# ESCUELA POLITÉCNICA NACIONAL

## ESCUELA DE POSTGRADO EN INGENIERIA Y CIENCIAS

# IMPLANTACION DE UN ESQUEMA DE SEGURIDAD PARA UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

**TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN INGENIERÍA ELÉCTRICA CON MENCION EN CONECTIVIDAD Y REDES DE TELECOMUNICACIONES**

**FALCONI CARDONA ROBERTO MARCIAL**

**HERRERA SILVA JUAN ALBERTO**

**DIRECTOR: Msc. Gustavo Samaniego**

**Quito, Noviembre 2006**

# DECLARACIÓN

Nosotros, Roberto Marcial Falconí Cardona y Juan Alberto Herrera Silva, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Roberto Marcial Falconí Cardona

Juan Alberto Herrera Silva

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Roberto Marcial Falconí Cardona y Juan Alberto Herrera Silva, bajo mi supervisión.

Msc. Gustavo Samaniego
DIRECTOR DE TESIS

**AGRADECIMIENTOS**

A Dios por darme la vida, salud y sabiduría para culminar mi Tesis y seguir adelante en mi carrera profesional.

A mi esposa que con su apoyo incondicional ha sabido brindarme toda su paciencia, cariño y apoyo, ha permitido que culmine otra etapa de mi vida.

Al Ing. Gustavo Samaniego, mi director de Tesis, quien ha sabido apoyarme durante mi carrera profesional y ha contribuido a la culminación de mi Tesis.

A todas las demás personas que con su ayuda hicieron posible la culminación de este trabajo.

Gracias a todos por su ayuda.

Juan

# DEDICATORIA

Este trabajo quiero dedicar a 2 personas lindas
que mantienen vivos mis sueños e ilusiones,
y que son parte de mi vida mi esposa
Marcela y mi hijo Roberto.

# CONTENIDO

# INDICE DE ILUSTRACIONES

# INDICE DE TABLAS

# INDICE DE ANEXOS



**Nota: Todos los Anexos se adjuntan en formato digital en un CD**

# RESUMEN

La presente Tesis de Maestría **"IMPLANTACIÓN DE UN ESQUEMA DE SEGURIDAD PARA UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP)"** tiene como objetivo principal el implantar un esquema de seguridad para un Proveedor de Servicios de Internet (ISP), que brinde las seguridades necesarias a los usuarios de estos servicios protegiéndoles de los ataques informáticos que podrían realizarse desde el Internet.

Para ello en el Capítulo I se define la Metodología de trabajo por etapas para realizar esta Tesis. Una vez definida cada una de las etapas de trabajo se presenta una revisión conceptual general de las Metodologías de Evaluación de Seguridades basadas inicialmente en "COBIT" y sus Guías de Auditoría, combinadas con la metodología de Evaluación de Riesgos NIST 800-30 y finalmente la metodología OSSTMM para Penetration Testing – Ethical Hacking. Se complementa este capítulo con un marco teórico sobre los fundamentos de los ISP´s y Servicios de Seguridad.

En el capítulo II, se presentan en detalle la ejecución de la Etapa 1 y Etapa 2 de nuestra metodología de trabajo. La Etapa 1 considera inicialmente la evaluación de la seguridad en la infraestructura actual de un ISP mediante la aplicación de la metodología de Auditoría Informática "COBIT". Este enfoque provee prácticas generalmente aceptadas por la industria para administración y control de la información y recursos IT. De esta metodología se utilizó los Objetivos de Control y las Guías de Auditoría relacionados a seguridad tecnológica.

Además se combinó con COBIT otras metodologías de Evaluación de Seguridad Informática, basadas en el análisis de riesgos según la Metodología NIST 800-30 y Test de Penetración para los servicios de red que proporciona el ISP y revisión de parámetros de seguridad en la configuración de sistemas operativos de servidores, bases de datos, aplicaciones de negocio y elementos activos de la red. En la Etapa 1 se identifica el nivel de riesgo y exposición, ante ataques

internos (en la red del ISP) y externos (a través de Internet) que podrían realizar personas externas al ISP.

En la Etapa 2 se emiten recomendaciones basadas en las Matrices de pruebas y de Evaluación de Control según la metodología de COBIT para corregir huecos y vulnerabilidades de seguridad tanto para los servicios de Internet (navegación, e-mail, ftp, web hosting, colocation, VoIP, video conferencia, entre otros) que proporciona el ISP, como para los parámetros de seguridad en la configuración de sistemas operativos de servidores, bases de datos, aplicaciones de negocio y elementos activos de la red.

Posteriormente el Capítulo III, cubre la Etapa 3 y Etapa 4 de la metodología de trabajo. En la Etapa 3 se analizó, diseñó e implantó un Esquema de Seguridad para el ISP, considerando los elementos críticos de la infraestructura, como: Routers, Firewall, Módems Satelitales, Servidores de Acceso, Autenticación, Correo, Web Hosting y la aplicación Facturación de Consumos.

Para la Etapa 3 se utilizó las recomendaciones dadas en la evaluación previa y las necesidades del negocio en cuanto a seguridad tecnológica, a fin de reducir al máximo el riesgo y exposición inicial ante ataques internos y externos que podrían realizar personas externas al ISP.

En la Etapa 4 se realiza un Seguimiento de Auditoría Informática para verificar que el Esquema de Seguridad implantado en el ISP contemple las recomendaciones de seguridad proporcionadas en la Etapa 2. Finalmente, se reevalúa el nivel de riesgo y exposición ante ataques luego de implantar el esquema de seguridad, con el fin de proveer seguridad a los usuarios que se conectan a Internet e identificar el estado final de seguridad que tiene el ISP.

En el capítulo IV se emiten las respectivas conclusiones y recomendaciones de la presente Tesis.

# CAPITULO I

# MARCO TEORICO

## 1.1 EL PROBLEMA Y SU IMPORTANCIA

A medida que el uso del Internet aumenta a nivel global, aparecen nuevas amenazas a la seguridad, tanto de los proveedores de servicios de Internet - ISP como de sus usuarios, estas amenazas generalmente se presentan como ataques vía Internet, virus, bombas lógicas, denegación de servicios, correo malicioso o no deseado, fraudes, robos, hackeos en general. En la actualidad la tecnología de Telecomunicaciones que proveen los ISP a sus usuarios corporativos y masivos presentan muchos riesgos a la seguridad que no pueden pasarse por alto.

De ahí la necesidad de que un ISP realice primero una evaluación general de sus seguridades, basada en niveles de riesgo y exposición ante posibles ataques, para que con esta base pueda implantar un Esquema de Seguridad adecuado, acorde a las necesidades de su negocio y de la situación actual del Internet a nivel mundial.

Para ello, podemos utilizar el Marco de Referencia COBIT (Control Objectives For Information and Related Technology), que es un modelo generalmente aplicable y aceptado para las buenas prácticas en seguridad tecnológica, en la administración y control de la tecnología de la información (IT).

