] DMZ (Zona Desmilitarizada): es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

[11] Cisco.com, INNOVA SECURE (https://innovasecure.com/que-es-un-firewall-y-cual-es-su-importancia-en-la-seguridad-informatica/)

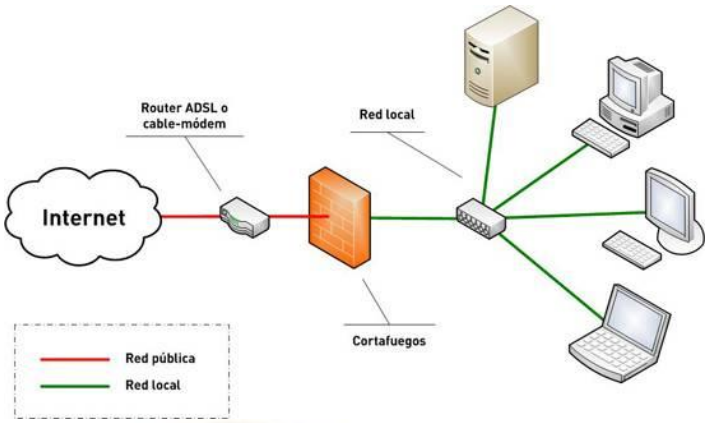


Figura 4: Esquema básico de seguridad con Firewall
Fuente: http://blog.deservidores.com/que-es-y-para-que-sirve-un-firewall/

Tipos de firewall

La descripción completa de los tipos de firewall se encuentra en anexos para mayor referencia.

Firewall proxy.

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como Gateway de una red a otra para una aplicación específica.

Firewall de inspección activa.

Un firewall de inspección activa, ahora considerado un firewall "tradicional", permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Este firewall monitorea toda la actividad, desde la apertura de una conexión hasta su cierre.

Firewall de administración unificada de amenazas (UTM)

Un dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus.

Firewall de próxima generación (NGFW)

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Arquitectura de Firewall[12]

Existen muchas formas de utilizar un Firewall en una empresa a estas formas de utilización se denomina arquitectura. La elección de la arquitectura depende del coste, el rendimiento y las necesidades de disponibilidad de la información que es protegida.

Las arquitecturas más comunes son:

i.- Cortafuegos de filtrado de paquetes

El modelo de cortafuegos más antiguo consiste en un dispositivo capaz de filtrar paquetes, lo que se denomina choke[13]. Está basado simplemente en aprovechar la capacidad que tienen algunos routers para bloquear o filtrar paquetes en función de su protocolo, su servicio o su dirección IP.

Esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad, donde el router actúa como de pasarela de la subred y no hay necesidad de utilizar proxies, ya que los accesos desde la red interna al exterior no bloqueados son directos. Resulta recomendable bloquear todos los servicios que no se utilicen desde el exterior, así como el acceso desde máquinas que no sean de confianza hacia la red interna.

Figura 5: Cortafuegos de filtrado de paquetes
Fuente: Arquitectura de los cortafuegos – Universidad Politécnica de Valencia

[12] OstecBolg – Seguridad virtual (https://ostec.blog/es/seguridad-perimetral/entendiendo-principales-topologias-de-firewall) Canal de difusión de la Universidad Rey Juan Carlos – España (https://www.youtube.com/user/universidadurjc/videos),
http://spi1.nisu.org/recop/al01/rmoreno/arquitecturas.html

[13] Choke es un dispositivo capaz de filtrar paquetes

ii.- Arquitectura Dual-Homed Host

Este modelo se compone de simples máquinas Unix, denominadas anfitriones de dos bases, equipadas con dos tarjetas de red: una se conecta a la red interna a proteger y la otra a la red externa. De este modo, los sistemas de la red interna se pueden comunicar con el dual-homed host, así como los sistemas del exterior también se pueden comunicar con el dual-homed host; es decir, el tráfico entre la red interna y el exterior está completamente bloqueado. En este caso el choke y el bastión coinciden en el mismo equipo.

Los dual-homed host pueden proporcionar un nivel de control muy elevado. Como no se permite el tráfico de paquetes entre la red interna y la externa, un paquete de fuente externa será indicativo de alguna clase de problema de seguridad. Todo el intercambio de datos entre las redes se realiza a través de servidores proxy situados en el host bastión. Para cada uno de los servicios que se deseen pasar a través del firewall, se ha de ejecutar un servidor proxy.

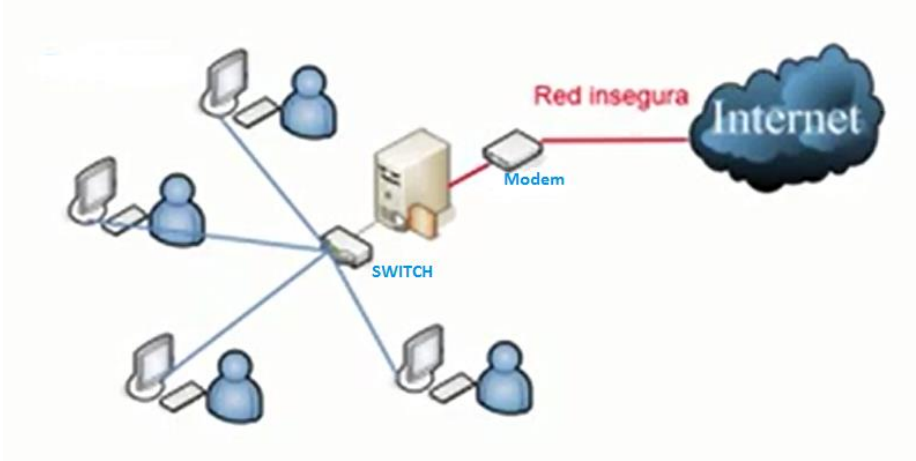


Figura 6: Arquitectura Dual-Homed Host
Fuente: Arquitectura de los cortafuegos – Universidad Politécnica de Valencia.

iii.- Arquitectura Screened Host

En esta arquitectura se combina un screening router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. El screening router está situado entre el host bastion y la red externa, mientras que el host bastión está situado dentro de la red interna.

El filtrado de paquetes en el screening router está configurado de modo que el host bastión es el único sistema de la red interna accesible desde la red externa. Incluso, únicamente se permiten ciertos tipos de conexiones. Cualquier sistema externo que intente acceder a los sistemas internos tendrán que conectar con el host bastión. Por otra parte, el filtrado de paquetes permite al host establecer las conexiones permitidas, de acuerdo con la política de e seguridad, a la red externa.

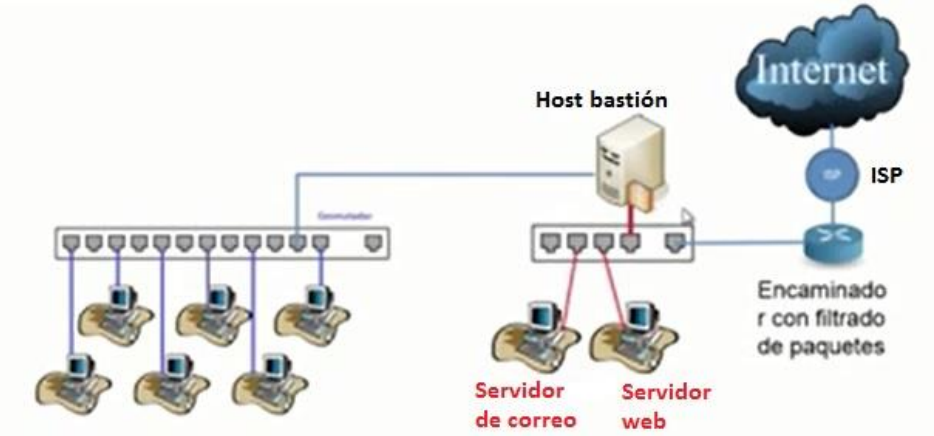


Figura 7: Arquitectura Screened Host
Fuente: Arquitectura de los cortafuegos – Universidad Politécnica de Valencia

iv.- Arquitectura Screeened Subnet

La arquitectura Screened Subnet también se conoce con el nombre de red perimétrica o zona desmilitarizada (DMZ). En los modelos anteriores, la seguridad se centraba completamente en el host bastión, de manera que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. En cambio, en este modelo se añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consigue reducir los efectos de un ataque exitoso al host bastión. La arquitectura DMZ intenta aislar la máquina bastión en una red perimétrica, de forma que si un intruso accede a esta máquina no consigue un acceso total a la subred protegida.

Se trata de la arquitectura de firewalls más segura, pero también más compleja. En este caso se emplean dos routers, exterior e interior, ambos

conectados a la red perimétrica. En dicha red perimétrica, que constituye el sistema cortafuegos, se incluye el host bastión. También se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de la red interna.

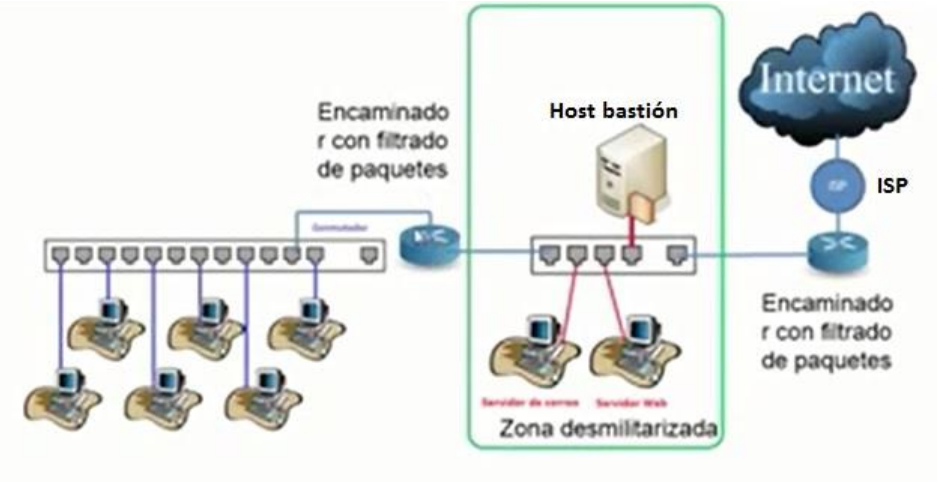


Figura 8: Arquitectura Screened Subnet
Fuente: Arquitectura de los cortafuegos – Universidad Politécnica de Valencia

v.- Otras arquitecturas

Una manera de incrementar en gran medida el nivel de seguridad de la red interna y al mismo tiempo facilitar la administración de los cortafuegos consiste en emplear un host bastión distinto para cada protocolo o servicio en lugar de un único host bastión. Muchas organizaciones no pueden adoptar esta arquitectura porque presenta el inconveniente de la cantidad de máquinas necesarias para implementar los cortafuegos.

2.2. Desarrollo.

En esta sección se detalla todas las actividades que se realizaron para la implementación de la Seguridad Perimetral, en las 7 distritales departamentales y la Dirección Nacional.

El proyecto se inició con la revisión de la norma ISO 27001 y el estándar TIA 942.

La norma ISO 270001 establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Contiene 11 secciones sobre controles de la seguridad de las cuales se hizo énfasis en políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos, seguridad física y del entorno, teniendo en cuenta las limitaciones tanto en infraestructura como económica ya descritas en la sección 2.1.3.2 (limitaciones del proyecto).

Asimismo, se analizó y estudio la factibilidad de cumplir con las recomendaciones del estándar TIA 942; respecto a los subsistemas de telecomunicaciones, arquitectura, eléctrica y mecánica, para la instalación del Centro de Procesamiento de Datos (CPD).

Seguidamente se procedió con el relevamiento de información para conocer el grado de recursos tecnológicos con los que se contaba en las distritales departamentales.

Teniendo conocimiento de los recursos y el estado de la red de datos, se realizó el diseño de la Red de Seguridad Perimetral, para posteriormente realizar un análisis de los equipos existentes en el mercado; así también se realizó un análisis de costos teniendo en cuenta que se tenía limitaciones económicas para la adquisición de los mismos.

Finalmente se describe la implementación de la red.

2.2.1. Relevamiento Infraestructura Tecnológica

En el inicio del proyecto, se definió claramente el planteamiento de los problemas, objetivos, establecimiento de la justificación y los alcances.

La base del desarrollo del proyecto está en el planteamiento de que no existía anteriormente un sistema de datos centralizado en la Dirección Nacional, por lo tanto, en el momento que se interconecten los servidores departamentales con el servidor central, este se encontraba expuesto ante ataques externos e internos.

Por lo tanto se realizó un relevamiento de información para conocer los recursos tecnológicos existentes en las 7 distritales departamentales y la Dirección Nacional con vista a la implementación de la seguridad perimetral de la red institucional.

Para esta relevamiento se realizaron entrevistas, las cuales respondieron a encuestas y formularios con la información relacionada con lo siguiente:

- Hardware e infraestructura: Tipo de hardware con el cual se contaba. Además se verifico la posibilidad de realizar obras civiles en la infraestructura, para la implementación de un centro de procesamiento de datos.

- Instalaciones eléctricas: Se verificó la existencia de instalaciones eléctricas con puestas a tierra, fuentes reguladas, instalaciones eléctricas independientes para el centro de datos y comunicaciones.

- Equipamiento informático: Se verificó la cualidad, estado y cantidad de equipos host y servidores.

- Software y licencias: Se verificaron licencias tanto de sistemas operativos y antivirus, en los equipos host y servidores.

- Comunicaciones y redes: Se verificó el tipo de conexión a internet y la existencia de cableado estructurado normado (TIA/EIA 568-B).

- Recursos humanos encargados de los sistemas: Se verificó que el personal tuviera los conocimientos en administración de base de datos, administración de redes e infraestructura, soporte, apoyo y capacitación en políticas de uso de los equipos.

Todo el relevamiento se realizó de manera personal, en cada una de las distritales departamentales, contando con la colaboración de los encargados de sistemas.

2.2.1.1. Hardware e Infraestructura.

Oficinas	Propiedad de los ambientes	Servidores Existentes y en Funcionamiento	El Centro de Procesamiento de Datos se encuentra en ambiente separado	Observaciones
DIRECCIÓN NACIONAL	Propia	Servidor Proxi. Servidor de aplicaciones	SI	
LA PAZ	Propia	Servidor de aplicaciones	SI	
COCHABAMBA	Propia	Servidor de aplicaciones	NO	
SANTA CRUZ	Propia	Servidor de aplicaciones	SI	
ORURO	Alquilada	Ninguno	NO	El sistema SIREBI v1 se encontraba en funcionamiento en la máquina del encargado de sistemas.
TARIJA	Alquilada	Servidor de aplicaciones	SI	El servidor de aplicaciones fue implementado en una PC Pentium IV.
BENI	Alquilada	Ninguno	NO	El sistema SIREBI v1 se encontraba en funcionamiento en la máquina del encargado de sistemas
PANDO	Alquilada	Ninguno	NO	El sistema SIREBI v1 se encontraba en funcionamiento en la máquina del encargado de sistemas

2.2.1.2. Instalaciones Eléctricas.

	OFICINAS							
	Dirección Nacional	La Paz	Cochabamba	Santa Cruz	Oruro	Tarija	Beni	Pando
¿Existe instalación de aterramiento para el sistema de energía y el centro de procesamiento de datos?	SI	SI	SI	SI	NO	SI	NO	NO
¿Existe una instalación eléctrica independiente para equipos informáticos de usuario?	SI	SI	NO	NO	NO	NO	NO	NO
¿Existe una instalación eléctrica independiente para el centro de procesamiento de datos?	SI	SI	NO	NO	NO	NO	NO	NO
¿Existe una instalación eléctrica independiente para equipos de telecomunicaciones?	SI	SI	NO	NO	NO	NO	NO	NO
¿Existen unidades ininterrumpidas de energía (UPS) (para el centro de procesamiento de datos)?	SI	SI	SI	SI	NO	SI	NO	NO

2.2.1.3. Equipamiento Informático.

Oficinas	Detalle de los equipos existentes
Dirección Nacional	- Existían aproximadamente 30 computadores personales con procesadores Pentium III y Pentium IV. - Existía 1 servidor HP XENON para servidor de aplicaciones. - Existía 1 PC HP Pentium IV para servidor proxi
La Paz	- Existían aproximadamente 20 computadores personales con procesadores Pentium III y Pentium IV. - Existía 1 servidor HP XENON para servidor de aplicaciones.
Cochabamba	- Existían aproximadamente 25 computadores personales con procesadores Pentium III y Pentium IV. - Existía 1 servidor HP XENON para servidor de aplicaciones.
Santa Cruz	- Existían aproximadamente 25 computadores personales con procesadores Pentium III y Pentium IV. - Existía 1 servidor HP XENON para servidor de aplicaciones.
Oruro	- Existían aproximadamente 6 computadoras personales con procesadores Pentium III y Pentium IV.
Tarija	- Existían aproximadamente 10 computadores personales con procesadores Pentium III y Pentium IV. - Existía 1 PC HP Pentium IV para servidor de aplicaciones y Base de Datos
Beni	- Existían aproximadamente 6 computadoras personales con procesadores Pentium III y Pentium IV.
Pando	- Existían aproximadamente 6 computadoras personales con procesadores Pentium III y Pentium IV.

2.2.1.4. Software y Licencias.

Se contaba con 4 licencias Windows 2000 Server, exclusivamente solo para los servidores. Un 80% de los equipos personales no contaba con licencias de sistema operativo y/o herramientas de ofimática.

Los equipos contaban con un conjunto de aplicaciones que permiten realizar las tareas ofimáticas. Así también, se contaba con un software antivirus y herramienta anti-spyware de Mcafee.

2.2.1.5. Comunicación y Redes.

Oficinas	Conexión a Internet		Cableado Estructurado	Velocidad Kbps
	ADSL	DIAL UP		
Dirección Nacional	SI		SI	1024
La Paz	SI		SI	1024
Cochabamba	SI		SI	1024
Santa Cruz	SI		SI	1024
Oruro	SI		NO	512
Tarija	SI		NO	512
Beni		SI	NO	56
Pando		SI	NO	56

2.2.1.6. Recursos Humanos Encargados de los Sistemas.

La unidad de sistemas de cada dirección departamental es directa responsable por la administración y seguridad de la información de los servidores. Por lo tanto, estas tienen conocimiento en técnicas de mantenimiento de hardware y software. Las redes locales están bajo el soporte del personal de sistemas. Sin embargo, fue necesario especializar a un técnico en las siguientes áreas:

- Administración de base de datos.
- Administración de redes e infraestructura.
- Soporte, apoyo y capacitación.

En la evaluación de habilidades y conocimientos del personal de sistemas, se notó que existían debilidades en RRHH de las departamentales Beni, Pando, por lo que se consideraron otros planes de contingencia y monitoreo, cuando se implementó la seguridad perimetral.

2.2.2. Diseño De Red De Seguridad Perimetral

Considerando la infraestructura y requerimientos actuales de la red de datos de la DIRCABI, se diseñó un modelo jerárquico[14] y la segmentación lógica de la red. Brindando así una solución para la seguridad de la información que administra el SIREBI v2.

En el modelo jerárquico, la red está organizada en capas que realizan tareas específicas, como ser:

- Conmutación (switching); controla a los usuarios y el acceso de grupos de trabajo (workgroup access) o los recursos de internetwork.

- Enrutamiento (routing); filtrado de paquetes, se implementa la seguridad y políticas de red, ruteo entre VLANs y otras funciones de grupo de trabajo.

- Switchear tráfico tan rápido como sea posible y se encarga de llevar grandes cantidades de tráfico de manera confiable y veloz.

Las ventajas de la implementación de este modelo son:

- Escalabilidad: Las redes jerárquicas pueden expandirse con facilidad.

[14] Modelo jerárquico se divide la red en varias capas independientes. Es una red plana que se divide en bloques más pequeños y fáciles de administrar. Cada capa del diseño desempeña una función específica.

- Redundancia: La redundancia a nivel del núcleo y de la distribución asegura la disponibilidad de la ruta.

- Rendimiento: Mejor comunicación al utilizar switches de alto rendimiento.

- Seguridad: La seguridad del puerto en el nivel de acceso y las políticas en el nivel de distribución, hacen que la red sea más segura.

- Facilidad de administración: La consistencia entre los switches en cada nivel hacen que la administración sea más simple. Se puede copiar la configuración de los switches.

- Facilidad de mantenimiento: Debido a que los dispositivos de cada nivel tienen funciones similares y bien definidas, este modelo permite a los administradores de red añadir, reemplazar o eliminar elementos de la red de forma sencilla. Este tipo de flexibilidad y adaptabilidad, hace que la red sea escalable.

Este modelo de red, divide el complejo problema del diseño de la misma en otros problemas más pequeños y manejables, ya que cada nivel identifica un conjunto diferente de problemas en el hardware y software. Los dispositivos del primer nivel están diseñados para aceptar tráfico de una red y pasarlo hacia las capas superiores. Este diseño está agrupado en tres capas: Capa Central (Core o Núcleo), Capa de Distribución y Capa de Acceso.

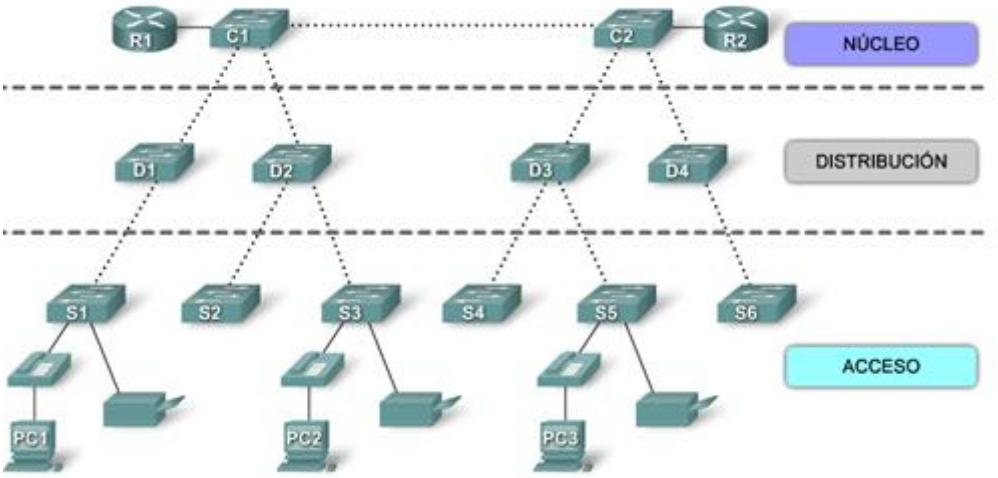


Figura 9: Modelo de Diseño Jerárquico
Fuente: Documentación CISCO.

En base a este modelo, se describirán los equipos utilizados en el diseño.

2.2.2.1. Capa Central (Core o Núcleo).

Esta capa ofrece una estructura de transporte fiable y optimizado para reenviar el tráfico a altas velocidades, es capaz de conmutar paquetes tan rápido como sea posible. Esta capa ofrece una ruta rápida entre los servidores de las distritales departamentales.

Además, dada la importancia de la velocidad, no hace funciones que puedan aumentar la latencia, como access-list, ruteo interVLAN, filtrado de paquetes, ni tampoco workgroup access. Esta capa debe proporcionar una alta confiabilidad y tolerancia a fallas.

De acuerdo a nuestras necesidades, en esta capa se instaló un router, el cual manejaría las comunicaciones entre los servidores de las distritales departamentales; es decir, en este equipo sólo está permitido enrutar tráfico hacia y desde las redes con las que se tiene confianza (red institucional), usando como medio de comunicación el Internet.

Las aplicaciones importantes y necesarias que tenía que soportar el equipo instalado fueron las siguientes:

- Acceso VPN con firewall y opciones de cifrado.
- Enrutamiento con gestión de ancho de banda.
- Integración de enrutamiento flexible y conmutación de baja densidad.
- Integración de redes de contenido.
- Integración de sistemas de detección de intrusos (IDS).
- Integración de sistemas de análisis de redes.

2.2.2.2. Capa de Distribución.

La capa de Distribución es el medio de comunicación entre la capa de acceso y la capa central. Las funciones, de esta capa son proveer ruteo, filtrado, acceso a la red WAN y determinar que paquetes deben llegar al Core. Además, determina cuál es la manera más rápida de responder a los requerimientos de red, por ejemplo, como traer un archivo desde un servidor.

Aquí además se implementaron las políticas de red, por ejemplo: ruteo, listas de acceso (access-list), filtrado de paquetes, cola de espera, se implementa la seguridad y políticas de red, la redistribución entre protocolos de ruteo (incluyendo rutas estáticas), ruteo entre VLANs y otras funciones de grupo de trabajo, se definen dominios de broadcast y multicast.

2.2.2.3. Capa de Acceso.

La capa de acceso de la red, es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual, la capa de acceso se denomina a veces como capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los

recursos, switches y usuarios finales. En la capa de acceso se pueden encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos, el tráfico de usuarios que demandan estos servicios, se desvía a la siguiente capa del modelo: la capa de distribución.

2.2.2.4. Esquema de la Arquitectura Propuesta e Implementada

Para el diseño, en una etapa inicial se consideraron algunas políticas administrativas e institucionales de DIRCABI, como ser las siguientes:

- Definir el nivel de monitorización, redundancia y control deseado en la organización; una vez definida la política a seguir, hay que definir cómo implementarla en el cortafuego indicando básicamente qué se va a permitir y qué se va a denegar (configuración de firewall y listas de acceso). Para esto existen dos aproximaciones generales: o bien se adopta una postura restrictiva (denegamos todo lo que explícitamente no se permita); o bien una permisiva (permitimos todo excepto lo explícitamente negado).

- Consideración económica, una de las limitaciones dentro del proyecto fue la parte económica por lo que se elaboraron dos tipos de estructura basándose en la densidad de información y documentación que generaban en las diferentes distritales departamentales, una estructura basada en equipos de seguridad físicos (hardware) y otra combinando hardware y software. Con este tipo de estructuras se logró que los gastos económicos disminuyeron significativamente, pero que puedan resguardar y proteger la información que administra DIRCABI.

La parte fundamental del diseño en la estructura, fue la decisión técnica que considera el tipo de arquitectura implementado, es decir, la ubicación del firewall en la red donde cumpla eficientemente su cometido.

Una vez definido la arquitectura, se eligieron los elementos físicos a utilizar como bastion[15]; Para tomar esta decisión existen dos principios básicos: mínima complejidad y máxima seguridad. Cuanto más simple sea el host bastion, cuanto menos servicios ofrezca, más fácil será su mantenimiento y por tanto mayor su seguridad. Mantener esta máquina especialmente asegurada es algo vital para que el cortafuegos funcione correctamente, ya que va a soportar por sí sola todos los ataques que se efectúen contra la red al ser elemento más accesible de ésta. Si la seguridad de la máquina bastion se ve comprometida, la amenaza se traslada inmediatamente a todos los equipos dentro del perímetro de seguridad. Una vez elegido un bastión se decidió que elemento se utilizara choke[16]. Generalmente suele ser un router con capacidad para filtrar paquetes, aunque también puede utilizarse un servidor Linux para realizar esta función.

Habiendo tomado las anteriores consideraciones se diseñaron los siguientes esquemas de red, basados en las arquitecturas de firewall, conocidas como ser:

- Cortafuegos de filtrado de paquetes (screening routers)
- Dual Homed.
- Screened Host.
- Screened Subnet.

Las mismas que fueron descritas en la sección de conceptos y definiciones (página 26 – Arquitectura de firewall).

[15] Se llama bastión al sistema que actúa como intermediario. Es el punto de contacto de los usuarios de la red interna de una organización con otro tipo de redes. El bastión filtra tráfico de entrada y salida.
[16] Choke es un dispositivo capaz de filtrar paquetes.

ESQUEMA DE SEGURIDAD PERIMETRAL DE LA DIRECCION NACIONAL, DEPARTAMENTALES LA PAZ, COCHABAMBA Y SANTA CRUZ.

La arquitectura adoptada para las distritales indicadas fue la Screened Subnet, ya que esta arquitectura tiene un "screening router", conectado entre el perímetro y la red externa, lo cual aísla fuertemente la red interna de Internet; y un firewall entre el perímetro y la red interna. Para destruir la red interna con este tipo de arquitectura, el atacante debe pasar por ambos elementos.

Los hosts bastiones son las máquinas más vulnerables en la red. Aunque se esfuerce en protegerse, estas son las máquinas que pueden ser atacadas, porque ellas son las máquinas que son vistas por la red externa.

Al aislar el host bastion en un perímetro, se puede reducir el impacto de atacar al host bastion.

Si un atacante logra destruir al host bastion, deberá lograr pasar por el switch de capa 3 de la capa de distribución.

