**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

****

**Facultad de Ingeniería en Electricidad y Computación**

**Licenciatura en Sistemas de Información**

**"Políticas y Seguridades para el Diseño de un Proveedor de Servicios de Internet - ISP”**

**TESIS DE GRADO**

**Previa a la obtención del Título de:**

**LICENCIADO EN SISTEMAS DE INFORMACION**

**Presentado por:**

**Leopoldo Javier Alava Vinueza**

**Jesennia del Pilar Cárdenas Cobo**

**Clemente Xavier Molina Anchaluisa**

**Guayaquil \_ Ecuador**

**2005**

# **AGRADECIMIENTO**

A Dios por las bendiciones que ha derramadas, en todo momento y aun mas cuando los ánimos, y a mis padres, ya que sin su apoyo jamás hubiéramos alcanzado los logros que ahora tenemos.

Jesennia Cárdenas Cobo

# **AGRADECIMIENTO**

A mis padres por alentarme y estar siempre junto a mi. A mis hermanos por su incondicional apoyo

Leopoldo Alava Vinueza

# **AGRADECIMIENTO**

A Dios, a mis padres, a mi esposa y a mi hijo por sus bendiciones, consejos y ayuda que me han sabido brindar siempre.

Xavier Molina Anchaluisa

## Dedicatoria

Dedico este trabajo a Dios y a mis padres, por el amor, apoyo, seguridad y confianza que me brindaron

Jesennia Cárdenas Cobo

## Dedicatoria

A mis padres que me dieron la vida, me vieron crecer y gracias a sus consejos, apoyo y comprensión supieron guiarme y al mismo tiempo fueron mi inspiración.

Leopoldo Alava Vinueza

## Dedicatoria

A Díos, a mi madre, a mi esposa y a mi hijo, que por todos el amor y confianza que han puesto en mi siempre y en especial a mi hijo Adam Xavier.

Xavier Molina Anchaluisa

**Declaración Expresa**

La responsabilidad por los hechos, ideas y doctrinas expuestas en esta tesis de grado nos corresponden exclusivamente; y el patrimonio intelectual de la misma a Licenciatura de Sistemas de Información, de la Escuela Superior Politécnica del Litoral.

Leopoldo Javier Alava Vinueza

Jesennia del Pilar Cárdenas Cobo

Clemente Xavier Molina Anchaluisa

**Tribunal de Grado**

**Ing. Mónica Villavicencio**

Coordinadora de la Licenciatura

en Sistemas de Información

**Ing. Albert Espinal**

Director de Tesis

**Ing. Cristina Abad**

Vocal Principal

**Ing. Marcelo Loor**

Vocal Principal

**resumen**

Una solución de seguridad no es algo que se pueda definir como un producto que se instala o se aplica en el momento. La seguridad es un proceso continuo de estudio sobre nuevos métodos, servicios y productos que están disponibles para atacar redes, sistemas, y aplicaciones. Son revisiones continuas, de actualización de políticas y procedimientos preventivos ante posibles ataques.

El presente proyecto se enfoca en la definición de seguridades para el diseño de un ISP (Proveedor de Servicios de Internet), y su correcta aplicación para prevenir ataques internos y externos que comprometan su integridad.

Los primeros capítulos del presente proyecto definen los elementos de hardware y software necesarios para la implementación de un ISP, luego políticas y procedimientos que permitirán la administración de estos elementos. Unificamos dentro de la seguridad los recursos de software, hardware y humano. Siendo este último uno de los mas importantes para el buen desempeño del proyecto, ya que si falla la parte humana, en el caso de un ataque social, todo puede fallar.

**CONCLUSION y recomendaciones**

La idea de la tesis es de conectar a la mayor cantidad de personas al Internet y con costos accesibles a todos los niveles sociales y como podríamos llegar a realizar esto, y una solución muy practica y sencilla es la conexión vía telefónica, ya que en estos momentos un alto porcentaje de los hogares puede conectarse a Internet mediante una conexión Dial Up.