“COBIT tiene su base en los objetivos de control de ISACF actualmente conocida como ISACA (Information Systems Audit and Control Association), pero han sido mejorados de acuerdo a los actuales estándares internacionales profesionales y específicos de la industria, este modelo de referencia tiene la facilidad de adaptarse a cualquier tipo de negocio y los objetivos de control que se han

definido en el modelo pueden ser aplicados independientemente del ambiente, plataformas y madurez tecnológica de la organización.” [13]

El modelo COBIT puede ser usado cotidianamente por gerentes de IT y auditores, enfocándose a las necesidades del negocio. COBIT puede ser integrado con otros modelos diferentes en áreas específicas de los cuales tenemos: ISO17799[14], ISO9000[15], ITIL[16], CMM[17] y OSSTMM[18].

Esta Tesis permitirá a los diferentes usuarios de los servicios proporcionados por el proveedor de servicios de Internet – ISP, disponer de una garantía de que la información que está utilizando vía Internet es segura para su uso.

---

[13] Fuente: ISACA, COBIT Framework, 3ra edición, Rolling Meadows, USA, 2000, Pág. 3
[14] **ISO 17799:** Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar e implantar o mantener la seguridad de una organización.
[15] **ISO9000:** Son directrices para que una organización pueda lograr la calidad de un producto o servicio de manera que las necesidades del cliente sean satisfechas.
[16] **ITIL:** Conjunto de bibliotecas que reúnen las mejores prácticas para la gestión de servicios de IT agrupadas en dos áreas Soporte al Servicio, Entrega al Servicio.
[17]**CMM:** Modelo de madurez para el desarrollo de aplicaciones que define 5 niveles siendo el 1 lo más bajo y 5 el nivel ideal.
[18]**OSSTMM:** Es un manual de seguridad, en el que participan abiertamente más de 130 profesionales de todo el mundo, y que cumple con los estándares ISO17799 / BS7799.

# 1.2 OBJETIVOS

## 1.2.1 OBJETIVO GENERAL

Implantar un esquema de seguridad para un Proveedor de Servicios de Internet (ISP), que brinde las seguridades necesarias a los usuarios de estos servicios protegiéndoles de los ataques informáticos que podrían realizarse desde el Internet.

## 1.2.2 OBJETIVOS ESPECÍFICOS

1. Evaluar la seguridad de la infraestructura actual de un ISP, utilizando la metodología de Auditoría Informática "**COBIT**" (**C**ontrol **OB**jectives for **I**nformation and related **T**echnology) en combinación con otras metodologías de Evaluación de Seguridad Informática, para identificar el nivel de riesgo y exposición, ante ataques internos (en la red del ISP) y externos (a través de Internet).

2. Emitir las recomendaciones necesarias para cerrar huecos y vulnerabilidades de seguridad en los servicios y en los elementos críticos de la infraestructura del ISP.

3. Realizar el análisis, diseño e implantación de un Esquema de Seguridad para un Proveedor de Servicios de Internet (ISP), contemplando las recomendaciones dadas en la evaluación previa y las necesidades del negocio, a fin de reducir al máximo el riesgo y exposición inicial ante ataques.

4. Reevaluar el nivel de riesgo y exposición ante ataques luego de implantar el esquema de seguridad, con el fin de proveerles seguridad a los usuarios que se conectan a Internet por el ISP.

## 1.3 METODOLOGÍAS DE EVALUACIÓN DE SEGURIDADES

Para la realización de esta Tesis de Maestría se ha contemplado la siguiente Metodología de trabajo:

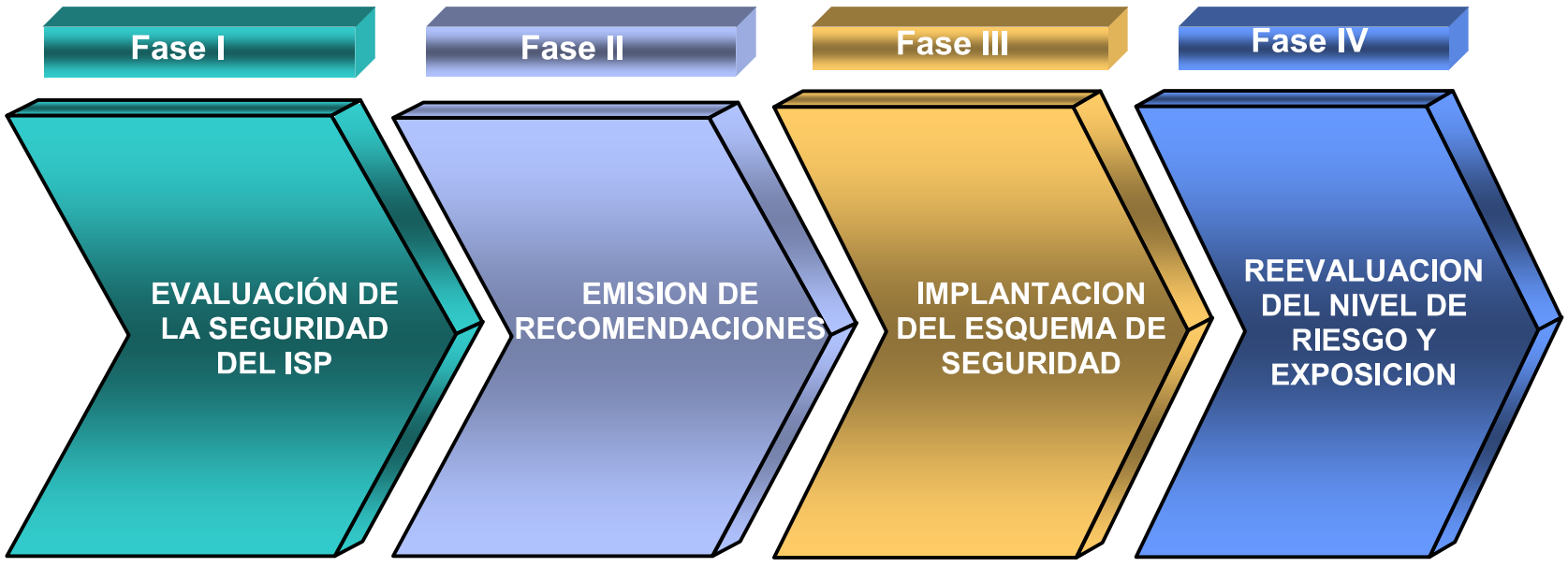



*Fig. 1.1 Metodología de Trabajo*

A continuación presentamos un detalle de cada una de estas fases.

***Etapa 1:***

El trabajo contempla inicialmente la evaluación de la seguridad en la infraestructura actual de un ISP mediante la aplicación de la metodología de Auditoría Informática **"COBIT"** (**C**ontrol **OB**jectives for **I**nformation and related **T**echnology, dado por el IT Governance Institute de la Asociación de Controles y Auditores de Sistemas de Información a nivel mundial - ISACA). Este enfoque provee prácticas generalmente aceptadas por la industria para administración y control de la información y recursos IT. De esta metodología utilizaremos los Objetivos de Control y las Guías de Auditoría relacionados a seguridad tecnológica.