Este tipo de arquitectura puede gestionar tres o más interface de red, permite definir políticas de seguridad y de acceso de una interface de red a cualquiera de las otras.

En el presente caso existían múltiples sub redes protegidas que deben ser directamente interconectadas por el firewall. Por lo tanto, se trabajó con VLANs, las mismas que fueron implementadas a través de un switch de capa 3.

La funcionalidad de los switch de capa 3 para la red de distribución, obedece a las políticas de seguridad que pueden aplicarse al tráfico de red. Se utilizan las listas de acceso para controlar como fluye el tráfico a través de la red.

El switch de capa de distribución también necesita admitir QoS para mantener la prioridad del tráfico que proviene de los switches de capa de acceso.

Asimismo, se hace notar que en el diseño no se contempla zonas DMZ, de acuerdo a lo indicado en las limitaciones del proyecto.

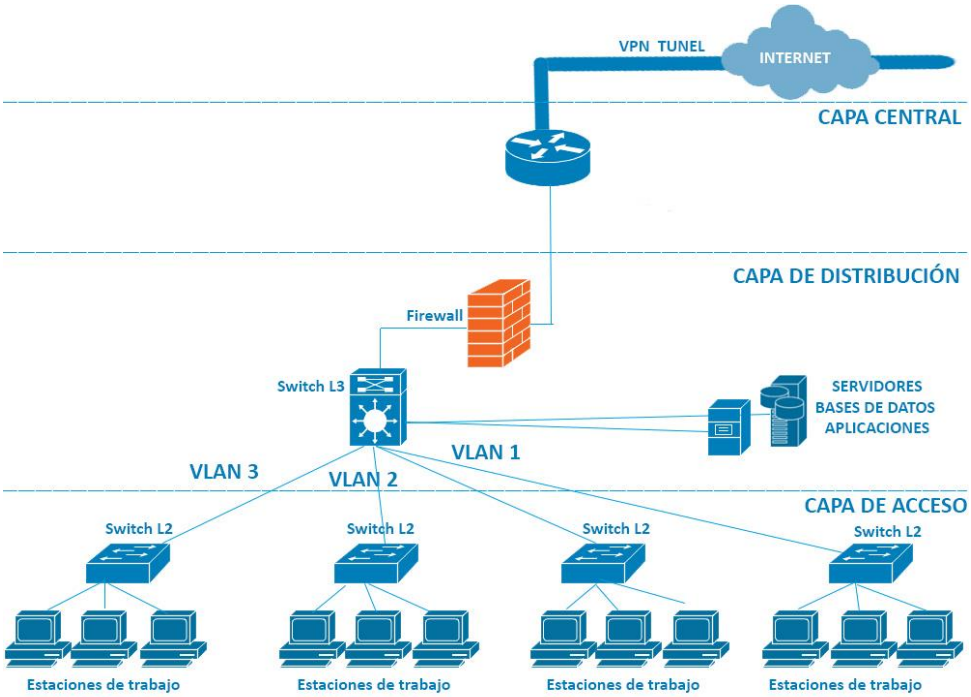


Figura 10
Fuente: Elaboración propia**.**

ESQUEMA DE SEGURIDAD PERIMETRAL DE LAS DIRECCIÓNES DEPARTAMENTALES TARIJA, ORURO, BENI Y PANDO

La arquitectura adoptada para las distritales indicadas, fue la Dual Homed Host, la que implica una computadora con dos interfaces de red. En las que una de las tarjetas se conecta a la red interna a proteger y la otra a la red externa a la Institución. En esta configuración el choke y el bastión coinciden en el mismo equipo Host Linux. El host actúa como router entre las dos redes que el conoce, es capaz de rutear paquetes IP desde una red a otra. Pero los paquetes IP de una red a la otra no son ruteados directamente. El sistema interno al firewall puede comunicarse con el dual-homed host, y los sistemas fuera de firewall también pueden comunicarse con él, pero los sistemas no pueden comunicarse directamente entre ellos.

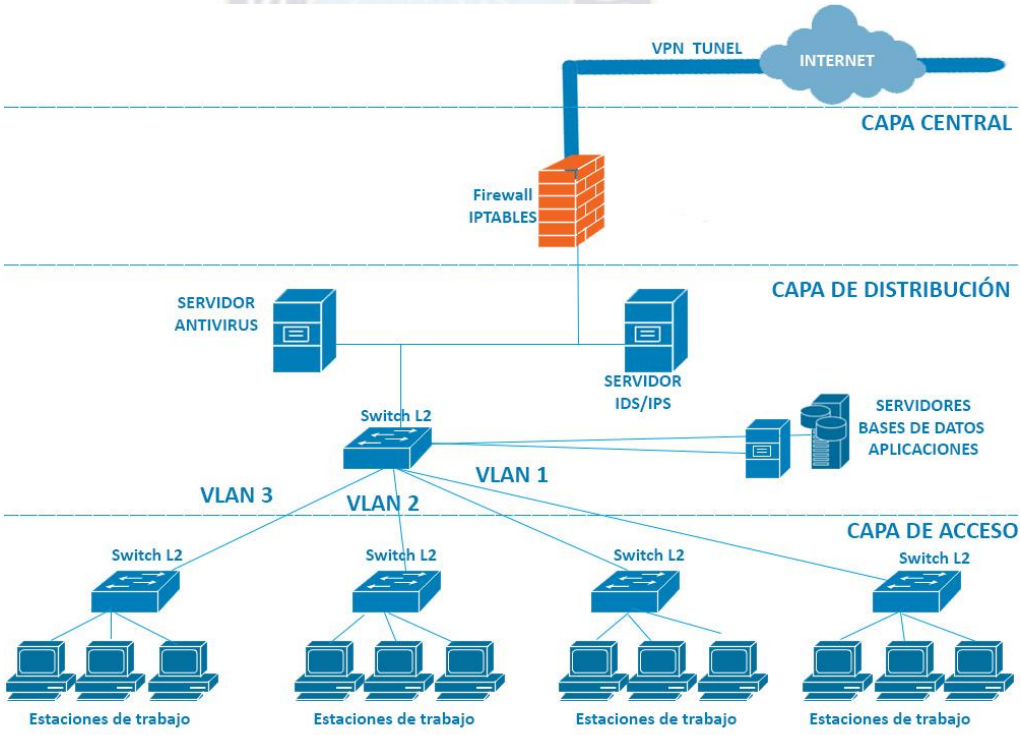


Figura 11
Fuente: Elaboración propia**.**

ESQUEMA DE SEGURIDAD PERIMETRAL GLOBAL

El Esquema Global fue la combinación de las arquitecturas Screened Subnet y Dual Home Host, dependiendo de la distrital departamental de DIRCABI.

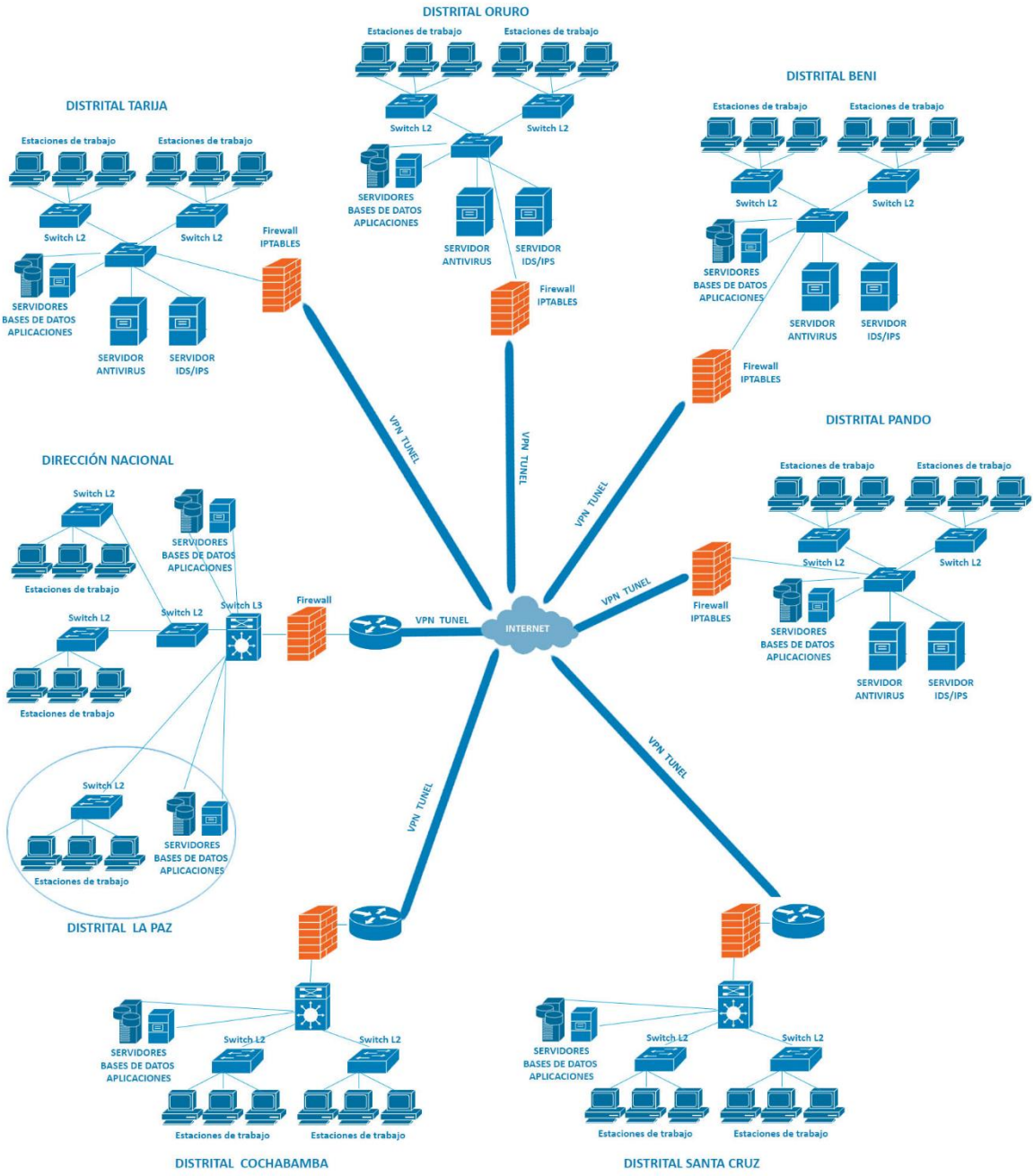


Figura 12.
Fuente: Elaboración propia**.**

2.2.3. Elección de la Solución

Para la selección de equipos y/o software que podrían cumplir los requerimientos de la seguridad perimetral, se tomaron en cuenta los siguientes factores:

- Compatibilidad y Flexibilidad: Para que la solución permita añadir funcionalidades y servicios, según los requisitos del usuario o del sistema en sí; disminuyendo la probabilidad de riesgos en el tiempo ante el posible de ataques informáticos.

- Escalabilidad: Para que la solución tenga la propiedad de aumentar la capacidad de trabajo o de tamaño de un sistema sin comprometer el funcionamiento y calidad normales del mismo.

- Proveedores: Que tengan una amplia experiencia en proyectos similares y que puedan ofrecer una amplia variedad de soluciones (productos) y que puedan proveer de servicios profesionales en capacitación para la implementación de los equipos.

- Costos: Las soluciones planteadas en cuanto a Firewalls físicos eran de gran costo, por lo cual se tuvieron las siguientes consideraciones:

    - Adquisición de equipos para el Servidor Nacional que tuvieran altas capacidades de soporte, funcionalidad y flexibilidad.

    - Adquisición de equipos para las distritales departamentales tomando en cuenta la densidad de información de bienes incautados que generan.

Esta disposición fue realizada por la Dirección Nacional, por lo tanto se tomó la decisión de realizar la combinación de hardware y software en aquellas distritales departamentales (Tarija, Oruro, Beni y Pando), donde la densidad de información de bienes incautados era de volumen pequeño comparado con la Dirección Nacional, Distrital La Paz, Distrital Santa Cruz y Distrital Cochabamba. Solución que marco una gran diferencia económica.

2.2.4. Adquisición de Equipos, Mantenimiento preventivo y correctivo del hardware e infraestructura tecnológica.

2.2.4.1. Infraestructura Centro Procesamiento de Datos.

Según el estándar TIA-942, la infraestructura de soporte de un centro de procesamiento de datos (CPD) debe estar compuesto por cuatro subsistemas como lo son telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico. De acuerdo a las limitaciones del proyecto (descritas en la sección alcances y limitaciones), solo se trabajó en los siguientes componentes:

- Telecomunicaciones: Cableado de racks, cableado horizontal, patch panels y patch cords.
- Arquitectura: Área de oficina, control de acceso.
- Sistema eléctrico: Sistema de aterramiento, panel de distribución y baterías (UPS).
- Sistema mecánico: Sistema de climatización.

Asimismo, la norma ISO 27001, se refiere a la seguridad de la información en las siguientes secciones:

- Seguridad física y del entorno, la cual tiene como objetivo evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización, riesgos o robos de los recursos; mediante la organización adecuada de las áreas de trabajo y de los activos en función de su criticidad.
- Gestión de comunicaciones y operaciones, cuya finalidad es mantener la integridad y disponibilidad de los servicios de información y telecomunicación, salvaguardando la información en las redes y protegiendo su infraestructura de apoyo.

- Control de accesos, su objetivo es controlar los accesos a la información evitando accesos no autorizados a los activos de la organización y protegiendo los servicios de la red.

- Gestión de incidentes en la seguridad de la información, tiene como objetivo comunicar los eventos en la seguridad de información, de manera oportuna, efectiva y ordenada, estableciendo responsabilidades y procedimientos de gestión. En caso de haberse encontrado una acción inapropiada de una persona o grupo dentro de la organización, se debe recolectar la evidencia, la misma que será retenida y presentada para tomar acciones legales.

- Aspectos de seguridad de la información en la gestión de la continuidad del negocio, su principal finalidad es reaccionar frente a las interrupciones operacionales de actividades del negocio, protegiendo sus procesos críticos frente a grandes fallas y desastres naturales.

Para la implementación de los CPD de las distritales departamentales, fueron tomadas en cuenta tanto la norma TIA-942 y la norma ISO 27001.

Las actividades realizadas en cada distrital departamental fueron:

Oficinas	Descripción de Actividades
Dirección Nacional y Departamental La Paz	
Cochabamba	- Instalación de mampara de vidrio templado. - Instalación de sistema de climatización.
Santa Cruz	- Mantenimiento al sistema de climatización existente.
Oruro	- Instalación de mampara de vidrio templado.
Tarija	- Instalación de mampara de vidrio templado. - Instalación de sistema de climatización.

Oficinas	Descripción de Actividades
Beni	- Instalación de mampara de vidrio templado. - Instalación de sistema de climatización.
Pando	- Instalación de mampara de vidrio templado. - Instalación de sistema de climatización.

Esta actividad se realizó con la contratación de terceras empresas, la cual estaba a cargo de cada dirección departamental, pero mi persona estuvo presente en la supervisión y recepción de los trabajos realizados.

2.2.4.2. Instalaciones Eléctricas.

Se realizó un mantenimiento preventivo y correctivo en el sistema eléctrico de las distritales departamentales, para cumplir con algunos requerimientos para el buen funcionamiento del CPD.

Las actividades realizadas fueron:

- Instalación y/o mantenimiento del sistema de aterramiento del edificio y/o del CPD. Esta actividad fue realizada previa evaluación del sistema, la cual estuvo a cargo de empresas externas, bajo la supervisión y aprobación del Director Distrital Departamental y el Director de Sistemas Nacional.

- Instalación eléctrica independiente para el centro de procesamiento de datos, equipo de telecomunicaciones, equipos informáticos de usuario. Para esto se instalaron tableros de distribución con los respectivos térmicos individuales para cada una de las dependencias.

- Instalación o mantenimiento de UPS. Con las siguientes características:

    - Rango de voltaje de entrada: CA 176 - 276 V.

    - Voltaje de salida: CA 220/230/240 V 50/60 Hz.

    - Capacidad de potencia: 7 kW / 10000 VA.

- Suministro de energía: 7 kW.
- Protección de circuito: disyuntor.
- Factor de forma externo (torre).
- Tecnología UPS en línea.
- Voltaje suministrado CA 220/230/240 V.
- Frecuencia suministrada 50/60 Hz.

- Instalación y/o mantenimiento de las tomas de corriente y tablero de distribución, con las siguientes especificaciones mínimas:
  - Tipo: Trifásico con barras de tierra y neutro.
  - Grado de protección: Clase IP-52
  - 20 Circuitos (mínimo).
  - Características eléctricas: Corriente nominal de 600A, corriente de corto circuito 10kA, tensión nominal de 400 V.
  - Térmicos de 100 Amp. (mínimo).
  - Tomas de corriente rectangular de 5,5x10x7,5 cm de fondo.
  - Cable ductos.
  - Conductores: los conductores deben ser continuos, sin empalmes, se utilizó los siguientes colores para identificar los circuitos:
    - Neutro: Negro Nº12 AWG
    - Fase tomacorrientes: Rojo Nº12 AWG.
    - Cable puesta a tierra: verde amarillo Nº12 AWG.

Todas estas actividades fueron limitadas por falta de presupuesto económico, por lo cual se priorizaron los ambientes del CPD de las distritales departamentales de La Paz, Cochabamba y Santa Cruz.

Oficinas	Descripción de Estado
Dirección Nacional y Departamental La Paz	- Revisión del sistema de aterramiento e instalación de una jabalina de 2,4 metros para el CPD. - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Adquisición de 1 UPS Marca LIEBERT GXT2-10000R230 de 10 KVA
Cochabamba	- Revisión del sistema de aterramiento e instalación de una jabalina de 2,4 metros para el CPD. - Instalación eléctrica independiente para el Centro de Datos. - Instalación eléctrica independiente para equipo de telecomunicaciones. - Instalación eléctrica independiente para equipos informáticos de usuario - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Adquisición de 1 UPS Marca LIEBERT GXT2-10000R230 de 10 KVA
Santa Cruz	- Revisión del sistema de aterramiento e instalación de una jabalina de 2,4 metros para el CPD. - Instalación eléctrica independiente para el Centro de Datos. - Instalación eléctrica independiente para equipo de telecomunicaciones. - Instalación eléctrica independiente para equipos informáticos de usuario - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Adquisición de 1 UPS Marca LIEBERT GXT2-10000R230 de 10 KVA

Oficinas	Descripción de Estado
Oruro	- Revisión del sistema de aterramiento del edificio donde funcionaba la distrital departamental. - Instalación eléctrica independiente para el Centro de Datos. - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Se realizó el mantenimiento y cambio de baterías al UPS que existían en la dirección nacional y se instaló en el Centro de Datos.
Tarija	- Revisión del sistema de aterramiento del edificio donde funcionaba la distrital departamental. - Instalación eléctrica independiente para el Centro de Datos. - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Se realizó el mantenimiento y cambio de baterías al UPS que existían en la dirección nacional y se instaló en el Centro de Datos.
Beni	- Revisión del sistema de aterramiento del edificio donde funcionaba la distrital departamental. - Instalación eléctrica independiente para el Centro de Datos. - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Se realizó el mantenimiento y cambio de baterías al UPS que existían en la departamental Cochabamba y se instaló en el Centro de Datos.
Pando	- Revisión del sistema de aterramiento del edificio donde funcionaba la distrital departamental. - Instalación eléctrica independiente para el Centro de Datos. - Mantenimiento de las tomas de corriente y tablero de distribución eléctrica. - Se realizó el mantenimiento y cambio de baterías al UPS que existían en la departamental Santa cruz y se instaló en el Centro de Datos.

2.2.4.3. Equipamiento Informático.

Se realizó la adquisición de equipos de seguridad de alta tecnología y servidores, priorizando a los CPD de la dirección nacional, distrital departamental de La Paz, Cochabamba y Santa Cruz; esta priorización fue determinada por la MAE (máxima autoridad ejecutiva) de la institución. Por lo tanto para las distritales departamentales siguientes, se realizó un mantenimiento preventivo de los servidores existentes.

En la gestión 2004, año en que se desarrolló el proyecto, los equipos de seguridad (tanto en hardware como en software), en el mercado eran limitados, los dispositivos CISCO eran los que contaban con los requerimientos de:

- Acceso ilimitado para atención telefónica.
- Acceso completo al soporte Web.
- Actualizaciones y mejoras al software de sistema operativo.
- Reemplazo de hardware, tiempo de respuesta al siguiente día hábil.
- En caso de falla del equipo activo, la falla debería ser atendida y solucionada en un lapso no mayor a cuatro (4) horas contadas a partir del reporte de la falla.
- Los equipos deben entregarse con la última versión de software disponible al momento de la entrega, se deben realizar las actualizaciones (updates) y actualización de nueva versión (upgrade) durante un año.

Por lo tanto, se realizó la adquisición de productos CISCO que cumplían con los requerimientos del proyecto, los cuales fueron:

- Router, los requerimientos mínimos fueron:
    - Ethernet 2 fast Ethernet (10/100 Base T)
    - Performance up to 20kbps.

- VPN (Virtual Private Network).
- Filtrados de paquetes IP y accounting.
- Acceso VPN y opciones de cifrado.
- Enrutamiento con gestión de ancho de banda
- Enrutamiento inter-VLAN.
- De arquitectura modular, por ejemplo con slots libres para agregar interfaces.
- Integración de enrutamiento flexible y conmutación de baja densidad.
- Integración de sistemas de detección de intrusos (IDS)
- Integración de sistemas de análisis de redes.
- Sistema operativo IOS o similar.

- PIX, los requerimientos mínimos fueron:
  - Cantidad de Usuarios con Licencia 10.
  - 2 puertos integrados 10/100Base T.
  - Firewall de inspección profunda para HTTP, FTP, ESMTP.
  - Aplicación de la postura de seguridad a clientes VPN
  - Enrutamiento dinámico OSPF (Open Shortest Path First – Abrir primero el camino más corto) por túneles VPN.
  - Enrutamiento PIM (Protocol Independent Multicast / multicast independiente de protocolo)

- Calidad de servicio (QoS).
- SSHv2 y SNMPv2c.

- SWITCH, los requerimientos mínimos fueron:
  - Conmutador de 24 puertos gestionado Capa 3, puertos 10/100 BaseT.
  - Protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI.
  - Soporte de DHCP, ARP, VLAN.
  - Soporte de Access Control List (ACL)
  - Quality of Service (QoS)
  - Sistema operativo IOS o similar.

Oficinas	Detalle de los equipos
Dirección Nacional	- Incremento de memoria RAM al servidor HP Xeon para servidor de aplicaciones. - Adquisición de Dos (2) Discos Duros SAS Hot Swap de 72 GB de 15000 rpm - Adquisición de un servidor HP Intel Xeon para Base de Datos. - Dos Tarjetas de Red 10/100/1000. - Adquisición de una unidad Tape drive HP Storageworks USB Rack - Adquisición de un router CISCO 2600 - Adquisición de un switch de capa 3 CISCO 3560 - Adquisición de tres switch de capa 2 de 24 puertos CISCO 2950 - Adquisición de un firewall CISCO PIX 515R

Oficinas	Detalle de los equipos
La Paz	- Incremento de memoria RAM al servidor HP Xeon para servidor de aplicaciones.
Cochabamba	- Incremento de memoria RAM al servidor HP Xeon para servidor de aplicaciones y Base de datos - Adquisición de una Tarjeta de Red 10/100/1000. - Adquisición de un router CISCO 2600 - Adquisición de un switch de capa 3 CISCO 3560 - Adquisición de un switch de capa 2 de 24 puertos CISCO 2950 - Adquisición de un firewall CISCO PIX 501
Oruro	- Adquisición de CPU Pentium IV, el mismo que fue utilizado como servidor de aplicaciones y base de datos - Adquisición de un switch de capa 2 de 24 puertos CISCO 2950 - Habilitación de una CPU para Firewall Panda BusinesSecure.
Tarija	- Adquisición de CPU Pentium IV, el mismo que fue utilizado como servidor de aplicaciones y base de datos - Adquisición de un switch de capa 2 de 24 puertos. CISCO 2950 - Habilitación de una CPU para Firewall Panda BusinesSecure.
Beni	- Adquisición de CPU Pentium IV, el mismo que fue utilizado como servidor de aplicaciones y base de datos - Adquisición de un switch de capa 2 de 24 puertos CISCO 2950 - Habilitación de una CPU para Firewall Panda BusinesSecure.
Pando	- Adquisición de CPU Pentium IV, el mismo que fue utilizado como servidor de aplicaciones y base de datos - Adquisición de un switch de capa 2 de 24 puertos CISCO 2950 - Habilitación de una CPU para Firewall Panda BusinesSecure.

2.2.4.4. Software y Licencias.

El sistema SIREBI v2 fue desarrollado mediante un motor de base de datos SQL SERVER 2000. Por lo tanto se adquirió una licencia del mismo para el servidor central localizado en el CPD de la Dirección Nacional.

Para la adquisición de la licencia en antivirus se tomaron en cuenta 3 factores, los cuales fueron:

- Protección: Una solución antivirus debe brindar protección continua para todos los dominios informáticos, todos los tipos de archivos y todos los elementos de red que podrían estar expuestos al ataque de un virus informático u otro tipo de malware. El programa debe ser capaz de detectar código malicioso y proteger todos los canales o puntos de entrada a la computadora, como correo electrónico, Internet, FTP, entre otros.

- Rendimiento: Mide, como afecta al rendimiento del sistema realizando tareas cotidianas como descargar, mover y copiar archivos, e instalar, desinstalar y ejecutar aplicaciones.

- Usabilidad. Una solución antivirus no debe emitir falsas alarmas o bloqueos durante la visita de páginas web; detección errónea de software seguro como malware durante el análisis de sistema, alertas erróneas previas y bloqueos de determinadas acciones durante la instalación y el uso de software seguro.

En la gestión 2004, año en que se desarrolló el proyecto, los dos antivirus que obtuvieron una alta calificación de 6 puntos (según la AVTEST –IT Security Institute[17]) en los 3 factores descritos anteriormente, fueron McAFee y Panda. Se escogió Panda, debido a que Panda incluía, en su propuesta de solución, un dispositivo físico denominado GateDefender; el cual realizaba filtrado Web,

[17] AV-TEST es el instituto de investigación independiente en materia de seguridad informática de Alemania. Los expertos de Magdeburgo llevan más de 15 años garantizando la ejecución de pruebas individuales y comparativas que aseguran la calidad de todos los productos de seguridad informática relevantes a nivel internacional.

filtrado de contenido, alta escalabilidad y balanceo de carga, monitoreo en tiempo real del tráfico de red.

Por lo tanto se realizó la adquisición de:

- Diez licencias Panda Businessecure con tecnologías TruPrevent que tenía las siguientes características y servicios:

    - Incorpora tecnologías preventivas (HIPS) capaces de identificar comportamientos anómalos o maliciosos en los programas utilizados por los funcionarios de la institución, de forma que es capaz de detectar con total certeza y bloquear virus desconocidos que no necesitan de la ejecución de ningún archivo para infectar el equipo.

    - Incorpora tecnologías de bloqueo de spam o correo no solicitado, filtrara contenidos peligrosos u ofensivos, e impedir el uso de software espía, marcadores telefónicos y otras herramientas utilizadas por hackers e intrusos. Todo esto unido a la capacidad preventiva de impedir uso de vulnerabilidades como el desbordamiento de buffer. Protección segura de las amenazas de Internet.

    - Panda AdminSecure: permite la administración segura y automatiza las tareas rutinarias para conseguir una protección efectiva en cualquier punto de la red institucional que considere vulnerable.

    - Panda File Secure: protege el compartir datos y aplicaciones en red.

    - Panda SmartClean2 en ClientShield permite a las estaciones de trabajo reparar de manera automática e inteligente los daños causados por virus sin necesidad de desplegar herramientas adicionales y evitar la congestión de las comunicaciones independientemente de la topología o ubicación de las estaciones de trabajo.

- Cuatro equipos Panda GateDefender 8050, implementados en las distritales departamentales de Oruro, Tarija, Beni y Pando, cuyas funciones y características principales fueron:

    - Protección completa: Analiza y protege los protocolos más utilizados (HTTP, FTP, SMTP. POP3, IMAP4 y NNTP) y tiene la capacidad de definir nuevos protocolos a ser protegidos.

    - Alto rendimiento, imperceptible para los usuarios: Reduce la carga de la red, optimizando sus recursos.

    - Administración sencilla y centralizada: gestiona desde cualquier punto de red mediante un navegador.