Los sistemas operativos que se usan para el funcionamiento de la empresa fueron elegidos en base a características, uso, interfaz, conectividad, seguridad, entro otros puntos, motivo por el que se escogieron los siguientes sistemas operativos:

**Linux:** Por sus diferentes versiones, seguridades, protocolos, etc, este sistema operativo es el más idóneo para la parte operacional de la empresa, ya que así podemos tener un mejor control sobre accesos de para el ingreso de los usuarios confiables y el control de usuarios no deseables, adicionalmente Linux esta siendo actualizado constantemente lo que permite que su actualización sea constante, y con esto se corregirán errores en un tiempo mucho menor.

**Windows:** Este sistema operativo fue elegido para el área administrativa de la empresa, su elección se debió a que la mayor parte de los usuarios saben o conocen el correcto manejo de las diferentes aplicaciones de Microsoft. Sus interfaces son muy amigables para con los usuarios, de esta manera el usuario no tiene problema con el manejo de las diferentes aplicaciones de Windows.

Los equipos y aplicaciones que se usarán para una conexión que brinden seguridad, estabilidad y confiabilidad a los clientes cuando deseen ingresar a Internet. Los equipos son:

* + Raduis.
  + Router.
  + Servidores.
  + RAS.

Las aplicaciones usadas para brindar un mejor servicio a los clientes y tener un rendimiento más alto son:

* + - Firewall
    - IDS
    - Red Hat Linux
    - Norton Antirus
    - ARCServer (Software para Respaldar Información)

Con un correcto funcionamiento e interacción entre los equipos y aplicaciones, se podrá brindar al cliente un buen servicio, de esta forma los usuarios darán buenas referencias de nosotros, así en corto tiempo se tendrá una cantidad mayor de usuarios y un mejor rendimiento financiero.