Además se combinarán con COBIT otras metodologías de Evaluación de Seguridad Informática, basadas en Test de Penetración para los servicios de red que proporciona el ISP y revisión de parámetros de seguridad en la configuración de sistemas operativos de servidores, bases de datos, aplicaciones de negocio y financieras, y elementos activos de la red.

En esta etapa inicial se identificará el nivel de riesgo y exposición, ante ataques internos (en la red del ISP) y externos (a través de Internet) que podrían realizar personas externas al ISP.

***Etapa 2:***

Partiendo de la evaluación inicial se emitirán recomendaciones para corregir huecos y vulnerabilidades de seguridad tanto para los servicios de Internet (navegación, e-mail, ftp, web hosting, colocation, VoIP, video conferencia, entre otros) que proporciona el ISP, como para los parámetros de seguridad en la configuración de sistemas operativos de servidores, bases de datos, aplicaciones de negocio y financieras, y elementos activos de la red.

***Etapa 3:***

En esta etapa se analizará, diseñará e implantará un Esquema de Seguridad para el ISP, considerando los elementos críticos de la infraestructura, como: Routers, Firewall, Servidores de Acceso, Autenticación, Correo, Web Hosting y aplicaciones tales como Facturación y otras de índole Financiero.

Para esta etapa se utilizarán las recomendaciones dadas en la evaluación previa y las necesidades del negocio en cuanto a seguridad tecnológica, a fin de reducir al máximo el riesgo y exposición inicial ante ataques internos y externos que podrían realizar personas externas al ISP.

***Etapa 4:***

Se realizará un Seguimiento de Auditoría Informática para verificar que el Esquema de Seguridad implantado en el ISP contemple las recomendaciones de seguridad proporcionadas en la Etapa 2.

Finalmente, se reevaluará el nivel de riesgo y exposición ante ataques luego de implantar el esquema de seguridad, con el fin de proveer seguridad a los usuarios que se conectan a Internet por un ISP.

### 1.3.1 METODOLOGIA Y PRODUCTOS COBIT®

El conjunto de guías y modelos COBIT proveen un marco referencial y un lenguaje común para la administración de sistemas de información, la auditoría de sistemas de información, las prácticas de control y la seguridad de la información, durante todo el ciclo de vida de los sistemas de información.

COBIT fue elaborado en primer lugar por la Information Systems Audit and Control Foundation (ISACF) en 1996. Para la publicación de la segunda edición en 1998 se realizó una revisión a los objetivos de control de alto nivel, a los objetivos de control detallados y la adición del Conjunto de Herramientas de Implementación. En la tercera edición participa un nuevo editor, el Instituto de Gobierno de IT (IT Governance Institute), el mismo que fue creado por la Information Systems Audit and Control Asosation (ISACA). El Instituto de Gobierno de IT toma un rol protagónico al incluir una publicación llamada las Directrices Gerenciales con el fin de expandir y tener un mejor entendimiento del gobierno de IT. La tercera Edición de COBIT será utilizada en el desarrollo de la presente Tesis.

COBIT provee prácticas generalmente aceptadas por la industria para administración y control de la información y recursos IT. De esta metodología utilizaremos los Objetivos de Control y las Guías de Auditoría relacionados a seguridad tecnológica.

En la tercera edición de COBIT se han definido las siguientes publicaciones:

**1. Resumen Ejecutivo**

El Resumen Ejecutivo COBIT explica los principales conceptos y principios del modelo, esta dirigido a principiantes en COBIT y a expertos administradores buscando información concreta ya que se explica que es el modelo COBIT, para que sirve, como se usa e identifica los cuatro dominios de COBIT y los 34 procesos de IT correspondientes.

**2. Marco Referencial**

El marco referencial COBIT es la base para el desarrollo de los demás elementos COBIT, desde su publicación en 1994 ha sido una guía para la organización de las actividades IT, describe los 34 objetivos de control de alto nivel, uno por cada proceso de IT, contenidos en cuatro dominios. Algo muy importante es que identifica cuales de los siete criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad) y los recursos de IT (sistemas de aplicación, tecnología, instalaciones, datos) son importantes para dar un soporte a los objetivos de negocio, una de las principales características del marco referencial es el vínculo existente entre el proceso IT y los requerimientos del negocio.

**3. Objetivos de Control**

Este documento proporciona 318 objetivos de control genéricos, agrupados por los 34 objetivos de control de alto nivel del marco referencial, se identifica cuales son las necesidades que deben ser administradas en cada proceso de IT, los mismos que ayudan a definir políticas claras y buenas prácticas para el control IT.

**4. Guías de Auditoría**

Las guías de auditoría sugieren cuales son los pasos de auditoría que deben seguirse para cada uno de los 34 objetivos de control IT de alto nivel, qué preguntas hacer, cómo evaluarlos y los riesgos que pueden producirse por no ser alcanzados, ya que el objetivo de las guías de auditoría es asegurar que las metas y los objetivos sean alcanzados. Toda esta información es de mucha ayuda para los equipos de auditores.

**5. Prácticas de Control**

Las prácticas de control ayudan a aquellas personas encargadas de diseñar e implementar controles específicos para administrar riesgos en proyectos de IT, las prácticas de control ayudan a mejorar el rendimiento de IT ya que proveen guías para saber que controles son necesarios y cuales son las mejores prácticas para alcanzarlos, las prácticas de control expanden las capacidades de COBIT al proveer un nivel adicional.

**6. Guías de Administración**

Las guías de administración o directrices gerenciales, contienen modelos de madurez, además sirven para determinar en que posición se encuentra la organización en base a benchmarkings[19]. Las guías de administración proveen factores críticos de éxito y cuales son las mejores prácticas administrativas para alcanzar los objetivos de control en IT.

La administración de IT debe asegurar que las metas y los controles claves están siendo alcanzados.

**7. Conjunto de Herramientas de Implementación**

El conjunto de herramientas COBIT toma las lecciones aprendidas por aquellas organizaciones que aplicaron COBIT rápidamente y de forma exitosa, las cuales son reunidas en un conjunto de herramientas que pueden ser usadas por otras organizaciones. En estas lecciones se indica la necesidad de incluir a los niveles gerenciales desde el principio del proceso, y que estos se encuentren preparados para explicar el marco de referencia tanto a nivel general como a nivel detallado.