    - Anti –spam: Bloquea el correo no deseado antes de su entrada a la red, trabaja de manera conjunta con Panda BusinesSecure.

    - Filtrado Web: permite al administrador de la red controlar el uso de los recursos de la red institucional y corta de raíz la recepción o acceso a contenidos de carácter ofensivos, lo que afectaría al ambiente y al rendimiento laboral.

      Este módulo analiza URLs accedidas a través de HTTP y bloquea el acceso a aquellas que no estén permitidas dentro de la lista de accesos, además permite monitorear los contenidos a los que accede cada punto de red.

    - Filtrado de contenido: detiene los contenidos potencialmente peligrosos.

    - Reduce la pérdida de productividad de cada punto de red.

    - Alta escalabilidad y balanceo de carga: gracias a su alta escalabilidad, Panda GateDefender se adapta a las necesidades de hasta 1000

usuarios o puestos de trabajo, ajustando su capacidad de análisis al tipo de tráfico y a las comunicaciones de la institución.

Además su sistema de balanceo de carga completamente automático y nativo, permite repartir el volumen de trabajo entre las diferentes unidades de la institución. Como resultado se incrementa la escalabilidad y el rendimiento de la protección del perímetro de la red.

- Monitoreo en tiempo real del tráfico de red y la actividad de los componentes adicionales en Panda BusinesSecure.

Con el fin de cumplir con la estrategia de seguridad de la información de DIRCABI, se realizó una evaluación de posibles amenazas, tomando como referencia los ataques más frecuentes que se daban en las capas del modelo OSI. Un ejemplo de estas se muestra en la siguiente tabla:

Capa modelo OSI	Ataques por capa
Aplicación	Buffer overflows, exploit code, software maliciosos, virus, gusanos, troyanos.
Presentación	NetBIOS enumeration, protocol attack
Sesión	Session hijacking, SYN attacks
Transporte	Port scanning, DOS ttacks
Red	IP attacks, routing attacks, ARP Poisoning, MAC flooding and ICMP assaults , Smurf
Enlace	Passive and active snniffing, MAC spoofing, and WEP cracking
Física	Hardware hacking, lock picking, physical access attacks.

Fuente: https://www.buenastareas.com/ensayos/Vulnerabilidades-Del-Modelo-Osi/800235.html

Con el avance tecnológico las amenazas también crecen en gran magnitud por lo tanto se realizaba un monitoreo constante de la red para minimizar los posibles riesgos de penetración de intrusos y software malicioso.

Así también como medidas de prevención se tomó las siguientes medidas en cuanto a navegación Web:

- Restringir el acceso a páginas web prohibidas, bloqueo de páginas web.
- Restringir el acceso a aplicaciones de descarga de documentación como Bittorrent y Ares.
- Restringir cualquier tipo de descarga como puede ser música, videos, imágenes, isos, etc.
- Restringir el uso de Chats como Mesenger.

Estas tareas fueron realizadas mediante el servicio SNMP de Windows Server, servicios integrados a las licencias adquiridas de Panda Businessecure y a los dispositivos PANDA GATEDEFENDER; configuración de ACL (listas de control de acceso) en routers, firewalls y switches capa3.

2.2.4.5. Comunicación y redes.

2.2.4.5.1. Servicio de Internet.

Un servicio importante para las comunicaciones entre los servidores era la conexión a Internet. Algunos departamentos ya contaban con el servicio de internet ADSL, por lo cual solo se tuvieron que realizar los trámites respectivos para que se nos pueda proveer de IPs públicas.

Las IPs públicas, permiten mantener conexiones con los servidores departamentales de manera continua y establecer los túneles VPN para la replicación de las bases de datos. Sin embargo, como la dirección IP es

pública, cualquiera se puede conectar al dispositivo si conoce dicha dirección IP. Es por eso que se implementó esta solución de la seguridad perimetral.

Una de las principales dificultades para contar con una conexión estable en las distritales departamentales de Beni y Pando, fueron las siguientes:

- El servicio de internet solo se podía obtener mediante una conexión Dial Up. Esto involucraba tener una conexión de IP dinámica, es decir, se asignaba una dirección IP diferente cada vez que se realizaba la conexión.

- La conexión a internet no era constante en el tiempo, tenía intermitencia cada 20 minutos como promedio.

De acuerdo con estas limitaciones, se trabajó de la siguiente forma:

- Se estableció la conexión de los servidores solo una vez al día.

- Se estableció comunicación constante con el responsable de sistemas departamental vía teléfono para poder realizar la conexión del túnel VPN, esto debido a la asignación de IP dinámico.

- En caso de no poder realizar la conexión a la departamental se tenía que comunicar a Dirección Nacional.

2.2.4.5.2. Red LAN

De acuerdo con el relevamiento realizado a las distritales departamentales de Oruro, Tarija, Pando y Beni, se determinaron que estas no contaban con cableado estructurado. Por lo tanto, se tuvo que realizar dicho cableado en las respectivas distritales departamentales, lo cual se detalla a continuación:

Oficinas	Detalle del cableado estructurado
Oruro	- Instalación Rack de pared con un Patch panel de 24 Puertos UTP cat. 5e. - 10 tomas de datos - Cableado estructurado para comunicación de datos categoría 5E UTP-SOLID NON PLENUM, de 4 pares Calibre 24 AWG. - Patch Cords con cordones redondos y conformados por 8 conductores trenzados de cobre 24 AWG, enchufes modulares de 8 posiciones (tipo RJ45) en ambos extremos.
Tarija	- Instalación Rack de pared con un Patch panel de 24 Puertos UTP cat. 5e. - 10 tomas de datos - Cableado estructurado para comunicación de datos categoría 5E UTP-SOLID NON PLENUM, de 4 pares Calibre 24 AWG. - Patch Cords con cordones redondos y conformados por 8 conductores trenzados de cobre 24 AWG, enchufes modulares de 8 posiciones (tipo RJ45) en ambos extremos.
Beni	- Instalación Rack de pared con un Patch panel de 24 Puertos UTP cat. 5e. - 10 tomas de datos. - Cableado estructurado para comunicación de datos categoría 5E UTP-SOLID NON PLENUM, de 4 pares Calibre 24 AWG. - Patch Cords con cordones redondos y conformados por 8 conductores trenzados de cobre 24 AWG, enchufes modulares de 8 posiciones (tipo RJ45) en ambos extremos.
Pando	- Instalación Rack de pared con un Patch panel de 24 Puertos UTP cat. 5e. - 10 tomas de datos. - Cableado estructurado para comunicación de datos categoría 5E UTP-SOLID NON PLENUM, de 4 pares Calibre 24 AWG. - Patch Cords con cordones redondos y conformados por 8 conductores trenzados de cobre 24 AWG, enchufes modulares de 8 posiciones (tipo RJ45) en ambos extremos.

2.2.5. Implementación de la Red de Seguridad Perimetral

Cumplidas las tareas descritas anteriormente, se procedió con la implementación de la seguridad perimetral. Este proceso se realizó en varias etapas, las mismas que serán detalladas a continuación:

Etapa 1 – Capacitación en la Administración de los equipos de seguridad adquiridos.

Esta capacitación fue realizada por la empresa proveedora de Routers, Switch y Firewall, la cual tuvo una duración de 14 horas teóricas (el tiempo fue limitado por la empresa proveedora). Seguidamente se aplicaría los conceptos adquiridos, mediante la configuración de los equipos.

En esta capacitación se repasaron los conceptos de Switching, Routing y Security.

Etapa 2 – Instalación de equipos.

Para esta etapa, se realizó un cronograma de actividades para la instalación de los equipos de seguridad y pruebas piloto de la comunicación entre servidores de la Dirección Nacional y la departamental Cochabamba.

Esta tarea se realizó con la ayuda y supervisión de los profesionales de la empresa proveedora y la participación de los encargados de sistemas de las departamentales de Cochabamba y Santa Cruz.

La configuración de los equipos se detalla en la sección de anexos (página 126), la configuración detallada se aplicó en todas las distritales departamentales.

Se detallan a continuación los equipos instalados en la Dirección Nacional y las 7 Distritales Departamentales.

DIRECCIÓN NACIONAL

La instalación estuvo de acuerdo con la estructura anteriormente diseñada, como indica la figura:

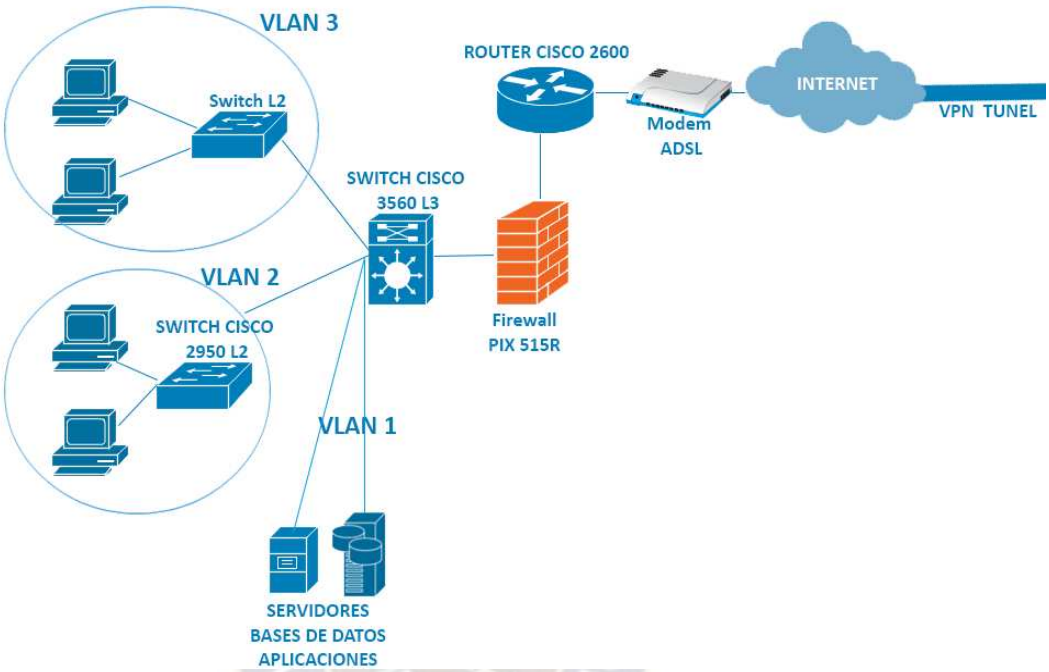


Figura 13
Fuente: Elaboración propia**.**

- Instalación Router CISCO 2600

    - Definición de enrutamiento dinámico, se basa en la utilización de algún protocolo de encaminamiento, de modo que los routers de nuestra red intercambien información sobre las redes y rutas que cada uno conoce. Las funciones de los protocolos de enrutamiento dinámico son:

        - Compartir información de forma dinámica entre routers.
        - Actualizar las tablas de enrutamiento de forma automática cuando cambia la topología.
        - Determinar cuál es la mejor ruta a un destino.

El protocolo usado fue RIP v2 (Routing Information Protocol), usa vectores de distancia para comparar matemáticamente las rutas y determinar la mejor ruta de acceso a cualquier dirección de destino determinado. Este protocolo permite:

- Propagación por multicast.
- Protocolo de enrutamiento classless (los puertos pueden tener diferente mascara de subred, utilización de VLSM (Variable Length Subnet Mask).

  - Definición de NAT: Para acceder al Internet, el proveedor de servicios de servicio de internet nos asignó un rango de IP Publicas, las cuales fueron traducidas con uso de NAT.

- Instalación FIREWALL PIX 515R

  - Los filtros de ingreso y salida de tráfico se configuraron de acuerdo a los requerimientos previamente analizados con el Director de Sistemas de la Dirección Nacional, para de esta manera tener un listado de los puertos que se abrirán para el acceso de determinados servicios externos que precisaba para la conexión a los servidores departamentales.

- Instalación switch de capa 3 CISCO 3560

  - Creación de VLAN para agrupar las diferentes estaciones de trabajo de acuerdo a la función y de los servidores además de mejorar la eficiencia de la red en un menor consumo de ancho de banda de la LAN.

Número de VLAN	Descripción
110	SISTEMAS
120	DIRECCIÓN NACIONAL
130	JURIDICA
140	OPERACIONES
150	ADMINISTRACIÓN
160	DIRECCIÓN DEPARTAMENTAL LA PAZ
170	JURIDICA LA PAZ
180	OPERACIONES LA PAZ
190	ADMINISTRACIÓN LA PAZ
100	VLAN NATIVA

Las VLAN se configuran en el Switch de la Capa de Distribución y se propagan a través de VTP a los Switches de la Capa de Acceso.

En los Switches de la Capa de Acceso se asocia cada puerto con la VLAN específica.

- Instalación de Switches de capa 2 CISCO 2950.

  Switches de capa de acceso donde se asocia cada puerto con la VLAN específica, anteriormente creada.

DIRECCIÓN DEPARTAMENTAL COCHABAMBA

- Instalación de servidor de aplicaciones y servidor de base de datos. Esta tarea fue realizada conjuntamente con el encargado de sistemas departamental.

La instalación estará de acuerdo a la estructura anteriormente diseñada, como indica la figura:

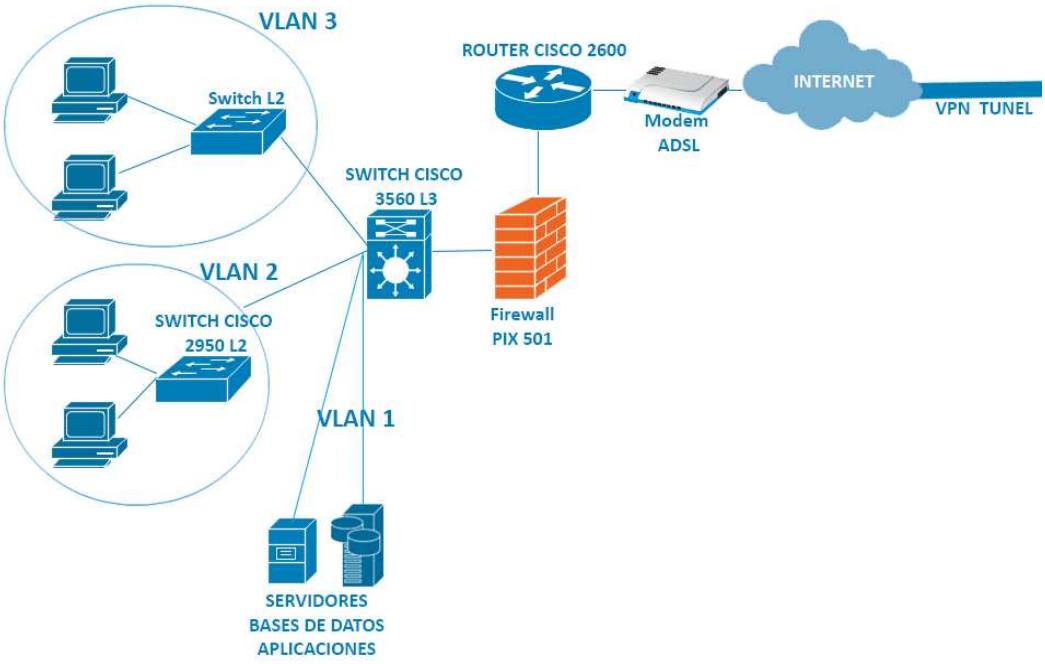


Figura 14
Fuente: Elaboración propia**.**

- Instalación Router CISCO 2600
    - Definición de enrutamiento dinámico.
    - Definición de NAT: Para acceder al Internet, el proveedor de servicios de servicio de internet nos asignó un rango de IP Publicas, las cuales fueron traducidas con uso de NAT.
- Instalación FIREWALL PIX 501
    - Los filtros de ingreso y salida de tráfico se configuraron de acuerdo a los requerimientos previamente analizados con el Director de Sistemas de la Dirección Nacional y de esta manera tener un listado de los puertos que se abrirán para el acceso de determinados servicios externos que precisaba para la conexión al servidor de la dirección nacional.

- Instalación Switch de capa 3 CISCO 3560

    - Creación de VLAN para agrupar las diferentes estaciones de trabajo de acuerdo a la función y de los servidores además de mejorar la eficiencia de la red en un menor consumo de ancho de banda de la LAN.

Número de VLAN	Descripción
110	SISTEMAS
120	DIRECCIÓN DEPARTAMENTAL
130	JURIDICA COCHABAMBA
140	OPERACIONES COCHABAMBA
150	ADMINISTRACIÓN COCHABAMBA

      Las VLAN se configuran en el Switch de la Capa de Distribución y se propagan a través de VTP a el Switch de la Capa de Acceso.

      En el Switch de la Capa de Acceso se asocia cada puerto con la VLAN específica.

- Instalación de Switch de capa 2 CISCO 2950.

  Switch de capa de acceso donde se asocia cada puerto con la VLAN específica, anteriormente creada.

Concluida esta etapa se realizaron pruebas de funcionamiento, este proceso se realizó de manera conjunta con los profesionales de la empresa proveedora.

- Creación de VPN.

  La configuración y creación de VPN se hizo uso de un servicio que viene con la licencia de Windows Server 2000. Este proceso se realizó de manera conjunta con los encargados de sistemas de Cochabamba y Santa Cruz.

Establecidas las conexiones VPN, se procedió a pruebas de replicación de las bases de datos del SIREBI v2.

Concluida esta Etapa 2 (de manera satisfactoria), se procedió a la instalación de la distrital departamental de Santa Cruz, cuya estructura era idéntica a la de Cochabamba.

DIRECCIÓNES DEPARTAMENTALES TARIJA, ORURO, BENI Y PANDO

- Instalación de servidor de aplicaciones y servidor de base de datos. Esta tarea fue realizada conjuntamente con el Encargado de Sistemas Departamental.

La instalación estará de acuerdo con la estructura anteriormente diseñada, como indica la figura:

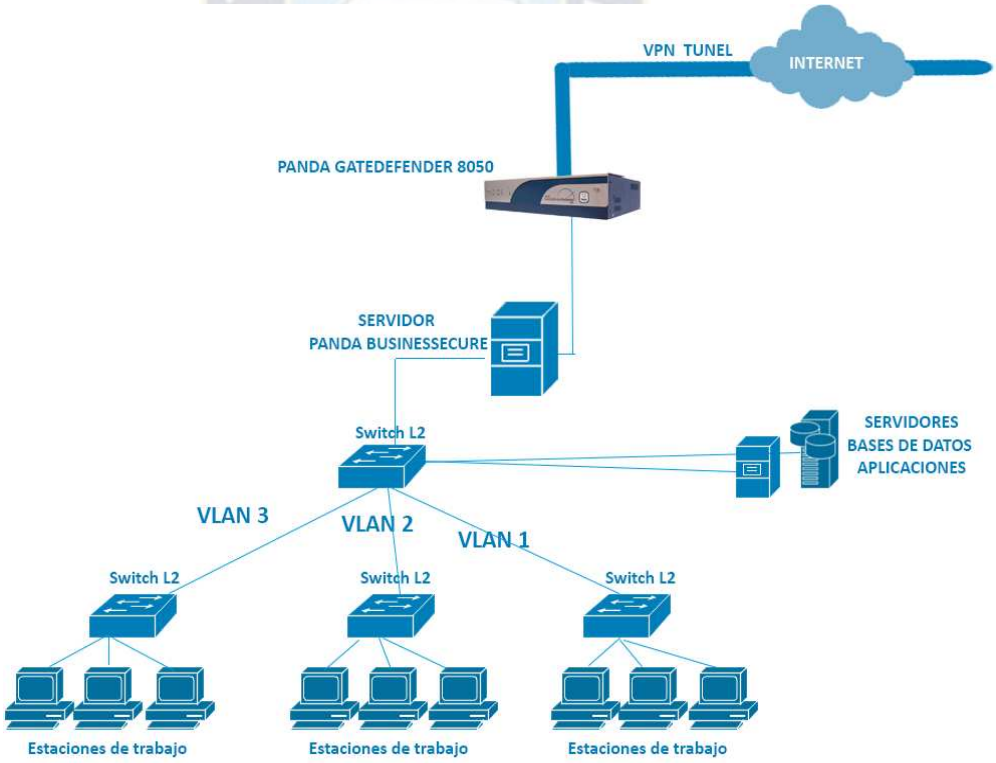


Figura 15
Fuente: Elaboración propia**.**

- Instalación FIREWALL PANDA GATE DEFENDER 8050 y PANDA BUSINESSECURE

    - Los filtros de ingreso y salida de tráfico se configuraron de acuerdo a los requerimientos previamente analizados con el Director de Sistemas de la Dirección Nacional y de esta manera tener un listado de los puertos que se abrirán para el acceso de determinados servicios externos que precisaba para la conexión al servidor de la dirección nacional.

Figura 16: PANDA Businessecure - Gatedefender
Fuente: Panda**.**

- Instalación de Switch de capa 2 CISCO 2950.

- En la fase inicial se identificaron debilidades en cuanto a conocimiento por parte de los encargados de sistemas de las Departamentales Beni y Pando, por lo que se realizó capacitación cuyas temáticas fueron:

    - Mantenimientos preventivos de los servidores.

    - Verificación de asignación de IPs dinámicos cuando se establezca la conexión Dial Up.

    - Habilitación de uso de escritorio remoto en horarios coordinados para realizar mantenimientos y control de procesos del servidor de base de datos.

2.3. Conclusiones y recomendaciones.

2.3.1. Resultados principales.

Se realizó el relevamiento de información de la situación actual de la red lógica y física de la DIRCABI a nivel nacional.

Se realizó la configuración de políticas en los firewalls, en el nivel de red, con el adecuado diseño de segmentación con políticas de acceso a las VLANs.

Se realizó el estudio de costos para la adquisición de los equipos, para la implementar la solución integrada.

Se instalaron los servidores de bases de datos en las 7 distritales departamentales y la dirección nacional.

Se implantó el Sistema de Registro de Bienes Incautados “SIREBI v2” en las 7 distritales departamentales y la dirección nacional.

El diseño de la red de seguridad perimetral de la Dirección de Registro de Bienes Incautados del Narcotráfico “DIRCABI”, cumple con los objetivos trazados.

La red implementada ofrece integridad de datos, confiabilidad y confidencialidad de la información, provista por los firewalls y las comunicaciones seguras mostradas en el desarrollo del proyecto.

Así también se cumple con el objetivo de disponibilidad de la información, haciendo que esta sea accesible cuando se la requiera, pero aún falta procedimientos que garanticen el funcionamiento ante cualquier caída de servicio por causa natural o física (carencia de sistemas redundantes o failover). Como protocolo de contingencia se creó un servidor de respaldo de base de datos dentro de la dirección nacional, para poder restablecer el servicio en el menor tiempo posible ante alguna caída

y se elaboró una propuesta de implementación de servidores espejos ubicados en otras instalaciones físicas.

La carencia en RRHH de personal capacitado en el área de sistemas, fue un problema preponderante para garantizar la disponibilidad de la información. Por tales circunstancias, el área de sistemas de la Dirección Nacional, realizo monitoreo de forma constante y diaria, accediendo a los servidores departamentales mediante escritorios remotos.

La estructura jerárquica diseñada estuvo organizada en capas que realizan tareas específicas. Las ventajas de la implementación de este modelo es que el administrador de la red pueda añadir, reemplazar y eliminar elementos de la red. Este tipo de flexibilidad y adaptabilidad hace que la red sea escalable.

Los nuevos ataques informáticos se incrementan, a medida que transcurre el tiempo, por lo cual se tiene que realizar un constante monitoreo de los mismos y realizar las posibles configuraciones en los firewalls implementados (PIX). Así también la actualización de su IOS y las aplicaciones IDS para reducir las posibles vulnerabilidades.

El antivirus Panda Businessecure y el equipo Panda Gatedefender cumplen con todas las funciones de filtrado y protección. Pero es necesario realizar evaluaciones periódicamente, en los factores de protección, rendimiento y usabilidad; ya que con las actualizaciones de la base de datos del antivirus y las aplicaciones, posiblemente pueda perjudicar el rendimiento y protección de la red.

El control de acceso al sistema operativo, a las aplicaciones, a la información y ordenadores portátiles fue administrado por la Dirección de Sistemas Nacional, tomando en cuenta los siguientes aspectos:

- Gestión de contraseñas.
- Procedimientos seguros de inicio de sesión.
- Identificación y autentificación de usuario.
- Desconexión automática de sesión.
- Restricción del acceso a la información.
- Comunicaciones móviles de ordenadores portátiles.

La confidencialidad de la Información que administra el Sistema de Registro de Bienes Incautados "SIREBI v2" esta resguardada con la implementación de la seguridad perimetral.

2.3.2. Recomendaciones.

- Se recomienda mejorar el sistema de tierra en los edificios y los CPD donde funcionan las distritales departamentales. Debido a las limitaciones, descritas en la sección de alcances y limitaciones, no se realizó la instalación de mallas de tierra para los ambientes respectivos.
- Se recomienda realizar monitoreo permanente de los accesos a la red para precautelar el óptimo funcionamiento del firewall.
- Se recomienda segmentar los servicios de red identificando puertos necesarios para la ejecución de aplicaciones críticas a las cuales los usuarios y proveedores tienen acceso, para incrementar la eficiencia de los accesos y evitar posibles ingresos no deseados a la red de la DIRCABI.
- Se recomienda monitorear los servicios de los servidores de aplicaciones de la DIRCABI para evitar aperturas de puertos no deseados.

- Se recomienda documentar e implementar una política de respaldos para salvaguardar la información y la configuración de cada uno de los servicios alojados en los servidores de la DIRCABI.

- Se recomienda complementar el esquema de seguridad perimetral con una adecuada política de contingencia y alta disponibilidad de los activos informáticos.

- El proyecto no cuenta con equipos de tolerancia a fallos (failover). Por lo tanto no tiene la capacidad de que el sistema continúe funcionando, aún en caso de producirse algún fallo en el sistema. Los fallos pueden ser no intencionados (Ej. caídas de sistemas, fallos en el cableado, fallo hardware) o intencionados por alguna parte no confiable del sistema. Esta debilidad tiene que ser supervisada y monitoreada de forma constante por la unidad de sistemas de la dirección nacional.

- Se recomienda implementar sistemas redundantes para garantizar la disponibilidad de la información a un 99.9% para evitar pérdidas económicas o de cualquier otro tipo. Mediante este sistema, incluso en el peor de los casos (la rotura de un disco duro, un desbordamiento de memoria que mate un proceso vital) puede seguir funcionando.

De acuerdo a la experiencia obtenida en el ámbito laboral y con el afán de contribuir de manera positiva para los futuros profesionales en el área de telecomunicaciones, se recomienda algunas actividades que se detallan a continuación:

- Realizar convenios con Universidades de países desarrollados en el área tecnológica para realizar CAPACITACIONES Online de nuevas tecnologías en el área de telecomunicaciones.

- Realizar talleres de diseño y desarrollo de software, a lo largo de mi experiencia vi la necesidad de aprender a programar centrales telefónicas convencionales, centrales telefónicas IP, configuración de routers,

firewalls en modo consola. Tareas que hubiesen sido sencillas si hubiera estado familiarizado con manejo de instrucciones y código de programación.

3. ANALISIS DE LA ACTIVIDAD.

3.1. Desempeño Laboral.

Las actividades desarrolladas, como indica la historia laboral de este documento se han desarrollado mucho antes de egresar de la Carrera de Ingeniería Electrónica en el Área de Telecomunicaciones. Esta experiencia me permitió conocer otras áreas de interés que de alguna manera se relacionaban de manera directa en el área de telecomunicaciones, como el desarrollo de software.

Los cargos y funciones ocupados me han permitido relacionarme con otros profesionales de diferentes áreas. Estas experiencias permiten desarrollar la capacidad de trabajo en grupo y el manejo de personal. Por ejemplo podría mencionar que se adquiere experiencia en el manejo administrativo de activos y de adquisición de los mismos.

En la implementación de este proyecto no solo se trabajó en la parte de diseño e implementación, también se tuvo que convencer a la parte financiadora, que era la Embajada Americana de que todo el requerimiento es necesario para conseguir los objetivos de seguridad de datos, para lo cual se tuvo que trabajar de manera conjunta con el Director Nacional, Unidad Administrativa y Operativa. Por tanto es aconsejable desarrollar estas capacidades de relacionamiento mediante actividades dentro de los contenidos programáticos de la carrera, orientados en una perspectiva de mejor preparación del estudiante para su futuro ingreso al mercado laboral.

El crecimiento tecnológico es constante hoy en día, por lo cual obliga a estar en constante capacitación en nuevas tecnologías. Este crecimiento también involucra que el mundo laboral se hace más competitivo y las empresas dentro de sus requerimientos necesitan que su personal este a la vanguardia en cuanto a conocimientos actuales.