**indice general**

INDICE GENERAL XIV

INDICE DE TABLAS XIX

INDICE DE GRAFICOS XX

INTRODUCCION 1

capitulo 1

**INTRODUCCION A LAS REDES DE COMPUTADORAS**

1.1. CONCEPTO GENERAL DE REDES 2

1.2. CLASIFICACIÓN DE LAS REDES 2

1.2.1. Red de Área Local (LAN) 3

1.2.2. Red de Área Metropolitana (MAN) 3

1.2.3. Red de Área Amplia (WAN) 4

1.3. ARQUITECTURAS DE REDES 5

1.4. COMPONENTES DE UNA RED 7

1.4.1. Dispositivos de Redes 7

1.4.2. Enlaces de Comunicaciones 8

1.5. MODELO DE REFERENCIA OSI 9

1.5.1. Capa Física 10

1.5.2. Capa de Enlace de Datos 11

1.5.3. Capa de Red 12

1.5.4. Capa de Transporte 13

1.5.5. Capa de Sesión 14

1.5.6. Capa de Presentación 14

1.5.7. Capa de Aplicación 15

1.6. ARQUITECTURA TCP /IP 16

1.6.1. Capa de Internet 16

1.6.2. Capa de Transporte 18

1.6.3. Capa de Aplicación 20

1.6.4. Capa de red 21

1.7. PROTOCOLOS Y DIRECCIONES 22

1.7.1. Protocolos Superiores 22

1.7.2. URL (Uniforme Resource Locator) 22

capitulo 2

**PROVEEDOR SERVICIO DE INTERNET ISP**

2.1. Reseña Histórica 26

2.2. Generalidades 28

2.3. Marco General 28

2.4. Visión del Cliente 29

2.5. Visión del Proveedor 30

2.6. Estructura de un ISP 33

2.7. Esquema de Conexión 35

2.8. Distribución de las Oficinas 36

capitulo 3

**ANALISIS DE PLATAFORMAS PARA EL PROVEEDOR DE SERVICIO DE INTERNET**

3.1. Selección de Sistemas Operativos 38

3.1.1. Clases y Análisis Sistemas Operativos 38

3.1.2. Características de Sistemas Operativos 41

3.1.3. Sistema Operativo Linux 44

3.1.3.1 Fiabilidad / Estabilidad 44

3.1.3.2 Rendimiento 45

3.1.3.3 Versatilidad 45

3.1.3.4 Comodidad 46

3.1.3.5 Seguridad 47

3.1.3.6 Conclusión 48

3.1.4. Sistema Operativo Solaris 49

3.1.4.1 Características 49

3.1.4.2 Herramientas para el Administrador del Sistema 50

3.1.4.3 Conclusión 51

3.1.5. Sistema Operativo Windows Server 2003 52

3.1.5.1 Características para Implementar, Administrar y Usar 52

3.1.5.2 Infraestructura segura 53

3.1.5.3 Confiabilidad y Disponibilidad 53

3.1.5.4 Creación de sitios Web de Internet e Intranet 54

3.1.5.5 Windows Server 2003, Web Edition 55

3.1.5.6 Resumen 55

3.2. Detección de Intrusos 56

3.2.1. Tipos de IDS 57

3.2.1.1 Por Situación 57

3.2.1.2 Clasificación según los modelos de detecciones 58

3.2.1.3 Por el Tipo de Respuesta 59

3.2.2. Arquitectura de IDS 60

3.2.3. Conclusiones 62

3.3. Firewall 63

3.3.1. Característica 63

3.3.2. Función 64

3.3.3. Tipos 65

3.3.3.1 Filtrado de Paquetes 65

3.3.3.2 Nivel de Aplicación 66

3.3.3.3 Híbridos 67

3.3.4. Arquitecturas 68

3.3.5. Para Intranets 69

3.3.6. Administración y Gestión 70

3.4. Otros Componentes Adicionales 70

3.4.1. Equipamiento de Redes CSU/DTU 72

3.4.2. Servidores de Acceso 72

3.4.3. Aplicaciones según Sistema Operativo 72

3.4.4. Servidores Web 73

3.4.5. Servidores para transferencia de Archivos 74

3.4.6. Servidor de resolución de Nombres 75

3.4.7. Software de Servidores de Correo Electrónico 75

3.4.8. Servidores de Proxy y Cache 76

3.4.9. Software para Bases de Datos 77

3.4.10. Paquetes de Contabilidad para ISP 78

3.5. Recomendación Final 78

3.5.1. Sistema Operativo Área Operativa 78

3.5.2. Conexión ISP – Cliente 79

capitulo 4

**SEGURIDAD Y SERVICIOS UN PROVEEDOR DE SERVICIO DE INTERNET**

4.1. Servicios Internet 81

4.1.1. Servicio de Resolución de Nombres DNS 81

4.1.1.1 Espacio de Nombres de Dominio 85

4.1.2. Servicio de correo electrónico 87

4.1.2.1 Servicio POP3 e IMAP 89

4.1.2.2 MTA Sendmail (SMTP) 91

4.1.3. Servicio World Web Wide (WWW) 91

4.1.4. Servicio FTP 92

4.1.5. Servicio PROXY-CACHE 93

4.2. Conectividad 93

4.3. Administración de redes 95

4.4. Seguridad 96

4.5. Equipamiento Computacional 96

4.6. Administración de clientes 98

capitulo 5

**POLÍTICAS DE SEGURIDAD INFORMÁTICA**

5.1. Políticas de Seguridad 100

5.1.1. Definición de Políticas de Seguridad Informática 100

5.1.2. Elementos de una Política de Seguridad Informática 101

5.1.3. Razones que Impiden la Aplicación de las Políticas de

Seguridad 102

5.2. Privacidad en la Red 102

5.2.1. Características para considerar una red segura 102

5.2.2. Riesgos o Amenazas a la Privacidad de las Redes 103

5.3. Políticas Generales 105

5.4. Antivirus 107

5.4.1. Correo electrónico de Clientes 107

5.4.2. Usuarios Internos 108

5.4.3. Medidas de Protección Efectivas 110

5.4.4. Referencia para Software de Antivirus 110