En la Fig. 1.2 se ilustra la jerarquización y composición de los contenidos del modelo COBIT:

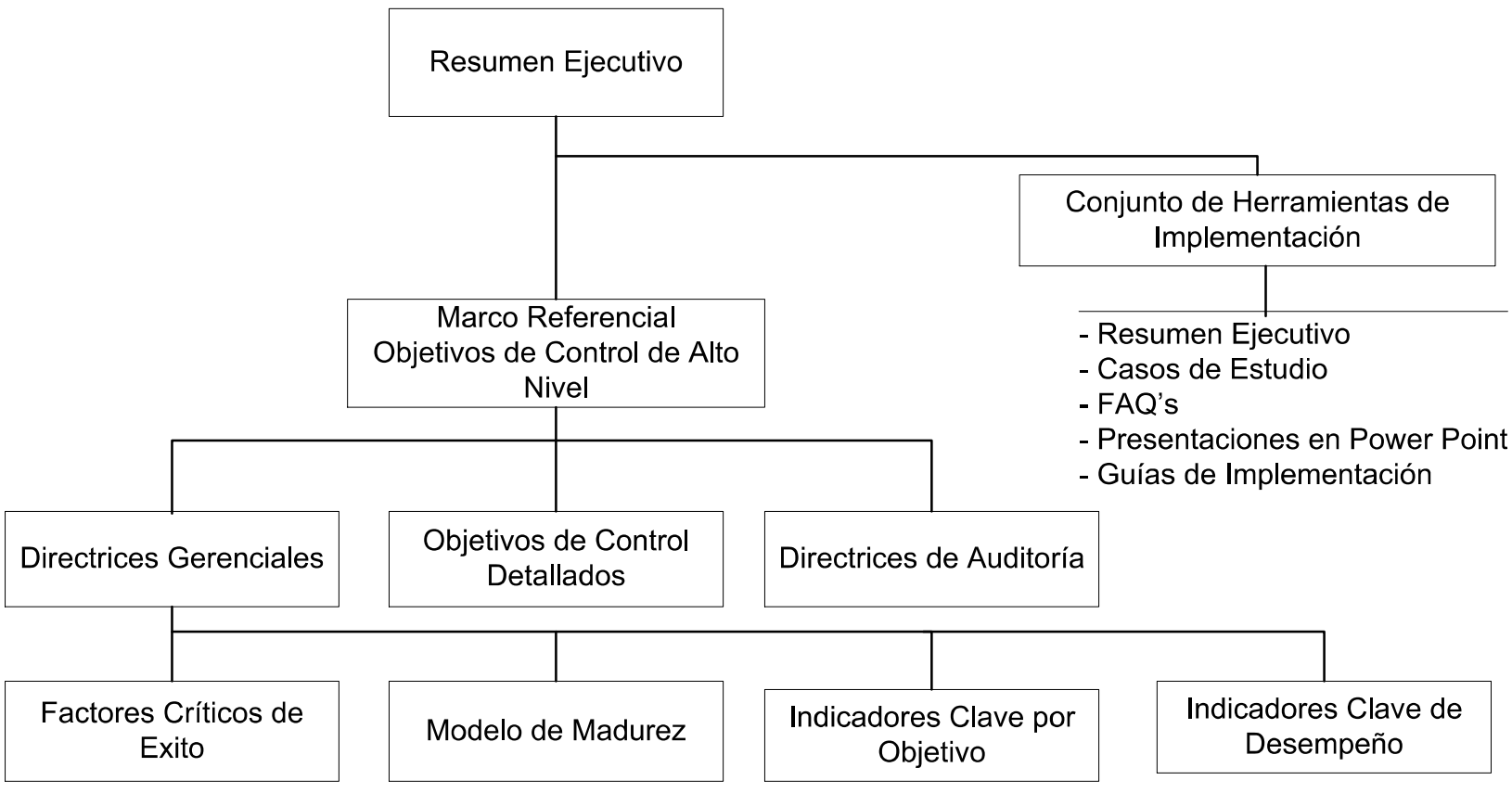



*Fig. 1.2 Productos de la Familia COBIT*

*Fuente: ISACA, COBIT Framework, 3ra edición, Rolling Meadows, USA, 2000, Pág. 19*

[19] Benchmarkings: Proceso en el que se compara la situación actual de una organización con las mejores prácticas de la industria.

#### 1.3.1.1 Dominios de COBIT

Los dominios definidos en el marco referencial (Ver Anexo A – Marco de Referencia de COBIT) han sido nombrados utilizando términos comunes en el día a día por la administración y son los siguientes:

- Planeación y Organización,
- Adquisición e Implementación,
- Entrega y Soporte,
- Monitoreo.

A continuación se definen cada uno de estos dominios:

**1. Planeación y Organización.-** En este dominio se cubre las estrategias, tácticas, la identificación de cual es la vía tecnológica que puede contribuir de mejor manera a alcanzar los objetivos del negocio. En adición la estrategia de visión necesita ser planeada, comunicada, administrada por diferentes perspectivas. Como punto final se debe establecer una organización y una estructura tecnológica apropiadas.

**2. Adquisición e Implementación.-** Para materializar la estrategia IT, las soluciones IT deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas en los procesos del negocio. En este dominio también se cubre los cambios y el mantenimiento de sistemas existentes, con el fin de asegurar que el ciclo de vida es aplicado por estos sistemas.

**3. Entrega y Soporte.-** Este dominio incluye los procesos de entrega o distribución desde las operaciones tradicionales hasta el entrenamiento tomando en cuenta aspectos de seguridad y continuidad de las operaciones. Con el propósito de entregar servicios, el proceso de soporte necesario también debe ser implementado. Este dominio incluye el actual procesamiento de datos el mismo que es ejecutado por los sistemas de aplicación, clasificados de forma frecuente como controles de aplicación.

**4. Monitoreo.-** Todos los procesos de IT necesitan ser evaluados de forma periódica en el tiempo, En este dominio se advierte a la administración la necesidad de asegurar los procesos de control independientes, estos procesos son definidos por auditorías externas e internas o por fuentes alternativas.

Los procesos IT pueden ser aplicados en varias capas de la empresa, cubriendo a la organización, la función IT, o al nivel de los propietarios de los procesos del negocio.

Los objetivos de control no satisfacen del mismo modo a los requerimientos del negocio, se puede diferenciar por grados de impacto, es por esto que el modelo de la misma manera que ha definido los objetivos de control para cubrir riesgos de negocio también determina la relación de los objetivos y su impacto con la consecución de las metas organizacionales.

- **Primario.-** Este es el grado en el cual el objetivo de control definido impactan de forma directa a los criterios de información considerados.
- **Secundario.-** En este grado se encuentra el objetivo de control que impactan a una extensión pequeña o de forma indirecta a los criterios de información.
- **En blanco.-** Se refiere a que los requerimientos del negocio son satisfechos de forma apropiada por otro criterio y/o proceso

De igual forma las medidas de control tampoco afectan en el mismo grado a los recursos IT.

### 1.3.1.2 Objetivos de Control COBIT relacionados con la Seguridad

Los *Objetivos de Control* han sido organizados por procesos/actividad y definidos de forma genérica sin importar la plataforma tecnológica bajo la que estén implementados los procesos, con la excepción de algunos ambientes de tecnología especiales que necesitan un análisis separado para objetivos de control.

Los *Objetivos de Control* no son más que objetivos detallados y específicos por cada proceso de IT; existen desde tres hasta un máximo de treinta objetivos de control por cada proceso dando una total de 318, tienen su base en estándares y regulaciones internacionales de IT. La principal función de los *Objetivos de Control* es la presentación de resultados y propósitos que se desean alcanzar aplicando mecanismos de control a los procesos de IT.

Los *Objetivos de Control* están dirigidos al personal de IT, a los profesionales de auditoría, quienes son los encargados de su evaluación, y lo más importante es que también están dirigidos a los dueños de los procesos de negocio.