3.2. Formación Recibida en la UMSA.

Considero que la formación recibida en la UMSA ha sido de beneficio en cuanto a mi formación como persona y como profesional en el área.

La primera etapa de cursos básicos donde nos inculcan conceptos teóricos de caculo, ecuaciones diferenciales nos enseñan a que existen varias soluciones para un determinado problema, que en la vida práctica se dan. Así también la capacidad de poder segmentar o dividir bloques grandes de información para poder realizar un análisis más profundo en las tareas encomendadas.

La segunda etapa de conocer conceptos teóricos y prácticos de circuitos eléctricos, componentes electrónicos y microprocesadores nos permiten observar de manera objetiva el funcionamiento de cualquier dispositivo electrónico y como estos pueden ayudar a que un proceso sea más eficiente y efectivo.

Las materias de mención como ser Teoría de Telecomunicaciones, Sistemas Digitales, Microprocesadores, Líneas de Transmisión, Procesamiento Digital de Señales, Sistemas de Computación, Sistemas de Comunicaciones, Antenas, Telefonía y Redes de Datos; nos preparan para el plano laboral y nos hacen ver que existen grandes desafíos en nuestra vida laboral futura.

Los conocimientos adquiridos en el proceso de formación, posibilitaron, ampliar y complementar las áreas de seguridad de comunicaciones, routing y switching. Los mismos que fueron aplicados para el desarrollo de este proyecto.

Los avances tecnológicos son grandes desafíos de vencer para lo cual tenemos un gran bagaje de conocimientos y conceptos adquiridos. Así también experiencias exitosas de profesionales, compañeros que nos motivan a resolver problemas, crear nuevas soluciones que puedan ayudar a la sociedad en general.

La experiencia laboral en el ámbito de telecomunicaciones, me permite afirmar que he recibido formación de excelencia en la Facultad de Ingeniería de la Universidad Mayor de San Andrés.

ABREVIATURAS UTILIZADAS

ACL: Listas de control de acceso (access control list).

CPD: Centro de Procesamiento de Datos.

DMZ: Zona Desmilitarizada (Demilitarized Zone).

DNS: Sistema de Nombres de Dominio (Domain Name System).

FTP: Protocolo de Transferencia de Archivos (File Transfer Protocol).

HTTP: Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol)

IDS: Sistemas de Detección de Intrusos (Intrusion Detection Systems).

IMAP4: Protocolo de Acceso a Mensajes de Internet (Internet Message Access Protocol)

IP: Protocolo de Internet (Internet Protocol).

IPS: Sistema de Prevención de Intrusos (Intrusion Prevention System).

NAT: Traducción de Direcciones de Red o Enmascaramiento de IP (Network Address Translation).

NNTP: Protocolo para la Transferencia de Noticias en Red (Network News Transport Protocol).

POP3: Protocolo de Oficina de Correo versión 3 (Post Office Protocol version 3).

QoS: Calidad de Servicio (Quality of Service).

SMTP: Protocolo para la Transferencia Simple de Correo (Simple Mail Transfer Protocol).

TIC: Tecnologías de la Información y la Comunicación.

UPS: Sistema de Energía Ininterrumpida (Uninterrumptible Power System).

URL: Localizador De Recursos Uniforme (Uniform Resource Locator).

VLAN: Red de Área Local Virtual.

VTP: Son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs.

VLSM: Máscara de Subred de Tamaño Variable (Variable Length Subnet Mask).

VPN: Red privada virtual (virtual private network).

RIP: El protocolo Routing Information Protocol (RIP) es un protocolo de enrutamiento del tipo vector distancia. Los protocolos de enrutamiento vector distancia calculan la mejor ruta para encaminar los paquetes IP hacia su destino correspondiente utilizando como métrica el número de saltos (Hop Count).

BIBLIOGRAFIA

- **Modelo De Arquitectura De Seguridad de la Información – MASI**
  Autores: Diego J. Parada, July A. Calvo, Angélica Flórez.
- **Interconexión de Dispositivos de Red Cisco**
  Steve McQuerry.
- **Fundamentos de Seguridad en Redes**
  Autor: Eric Maiwald.
- **CCNA Security (IINS)**
  Cisco Networking Academy.
- **Lineamientos para la creación de una VPN.**
  Autor: Rafael Reyes Moreno.
- **Cisco Systems Security**
  http://www.cisco.com/c/en/us/products/security/product-listing.html.
- **Cisco SAFE: Un Modelo De Seguridad Para Las Redes De Las Empresas**
  http://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf.
- **Herramienta De Evaluación De Seguridad De Microsoft (MSAT)**
  https://technet.microsoft.com/es-es/library/cc185712.
- **Hacking Etico**
  Autor: Carlos Tori.
- **Modelo De Referencia OSI**
  https://es.wikipedia.org/wiki/Modelo_OSI
- **VLAN Trunking Protocol**
  https://www.datuopinion.com/vtp.
- **Sistemas de Detección de Intrusos**
  http://www.rediris.es/cert/doc/unixsec/node26.html

ANEXOS Y DEFINICIONES

CONFIDENCIALIDAD[18]

La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

AUTENTICIDAD[19]

Es la propiedad que permite la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

SOFTWARE ANTIVIRUS[20]

Aplicación que consiste en un tipo de software cuya misión fundamental es la de hallar y, de ser posible, eliminar las amenazas detectadas, dejando entonces al sistema libre de Virus Informáticos y deshaciéndonos de todos estos Programas Maliciosos que afectan el rendimiento y funcionamiento del equipo.

SISTEMAS DE DETECCIÓN DE INTRUSOS[21]

Un sistema de detección de intrusos (IDS) es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. La forma en que un IDS detecta las anomalías pueden variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a sus recursos.

INTEGRIDAD[19]

La propiedad de salvaguardar la exactitud e integridad de los activos.

DISPONIBILIDAD[19]

La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

---

[18] Documento ISO IEC 27001 2005-10-5

[19] Blog ISO TOOLS (https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/)

[20] https://sistemas.com/antivirus.php

[21] MIT - http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

PERÍMETRO[22]

El perímetro es la división tanto física como lógica entre lo que está dentro de la red y aquello que está fuera.

NO REPUDIO[20]

Este objetivo garantiza la participación de las partes en una comunicación.

DoS[23]

Ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado.

CHOKE[24]

Dispositivo capaz de filtrar paquetes.

PROXI[25]

Un servidor proxy es un ordenador que sirve de intermediario entre un navegador web e Internet. El proxy contribuye a la seguridad de la red.

DIRECCIONES BROADCAST[26]

Una dirección Broadcast o de difusión identifica todas las máquinas dentro de una red de comunicación. Como se puede ver por la siguiente imagen, un paquete enviado de la máquina con la dirección 172.16.4.1 es recibido por todas las máquinas de esa red.

[22] https://www.welivesecurity.com/
[23] https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos
[24] http://www.eumed.net/cursecon/ecoinet/seguridad/cortafuegos.htm
[25] https://es.ccm.net/faq/2755-que-es-un-proxy
[26] https://ccnadesdecero.es/diferencia-entre-unicast-broadcast-y-multicast/

DIRECCIONES MULTICAST[26]

Una dirección de Multicast o multidifusión identifica un grupo de interfaces, cada interfaz puede pertenecer a otros grupos. Los paquetes enviados a esas direcciones se entregan a todas las interfaces que forman parte del grupo.

BASTION[27]

También denominado Gates, se conoce a un sistema especialmente asegurado, pero en principio vulnerable a todo tipo de ataques por estar abierto a Internet, que tiene como función ser el punto de contacto de los usuarios de la red interna de una organización con otro tipo de redes.

ROUTER[28]

Dispositivo de capa 3 (capa de red) que permite conectar una red de computadoras a otra. Asegura el enrutamiento de paquetes entre dos redes o determina la ruta que debe tomar el paquete de datos.

SWITCH[29]

Dispositivo de capa 2 (capa de enlace), tiene como función primaria concentrar "inteligentemente" las conexiones de red de tipo local LAN y evaluar las direcciones destino entre dispositivos, para establecer comunicación ágil y exclusiva entre ellos. Extraído de InformaticaModerna.com. Otras funciones secundarias y opcionales, son las de suministrar corriente eléctrica a ciertos dispositivos de red remotos y generar redes locales virtuales.

[27] https://www.rediris.es/cert/doc/unixsec/node23.html
[28] https://es.ccm.net/contents/299-equipos-de-red-router
[29] http://www.informaticamoderna.com/Switch.htm

TIPOS DE REDES

En primer lugar, se distingue la red LAN (Local Área Network) como una de las redes informáticas más utilizadas en función a su alcance. Es una red de datos que cubre un área geográficamente pequeña y limitada, que conectan las estaciones de trabajo, terminales, dispositivos ya sea en un edificio, oficina o campus. Una LAN consiste en computadoras, dispositivos periféricos, dispositivos de Red, Tarjetas de Interface de Red (NICs). Proveen conectividad todas las 24 horas y utilizan las normas de la capa física y la capa de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son algunas de las tecnologías LAN más comunes aunque el estándar más utilizado es el Ethernet.

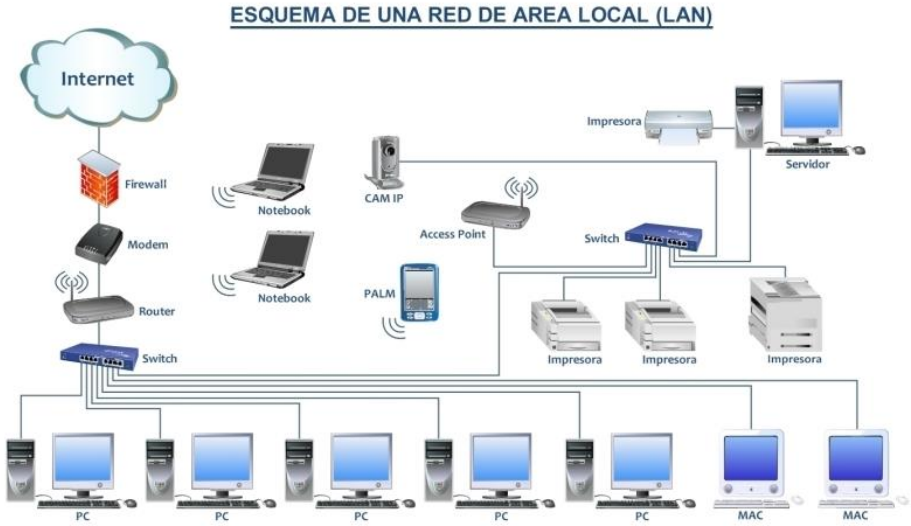


Figura 17: Red LAN
Fuente: https://redessegunsudistanciadetransmision.wordpress.com/red-lan

En contraposición a las redes LAN, se encuentran las redes WAN (Wide Área Network). Esta red se diferencia de LAN en que cubre una gran zona geográfica, incluso a nivel de escala de un país. La principal función de este tipo de redes informáticas es interconectar diversas LANs. La red WAN funciona a través de routers que permiten escoger el trayecto más apropiado para llegar a un nudo de red. Actualmente, una de las redes WAN más conocida es Internet.

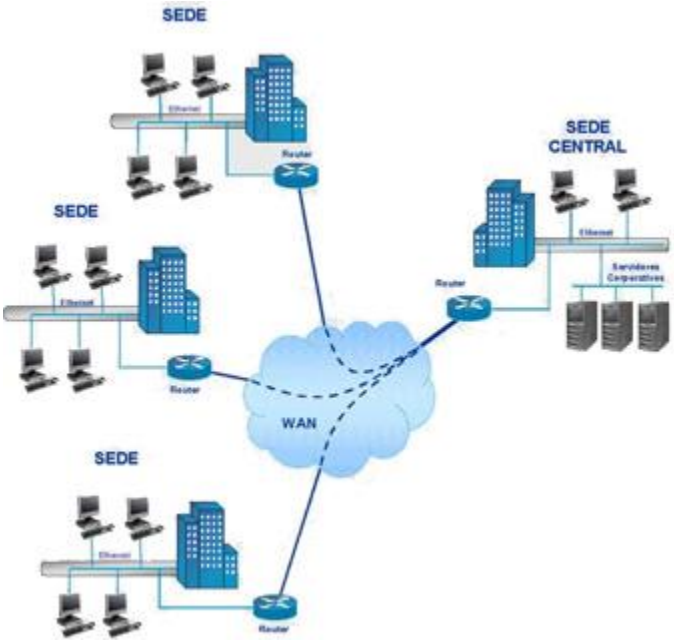


Figura 18: Red WAN
Fuente: https://sites.google.com/a/galileo.edu/proyectofinal8203/redes-de-computadoras/redes-wan

Otra de las redes más utilizadas en informática es la red MAN (Metropolitan Área Network; red metropolitana). Están formadas por computadoras y routers interconectados por enlaces de alta velocidad como, por ejemplo, la fibra óptica. Por lo tanto, su función es interconectar diversas LANs, a una velocidad relativamente alta, que se sitúan geográficamente cerca, aproximadamente unos 10 kilómetros. Además, las redes MAN permiten comunicar dos nudos a distancia como si lo hicieran en una misma red local.

Continuando en relación a su alcance, también se encuentran las redes CAN (Controller Área Network) entre las más utilizadas. La red CAN es un sistema de comunicación, en tiempo real, que une componentes inteligentes, así como también sensores en una máquina o un proceso. Este tipo de redes informáticas permite intercambiar hasta 2048 variables. La transmisión de datos puede efectuarse mediante un enlace infrarrojo, fibra óptica o radio.

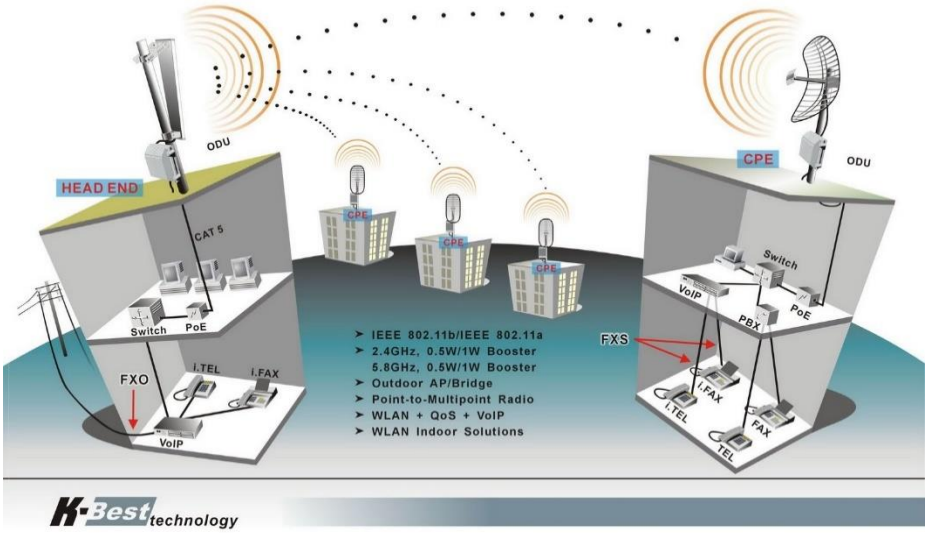


Figura 19: Red CAN
Fuente: http://robertquinto.blogspot.com/2011/06/redes-ii-3.html

Por otra parte, cabe destacar la red Peer to Peer (P2P), clasificada por su relación funcional. La característica principal de este tipo de redes es que cada cliente es también un servidor. Además, la Peer to Peer puede estar centralizada o, por el contrario, descentralizada. Las principales ventajas de este tipo de red son su bajo coste y la facilidad y rapidez de su instalación.

Por último, y según su direccionalidad, pueden encontrarse las redes Simplex, Half Duplex y Full Duplex entre las más utilizadas. La primera, red Simplex, se caracteriza por una conexión en la que los datos circulan en un solo sentido; la segunda, red Half Duplex, la conexión puede circular en los dos sentidos pero nunca al mismo tiempo y no permite aumentar la velocidad de transmisión; y la tercera, red Full Duplex, en la que los datos pueden circular simultáneamente en los dos sentidos, es decir, desde el emisor al receptor y viceversa.

En conclusión, como hemos podido apreciar, se utilizan diferentes tipos de redes informáticas y pueden clasificarse según su alcance, tipo de conexión, relación funcional, direccionalidad, grado de difusión, topología, autentificación y función.

TIPOS DE ATAQUES INFORMÁTICOS [30]

Entre los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

Los principales tipos de ataques son:

i. Actividades de reconocimiento de sistemas: Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

ii. Detección de vulnerabilidades en los sistemas: Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como "exploits").

iii. Robo de información mediante la interceptación de mensajes: Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

iv. Análisis del tráfico: Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers". Así, se conoce como "eavesdropping" a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

Una organización podría protegerse frente a los "sniffers" recurriendo a la utilización de redes conmutadas ("switches" en lugar de "hubs") y de redes locales virtuales (VLAN).

v. Ataques de suplantación de la identidad

IP Spoofing: Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada "IP Spoofing" ("enmascaramiento de la

[30] Alvaro Gomez Vieites - https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

dirección IP"), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado.

DNS Spoofing: los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico.

SMTP Spoofing: el envío de mensajes con remitentes falsos ("masquerading") para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario.

Captura de cuentas de usuario y contraseñas: también es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como los programas de software espía o los dispositivos de hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador ("keyloggers").

Modificaciones del tráfico y de las tablas de enrutamiento: los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos.

v. Conexión no autorizada a equipos y servidores: existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos destacar las siguientes:

• Violación de sistemas de control de acceso.

• Explotación de "agujeros de seguridad"
("exploits").

• Utilización de "puertas traseras" ("backdoors"), conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, que permiten acceder o tomar el control del equipo saltándose los controles de seguridad.

• Utilización de "rootkits", programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo.

• “Wardialing”: conexión a un sistema informático de forma remota a través de un módem. Los “wardialers” son dispositivos que permiten realizar de forma automática multitud de llamadas telefónicas para tratar de localizar módems que se encuentren a la espera de nuevas conexiones y que no hayan sido protegidos y configurados de forma adecuada.

vi. Consecuencias de las conexiones no autorizadas a los sistemas informáticos: pueden acarrear graves consecuencias para la organización afectada por este tipo de ataques e incidentes, entre las que podríamos destacar las siguientes: acceso a información confidencial, utilización inadecuada de determinados servicios por parte de usuarios no autorizados, transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización (“mail relaying”), creación de nuevas cuentas de usuario con privilegios administrativos, que faciliten posteriores accesos al sistema comprometido, consumo del ancho de banda de la red, modificación o destrucción de archivos y documentos guardados en un servidor.

vii. Ataques de Inyección de Código SQL: SQL, “Structured Query Language” (Lenguaje de Consulta Estructurado), es un lenguaje textual utilizado para interactuar con bases de datos relacionales.

viii. Ataques contra los sistemas criptográficos: los ataques contra la seguridad de los sistemas criptográficos persiguen descubrir las claves utilizadas para cifrar unos determinados mensajes o documentos almacenados en un sistema, o bien obtener determinada información sobre el algoritmo criptográfico utilizado.

viii. Denegación del Servicio (Ataques DoS – Denial of Service): los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.

VPN - Red Privada Virtual

Que es una VPN

Es una red privada virtual que interconecta dos redes a través de una red pública como lo es internet. Estas nacieron con el fin de intercomunicar redes sin importar la tecnología de transmisión usada.

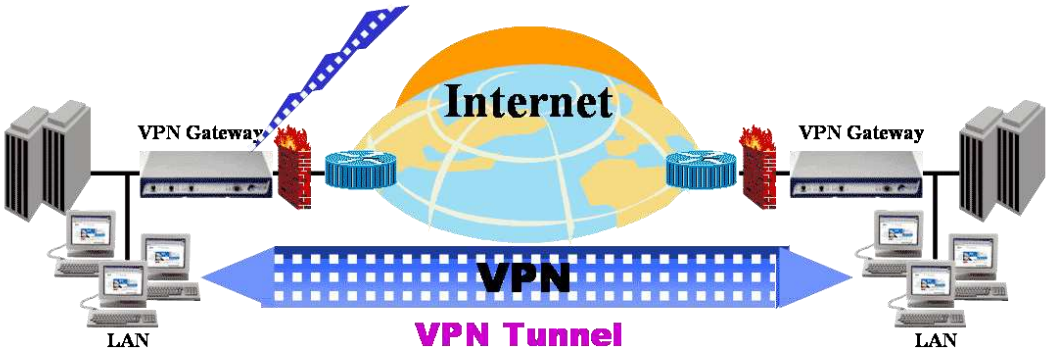


Figura 20: Acceso VPN Red Privada Virtual
Fuente: http://culturacion.com/que-es-una-vpn/

Las VPN permiten que sin importar el tipo de tecnología de transmisión usado, estas sean traducidas a protocolos de seguridad como:

- IPsec
- L2TP
- PPTP

Ventajas de una VPN

Seguridad:

Permite una transmisión segura, pero teniendo en cuenta que los datos no van cifrados, la transmisión es segura gracias a que el canal es seguro

Confidencialidad:

Gracias a que el canal que se establece es un túnel seguro para el paso de la información, mediante protocolos como IPsec.

Video, voz y datos:

Se puede cursar tráfico de datos, imágenes en movimiento y voz simultáneamente.

Integridad del medio:

Esta se mantiene porque el canal es seguro, la información NO va cifrada, va ENCAPSULADA, por medio de uno de los protocolos de seguridad. Independientemente del encapsulado del canal, los datos o la información se pueden encriptar antes de salir por la VPN, esto dependerá del criterio del administrador de seguridad.

Bajo costo:

Esto debido a que solo necesita el acceso a internet y dependiendo del tipo de VPN (peer to peer o peer to clients) 1 o 2 direcciones públicas FIJAS.

Transparencia para el usuario:

Para el usuario final el proceso realizado en la VPN es transparente.

Ubicuidad:

Puede extenderse a cualquier sitio.

Múltiples formas de acceso:

Por línea dedicada conmutada; por medio físico o inalámbrico.

Flexibilidad:

Facilidad para agregar o retirar conexiones Remotas, pues todas son conexiones virtuales.

Modularidad:

La capacidad de la red puede crecer gradualmente, según como las necesidades de conexión lo demanden.

Desventajas de una VPN

Configuración de políticas:

Se deben establecer correctamente las políticas de seguridad y de acceso.

Disponibilidad:

Esto debido a que si hay una caída de internet no puede existir ningún canal de contingencia.

Carga de para el cliente:

Mayor carga en el cliente VPN porque debe encapsular los paquetes de datos y encriptarlos, esto produce una cierta lentitud en las conexiones.

Seguridad del canal:

Una VPN se considera segura, pero no hay que olvidar que la información sigue viajando por Internet (no seguro y expuestos a ataques).

Tipos VNP

VPN peer to peer (firewall to firewall)

Esta consiste en una conexión punto a punto que se establece entre 2 dispositivos de seguridad que "hablan" el mismo protocolo. Estas son bidireccionales.

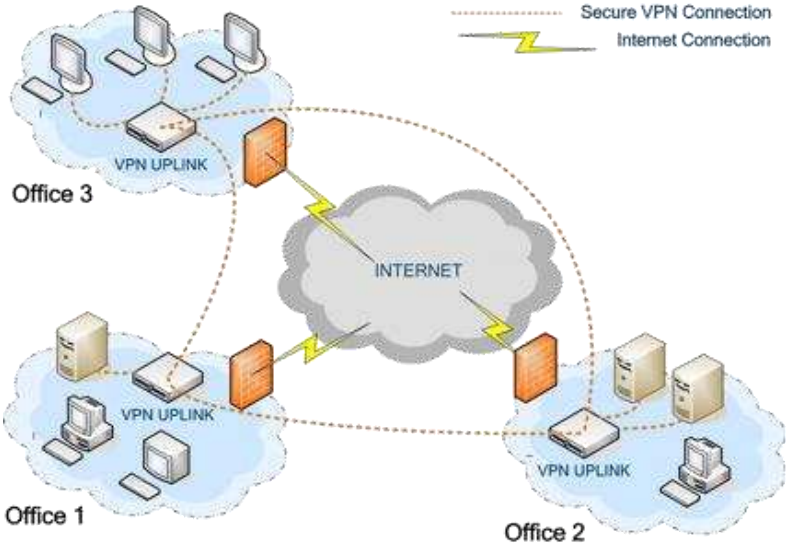


Figura 21: VPN peer to peer
Fuente: http://www.vpnuplink.com/en/index.html

Normalmente se utilizan firewalls o routers con características de firewall o gateways de VPN, estos últimos se conocen como dispositivos de propósito específico, ya que la única función que tienen es proporcionar el punto final de una VPN.

VPN peer to clients

Estas VPN están diseñadas para usuarios móviles, los cuales desde cualquier lugar de internet y a través de un software especial de cliente de VPN que es distribuido por el fabricante del equipo finalizador de la VPN (cisco, Uniper, Check point, nokia, etc) puede conectarse a la VPN.

Las VPN peer to clientes son unidireccionales, siempre desde el cliente hacia el servidor, es decir siempre el cliente es quien pide el establecimiento de la conexión.

Físicamente lo único que necesita el cliente es el computador y la conexión a internet desde cualquier parte del mundo teniendo el software.

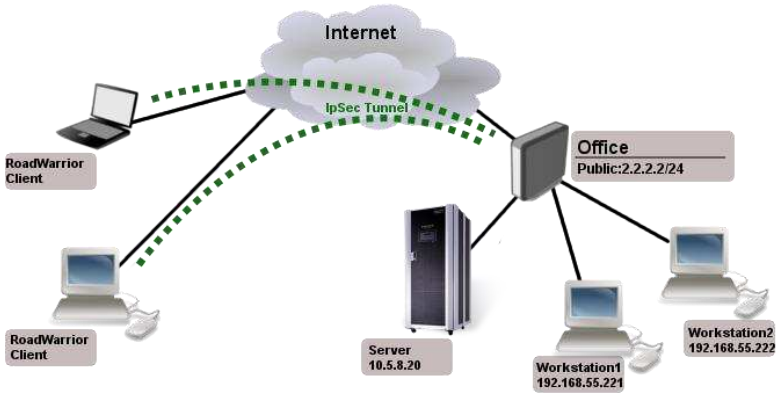


Figura 22: VPN peer to client
Fuente: https://wiki.mikrotik.com/wiki/Manual:IP/IPsec

Infraestructura de VPN

Para el diseño de una VPN hay que realizar las siguientes operaciones:

- Diseñar una topología de red y firewalls, teniendo en cuenta los costos y la protección.
- Escoger un protocolo para los túneles, teniendo en cuenta los equipos finales y las aplicaciones finales.
- Diseñar una PKI (Public Key Infraestructure), Teniendo en cuenta las necesidades del protocolo. En el mercado hay ofertas de productos que tienen integradas varias de las opciones anteriores:
    - Altavista Tunnel, Digital (para redes IP y protocolo propietario)
    - Private Internet Exchange (PIX), Cisco Systems (para redes IP y protocolo propietario).
    - S/WAN, RSA Data Security (para redes IP y protocolo estándar (IPSec))

Una buena solución VPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial.

Seguridad:

Dentro de este punto se destacan: el control de acceso para garantizar la seguridad de las conexiones de la red, el cifrado para proteger la privacidad de los datos y la autenticación para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.

Control de tráfico:

El segundo componente crítico en la implementación de una efectiva VPN es el control de tráfico que garantice solidez, calidad del servicio y un desempeño veloz. Las comunicaciones en Internet pueden llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo. Aquí es donde entra a jugar parámetros como la prioridad de los datos y garantizar el ancho de banda.

Manejo empresarial:

El componente final crítico en una VPN es el manejo empresarial que esta tenga. Esto se mide en una adecuada integración con la política de seguridad de la empresa, un manejo centralizado desde el punto inicial hasta el final, y la escalabilidad de la tecnología. Las VPN se caracterizan también por su flexibilidad. Pueden ser conexiones punto-punto o punto-multipunto. Reemplazando una red privada con muchos y costosos enlaces dedicados, por un solo enlace a una ISP que brinde un punto de presencia en la red (POP por sus siglas en inglés), una compañía puede tener fácilmente toda una infraestructura de acceso remoto, sin la necesidad de tener una gran cantidad de líneas telefónicas análogas o digitales, y de tener costosos pools de módems o servidores de acceso, o de pagar costosas facturas por llamadas de larga distancia.