5.5. Correo Electrónico 111

5.6. Seguridad de Sistema Detector de Intruso - IDS 112

5.6.1. Políticas par Riesgos Medios 114

5.6.2. Políticas para Riesgos Altos 115

5.7. Seguridad para el Servidor de Servicio de Nombres de

Dominio - DNS 116

5.7.1. Métodos para Asegurar el Servidor 116

5.7.1.1Servicio de DNS redundante 117

5.7.1.1Servidor en su Red Perimetral 117

5.7.1.1Control de Interfaces 117

5.7.1.1Limitar Tráfico por IP 118

5.7.1.1Encriptación 118

5.7.1.1Proteger Cache 118

5.7.1.1Autorizar las actualizaciones Dinámicas de DHCP 118

5.8. Seguridad para Firewall 119

5.9. Consideraciones finales de la seguridad 120

5.10. Conclusión 122

capitulo 6

**ESTUDIO ECONOMICO**

6.1. Soluciones Propuestas 123

6.1.1. Primera Alternativa 123

6.1.2. Segunda Alternativa 124

6.1.3. Conclusión 124

6.2. Proyección de Ingresos 125

6.3. Costos de Equipos y Licencias 125

6.3.1. Comunicación y Computación 126

6.3.2. Licencias de Programas y Aplicaciones 127

6.3.3. Características de Equipos 128

6.4. Gastos de Operación 131

6.5. Gastos Administrativos y Generales 132

6.5.1. Gastos Administrativos 132

6.5.2. Generales 133

6.6. Flujo de Caja 134

6.7. Punto de Equilibrio 135

ANEXO A

ANEXO B

ACRONIMOS

BIBLIOGRAFIA

**indice de tablas**

capitulo 1

TABLA 1.1. Protocolos típicos de Internet y su función 21

TABLA 1.2. Uso de caracteres inseguros en direcciones URL 25

capitulo 3

Tabla 3.1. Comparación de Sistemas Operativos 39

Tabla 3.2. Características de los Sistemas Operativos 41

capitulo 4

Tabla 4.1. Dominios genéricos 33

Tabla 4.2. Relación de de Direcciones IP con DNS 85

capitulo 6

Tabla 6.1.Proyección de Ingresos 125

Tabla 6.2. Equipos de Computación y Comunicación 126

Tabla 6.3. Software e Infraestructura 127

Tabla 6.4. Descripción de Servidor para e-Mail y Administrativo 128

Tabla 6.5. Descripción de Servidor para Internet 129

Tabla 6.6. Descripción de Equipo para Estaciones de Trabajo 130

Tabla 6.7. Descripción de Impresoras 130

Tabla 6.8. Descripción de Firewall 131

Tabla 6.9. Descripción de Gastos de Operación 131

Tabla 6.10. Descripción de Gastos de Personal 132

Tabla 6.11. Descripción de Gastos Generales 133

Tabla 6.12. Flujo de Caja 134

**indice de graficos**

capitulo 1

FIGURA 1.1. Relación entre hosts y la subred 4

FIGURA 1.2. Capas, protocolos e interfaces en una red 6

FIGURA 1.3. El modelo de referencia OSI 10

FIGURA 1.4. Comparación arquitectura TCP/IP con el modelo OSI 15

FIGURA 1.5. Protocolos y redes en el arquitectura TCP/IP 16

capitulo 2

Figura 2.1. Conexión de un ISP cliente a su proveedor 28

Figura 2.2. Visión del Cliente de un ISP 30

Figura 2.3. Estructura de un ISP 33

Figura 2.4. Esquema de Enlaces 35

Figura 2.5. Distribución de Oficinas 36

capitulo 3

Figura 3.1. Red con IDS 57

Figura 3.2 Distribución de los censores dentro de un ISP. 61

capitulo 4

Figura 4.1. Semejanzas entre la estructura del DNS y el

sistema de ficheros de Linux 86

Figura 4.2. Esquema del correo electrónico Internet 88

Figura 4.3. Representación esquemática del servicio

de correo electrónico 89

capitulo 6

Figura 6.1. Punto de Equilibrio 135

# INTRODUCCION

En la actualidad el análisis y diseño de las redes de computadores considera con mayor frecuencia los servicios ofrecidos por la *“red*”, por ejemplo: Web, correo electrónico, etc. De este modo, cobra relevancia el conocimiento y comprensión de los servicios y sus mecanismos de implementación. Este proyecto aborda el tema de los servicios Internet a través de un ISP (Proveedor de Servicios de Internet).

Establecer un esquema sistemático para el inicio de operación del ISP, para lo cual hay que considerar estructuras y arquitecturas de las redes, además de modelos de referencia y todos los elementos que intervienen en el diseño de una red y comunicación.

Se determinan los servicios básicos que presta un ISP. Con esta base se planifica la segmentación del proceso de implementación del ISP mínimo. Por último se realiza una descripción de las políticas y seguridades que se deberán contemplar dentro del ISP.

Esta tesis contiene los siguientes temas: Introducción a los ISP, selección del Sistema Operativo, habilitación de los servicios de Internet, mecanismos de seguridad, políticas de seguridad y análisis financieros de los costos de inversión.