En esta Tesis se han utilizado específicamente los *Objetivos de Control COBIT relacionados con la Seguridad,* como se observa en la Fig. 1.3:

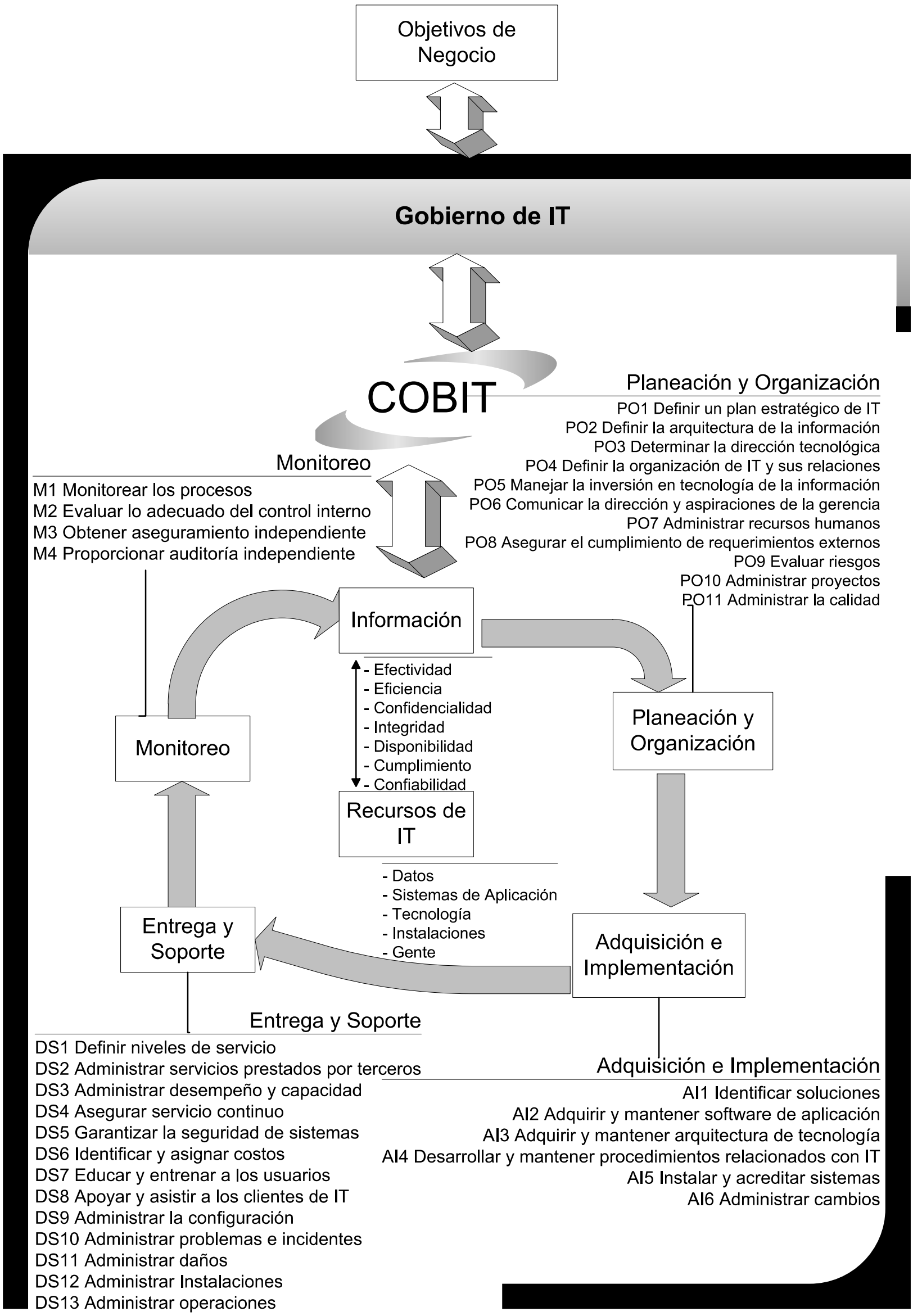



*Fig. 1.3 Procesos de IT COBIT definidos en los cuatro dominios*

*Fuente: ISACA, COBIT Framework, 3ra edición, Rolling Meadows, USA, 2000, Pág. 7*

En resumen los *Objetivos de Control* definen mecanismos de control detallados para lograr eficiencia, efectividad y economía en el uso y administración de los recursos IT.

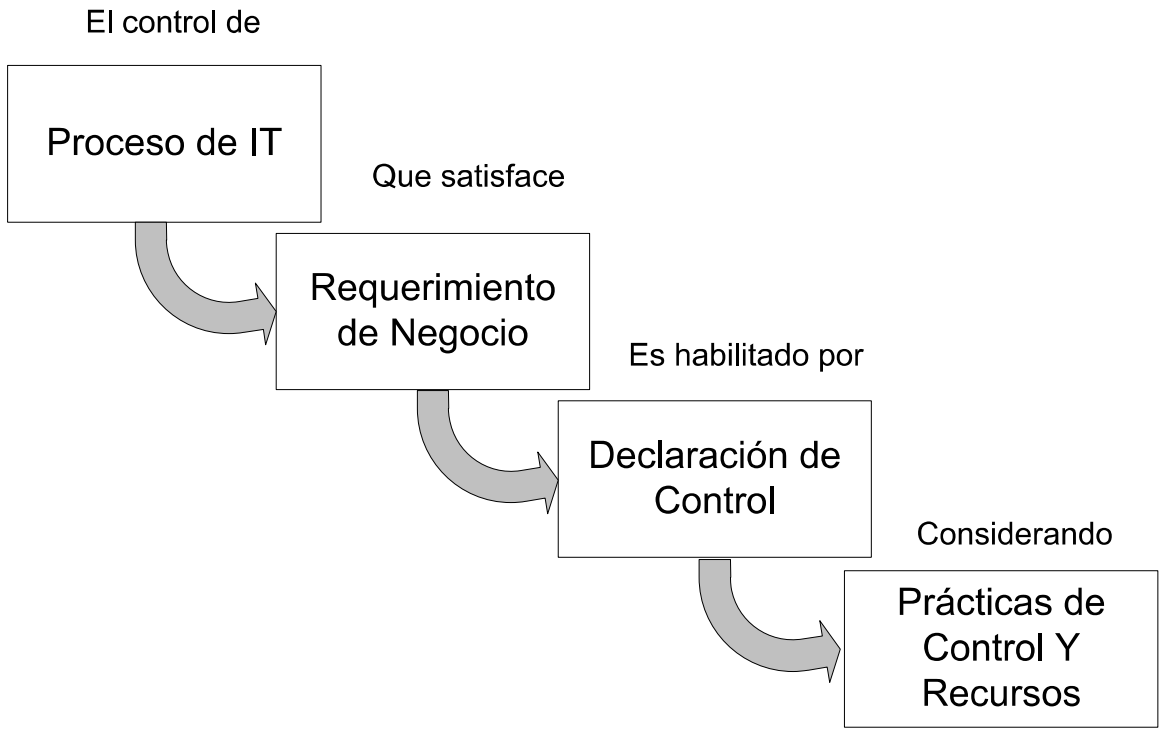



*Fig. 1.4 Componentes de los Objetivos de Control*
*Fuente: ISACA, COBIT Framework, 3ra edición, Rolling Meadows, USA, 2000, Pág. 21*

Para cada Dominio detallado existe una lista de objetivos de control de alto nivel. ver Anexo B (Objetivos de Control de Alto Nivel).