Parámetros de Configuración VPN

La autenticación es parte vital dentro de la estructura de seguridad de una VPN. Sin ella no se podría controlar el acceso a los recursos de la red corporativa y mantener a los usuarios no autorizados fuera de la línea. Los sistemas de autenticación pueden estar basados en uno de los siguientes tres atributos: algo que el usuario tiene (por ejemplo la llave de una puerta); algo que el usuario sabe (por ejemplo una clave); o algo que el usuario es (por ejemplo sistemas de reconocimiento de voz o barrido de retinas). Es generalmente aceptado el uso de un método sencillo de autenticación tal como el password, pero no es adecuado para proteger sistemas. Los expertos recomiendan los llamados sistemas de autenticación complejos, los cuales usan al menos dos de los atributos de autenticación anteriores. Los aspectos a tener en cuenta para realizar el proceso de configuración de una VPN son los siguientes:

Definir el tipo de VPN:

Peer to peer

Peer to clients

Protocolos de la VPN:

IPsec

L2TP

PPTP

Siempre se deben utilizar los mismos protocolos tanto en el origen como en el destino de la VPN.

El protocolo más ampliamente aceptado por sus garantías se seguridad es el IPsec.

IP Públicas:

La red 1 configura la IP pública de la red 2 y la red 2 configura la IP pública de la red 1.

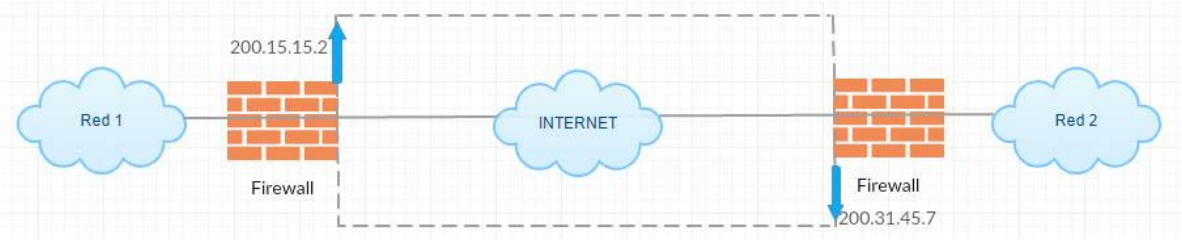


Figura 23: Diagrama de configuración IP´s públicas
Fuente: Elaboración propia.

Dominios de encriptación:

Los cuáles serán las redes PRIVADAS de cada una de las empresas, es decir la LAN de la red opuesta.

Configurar el peer en cada red:

Cada uno incluye su propia dirección peer, es decir, su dirección pública.

Pre-share key:

Es un password compartido que se debe configurar en los dos extremos para poder establecer la conexión, este password es para verificarse entre sí, no quiere decir que cada vez que establezca la conexión deba ingresar el password. En caso de olvidar el password en uno de los extremos, simplemente se debe cambiar en ambos extremos y la verificación vuelve a establecerse.

Tipo de encriptación para el pre-share key:

El tipo de encriptación utilizado para establecer el pres-hare key es simétrico, esto quiere decir que la red 1 cifra o encripta con una llave privada, la comparte a la red 2 y este des-encripta usando la misma llave.

Existen tres tipos de encriptación simétrica:

- DES: Data Encriptyon security, es un método que utiliza una llave de 64 bits; 8 de control o paridad y 56 para cifrado.
- TRIPLE DES o 3DES: Es un método de encriptación basado en DES el cual usa una llave de 128 bits; 16 de control o paridad y 112 de encriptación. Este método hace un cifrado DES tres veces antes de enviar la información.
- AES: Advanced Encriptyon Estándar, este método usa 128 o 256 bits, su tiempo de cifrado es más lento debido a la complejidad de sus procesos.

Vale la pena anotar que el método de encriptación DES ya fue vulnerado y hoy en día es poco utilizado.

Algoritmos de hash:

Hash es un código que se genera a partir de la información y sirve para comprobar la integridad del mensaje cuando llega al destino, en otras palabras el proceso de hash es muy similar al proceso denominado checksum en el cual se hace una comprobación de la información aplicando un algoritmo de comprobación en el origen y comparándolo con un algoritmo igual aplicado en el destino, si este código no es exactamente igual quiere decir que la información recibida es corrupta. Para realizar estos procesos, se utilizan algoritmos como:

- MD5 (Este código ya fue vulnerado)
- SHA1

Lo recomendable en la configuración de la VPN es utilizar AES con SHA1

Exchange key:

Es un tipo de encriptación asimétrica, esto quiere decir que se utilizan dos pares de llaves; un par de llaves públicas y un par de llaves privadas. En el momento de realizar el proceso de cifrado, debo hacerlo con la llave pública de la red destino y ese destino (el host o la red) debe descifrar con su llave privada, este proceso se repite en ambos sentidos. Para realizar estos procesos de encriptación se utilizan los algoritmos de Diffie-Helman de 768, 1024 y 2048 bits. Por lo general las llaves públicas se almacenan y comparten en un servidor SFTP o FTPS.

Tiempo de vida de la VPN:

Es el tiempo que intenta conectarse la VPN, este tiempo se configura en el firewall y está dado en segundos.

La Infraestructura de Llave Pública o PKI:

Es la integración de:

- La Criptografía de llave pública o asimétrica, usada para la firma digital.
- La Criptografía de llave simétrica usada para cifrar.
- Hash
- La Gestión de los pares de Llaves Público / Privados (El no compromiso de la llave privada, a través de un procedimiento de distribución segura de llaves.)

Protocolos para establecer VPN

PPTP (Point-to-Point Tunneling Protocol)

Protocoló desarrollado para proveer conexión entre usuarios de acceso remoto y servidores de red una red privada virtual. Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si dispararán directamente al servidor. En vez de disparar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego llaman al servidor RAS a través de Internet utilizando PPTP.

IPSEC

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme. IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP). Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación. Por autenticidad se entiende por la validación de remitente de los datos. Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo. AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad.

La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino. ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

L2TP (Layer-2 Tunneling Protocol)

Facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran. El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local.

CONCLUSIÓN: De los tres protocolos de encapsulamiento usados en las VPN, el más utilizado el IPsec, debido a la robustez y la seguridad que le brinda al canal, por otra parte, L2TP y PPTP ya han sido vulnerados y por tal motivo no son empleados en las mejores prácticas de seguridad.

MODELO OSI

El modelo de interconexión de sistemas abiertos, también llamado OSI (open system interconnection) es el modelo de red descriptivo propuesto por la Organización Internacional para la Estandarización (ISO).

Es una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

Constituye por tanto un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

En este estándar no se define una implementación de una arquitectura de red, sino que se establece un modelo sobre el cual comparar otras arquitecturas y protocolos.

El modelo OSI establece una arquitectura jerárquica estructurada en 7 capas. La idea es descomponer el proceso complejo de la comunicación en varios problemas más sencillos y asignar dichos problemas a las distintas capas, de forma que una capa no tenga que preocuparse por lo que hacen las demás. Según la estructura jerárquica, cada capa realiza servicios para la capa inmediatamente superior, a la que devuelve los resultados obtenidos, y a su vez demanda servicios a la capa inmediatamente inferior.

Modelo OSI: Un modelo de siete niveles o siete capas

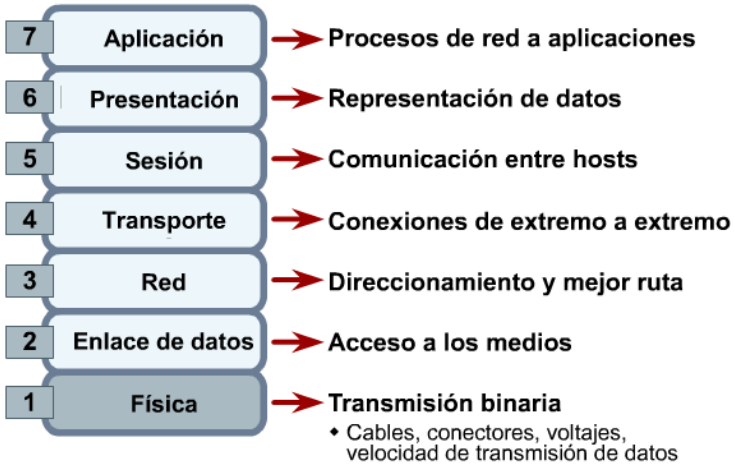


Figura 24: Modelo OSI
Fuente: https://edu.glogster.com/glog/modelo-osi-4152/27e3f5bbgvs.

Séptimo Nivel - Nivel o Capa de aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario, por esta razón es también el nivel que tiene el mayor número de protocolos existentes, ya que los usuarios son los que tienen un gran número de necesidades.

Este nivel es responsable por convertir las diferencias que existen entre los varios sistemas operativos y aplicativos para un padrón, es decir, esta camada recibe las informaciones que viene del usuario que llamamos SDU (Service Data Unit) y adiciona la información de control que llamamos de PCI (Protocol Control Information) para que tengamos como salida la conocida PDU (Protocol Data Unit).

Los protocolos más conocidos de esta capa son: NFS, AFP, HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, entre otros.

Sexto Nivel – Nivel o Capa de presentación

Es una camada intermedia entre la sesión y aplicación.

Es responsable que la información se pueda enviar de manera que el receptor la pueda entender.

En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos.

Por ejemplo, la conversión para que protocolos como el tcp/ip puedan hablar con el ipx/spx.

Esta capa también permite cifrar los datos y comprimirlos.

Por ejemplo: la conversión de datos de ASCII para EBCDIC.

La criptografía de datos también es hecha en esta capa.

Por lo tanto, podría decirse que esta capa actúa como un traductor universal.

Quinto nivel – Nivel o capa de sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole.

La capa de sesión tiene que preocuparse con la sincronización entre hosts, para que la sesión abierta entre ellos se mantenga arriba.

Los protocolos más conocidos de esta capa son: SMTP, FTP, SAP, SSH, ZIP, RCP, SCP, Netbios, ASP, entre otros.

Cuarto Nivel – Nivel o capa de transporte

La capa de transporte garantiza que los mensajes lleguen a su destinatario sin errores, en la secuencia correcta y sin pérdidas de datos.

Los protocolos de capas superiores no tienen cualquier preocupación por la transferencia de datos.

También es esta capa que se encarga de recibir los datos enviados por la capa de sesión.

Después de fragmentarlos para que se envié a la capa de red.

En la recepción hace el proceso inverso.

Juntando los paquetes enviados por la capa de red en segmentos para la capa de sesión.

La capa de transporte separa las capas de nivel de aplicación (capas de la 5 hasta la 7) de las capas de nivel físico (capas de la 1 hasta la 3).

Esta capa hace la comunicación entre esos dos grupos y determina la clase de servicio necesaria.

La clase de servicio puede ser orientada a la conexión.

Con el control de los errores y servicio de confirmación de la recepción de paquetes (TCP).

La clase de servicio también puede no ser orientada a la conexión.

Sin todo los controles de error y recepción de paquetes (UDP).

El hardware y/o software que está adentro de la capa de transporte, se comunica con sus usuarios por medio de las reglas de servicio que se intercambian por medio de uno o más TSAP (Transport Service Access Point), que son manejadas acorde al tipo de servicio prestado.

Estas reglas son transportadas por las TPDU (Transport Protocol Data Unit).

El tamaño y la complejidad de un protocolo de transporte va a depender del tipo de servicio que él puede obtener en la capa de red, o sea, en una capa de red que pueda hacer el transporte con más confianza con capacidad de circuito virtual, una capa de transporte mínima es necesaria.

Si la capa de red no es muy confiable o si solo tiene el soporte a datagramas, el protocolo de transporte tendrá que incluir tareas externas de detección y recuperación de errores.

Modos de los protocolos de transporte

Clases de la capa de Transporte:

Las funciones implantadas por la capa de transporte están directamente relacionadas a la calidad del servicio deseado, con este pensamiento se crearon cinco clases de protocolos orientados a la conexión:

Clase 0: es la más simple de todas, en ella no hay ninguno mecanismo de detección y recuperación de errores;

Clase 1: en esta clase se hace solamente la recuperación de errores básicos señalizados por la red;

Clase 2: esta clase permite que varias conexiones de transporte sean multiplexadas arriba de una única conexión de red, en ella también se puede implantar mecanismos de control de flujo;

Clase 3: en esta clase podemos definir la recuperación de los errores señalizados por la red y que varias conexiones de transporte sean multiplexadas arriba de una conexión de red;

Clase 4: esta clase permite que se configure la detección y recuperación de errores y también que varias conexiones de transporte sean multiplexadas arriba de una única conexión de red.

Los protocolos más conocidos de esta capa son: TCP, UDP, ZIP, NBP, IPX/SPX.

Tercer Nivel – Nivel o capa de red

La capa de red provee los medio funcionales y de procedimiento para que se haga la transferencia de tamaño variable de datos en secuencias, de una origen en un host que se encuentra en una red de datos para un host de destino que se encuentra en una red de datos diferente, tratando de mantener la calidad de servicio que habría sido requerida por la capa de transporte.

Los dispositivos que facilitan tal tarea se denominan encaminadores o enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés routers.

Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne.

Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

La capa de red hace el enrutamiento de funciones, y también puede hacer la fragmentación y rearmado de datos.

También pueden enviar reportes de los errores en la entrega de paquetes.

Los protocolos más conocidos de esta capa son: IP, IPX/SPX, X.25, APPLETALK, RIP, IGRP, EIGRP, OSPF, BGP, IS-IS, entre otros.

Según Nivel – Nivel o capa de enlace de datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico.

Lo que permite que las capas superiores a ella, estén seguras de que la transmisión de datos a través del vínculo físico se va a realizar prácticamente sin errores.

Esta capa se ocupa del direccionamiento físico, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo.

Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores.

Ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos, para regular la forma de la conexión entre computadoras así determinando el paso de tramas.

Trama = unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes.

Es importante mantener una excelente adecuación al medio físico (los más usados son el cable UTP, par trenzado o de 8 hilos, y la fibra óptica, multimodo y monomodo), con el medio de red que re direcciona las conexiones mediante un router.

El dispositivo que usa la capa de enlace es el Switch.

El Switch se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios:

- servidores.
- computadoras.
- teléfonos IP.
- teléfonos móviles.
- impresoras.
- diferentes dispositivos con acceso a la red.

Los protocolos más conocidos de esta capa son: ARP, PPP, LAPB, SLIP, SDLC, HDLC, LAPD, Frame Relay, IEEE, entre otros.

Primer Nivel – Nivel o capa físico

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), cable coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

La capa física también es responsable por definir se la transmisión puede o no, ser realizada en los dos sentidos simultáneamente.

Los protocolos más conocidos de esta capa son: IEE 1394, DLS, RDSI, Bluetooth, GSM, USB, ADSL, entre otros.

TIPOS DE FIREWALL.[31]

Firewall proxy.

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir.

Firewall de inspección activa.

Un firewall de inspección activa, ahora considerado un firewall "tradicional", permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Este firewall monitorea toda la actividad, desde la apertura de una conexión hasta su cierre. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

Firewall de administración unificada de amenazas (UTM)

Un dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.

Firewall de próxima generación (NGFW)

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:

• Funcionalidades de firewall estándares, como la inspección con estado.

• Prevención integrada de intrusiones.

[31] Cisco.com, INNOVA SECURE (https://innovasecure.com/que-es-un-firewall-y-cual-es-su-importancia-en-la-seguridad-informatica/)

• Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas.
• Rutas de actualización para incluir fuentes de información futuras.
• Técnicas para abordar las amenazas de seguridad en evolución.

Si bien estas funcionalidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más.

NGFW centrado en amenazas.

Estos firewalls incluyen todas las funcionalidades de un NGFW tradicional y también brindan funciones de detección y corrección de amenazas avanzadas. Con un NGFW centrado en amenazas, puede hacer lo siguiente:

• Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo.
• Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas en forma dinámica.
• Detectar mejor la actividad sospechosa o evasiva con correlación de eventos de terminales y la red.
• Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, incluso después de la inspección inicial.
• Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque.

MODELO DE DISEÑO JERÁRQUICO

Capa Central (Core o Núcleo).

Esta capa ofrece una estructura de transporte fiable y optimizado para reenviar el tráfico a altas velocidades, es capaz de conmutar paquetes tan rápido como sea posible. Esta capa ofrece una ruta rápida entre los Servidores de las Distritales Departamentales.

Además, dada la importancia de la velocidad, no hace funciones que puedan aumentar la latencia, como access-list, ruteo interVLAN, filtrado de paquetes, ni tampoco workgroup Access. Esta capa debe proporcionar una alta confiabilidad y tolerancia a fallas.

Las aplicaciones importantes y necesarias de esta capa son:

- Acceso VPN con firewall y opciones de cifrado.
- Enrutamiento con gestión de ancho de banda.
- Integración de enrutamiento flexible y conmutación de baja densidad.
- Integración de redes de contenido.
- Integración de sistemas de detección de intrusos (IDSs).
- Integración de sistemas de análisis de redes.

Capa de Distribución.

La capa de Distribución es el medio de comunicación entre la capa de acceso y la capa central. Las funciones de esta capa son proveer ruteo, filtrado, acceso a la red WAN y determinar que paquetes deben llegar al Core. Además, determina cuál es la manera más rápida de responder a los requerimientos de red, por ejemplo, cómo traer un archivo desde un servidor.

Aquí además se implementan las políticas de red, por ejemplo: ruteo, access-list, filtrado de paquetes, cola de espera, se implementa la seguridad y políticas de red (traducciones NAT y firewalls), la redistribución entre protocolos de ruteo. (Incluyendo rutas estáticas), ruteo entre VLANs y otras funciones de grupo de trabajo, se definen dominios de broadcast y multicast. Los Firewalls instalados de acuerdo a nuestras necesidades tenían que tener las siguientes capacidades:

- Algoritmo de seguridad adaptable (ASA) de vanguardia y firewalling de inspección de estado.
- El proxy de acceso directo autentica y autoriza las conexiones, mientras que mejora el rendimiento

- Traducción de direcciones de red (NAT).
- Compatibilidad con VPN basadas en IPsec y L2TP / PPTP.
- Compatibilidad con el filtrado de URL de alto rendimiento mediante la integración con las soluciones de filtrado de URL basadas en Websense.
- Mail Guard elimina la necesidad de un servidor de retransmisión de correo externo en la red perimetral.
- DNS Guard protege de forma transparente las búsquedas de nombres y direcciones salientes.
- La Guardia contra inundaciones y la Guardia de fragmentación protegen contra los ataques de denegación de servicio.
- Capacidad extendida de autenticación, autorización y contabilidad.
- Net Aliasing combina de forma transparente redes superpuestas con el mismo espacio de direcciones IP.
- Integración con los sistemas de detección de intrusiones para evitar conexiones de direcciones IP maliciosas conocidas.
- Protocolo simple de administración de red (SNMP) y syslog para administración remota.

En esta capa se instaló un Switch el cual tenía las siguientes características mínimas:

- 24 puertos Ethernet 10/100 Base T con Power over Ethernet (PoE).
- Soporte de DHCP.
- Alta disponibilidad.
- Soporte de Access Control List (ACL)
- Quality of Service (QoS).
- Soporte VLAN para segmentación de red.
- Enrutamiento VLAN.

En el nivel de red es importante tener en cuenta las políticas de seguridad que se pueden aplicar al tráfico de red, utilizando listas de acceso (ACL) para controlar el tráfico que fluye a través de la red. Una lista de acceso permite al Switch impedir o autorizar cierto tipo de tráfico, además permiten controlar que dispositivos de red pueden comunicarse en la red.

Una lista de acceso es una serie de sentencias de permiso o denegación que se aplican a direcciones o protocolos, que para ser aplicadas el Switch necesita inspeccionar cada uno de sus elementos y comprobar si coincide o no con cada una de las reglas definidas en la ACL.
Las VLANs al igual que cualquier otra tecnología, debe seguir ciertas reglas que permiten la transferencia de información de forma adecuada. Los potocolos que maneja las VLANs son variantes del 802.1Q como el ISL (Inter Switch Link) y el VTP (VLAN Trunk Protocol) de CISCO.
El protocolo 802.1Q tiene la finalidad de interconectar múltiples redes con enrutadores, compartiendo virtualmente el mismo medio físico.
El protocolo VTP (Vlan Trunk Protocol), propietario de CISCO, tiene la función principal de mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común, mediante la utilización de ramas de enlace troncal para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio.
Este Switch nos permitió la segmentación de la red en Dirección Nacional, Área Sistemas, Área Administración, Área Jurídica y Área Operaciones, esta segmentación también se replica a las distritales departamentales.
Nuestro diseño no contempla Servidores de acceso público, es decir no se cuenta con una zona DMZ, los servidores de aplicaciones funcionan únicamente a nivel interinstitucional.
En esta capa también se debe contemplar la implementación de antivirus y sistemas analizadores de contenido. En este sentido la institución realizo la adquisición de licencias Panda BusinesSecure.

Capa de Acceso.

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales. En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos,

el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

En esta capa se implementó un Switch que cumpla las siguientes funciones:

- Alta disponibilidad
- Protocolo IEEE 802.1x con seguridad de puerto, que autentica el puerto y administra el acceso a la red para todas las direcciones MAC, incluida la del cliente.
- Secure Shell (SSHv2).
- Protocolo simple de administración de red (SNMP).
- Clasificación y marcación de QoS, y límites de confianza
- Inspección del protocolo de resolución de direcciones (ARP)
- Listas de control de acceso virtual (VACL)
- Power Over Ethernet (PoE).
- Ancho de banda compartido
- Ancho de banda conmutado
- Filtrado de la capa MAC.
- VLAN.
- Soporte protocolo VTP (VLAN Trunking Protocol).

La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch. En consecuencia, es una importante primera línea de defensa para una red.

De acuerdo al modelo planteado se diseñó 2 tipos de estructura basándonos en la densidad de información y documentación que generaban en las diferentes distritales departamentales, un diseño basado en equipos de seguridad físicos (hardware) y otra combinando hardware y software.

VLAN (VIRTUAL LOCAL AREA NETWORK)

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

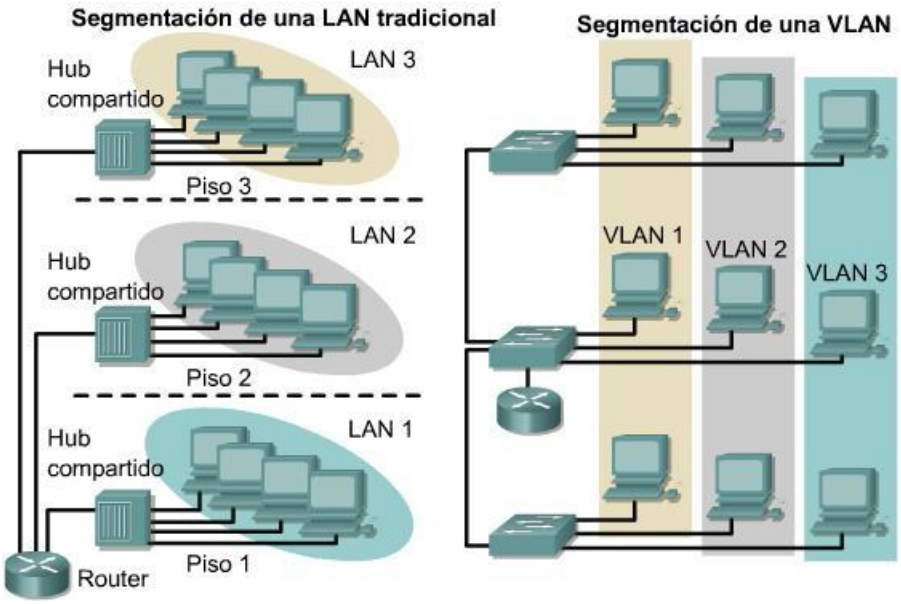


Figura 25: VLAN
Fuente: http://cursos.clavijero.edu.mx/cursos/069_cIII/modulo4/imagenes/tema4.1/

Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolos, etc.).

Tipos de VLAN

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo. Así, la VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador. La VLAN de nivel 2 (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación.

Además de las anteriores, existe la VLAN de nivel 3, que incluye diferentes tipos. La VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los

datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente. La VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Ventajas de la VLAN

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece diversas ventajas: una mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores; un aumento de la seguridad, puesto que la información se encapsula en un nivel adicional y puede ser analizada; una disminución en la transmisión de tráfico en la red.

Qué estándares definen a las VLAN

Las VLAN están definidas por los estándares IEEE 802.1D, 802.1p, 802.1Q y 802.10. Para obtener más información, te aconsejamos que consulte los siguientes documentos: IEEE 802.1D, IEEE 802.1Q y IEEE 802.10.

IDS/IPS

CARACTERÍSTICAS

Los sistemas IDS/IPS son un paso más adelante en la seguridad perimetral, son el paso siguiente, a los firewalls. Los IDS/IPS suponen un paso avanzando en la seguridad perimetral, estos sistemas una vez actualizados son capaces de reconocer vulnerabilidades de las aplicaciones más comunes a puertos abiertos en el firewall, la diferencias son básicamente dos. Actualmente algunos firewalls son capaces de llevar incorporado
IDS/IPS.

IDS: SISTEMAS DE DETECCIÓN DE INTRUSOS (INTRUSION DETECTION SYSTEMS).

Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema. Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host. Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa.

No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

Los IDS: aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

Tipos de IDS

HIDS (HostIDS):

El principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones. Un IDS basado en host analiza diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde afuera).

Los IDS basados en host consultan diferentes tipos de registros de archivos (kernel, sistema, servidores, red, cortafuegos, y más) y comparan los registros contra una base de datos interna

de peculiaridades comunes sobre ataques conocidos. Los IDS basados en host de Linux y Unix hacen uso extensivo de syslog y de su habilidad para separar los eventos registrados por severidad (por ejemplo, mensajes menores de impresión versus advertencias importantes del kernel). El comando syslog está disponible cuando se instala el paquete sysklogd, incluido con Red Hat Enterprise Linux. Este paquete proporciona el registro de mensajes del sistema y del kernel. Los IDSes basados en hosts filtran los registros (lo cual, en el caso de algunas redes y registros de eventos del kernel pueden ser bastante detallados), los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados por el administrador. Los IDS's basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes. Funciona verificando una base de datos de archivos confidenciales (y cualquier archivo añadido por el administrador) y crea una suma de verificación de cada archivo con una utilidad de resumen de archivos de mensajes tal como md5sum (algoritmo de 128-bit) o sha1sum (algoritmo de 160-bit).

El IDS basado en host luego almacena las sumas en un archivo de texto plano y periódicamente compara las sumas de verificación contra los valores en el archivo de texto. Si cualquiera de estas sumas no coinciden, el IDS alertará al administrador a través de un correo electrónico o a un mensaje al celular.

Ventajas:

- Los IDSs basados en host, al tener la capacidad de monitorear eventos locales a un host, pueden detectar ataques que no pueden ser vistos por un IDS basado en red.
- Pueden a menudo operar en un entorno en el cual el tráfico de red viaja encriptado, ya que la fuente de información es generada antes de que los datos sean encriptados y/o después de que el dato sea desencriptado en el host destino.

Desventajas:

- Los IDS's basados en hosts son más costosos de administrar, ya que deben ser gestionados y configurados en cada host monitorizado.
- Si la estación de análisis se encuentra dentro del host monitoreado, el IDS puede ser deshabilitado si un ataque logra tener éxito sobre la máquina.
- No son adecuados para detectar ataques a toda una red (por ejemplo, escaneos de puertos) puesto que el IDS solo ve aquellos paquetes de red enviados a él.

- Pueden ser deshabilitados por ciertos ataques de DoS.
- Usan recursos del host que están monitoreando, influyendo en el rendimiento del sistema monitorizado, así que se debe ser cuidadoso al momento de elegir en que tipo de servidor se va a instalar puesto que si el servidor es crítico, el rendimiento del equipo descenderá dramáticamente.

NIDS (NetworkIDS):

Un IDS basado en red, detecta ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red. Los sistemas de detección de intrusos basados en la red operan de una forma diferente que aquellos IDS basados en host. La filosofía de diseño de un IDS basado en la red es escanear los paquetes de red al nivel del enrutador o host, auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información extendida. Basándose en estos paquetes sospechosos, un IDS basado en la red puede escanear su propia base de datos de formas de ataques a la red y asignarles un nivel de severidad para cada paquete. Si los niveles de severidad son lo suficientemente altos, se enviará un correo electrónico o un mensaje de pager de advertencia a los miembros del equipo de seguridad para que ellos puedan investigar la naturaleza de la anomalía. Los IDS basados en la red se han vuelto muy populares a medida en que la Internet ha crecido en tamaño y tráfico.

Los IDS que son capaces de escanear grandes volúmenes de actividad en la red y exitosamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escaners, snifers y otras herramientas de auditoria y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como:

- Engaño de direcciones IP (IP Spoofing).
- ataques de denegación de servicio (DoS).
- Envenenamiento de caché arp.
- Corrupción de nombres DNS.
- Ataques de hombre en el medio

Ventajas:

- Un IDS bien localizado puede monitorear una red grande.

- Los NIDS's tienen un impacto pequeño en la red, siendo normalmente dispositivos pasivos que no interfieren en las operaciones habituales de ésta.
- Se pueden configurar para que sean muy seguros ante ataques haciéndolos invisibles dentro de la red.

Desventajas:

- Pueden tener dificultades procesando todos los paquetes en una red grande o con mucho tráfico y pueden fallar en reconocer ataques lanzados durante periodos de tráfico alto. Algunos vendedores están intentando resolver este problema implementando IDS's completamente en hardware, lo cual los hace mucho más rápidos.
- Los IDS's basados en red no analizan la información encriptada. Este problema se incrementa cuando la organización utiliza encriptación en el propio nivel de red (IPSec) entre hosts, pero se puede resolver con una política de seguridad más relajada (por ejemplo IPSec en modo túnel).
- La mayoría de los IDSs basados en red no saben si el ataque tuvo o no éxito, lo único que pueden saber es que el ataque fue lanzado. Esto significa que después de que un NIDS detecte un ataque, los administradores deben manualmente investigar cada host atacado para determinar si el intento de penetración tuvo éxito o no.
- Algunos NIDS tienen problemas al tratar con ataques basados en red que viajan en paquetes fragmentados. Estos paquetes hacen que el IDS no detecte dicho ataque o que sea inestable y pueda caer.

El modo de configuración de estos dispositivos dentro de la red se realiza ubicando el IDS de red en uno de los puertos del switch que esté ubicado en la red que deseemos escanear y configurando un espejo entre el puerto del switch en el cual está conectado el IDS y el puerto del swicth en el cual está ubicada la red que se va a escanear, en la _gura que está a continuación se puede ver este proceso de forma más clara.

DIDS (DistributedIDS):

Sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para

cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN). Sistemas pasivos y sistemas reactivos En un sistema pasivo, el sensor detecta una posible intrusión, almacena la información y manda una señal de alerta que se almacena en una base de datos. En un sistema reactivo, el IDS responde a la actividad sospechosa reprogramando el cortafuego para que bloquee tráfico que proviene de la red del atacante.

IPS: SISTEMAS DE PREVENCIÓN DE INTRUSOS (INTRUSION PREVENTION SYSTEMS)

Las nuevas vulnerabilidades de seguridad están provocando ataques cada vez más numerosos y sofisticados, tanto internos como externos, que ponen en evidencia a los cortafuegos convencionales. Para detener tales ataques, los sistemas de prevención de intrusiones (IPS) aportan una línea frontal y escalable de defensa a los servidores mal configurados o con vulnerabilidades al descubierto.

Si los sistemas de detección de intrusiones o IDS (Intrusion-Detection Systems) monitorean el tráfico de red y envían alertas sobre actividades sospechosas, los IPS (Intrusion-Prevention Systems) están diseñados para bloquear los ataques, examinando detenidamente todos los paquetes entrantes y tomando en consecuencia decisiones instantáneas para permitir o impedir el acceso. Para ello, se cargan con filtros que detienen los ataques producidos contra las vulnerabilidades de todo tipo que presentan los sistemas. Cuando se detecta una nueva vulnerabilidad, se crea un filtro específico y se añade al IPS, de modo que cualquier intento malicioso de explotarla es bloqueado inmediatamente. Estos dispositivos pueden inspeccionar los flujos de datos en su totalidad a fin de detectar todos los tipos de ataques que explotan las vulnerabilidades desde el Nivel 2 (control de acceso al medio) al Nivel 7 (aplicación). Por el contrario, los cortafuegos convencionales, como se limitan a realizar inspecciones a Nivel 3 o Nivel 4, son incapaces de detectar los ataques al nivel de aplicación escondidos dentro de la carga de los paquetes.

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas.
- Detección Basada en Políticas.
- Detección Basada en Anomalías.
- Detección Honey Pot.

Detección Basada en Firmas:

Una firma tiene la capacidad de reconocer una determina cadena de bytes en cierto contexto, y entonces lanza una alerta. Por ejemplo, los ataques contra los servidores Web generalmente toman la forma de URLs.

Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor Web. Sin embargo, como este tipo de detección funciona parecido a un Antivirus, el Administrador debe verificar que las firmas estén constantemente actualizadas.

Detección Basada en Políticas:

En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad.

Por ejemplo, determinar que hosts pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Detección Basada en Anomalías:

Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'. En este tipo de detección tenemos dos opciones:

- 1. Detección Estadística de Anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.
- 2. Detección No Estadística de Anormalidades: En este tipo de detección, es el administrador quien define el patrón 'normal' de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

Detección Honey Pot (Jarra de Miel):

Aquí se utiliza un 'distractor'. Se asigna como Honey Pot un dispositivo que pueda lucir como atractivo para los atacantes. Los atacantes utilizan sus recursos para tratar de ganar acceso en

el sistema y dejan intactos los verdaderos sistemas. Mediante esto, se puede monitorear los métodos utilizados por el atacante e incluso identificarlo, y de esa forma implementar políticas de seguridad acordes en nuestros sistemas de uso real.

Tipos de IPS

Están clasificados en 4 tipos:

- **Prevención de intrusos basados en red (NIPS):**
  Monitorea toda la red buscando tráfico sospechoso analizando la actividad de los protocolos.
- **Sistema de prevención de intrusos inalámbrico (WIPS):**
  Monitorea toda la red inalámbrica buscando tráfico sospechoso analizando los protocolos de red inalámbrica.
- **Análisis de comportamiento de red (NBA):**
  Examina el tráfico de la red para identificar amenazas que generan un flujo de tráfico inusual, Tal y como un ataque distribuido de denegación de servicio (DoS), ciertas formas de malware, y violaciones a las políticas.
- **Prevención de intrusos basados en host (HIPS):**
  Un paquete de software instalado que monitorea un solo host buscando actividad sospechosa analizando eventos ocurridos dentro de ese host.

CARACTERISTICAS EQUIPOS CISCO

ROUTER CISCO 2600

Figura 26: Router CISCO 2600

Características principales:

- Ethernet, 2 Fast Ethernet (10/100 Base T) Performance up to 20 kbps, DRAM 128/256 MB, Incluye Cisco IOS Software IP Base.
- Integración multiservicio de voz y datos.
- Acceso VPN con firewall y opciones de cifrado.
- Servicios de acceso de marcación analógica.
- Enrutamiento con gestión de ancho de banda.
- Enrutamiento entre VLAN.
- Entrega de acceso DSL de clase empresarial de alta velocidad.
- Integración de enrutamiento flexible y conmutación de baja densidad.
- Integración de redes de contenido.
- Integración de sistemas de detección de intrusos (IDS).Integración de sistemas de análisis de redes.

FIREWALL PIX 515R

Figura 27: FIREWALL PIX 515E-R (R)

Características principales:

- Procesador 433 MHZ, Cantidad de Usuarios con Licencia sin límite, RAM 64MB, 3 puertos integrados 10/100Base T, 10 Interfaces Virtuales (VLAN) 10, Compatibilidad con VLAN, Cantidad Máxima de Conexiones 48000.
- Firewall de inspección profunda para HTTP, FTP, ESMTP (Extended Simple Mail Transport Protocol), etc.
- Bloqueo de aplicaciones en túneles y entre iguales, mensajería instantánea
- Aplicación de la postura de seguridad a clientes VPN
- Enrutamiento dinámico OSPF (Open Shortest Path First – Abrir primero el camino más corto) por túneles VPN.
- Recuperación tras fallas de Activo/Activo con compatibilidad de enrutamiento asimétrico.
- Recuperación tras fallas con información de estado de VPN de acceso remoto y de sitio a sitio.
- Enrutamiento PIM (Protocol Independent Multicast / multicast independiente de protocolo)
- Calidad de servicio (QoS).

- SSHv2 y SNMPv2c.

SWITCH de capa 3 CISCO 3560

Figura 28: SWITCH CISCO 3560

Características principales:

- Conmutador de 24 puertos gestionado Capa 3, Puertos 10/100/1000 Base T, RAM 256 MB, protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI.
- Sustitución módulo hot swap, conmutación Layer 2.
- Soporte de DHCP.
- Soporte ARP.
- Soporte VLAN.
- Alta disponibilidad, Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP.
- Soporte de Access Control List (ACL)
- Quality of Service (QoS)

SWITCHS de capa 2 CISCO 2950.

Figura 29: SWITCH CISCO 2950

Caracteristicas principales:

- Ethernet 24 puertos 10/100Base T y 2 puertos 10/100/100.
- Alta disponibilidad

- Protocolo IEEE 802.1x con seguridad de puerto, que autentica el puerto y administra el acceso a la red para todas las direcciones MAC, incluida la del cliente.
- Secure Shell (SSHv2). Protocolo simple de administración de red (SNMP).
- Clasificación y marcación de QoS, y límites de confianza
- Listas de control de acceso virtual (VACL)
- Power Over Ethernet (PoE).
- Ancho de banda compartido
- Ancho de banda conmutado
- Filtrado de la capa MAC.
- VLAN.

FIREWALL PIX 501

Figura 30: FIREWALL PIX 501 (R)

Características principales:

- Procesador 133 MHZ, Cantidad de Usuarios con Licencia 10, RAM 16MB, 4 puertos integrados 10/100Base T, Cantidad Máxima de Conexiones 7500.
- Firewall de inspección profunda para HTTP, FTP, ESMTP (Extended Simple Mail Transport Protocol), etc.
- Bloqueo de aplicaciones en túneles y entre iguales, mensajería instantánea
- Aplicación de la postura de seguridad a clientes VPN
- Enrutamiento dinámico OSPF (Open Shortest Path First – Abrir primero el camino más corto) por túneles VPN.
- Recuperación tras fallas de Activo/Activo con compatibilidad de enrutamiento asimétrico.
- Recuperación tras fallas con información de estado de VPN de acceso remoto y de sitio a sitio.
- Enrutamiento PIM (Protocol Independent Multicast / multicast independiente de protocolo)
- Calidad de servicio (QoS).
- SSHv2 y SNMPv2c.

CONFIGURACIÓN EQUIPOS

SWITCH DE DISTRIBUCIÓN

Switch>en

Switch#configure terminal

Switch(config)#hostname Sw-Dis-1

Sw-Dis-1(config)#end

Sw-Dis-1#

SWITCH DE ACCESO 1

Switch>en

Switch#configure terminal

Switch(config)#hostname Sw-Acc-1

Sw-Acc-1(config)#end

Sw-Acc-1#

CONFIGURACIÓN VLANS

Número de VLAN	Descripción
110	SISTEMAS
120	DIRECCIÓN NACIONAL
130	JURIDICA
140	OPERACIONES
150	ADMINISTRACIÓN
160	DIRECCIÓN DEPARTAMENTAL LA PAZ
170	JURIDICA LA PAZ
180	OPERACIONES LA PAZ
190	ADMINISTRACIÓN LA PAZ
100	VLAN NATIVA (Troncal)

Las VLAN se configuran en el Switch de la Capa de Distribución y se propagan a través de VTP a los Switches de la Capa de Acceso.

En los Switches de la Capa de Acceso se asocia cada puerto con la VLAN específica.

Para configurar se introduce los siguientes comandos:

Linea de codigo	Descripción
Sw-Dis-1>enabled	Habilita modo de configuración
Password:	Solicitud de password
Sw-Dis-1#confi term	Configuración de terminal
Sw-Dis-1(config)#vlan 110	Asignación número de VLAN 110
Sw-Dis-1(config-vlan)#name Sistemas	Asignación nombre SISTEMAS
Sw-Dis-1(config-vlan)#exit	salir
Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 120 Sw-Dis-1(config-vlan)#name Direccion Nacional Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 130 Sw-Dis-1(config-vlan)#name Juridica Na Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 140 Sw-Dis-1(config-vlan)#name Operaciones Na Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 150 Sw-Dis-1(config-vlan)#name Administracion Na Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 160 Sw-Dis-1(config-vlan)#name Direccion LP Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)#	Para cada una de las VLANs asignadas se configura de la misma forma anterior.

Sw-Dis-1(config)#vlan 170 Sw-Dis-1(config-vlan)#name Juridica LP Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 180 Sw-Dis-1(config-vlan)#name Operaciones LP Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)# Sw-Dis-1(config)#vlan 190 Sw-Dis-1(config-vlan)#name Administracion LP Sw-Dis-1(config-vlan)#exit Sw-Dis-1(config)#	

Para asociar las VLAN en cada uno de los puertos se implementa la siguiente configuración en cada uno de los Switches de la Capa de Acceso:

En el switch de Acceso 1:

Linea de codigo	Descripción
Sw-Acc-1#conf terminal	Habilitación en modo de configuración
Sw-Acc-1(config-if)#interface FastEthernet0/10	Asignación de puerto
Sw-Acc-1(config-if)#description Usuario Sistemas	Asignación de una descripción de la VLAN que pertenece
Sw-Acc-1(config-if)#switchport access vlan 110	Los puertos del SWITCH accederán a la VLAN 110
Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/11 Sw-Acc-1(config-if)#description Usuario Direccion Nacional Sw-Acc-1(config-if)#switchport access vlan 120	Se repite el mismo proceso para cada una de las VLANs asignadas anteriormente.

Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/12 Sw-Acc-1(config-if)#description Usuario Juridica Nac Sw-Acc-1(config-if)#switchport access vlan 130 Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/13 Sw-Acc-1(config-if)#description Usuario Operaciones Nac Sw-Acc-1(config-if)#switchport access vlan 140 Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/14 Sw-Acc-1(config-if)#description Usuario Administracion Nac Sw-Acc-1(config-if)#switchport access vlan 150 Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/15 Sw-Acc-1(config-if)#description Usuario Direccion LP Sw-Acc-1(config-if)#switchport access vlan 160 Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/16 Sw-Acc-1(config-if)#description Usuario Juridica LP Sw-Acc-1(config-if)#switchport access vlan 170 Sw-Acc-1#conf terminal Sw-Acc-1(config-if)#interface FastEthernet0/17 Sw-Acc-1(config-if)#description Usuario Operaciones LP Sw-Acc-1(config-if)#switchport access vlan 180 Sw-Acc-1#conf terminal	

Sw-Acc-1(config-if)#interface FastEthernet0/18 Sw-Acc-1(config-if)#description Usuario Administracion LP Sw-Acc-1(config-if)#switchport access vlan 190	

Verificación de las VLAN creadas en el Switch de Acceso 1

Sw-Acc-1#show vlan

Verificación de las VLAN creadas en el Switch de Distribución 1

Sw-Dis-1>en

Password:

Sw-Dis-1#show vlan

Definimos la VLAN nativa como VLAN 100 y la configuramos en los puertos que conectan los switches de Acceso y Distribución. Así tambien se debe configuro el puerto como un puerto troncal.

Sw-Dis-1#conf ter

Sw-Dis-1(config)#interface fastEthernet 0/1

Sw-Dis-1(config-if)#switchport mode trunk

Sw-Dis-1(config-if)#switchport trunk native vlan 100

Sw-Dis-1(config-if)#

Sw-Acc-1#conf ter

Sw-Acc-1(config)#interface fastEthernet 0/2

Sw-Acc-1(config-if)#switchport mode trunk

Sw-Acc-1(config-if)#switchport trunk native vlan 100

Sw-Acc-1(config-if)#

CONFIGURACION VTP (VLAN TRUNKING PROTOCOL)

Para la correcta propagación de las VLAN implementaremos el protocolo VTP en el switch de distribución el cual será el servidor VTP y los switches de acceso será cliente VTP.

Sw-Dis-1 (config)#vtp domain DIRCABI

Sw-Dis-1 (config)#vtp password drnac2538

Sw-Dis-1 (config)#

Sw-Dis-1 (config)#vtp version 2

Sw-Dis-1(config)#vtp mode server

Sw-Dis-1#show vtp status

En el switch de acceso se configuro en modo cliente

Sw-Acc-1#configure terminal

Sw-Acc-1(config)#vtp mode client

Sw-Acc-1(config)#

Sw-Acc-1#

Sw-Acc-1>en

Sw-Acc-1#show vtp status

DIRECCIONAMIENTO IP

Se utilizo la red privada 192.168.1.0

1	2	3	4	5	6	7	8	Bits prestados
128	64	32	16	8	4	2	1	Variación
128	192	224	240	248	252	254	255	Mascara de Red

Para cubrir las necesidades de direccionamiento IP, necesitamos 9 subredes.

2^n≥9, en donde n es la cantidad de bits que se tomaron prestados. Así que tomaremos 4 bits prestados, por lo tanto obtendremos 16 subredes.

Con los 4 bits restantes, con la siguiente formula obtendremos la cantidad de host por subred

2^n- 2 = número de host disponible /subred

2^4- 2 = 14 host / subred

Con estos datos, nuestra red es 192.168.1.0 con mascara 255.255.255.240

En la siguiente tabla se plantea un esquema de direccionamiento de nuestra red.

Dirección de red	Rango de dirección IP Utilizables	Dirección de broadcast	Descripción
192.168.1.0	192.168.1.1-192.168.1.14	192.168.1.15	Sistemas
192.168.1.16	192.168.1.17-192.168.1.30	192.168.1.31	Dirección Nac
192.168.1.32	192.168.1.33-192.168.1.46	192.168.1.47	Juridica Nac
192.168.1.48	192.168.1.49-192.168.1.62	192.168.1.63	Operaciones Nac
192.168.1.64	192.168.1.65-192.168.1.78	192.168.1.79	Administración Nac
192.168.1.80	192.168.1.81-192.168.1.94	192.168.1.95	Dirección LP
192.168.1.96	192.168.1.97-192.168.1.110	192.168.1.111	Juridica LP
192.168.1.112	192.168.1.113-192.168.1.126	192.168.1.127	Operaciones LP
192.168.1.128	192.168.1.129-192.168.1.142	192.168.1.143	Administración LP
192.168.1.144	192.168.1.145-192.168.1.158	192.168.1.159	

CONFIGURACIÓN DHCP

La configuración de un servidor de DHCP conlleva definir un conjunto de direcciones para asignar, de acuerdo a nuestro diseño.

Linea de codigo	Descripción
Sw- Dis -1(config)#ip dhcp pool Sistemas	Crea un conjunto de IPs con el nombre SISTEMAS y provoca que el router entre en el modo de configuración de DHCP
Sw- Dis -1(dhcp-config)#network 192.168.1.0 255.255.255.240	Definición de la red y la mascara de subred, de acuerdo a nuestro diseño.
Sw- Dis -1(dhcp-config)#default-router 192.168.1.1	Especifica la dirección de la puerta de enlace en la red LAN
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4	Especifica los servidores de nombres de dominio. En este caso asignamos el DNS público de google.
Sw- Dis -1(config)#ip dhcp pool Direccion Nac Sw- Dis -1(dhcp-config)#network 192.168.1.16 255.255.255.240	Se repite el mismo proceso para cada una de las SUBREDES calculadas y asignadas anteriormente.

Sw- Dis -1(dhcp-config)#default-router 192.168.1.17 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Juridica Nac Sw- Dis -1(dhcp-config)#network 192.168.1.32 255.255.255.240 Sw- Dis -1(dhcp-config)#default-router 192.168.1.33 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Operaciones Nac Sw- Dis -1(dhcp-config)#network 192.168.1.48 255.255.255.240 Sw- Dis -1(dhcp-config)#default-router 192.168.1.49 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Administracion Nac Sw- Dis -1(dhcp-config)#network 192.168.1.64 255.255.255.240 Sw- Dis -1(dhcp-config)#default-router 192.168.1.65 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Direccion LP Sw- Dis -1(dhcp-config)#network 192.168.1.80 255.255.255.240 Sw- Dis -1(dhcp-config)#default-router 192.168.1.81 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Juridca LP Sw- Dis -1(dhcp-config)#network 192.168.1.96 255.255.255.240	

Sw- Dis -1(dhcp-config)#default-router 192.168.1.97 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Operaciones LP Sw- Dis -1(dhcp-config)#network 192.168.1.112 255.255.255.240 Sw- Dis -1(dhcp-config)#default-router 192.168.1.113 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4 Sw- Dis -1(config)#ip dhcp pool Administracion LP Sw- Dis -1(dhcp-config)#network 192.168.1.128 255.255.255.240 Sw- Dis -1(dhcp-config)#default-router 192.168.1.129 Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4	

ACCESS-LIST

El acceso a Internet tiene que ser monitoreado para asegurar nuestra red ante amenazas, para lo cual creamos listas de acceso que restringe el acceso a los dispositivos en rangos de tiempo fuera de oficina.

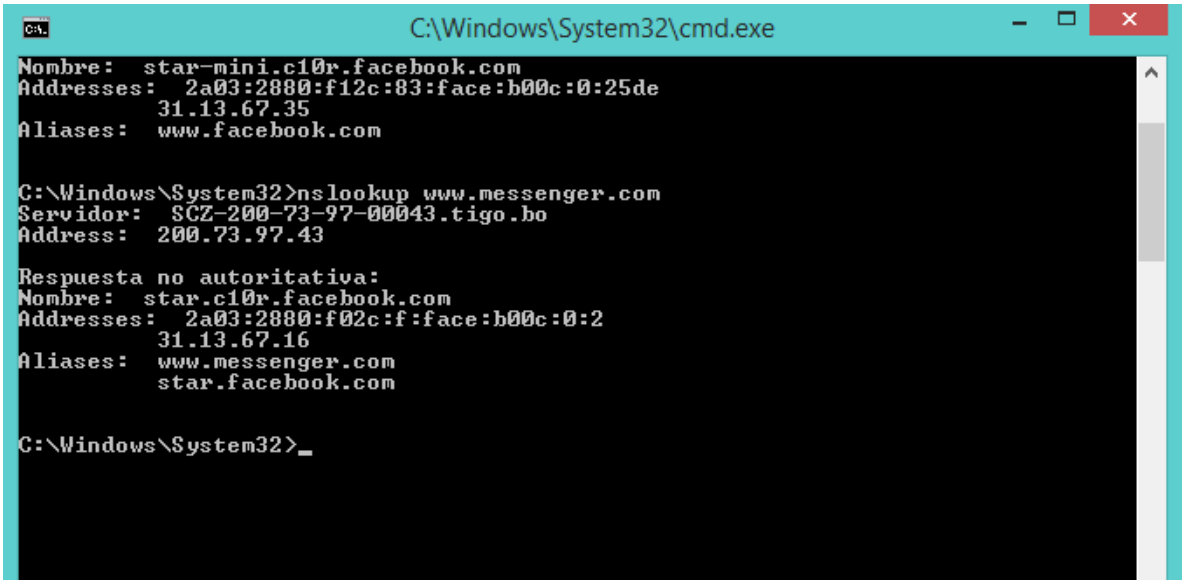
Para esto se creó una lista de acceso por tiempo, la cual se activa a una hora especifica denegando el acceso a un sitio especifico, por ejemplo caso del Messenger, se desactivará por las mañanas y horarios fuera de oficina.

Lo primero que se hizo fue definir un rango de tiempo, pero para esto se debe definir la fecha y hora del equipo con el comando Clock Set.

Sw-Dis-1(config)#Time-range DIASLABORABLES

Sw-Dis-1(config-time-range)#periodic Monday Tuesday Wednesday Thursday Fridays 14:00 to 17:00

Previamente debemos descubrir la dirección IP de Messenger con el comando NSLOOKUP www.messenger.com en una ventana de comandos.



Creamos la lista de acceso:

Sw-Dis-1(config)#access-list 150 deny TCP 192.168.1.0 0.0.255.255 31.13.67.16 time-range DIASLABORABLES

El siguiente paso es aplicarla la lista de control de acceso a la interfaz de salida con el siguiente comando:

Sw-Dis-1(config)#interface f0/2

Sw-Dis-1(config-if)#ip access-group 150 out

SEGURIDAD DE LOS PUERTOS DE LOS SWITCHES DE ACCESO

Los puertos de Switch de Acceso se deben asegurar estos son un punto de entrada potencial a usuarios sin autorización.

CONFIGURACION DEL SWITCHPORT SECURITY EN LA INTERFACE FASTEHTERNET 0/5

Sw-Acc-1#conf ter

Sw-Acc-1(config)#inter fastEthernet 0/5

Sw-Acc-1(config-if)#switchport mode access

Sw-Acc-1(config-if)#switchport port-security maximum 1

Sw-Acc-1(config-if)#switchport port-security violation shutdown

Sw-Acc-1(config-if)#switchport port-security mac-address sticky

Sw-Acc-1(config-if)#

VERIFICACION DE LOS PUERTOS ASEGURADOS

Sw-Acc-1#show port-security interface fastEthernet 0/5

Sw-Acc-1#sh port-security interface fastEthernet 0/6

Sw-Acc-1#show port-security address

PROTOCOLO SYSLOG

Este protocolo informa la actividad, eventos y condiciones de error de los equipos y sus procesos enviando mensajes, que contiene la información del evento, a un dispositivo o búfer a la consola del equipo.

Sw-Dis-1>ena

Sw-Dis-1#configure terminal

Sw-Dis-1#clock set 12:48:12 20 jan 2005

Sw-Dis-1#conf terminal

Sw-Dis-1(config)#service timestamps log datetime msec

Sw-Dis-1(config)#logging on

Sw-Dis-1(config)#logging trap debugging

Sw-Dis-1(config)#logging 192.168.1.145

Sw-Dis-1(config)#logging host 192.168.1.145

Sw-Dis-1(config)#

Sw-Dis-1#show logging Syslog

NAT (NETWORK ADDRESS TRANSLATION)

Para acceder al Internet, los proveedores ISP nos asignaron un rango de Direcciones IP Publicas: 200.87.134.114 hasta 200.87.134.118 con la máscara 255.255.255.248.

Este rango se va ingresar con el siguiente comando:

Ip nat pool NAT-DIRCABI 200.87.134.114 200.87.134.118 netmask 255.255.255.248 en modo de configuración global.

El siguiente paso es definir el tráfico que va a someterse a la traducción, en nuestro caso son todas las direcciones de las subredes 192.168.1.0 /28 y se lo hara con una acces list estándar:

Access-list 1 permit 192.168.1.0 0.0.0.255.255

Y después el siguiente paso es asociar la lista de control del acceso con el pool creado con el siguiente comando y sobrecargarlo

ip nat inside source list pool NAT-DIRCABI overload

Una vez creado el pool y clasificado el tráfico, se definió las interfaces de entrada y salida de tráfico.