Los objetivos de control de alto nivel engloban a varios objetivos de control específicos, en total son 318, para mayor detalle referirse al Anexo C (Objetivos de Control Específicos).

## 1.3.2 METODOLOGÍAS DE PENETRATION TESTING – ETHICAL HACKING

### 1.3.2.1 Conceptos Generales

El objetivo consiste en realizar un intento de intrusión controlado a los sistemas de información de la compañía, con el objetivo de identificar las vulnerabilidades a las que están expuestas las redes y definir los planes de acción para mitigar los riesgos.

Se busca emular a todos los tipos de intrusos y obtener evidencias concretas del resultado obtenido.

Las pruebas fehacientes de que se ha realizado la intrusión con éxito pueden depender del tipo de ataque realizado, definiéndose en SI se permite o NO la realización final del ataque, identificando vulnerabilidades a través de:

- **Captura del Trofeo:** obtención de algún tipo de archivo de los servidores o redes
- **Sembrado de pruebas:** en los servidores
- **Otros**: captura de paquetes, limitación del servicio del recurso, etc.

Se intentan accesos vía: Red Física, Web, Telefónica, Transmisiones y Emanaciones e Ingeniería Social.

Ambientes de las Pruebas de Intrusión (Penetration Test):

- **Caja Blanca** (con información del objetivo)
- **Caja Negra** (sin información del objetivo)
- **Caja Gris** (Híbrido)

#### 1.3.2.2 Penetration Test Externos

Se compone de un elevado número de pruebas, entre las que se pueden nombrar:

- Ingeniería Social.
- Ataques de Reconocimiento.
- Detección de conexiones externas.
- Obtención de rangos de direcciones en Internet.
- Detección de protocolos.
- Evaluación (Scanning) de puertos TCP, UDP e ICMP.
- Análisis a Dispositivos de comunicaciones
- Análisis de seguridad de conexiones remotas.
- Scanning de vulnerabilidades.
- Prueba de ataques de denegación de servicio.
- Ejecución  de explotación de código (codigo exploit) aplicable.

### 1.3.2.3 Penetration Test Internos

Adicionalmente a las pruebas anteriores se pueden agregar:

- Análisis de protocolos internos.
- Pruebas (Test) a nivel de autenticación de usuarios.
- Análisis de la seguridad de los Servidores.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Ejecución de explotación de código (codigo exploits)
- Intento de Denegación de Servicio (DOS) desde la red interna.
- Captura de secuencia de teclas (Keylogging)
- Lectura de tráfico de red para la obtención de usuario y password, lectura de correos, etc.

En este tipo de intrusiones tanto las herramientas, como las diferentes pruebas que se van utilizando y realizando, se van redefiniendo a medida que se ejecutan y se observan los resultados.

La Fig. 1.5 muestra los Tipos de pruebas (Test) basados en tiempo y Costo

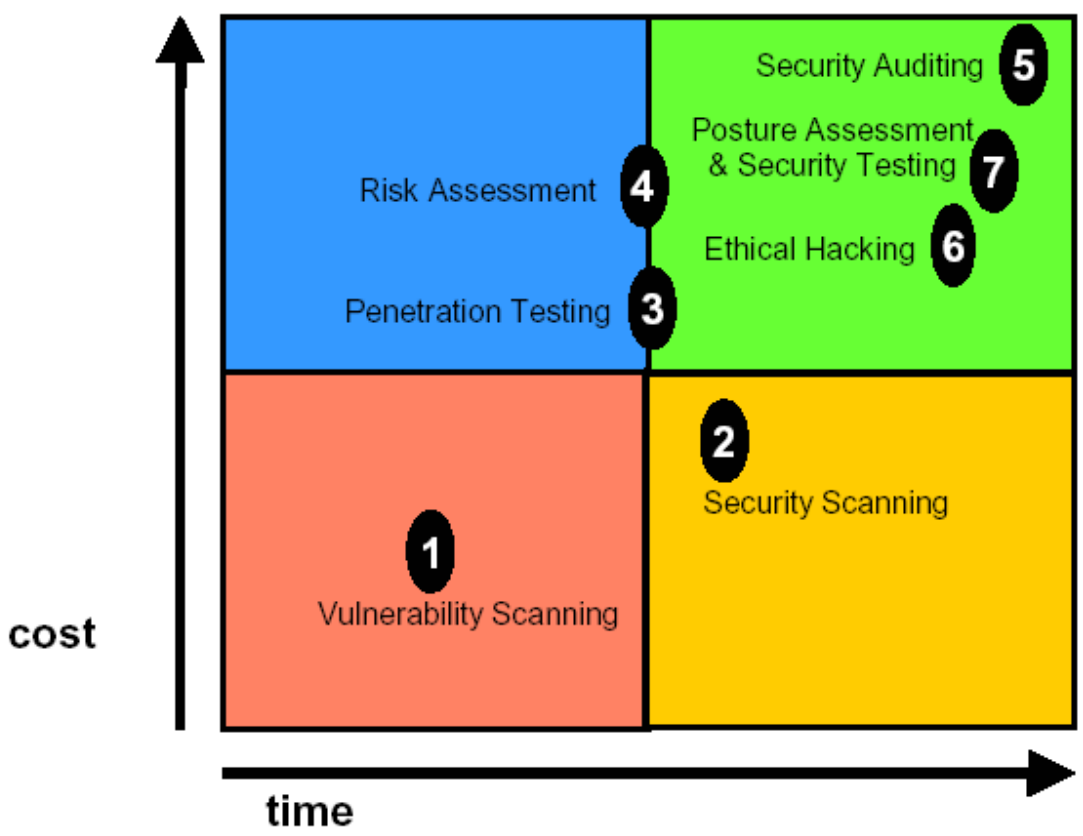



*Fig. 1.5 Tipos de Test*

*Fuente: ISEC - 2004,*

### 1.3.2.4 Etapas de un Penetration Test

El enfoque metodológico de trabajo para un Penetration Test es el siguiente:

1. Reconocimiento Superficial
2. Reconocimiento en Profundidad y Enumeración
3. Definición de las Herramientas a Utilizar
4. Ataque Puro
5. Redefinición de pruebas y herramientas a utilizar en base a resultados obtenidos
6. Borrado de rastro y evidencias
7. Consolidación
8. Documentación formal y desarrollo de Informes Finales (Técnico y Ejecutivo)

### 1.3.2.5 Metodologías Estandarizadas:

**OSSTM (Open Source Security Test Metodology)[20]**

El OSSTMM es un manual de seguridad, en el que participan abiertamente más de 130 profesionales de todo el mundo, y que cumple con los estándares ISO17799 / BS7799 y las normas dictadas por los siguientes organismos:

El OSSTM está alineado con Estándares Internacionales y Leyes Vigentes como: la Agencia de Protección de Datos Personales (APD y su Ley LOPD)- España; USA Government Information Security Reform Act of 2000, section 3534(a)(1)(A) - Estados Unidos; Deutsche Bundesdatenschutzgesetz (BDSG) - Alemania: y, Canada Act Respecting the Protection of Personal Information in the Private Sector (1993) - Canadá:

---

[20] OSSTMM – www.isecom.org

El **OSSTMM** es un conjunto de reglas y directrices para el qué, cómo y el por qué de las pruebas de los eventos. Para que una prueba deba ser considerada dentro del OSSTM debe:

- **Ser cuantificable**
- **Consistente**
- **Válido en el tiempo mas allá del "Ahora"**
- **Cumplir con las leyes individuales y locales y el derecho a la privacidad**

Las pruebas (test) de seguridad realizadas mediante la **OSSTM** no es una imagen instantánea **(snapshot)** del objetivo, sino que sirve como una herramienta de evaluación de la seguridad que **perdura en el tiempo para cuantificar el nivel de riesgo**.