CONFIGURACIÓN PIX

Linea de codigo	Descripción
pixfirewall> en	Habilita modo de configuración
Password:	Solicitud de password
pixfirewall# config terminal	Ingresa en modo de configuración de terminal
interface ethernet0 auto	Definición de la velocidad del puerto 0 en modo automático
interface ethernet1 100full	Definición de puerto a 100 Mbps full duplex
nameif ethernet0 outside security0	El comando nameif tiene dos trabajos grandes que realizar. Nombra la interfaz y asigna un nivel de seguridad
nameif ethernet1 inside security100	
enable password Mdircabi encrypted	Habilitación de la encriptación del password
passwd Mdircabi encrypted	Encriptando password
hostname secpixdircabi	Asignación de nombre SECPIXDIRCABI
fixup protocol ftp 21 fixup protocol rsh 514 fixup protocol rtsp 554	Habilitación de los puertos : FTP puerto 21 RSH puerto 514, logs del sistema

fixup protocol sip 5060 fixup protocol sip upd 5060 fixup protocol smtp 25 fixup protocol sqlnet 1521	SIP puerto 5060, control iniciación, modificación y finalización de sesiones. SMTP puerto 25, SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo). SQLNET puerto 1521, Base de datos puerto de escucha por defecto.
access-list 201 permit ip 192.168.1.0 255.255.255.248 192.168.0.0 255.255.0.0 access-list 201 permit ip 192.168.1.0 255.255.255.248 host 200.87.140.114 access-list 201 permit tcp 192.168.1.0 255.255.255.0 host 200.87.140.114 eq 80	Creación listas de acceso con las direcciones de red permitidas y sus respectivas mascaras de red
pager lines 24	Establecer el número de líneas en una página antes de que aparezca el mensaje "--- Más ---" para las sesiones de Telnet
mtu outside 1500 mtu inside 1500	Definición de unidad de transmisión máxima fuera de la red perimetral y dentro de la red.
ip address outside 192.168.0.0 255.255.0.0	Definición de las IP que viajan desde el exterior hacia el interior
ip address inside 192.168.1.1 255.255.255.248	Definición de las IP que viajan desde el interior hacia el exterior. Puerta de enlace 192.168.1.1
ip audit info action alarm ip audit attack action alarm pdm history enable	Cuando la alarma genera un mensaje del sistema que muestra que un paquete coincide con una firma, el descarte el paquete, el reinicio lo descarta y cierra la conexión. Si no

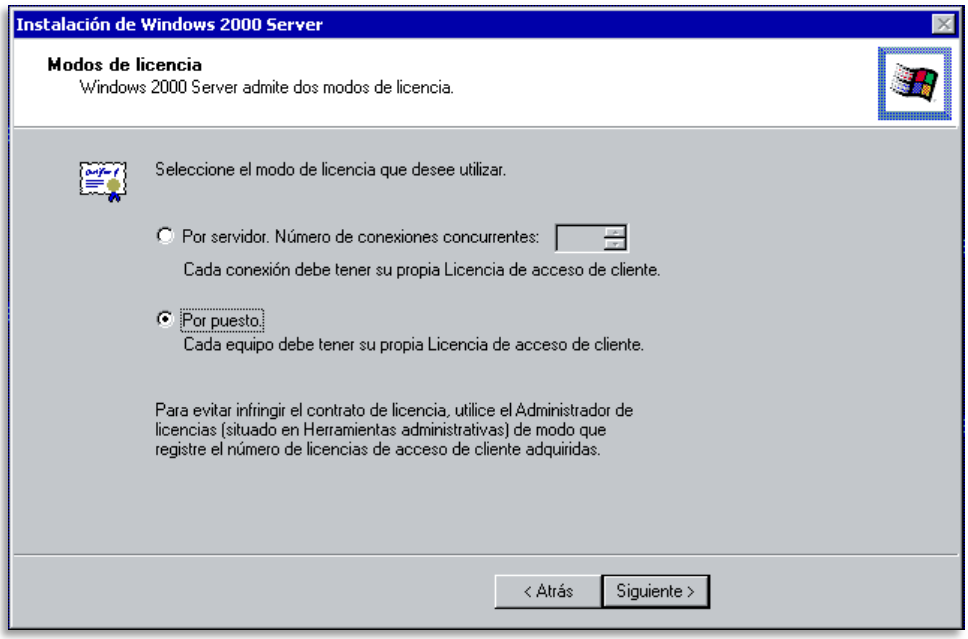
	define una acción, la acción predeterminada es generar una alarma. Así también habilitamos el PDM para monitorear las alarmas.
arp timeout 14400	Este campo establece la cantidad de tiempo antes de que el PIX reconstruya la tabla ARP, entre 60 y 4294967 segundos. El valor predeterminado es 14400 segundos. La reconstrucción de la tabla ARP actualiza automáticamente la información del nuevo host y elimina la información del host antiguo.
global (outside) 1 192.168.0.1-192.168.0.20 255.255.255.0 nat (inside) 1 192.168.1.0 255.255.255.248	Definición de las rutas publicas definidas con NAT.
access-group 201 in interface inside timeout xlate 3:00:00 timeout conn 1:00:00 half closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip media 0:02:00 timeout uauth 0:05:00 absolute	Permite acceso a la lista de acceso 201 en tiempos definidos.
aaa-server TACACS+ protocol tacacs+ aaa-server TACACS+ max-failed-attempts 3 aaa-server TACACS+ deadtime 10 aaa-server RADIUS protocol radius aaa-server RADIUS max-failed-attempts 3 aaa-server RADIUS deadtime 10 aaa-server LOCAL protocol local	El TACACS+ proporciona estos servicios del Authentication, Authorization, and Accounting (AAA):

	Autenticación de los usuarios que intentan iniciar sesión al equipo de red. Autorización de determinar qué nivel de usuarios del acceso debe tener. El considerar para no perder de vista todos los cambios el usuario hace
no snmp-server enable traps	Deshabilita el envío de todas las capturas SNMP, para no saturar el sistema
floodguard enable	Floodguard le permite reclamar recursos de firewall si el subsistema de autenticación de usuarios se queda sin recursos. Si una conexión uauth entrante o saliente está siendo atacada o usada en exceso, el firewall activará reclamar recursos de usuario TCP.
telnet 192.168.1.0 255.255.255.248 inside telnet timeout 5 ssh timeout 5 console timeout 0 wr mem reload	Habilita telnet para la subred SISTEMAS. Guarda la configuración. Reiniciamos sistema.

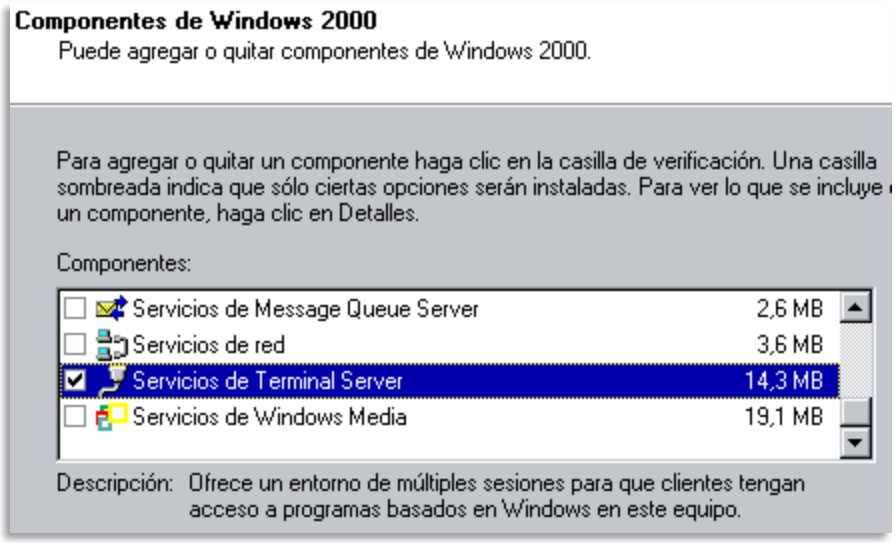
INSTALACIÓN TERMINAL SERVER Y VPN EN WINDOWS SERVER

Instalamos el sistema operativo Windows 2000 Server en un PC con la siguiente configuración:

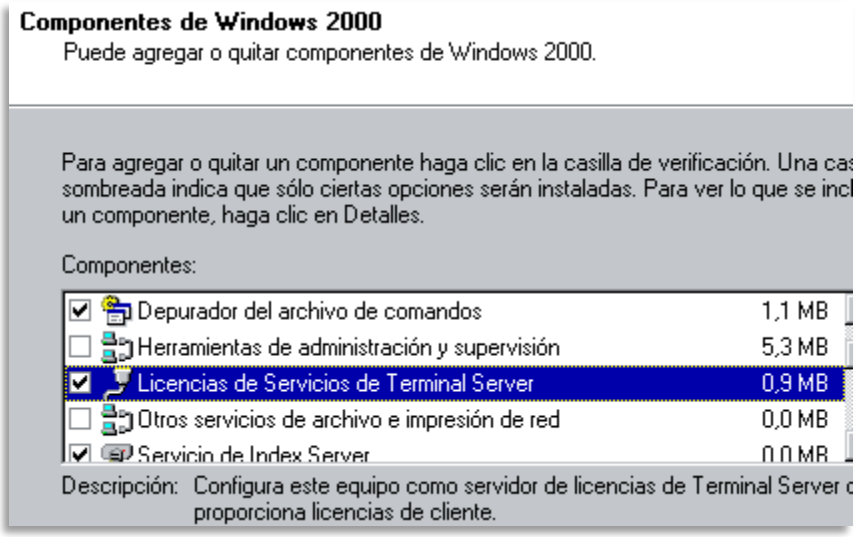
a) Modo de licencia de cliente “Por puesto”, si ya tenemos instalado el sistema operativo, esta opción se puede cambiar desde RDP.



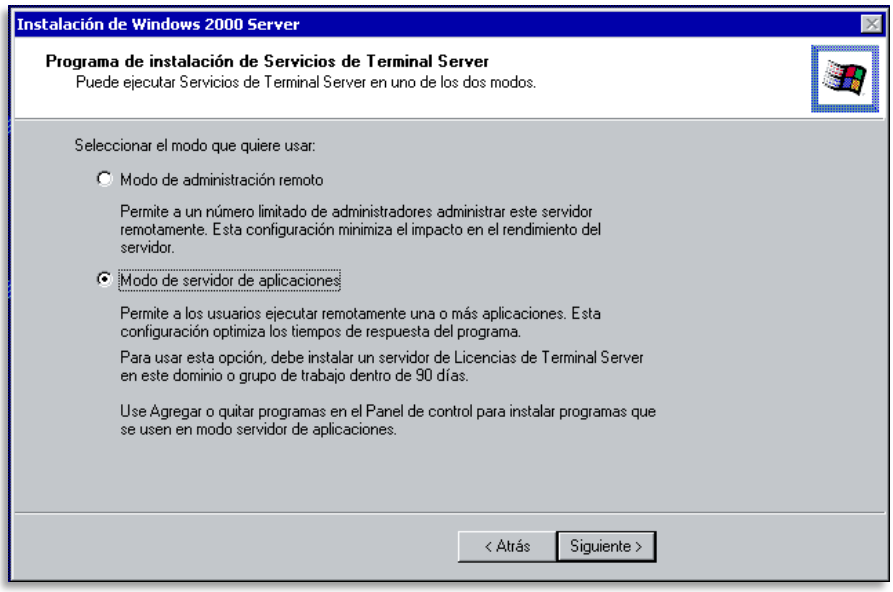
b) Desde las opciones de instalación de Windows 2000 Server o desde "Agregar o Quitar programas" - "Componentes de Windows" (si ya lo tenemos instalado) marcaremos "Servicios de Terminal Server":



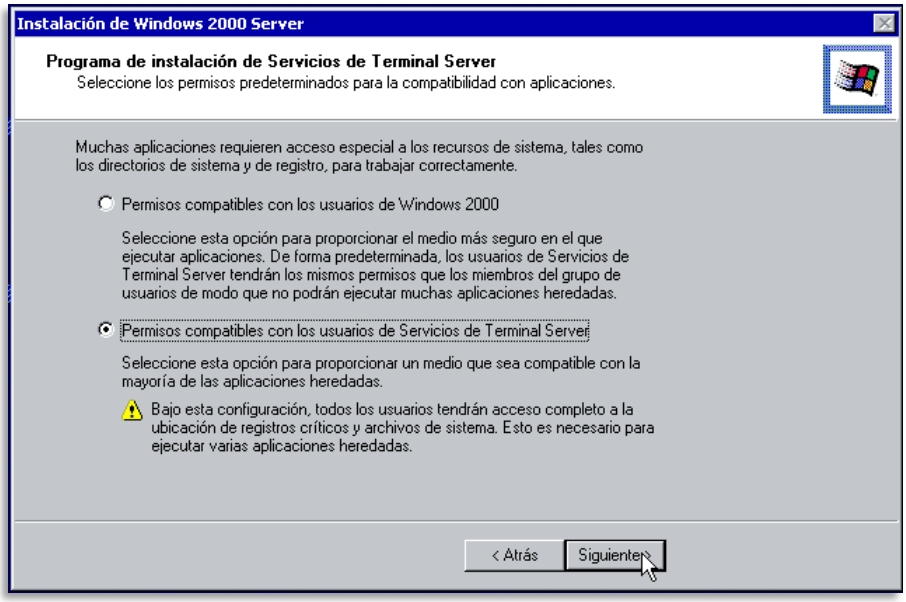
c) Marcaremos para instalar también “Licencias de servicios de Terminal Server”:



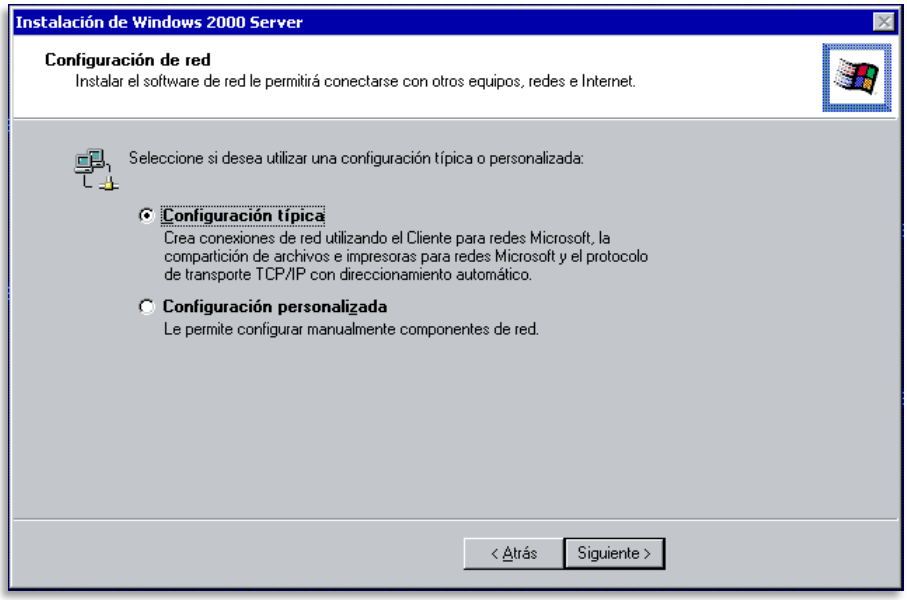
d) En la instalación marcaremos la opción "Modo de servidor de aplicaciones":



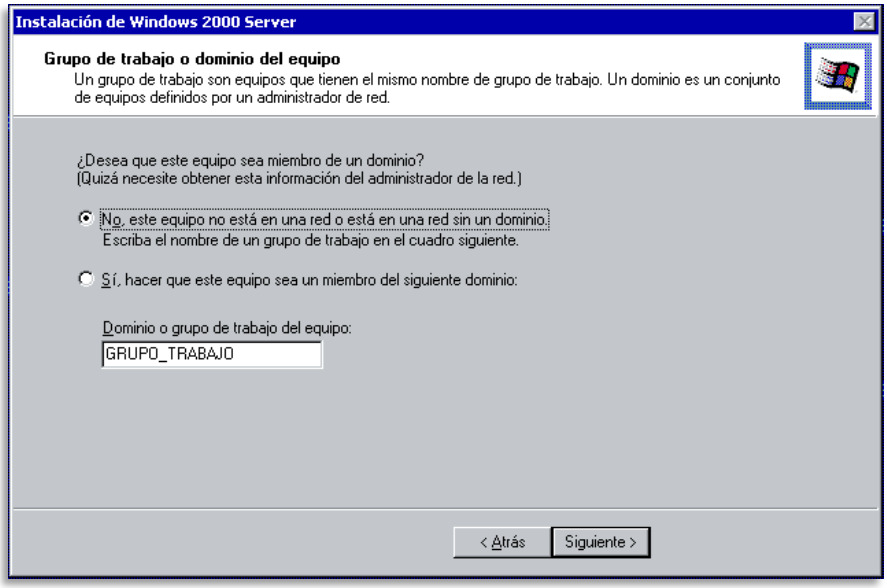
e) En la instalación de Windows 2000 Server marcaremos la opción "Permisos compatibles con los usuarios de Servicios de Terminal Server:



f) Para el caso de la configuración de red en la instalación de Windows 2000 Server, será conveniente marcar la opción "Configuración personalizada" e introducir una IP fija para el servidor, este paso también será posible hacerlo si ya tenemos instalado Windows 2000 Server (desde las propiedades de red):



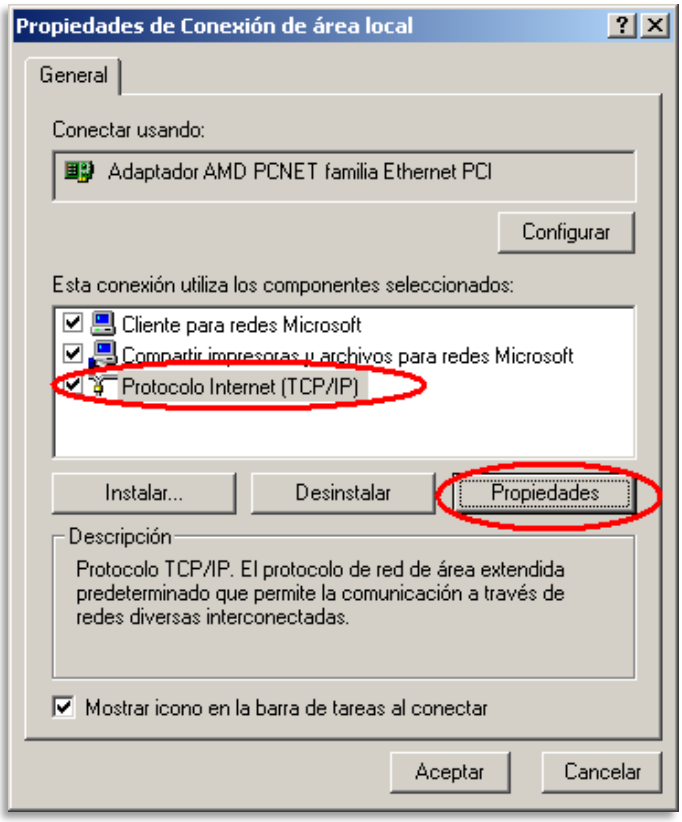
g) No es necesario que el equipo pertenezca a un dominio:



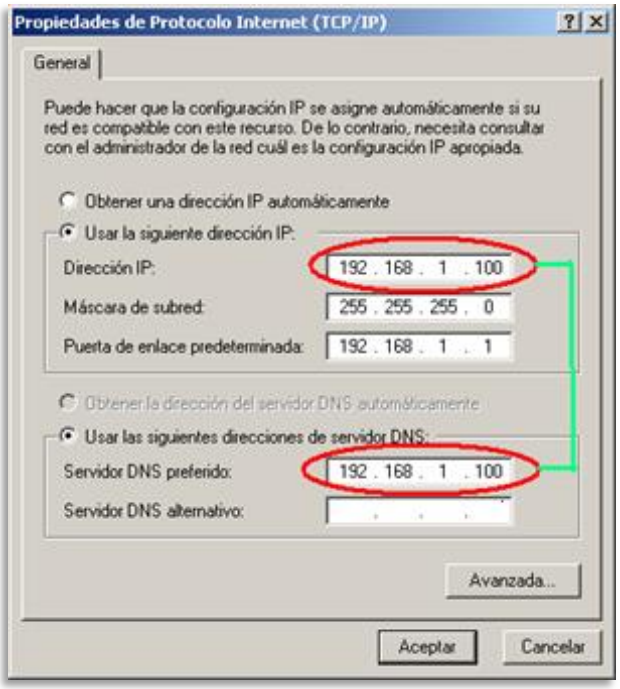
Configuración de Terminal Server y Enrutamiento y acceso remoto

Una vez instalado Windows 2000 Server, configuraremos la red (si no lo hemos hecho en el proceso de instalación), desde Conexiones de red y acceso telefónico, botón derecho sobre "Conexión de área local", seleccionando "Propiedades":

Seleccionaremos "Protocolo Internet (TCP/IP)" y pulsaremos en "Propiedades":



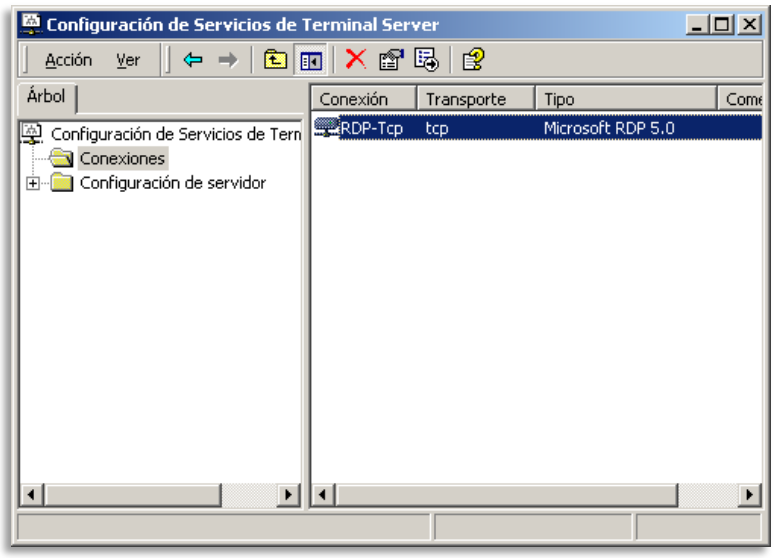
Introduciremos la IP del servidor, la máscara de subred, la puerta de enlace, el servidor DNS preferido (es recomendable que sea la IP del propio servidor), el servidor DNS alternativo:



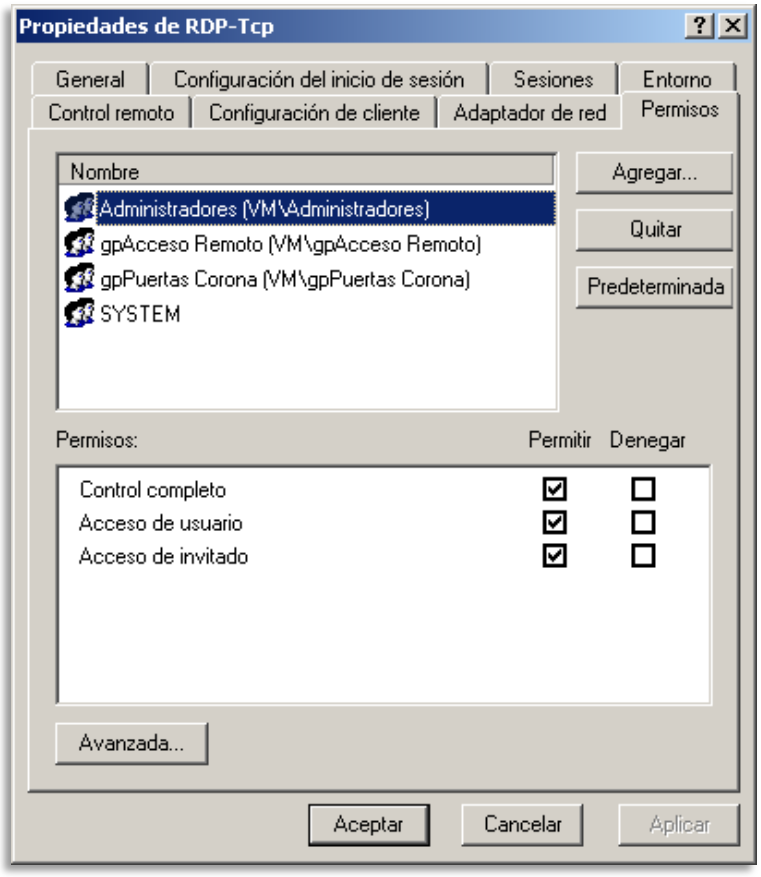
Tras configurar la red del servidor e instalar los servicios de terminal server, deberemos abrir el puerto correspondiente a la VPN (1723) en el router y cortafuegos de nuestra red.

Configuración de la seguridad y otras opciones de Terminal Server (RDP-Tcp).

Para decidir qué usuarios o grupos de usuarios tendrán acceso a Terminal Server desde la Red Local y desde fuera de la red (Internet) y para configurar (suplantar) las opciones de conexión de los usuarios lo configuraremos desde: "Herramienas administrativas" - "Configuración de Servicios de Terminal Server" - "Conexiones" - "RDP-Tcp":



En la pestaña "Permisos" de RDP-Tcp" agregaremos los usuarios y grupos de seguridad que tendrán acceso a Terminal Server.



Desde "RDP-Tcp" podremos configurar otras opciones para los usuarios que accedan mediante conexión a escritorio remoto a nuestro servidor de terminales (terminal server).

En la parte izquierda, seleccionando "Configuración de servidor" podremos configurar otras opciones de conexión (por ejemplo podremos cambiar el modo de Terminal server para que sólo admita conexiones para administración o como actualmente lo tenemos, en modo "Servidor de aplicaciones". Podremos indicar otras opciones:

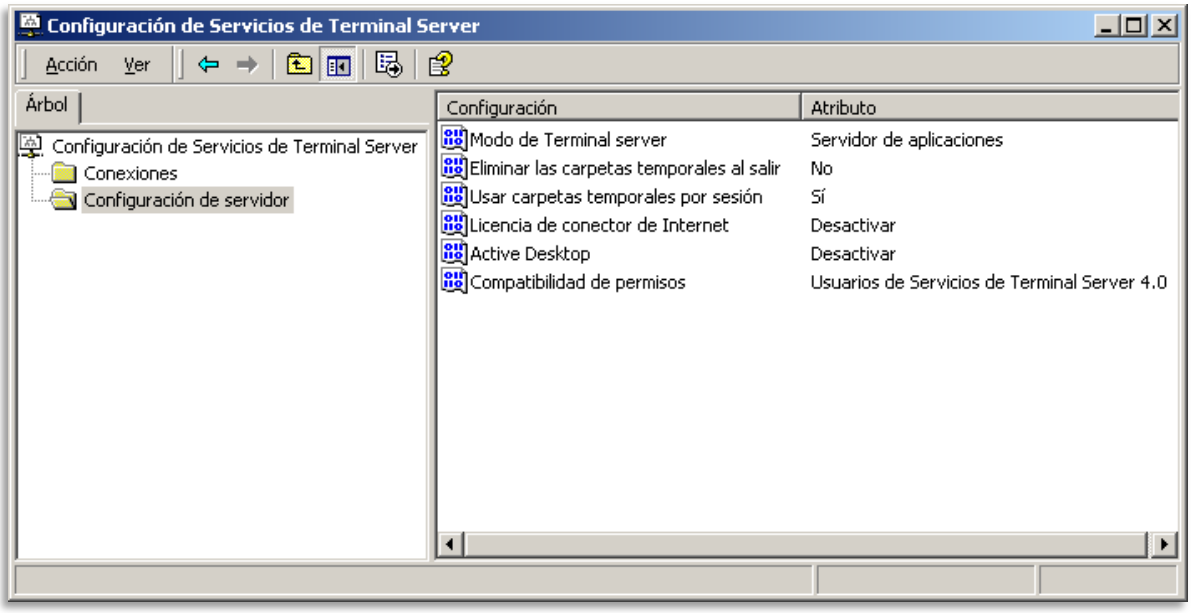
Eliminar las carpetas temporales al salir.

Usar carpetas temporales por sesión.

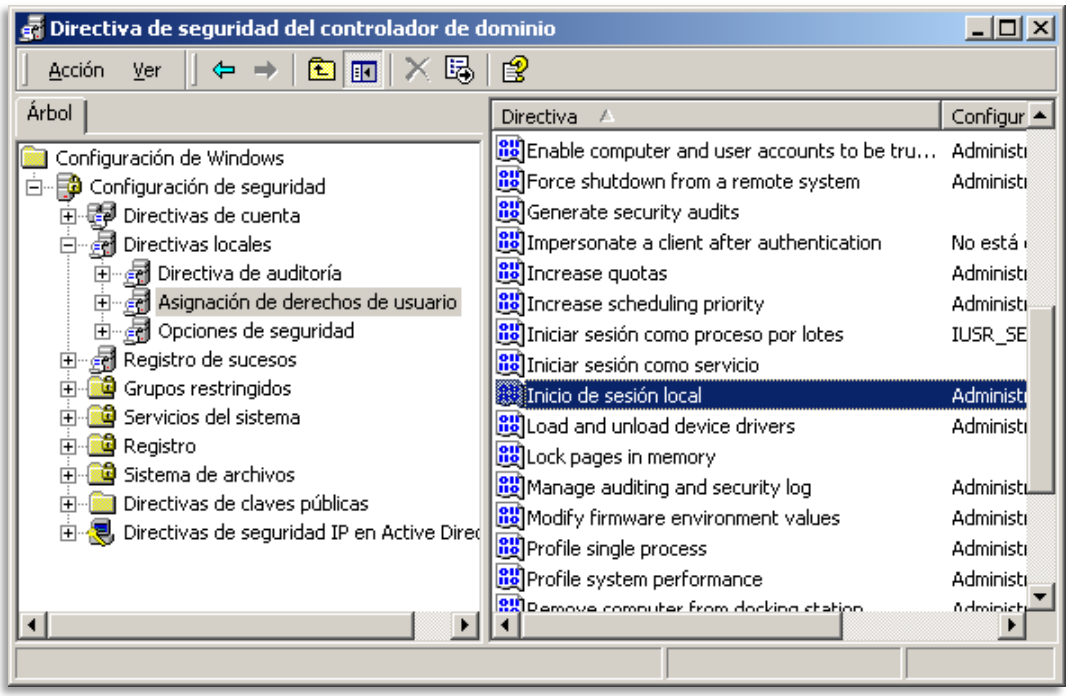
Licencia de conector de Internet.

Active Desktop.

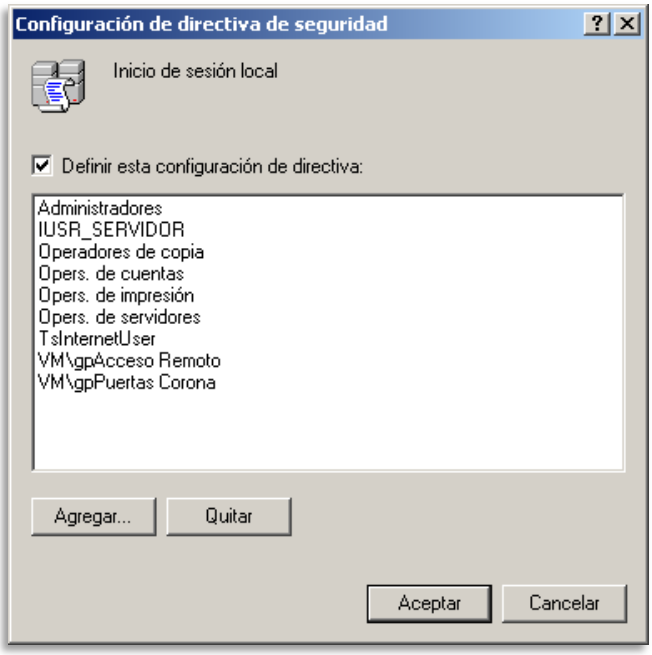
Compatibilidad de permisos.



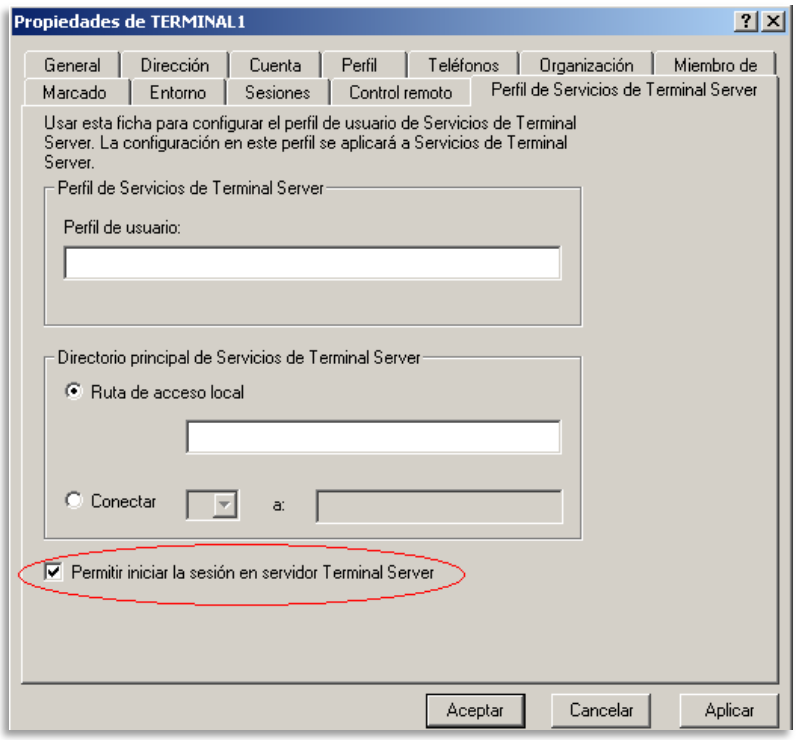
Para decidir qué usuarios o grupos de usuarios podrán tener acceso al servidor, también hay que configurar la Directiva de seguridad, para ello accedemos a "Directiva de seguridad del controlador de dominio", en la parte izquierda pulsaremos en "Configuración de seguridad", "Directivas locales", "Asignación de derechos de usuario", en la parte derecha "Inicio de sesión local":



Agregaremos aquí los grupos de seguridad y usuarios que tendrán acceso:

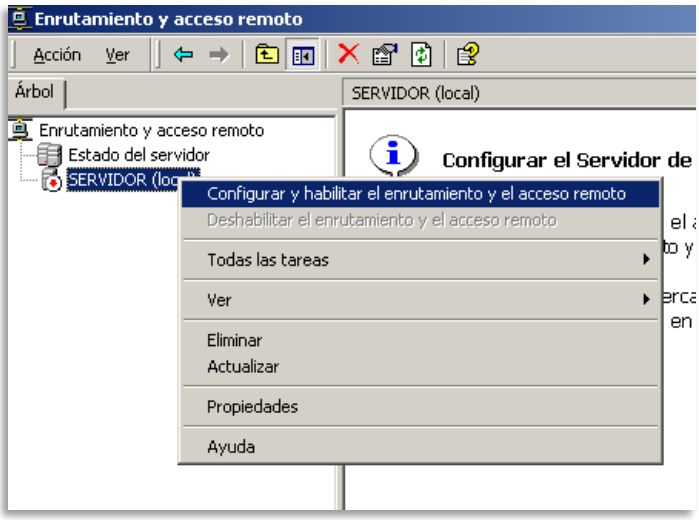


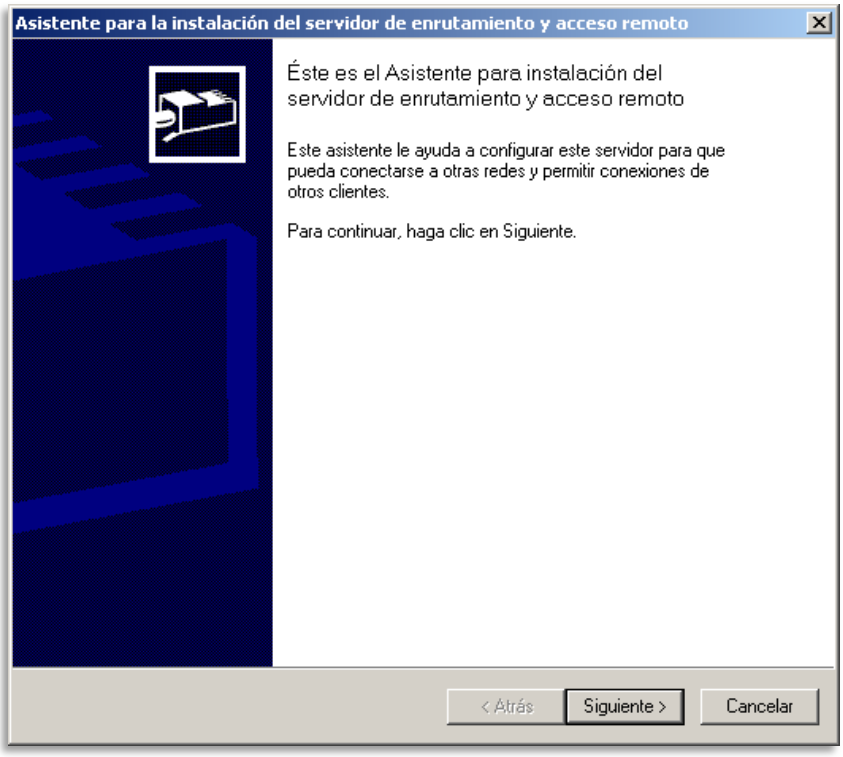
En la pestaña "Perfil de Servicios de Terminal Server" de las propiedades del usuario, marcaremos o desmarcaremos la opción "Permitir iniciar la sesión en servidor Terminal Server":



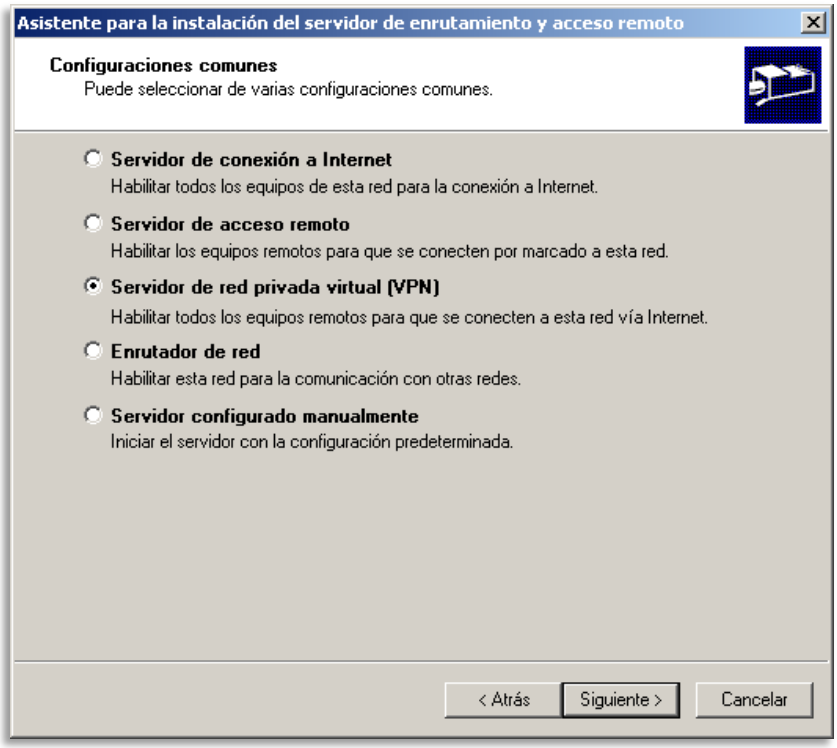
Activación servicio Enrutamiento y acceso remoto (VPN) en Windows 2000 Server

Para permitir el acceso a determinados usuarios desde fuera de la LAN utilizaremos la VPN, para ello activaremos el “Enrutamiento y acceso remoto”, desde “Herramientas administrativas”, “Enrutamiento y acceso remoto”, botón derecho sobre el nombre del servidor, en el menú emergente seleccionaremos "Configurar y habilitar el enrutamiento y acceso remoto:

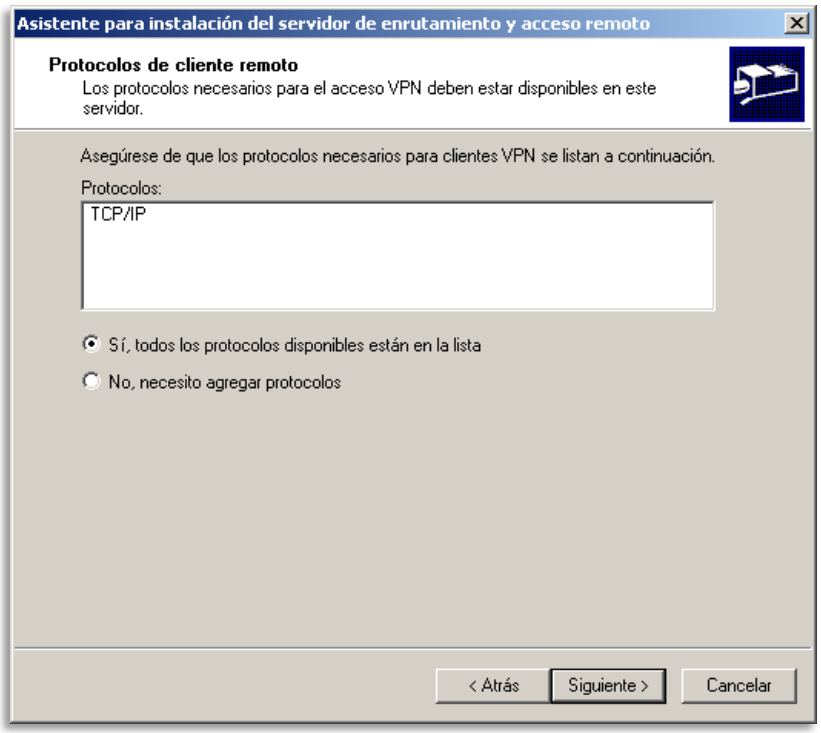




Marcaremos la opción "Servidor de red privada virtual (VPN)" y pulsaremos "Siguiente":

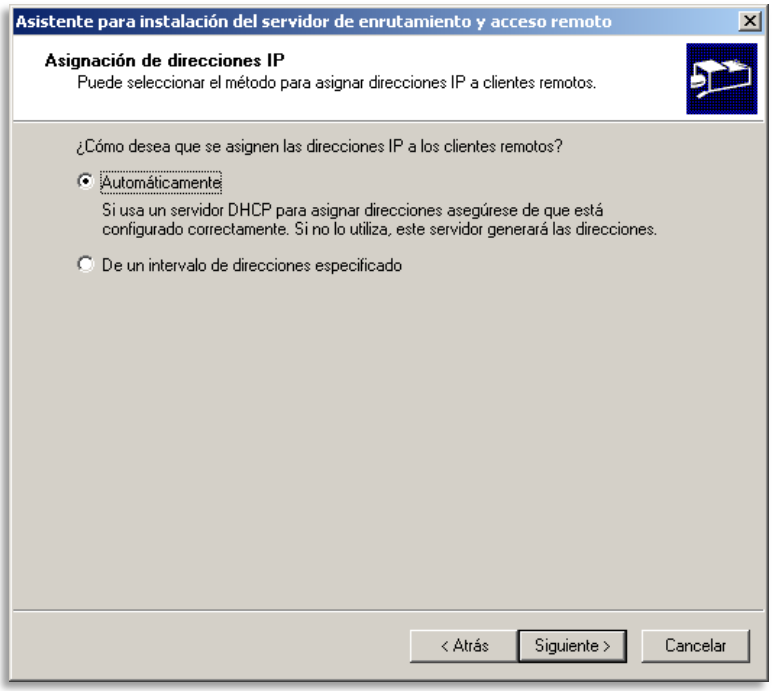


Nos mostrará los protocolos de cliente remoto, en nuestro caso "TCP/IP":

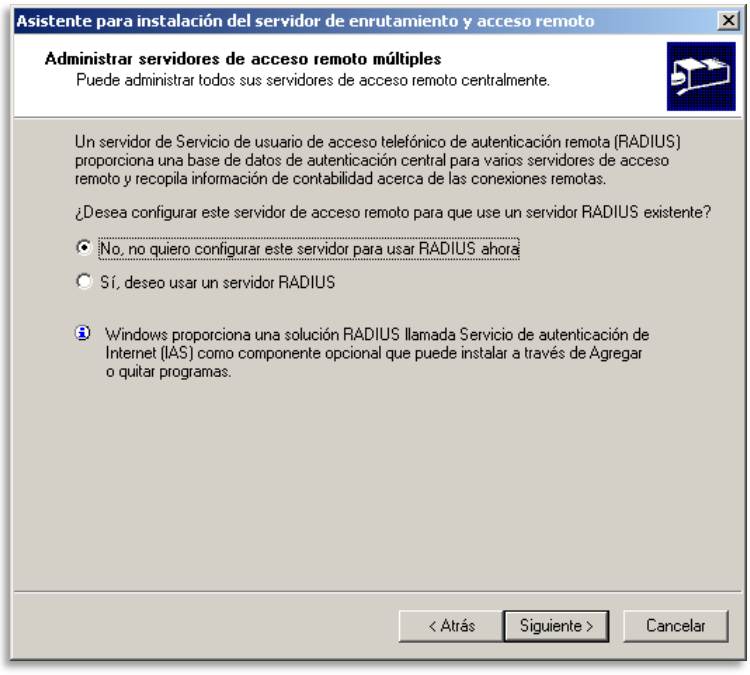


En la asignación de direcciones IP podremos marcar la opción "Automáticamente" para que sea el servidor de DHCP de nuestra red el que asigne las IPs, si no disponemos de servidor

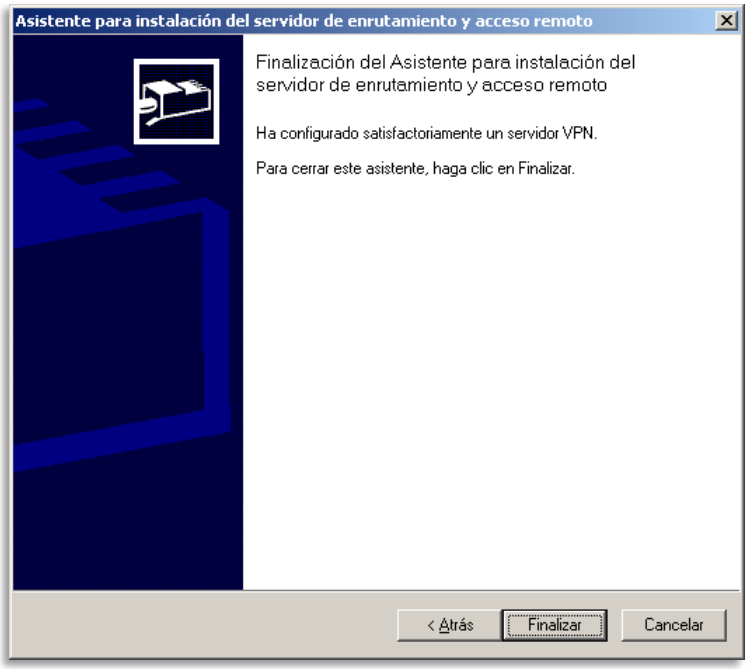
de DHCP en nuestra red y marcamos esta opción será el propio servidor el que genere las direcciones IP para los clientes que accedan mediante la VPN. Si queremos indicar un rango de IP manual marcaremos la opción "De un intervalo de direcciones especificado":



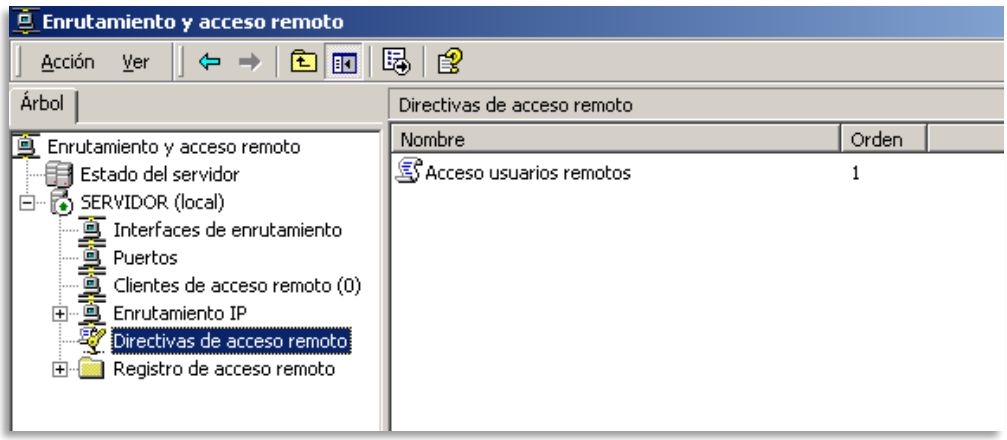
Si desea utilizar la autenticación RADIUS habrá que marcar la opción "Sí, deseo usar un servidor RADIUS", en caso contrario marcaremos la opción "No, no quiero configurar este servidor para usar RADIUS ahora":



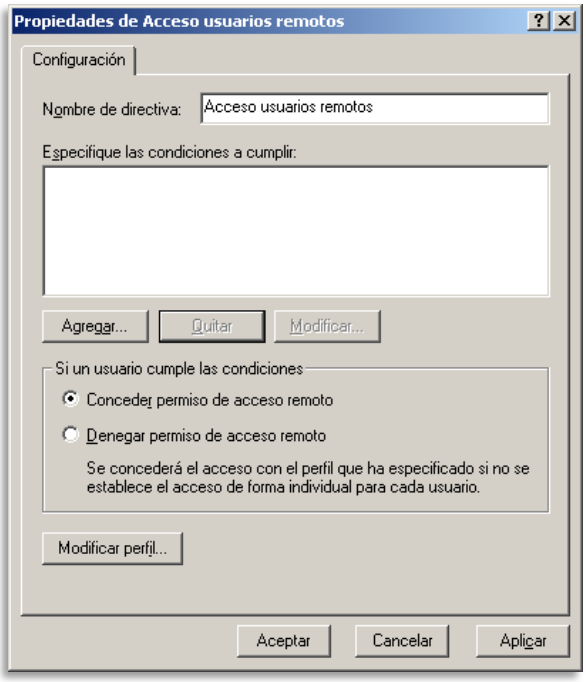
Antes de la instalación del servicio de "Enrutamiento y acceso remoto" el asistente nos mostrará la siguiente ventana, pulsaremos "Finalizar" para concluir el proceso:



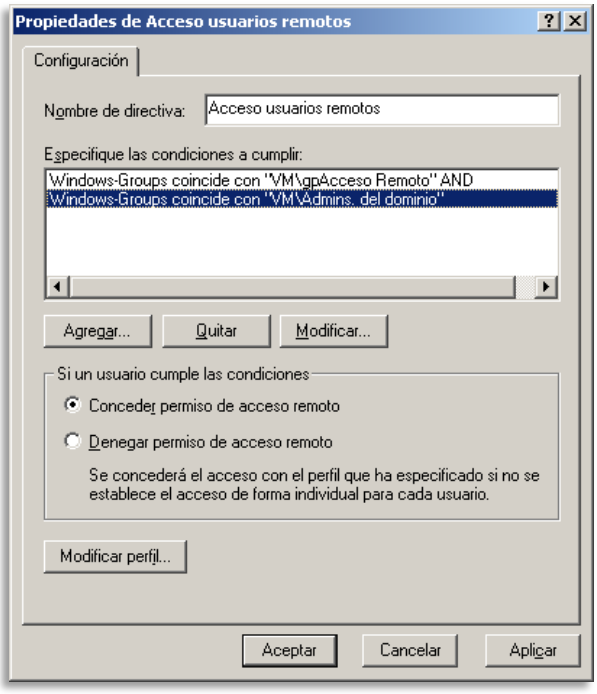
Tras la activación del servicio, tendremos nuevas opciones en "Enrutamiento y acceso remoto", por ejemplo "Directivas de acceso remoto", desde esta directiva indicaremos qué usuarios o grupos tendrán permiso para acceder mediante VPN al servidor, a la derecha seleccionaremos "Acceso usuarios remotos":



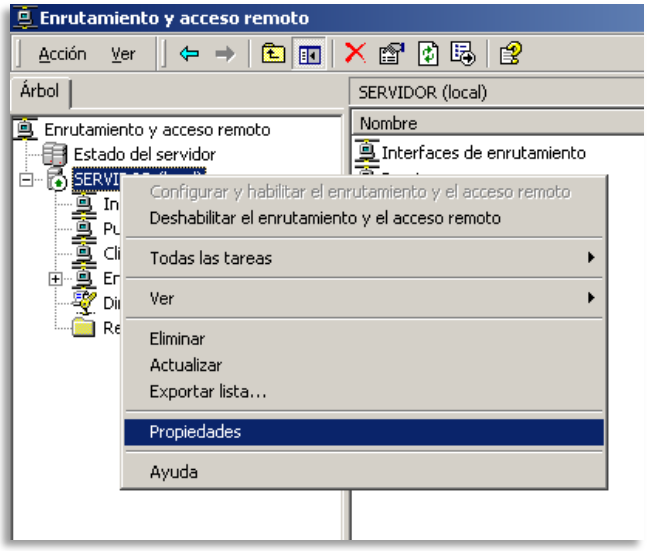
Marcaremos "Conceder permiso de acceso remoto", pulsaremos "Agregar" en la ventana de "Propiedades de Acceso usuarios remotos":



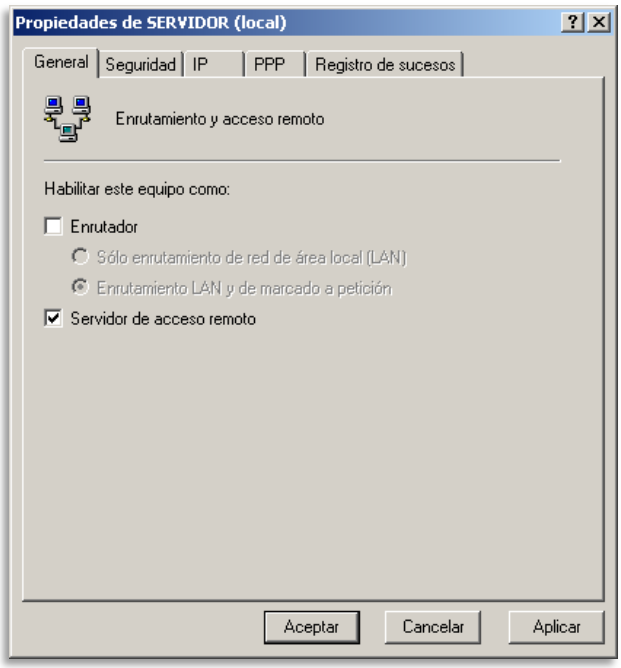
Agregaremos los grupos de seguridad que queramos que tengan acceso a la VPN:



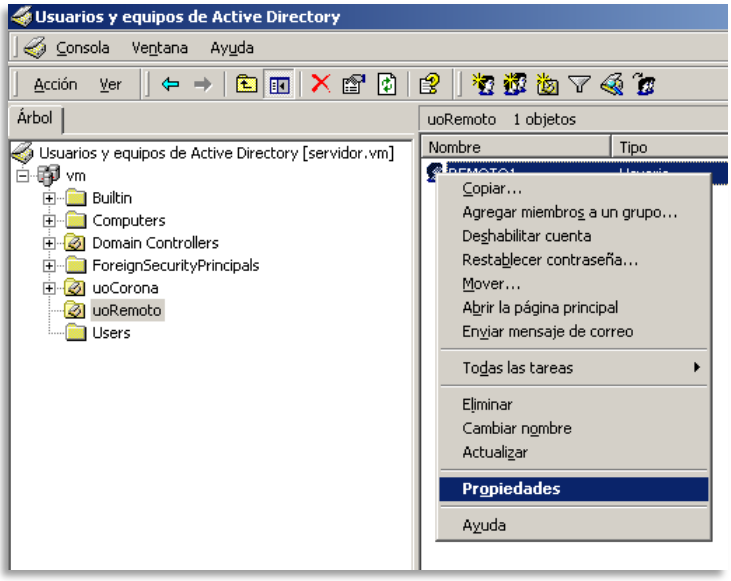
Pulsando con el botón derecho del ratón sobre el servidor, seleccionando "Propiedades" accederemos a las propiedades del servidor para la VPN (enrutamiento y acceso remoto):



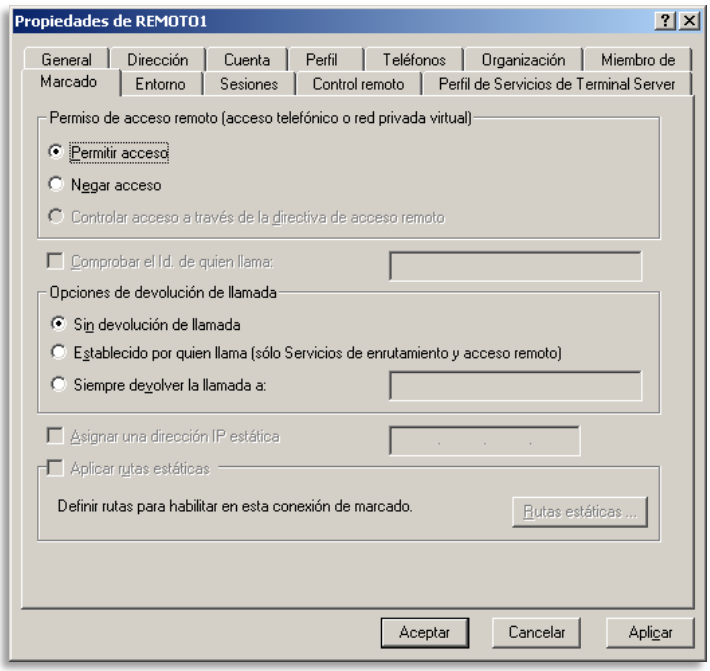
Podremos desmarcar la opción "Enrutador" pues no será necesaria, sí ha de estar marcada la opción "Servidor de acceso remoto":



Por último, deberemos activar en todos los usuarios que queramos que tengan acceso remoto desde fuera de la LAN (mediante VPN) la opción “Permitir acceso”, para ello accederemos a "Usuarios y equipos de Active Directory", seleccionaremos el usuario, accederemos a sus propiedades:



Y en la pestaña "Marcado" marcaremos la opción "Permitir acceso" de "Permiso de acceso remoto (acceso telefónico o red privada virtual)":



Con los pasos anteriores tendremos configurado el servidor de Windows 2000 Server para permitir acceso remoto mediante VPN y Terminal Server.