## OSSTMM - Metodología[21]

### 1.- Examinar la red

Es el primer paso a realizar y se determinan los siguientes datos:

- Nombres de dominio
- Nombres de los servidores
- Direcciones IP
- Mapa de la red
- Información sobre el ISP
- Propietarios de los servicios y/o servidores

Para lograr los resultados anteriores también se pueden analizar:

- los enlaces en las páginas web, buscando posibles enlaces internos
- información puesta en grupos de noticias desde la entidad analizada
- los encabezamientos de los correos-e buscando información interna de la entidad

[21] OSSTMM – Metodología desarrollada por Pete Herzog – http://www.ideahamster.org

**2.- Búsqueda de puertos**

En cada máquina pueden estar abiertos 65536 puertos TCP y UDP, pero no todos tienen la misma importancia

En esta búsqueda se debe obtener:

- Puertos abiertos, cerrados y filtrados
- Direcciones IP de los sistemas activos
- Lista de protocolos encapsulados descubiertos
- Protocolos de enrutamiento
- Servicios activos
- Mapa de red

**3.- Identificación de Sistemas Operativos**

En esta fase tratamos de detectar los sistemas operativos que se ejecutan en los diversos servidores encontrados

Como resultado debemos obtener:

- Sistema Operativo
- Versión del SO
- Parches aplicados

**4.- Pruebas de servicios**

En esta fase intentamos determinar que aplicación está detrás de cada puerto abierto

Como resultado debemos obtener:

- Aplicación que se está ejecutando
- Parches de esa aplicación

**5.- Búsqueda automatizada de vulnerabilidades**

En esta fase buscamos huecos y vulnerabilidades en los sistemas.

Debemos hacer pruebas cruzadas con al menos dos herramientas distintas

Como resultado debemos obtener:

- Lista de sistemas vulnerables
- Tipo de aplicación o servicio por vulnerabilidad
- Parches aplicados al sistema

En esta fase se realiza una búsqueda utilizando todos los medios que tengamos a nuestro alcance: sitios Web, IRC, grupos de noticias, etc.

El objetivo es encontrar otras vulnerabilidades en los sistemas y servicios identificados.

**6.- Verificación manual**

En esta etapa se debe validar los resultados y es el momento de eliminar los falsos positivos.

Hay que verificar si en nuestro contrato se encuentra este estudio, pues podemos afectar los sistemas en producción.

**7.- Pruebas de aplicaciones**

En esta etapa se analizan las aplicaciones utilizadas en la entidad u organización.

Como resultado se debe obtener:

- Lista de aplicaciones
- Lista de componentes de estas aplicaciones
- Lista de vulnerabilidades
- Lista de las relaciones de confianza en estas aplicaciones

**8.- Pruebas de cortafuegos**

Las listas de control de acceso (ACL) en los enrutadores y cortafuegos son otro punto importante a medir.

Validar que estas ACL implementan las políticas de la entidad

En esta prueba se debe obtener:

- Información sobre el/los cortafuegos
- Información sobre el/los enrutadores
- Un bosquejo de las políticas representadas por las ACL

**9.- Pruebas de Sistemas de Detección de Intrusos (IDS)**

Esta prueba está orientada a determinar la sensibilidad de los IDS instalados.

Obtener los siguientes datos:

- Tipo de IDS
- Comportamiento del IDS bajo una carga extrema
- Tipos de paquetes descartados por el IDS
- Protocolos descartados por el IDS
- Tiempo de reacción del IDS

- Tipo de alarmas del IDS
- Sensibilidad del IDS
- Reglas del IDS

**10.- Revisión de las políticas de seguridad**

En esta etapa se debe validar que las políticas dictadas por la entidad no están en contradicción con los datos recolectados.

Aquí se pueden analizar los módem internos y máquinas de fax

Se debe obtener:

- Lista de las diferencias entre lo dispuesto y lo real
- Listado de conexiones entrantes no acordes a la política
- Listado de conexiones salientes no acordes a la política

**11.- Análisis de contraseñas**

En esta etapa se intenta encontrar cuentas con claves fáciles.

Debemos obtener como resultado:

- Ficheros de claves resistentes o rotos
- Lista de usuarios con nivel de usuario o administrador
- Lista de sistemas vulnerables por contraseñas
- Lista de documentos con contraseñas débiles
- Lista de sistemas con usuarios cuya clave sea el mismo nombre de usuario

**12.- Pruebas de Denegación de Servicios (DOS)**

En estas pruebas se debe validar el funcionamiento de la entidad cuando uno de sus sistemas cae bajo un ataque de denegación de servicio y cuáles son los puntos más vulnerables.

En esta prueba se obtiene:

- Lista de puntos débiles en el sistema
- Una línea base del funcionamiento del sistema
- Comportamiento de los sistemas bajo carga extrema
- Lista de sistemas vulnerables a DOS

**13.- Revisión de las bitácoras de IDS y servidores de logs**

En algunos casos, el analista no obtiene toda la información necesaria del estudio del IDS.

En esta prueba se obtiene:

- Lista de falsos positivos en el IDS
- Lista de alarmas no registradas por el IDS
- Lista de paquetes que entraron, ordenados por puertos
- Lista de protocolos que se utilizaron en la red
- Lista de caminos no monitoreados en la red

**14.- Ingeniería social**

Como resultado de esta etapa se obtiene información útil para acceder a los sistemas o sobre inseguridades presentes.

Se puede llamar a un administrador y decirle que se ha olvidado la clave o contactar con un usuario y pedirle la clave simulando ser el administrador.

**15.- Pruebas de conexiones inalámbricas**

En esta fase se debe encontrar los puntos de acceso inalámbrico de la red y el alcance de estas entradas.

Se debe validar que las conexiones así establecidas son seguras y no pueden ser trampeadas.

**Consideraciones del Evaluador de Seguridad (Security Tester):**

1. Las soluciones deben ser prácticas y realistas.
2. El test debe ser creativo y metódico.
3. El test necesita estar apropiadamente valorado y los riesgos apropiadamente identificados.
4. El test debe cumplir con varias leyes.
5. El nivel de riesgo que se determine debe poder ser medido y cuantificado
6. El security tester debe transmitir confianza al cliente.
7. Los “Security testers” deberán conocer las herramientas que utilizarán durante el test como así también su procedencia, también se requiere que las mismas sean probadas en ambientes controlados antes de su utilización.
8. No se contemplan los ataques de DOS dentro del test, salvo expreso pedido y autorización del cliente.
9. La ingeniería social solo podrá ser utilizada previa autorización y solo contra empleados de la organización, no podrá incluir a clientes o proveedores de la misma.

10. Si durante el test se descubre una vulnerabilidad de alto riesgo ésta deberá ser comunicada de inmediato al cliente junto con la solución a la misma.

## 1.3.3 EVALUACION DE SEGURIDADES CON COBIT®

Entre los productos que el modelo COBIT presenta encontramos; las “Guías de auditoría”, que contienen la estructura para llevar a cabo el trabajo de campo y la ejecución del procedimiento de auditoría.

### 1.3.3.1 GUÍAS DE AUDITORÍA COBIT:

Las guías de auditoría (Ver Anexo H) son el vínculo entre el modelo de referencia y los objetivos de control de COBIT, son las herramientas que facilitan la verificación de los objetivos de control seleccionados para la evaluación del ambiente de control de IT, no se debe confundir a las Guías de Auditoría como:

- Las herramientas para crear un completo plan de auditoría.
- Las herramientas que enseñen las bases y fundamentos del amplio campo de la auditoría.
- Las herramientas que expliquen con alto nivel de detalle como deben realizar documentar y evaluar planes informáticos organizacionales.
- Las herramientas definitivas en el proceso de auditoría.

Las guías de auditoría permiten al auditor de IT realizar las revisiones específicas de los procesos de tecnología en comparación con los objetivos de control propuestos por COBIT, ayuda a la administración a revisar si los controles establecidos son suficientes o si requieren ser mejorados.

Los modelos más comunes para evaluar los controles son a través de la ejecución de un modelo de auditoría o con la aplicación de un análisis de riesgo.

Las guías de auditoría de COBIT consideran como objetivos de auditoría a los siguientes puntos:

- Proporcionar a la administración información que permita obtener una evaluación razonable de si los objetivos de control están siendo alcanzados.
- Identificar el riesgo resultante de las debilidades de control y recomendar a la administración tomar las acciones correctivas.

La estructura de un proceso normal de auditoría se cubre en las siguientes etapas: Identificación y documentación, Evaluación, Ejecución de Pruebas de cumplimiento, Pruebas sustantivas.

Con esta base los procedimientos de IT pueden ser auditados.

1. Mediante entrevistas a los administradores y al personal apropiado de IT, obtener comprensión de: los requerimientos del negocio relacionándolos con los riesgos asociados, estructura organizacional, roles y responsabilidades, políticas y procedimientos, leyes y regulaciones, controles existentes, reportes de la administración.
2. Evaluación de controles establecidos o existentes, verificando: que los procedimientos se encuentren documentados, que existan entregables adecuados, la definición de responsabilidades y la obligación de dar cuenta se encuentra claramente definida.
3. Evaluando el cumplimiento y probando que los controles trabajen de la manera en la que han sido diseñados
4. Identificar el riesgo asociado a las debilidades de control.

### 1.3.3.2 JUSTIFICACIÓN DE LA UTILIZACIÓN DEL MODELO COBIT®

COBIT (Control Objectives for Information and Related Technology) es el resultado de un proceso de investigación profunda, en el que se incluyen las mejores prácticas, es decir, todo esta basado en prácticas existentes. Por su gran cantidad de contenido COBIT no esta dirigido solo a auditores, si no también a administradores de IT y a la alta gerencia. En la actualidad para las organizaciones es muy importante mantener un adecuado ambiente de control interno, en COSO[22] este ambiente de control se identifica como la base de la pirámide, COBIT que tiene su base en COSO mantiene el mismo concepto pero con un enfoque total hacia IT y a la ventaja que significa para el negocio mantener un adecuado control de IT. Por todo lo expuesto concluimos que COBIT es hacia donde todas las organizaciones, que desean que la tecnología de la información

[22] **COSO:** Informe de Control Interno (COMMITTEE OF SPONSORING ORGANIZATIONS).

sea un valor agregado al negocio, deben enfocar sus planes y objetivos estratégicos.

El uso de las guías de Auditoría de COBIT es de gran ayuda para auditores, en este componente de la familia de COBIT se incluyen todas las actividades que se deben realizar para determinar si un objetivo de control es alcanzado. Para el caso de objetivos de control que no estén siendo alcanzados se determina lineamientos para sustanciar el riesgo que implica el no alcanzar el objetivo de control.

### 1.3.4 METODOLOGÍA PARA EVALUACIÓN DE RIESGO NIST 800-30

La evaluación del riesgo se constituye en el primer paso de toda metodología de administración de riesgo, las organizaciones maduras en procedimientos de control interno la usan para determinar los riesgos y clasificarlos dependiendo de su impacto en la organización. El riesgo viene dado en función de la probabilidad de la ocurrencia de las amenazas las que generan potenciales vulnerabilidades.

Mantener una adecuada administración del riesgo permite minimizar los daños a causa de las amenazas como el acceso, robo, cambios de información por parte de personas no autorizadas las que pueden estar tanto dentro de la organización como fuera. Sin una evaluación de riesgo una empresa no esta en la capacidad de conocer sus vulnerabilidades que generan un impacto negativo en las operaciones diarias.

Para determinar la probabilidad de que se presenten eventos adversos se deben identificar las vulnerabilidades versus la efectividad de controles existentes en los dominios de IT, el impacto va relacionado a la gravedad para la organización en caso de presentarse daños por la ocurrencia de incidentes y problemas sobre las vulnerabilidades.

Esta metodología cubre nueve pasos y son:

1. Caracterización del Sistema
2. Identificación de las Amenazas
3. Identificación de vulnerabilidades

4. Análisis de controles
5. Determinación de la probabilidad
6. Análisis del impacto
7. Determinación del riesgo
8. Recomendaciones de los controles
9. Resultados

Los pasos 8 y 9 de la metodología de la evaluación del riesgo, se cubren con el resultado de la verificación de los controles aplicando las guías de auditoría de COBIT.

Para la determinación del riesgo se propone la tabla 1.1:

| **MATRIZ EVALUACIÓN DE RIESGOS** | | | | | | |
|---|---|---|---|---|---|---|
| **Organización:** | | | | | | |
| **Caracterización del Sistema** | **Identificación de Amenazas** | **Identificación de Vulnerabilidades** | **Controles Existentes** | **Determinación de la Probabilidad** | **Análisis del impacto** | **Determinación del Riesgo** |
| | | | | | | |
| | | | | | | |

*Tabla 1.1 Matriz de Riesgos*
*Fuente: Los Autores*

La Caracterización del Sistema es el primer paso y permite definir el alcance del esfuerzo para la evaluación del riesgo, para el caso de estudio aplicable en este trabajo se establecieron dos de los cuatro dominios de COBIT relacionados con la Seguridad de la infraestructura Tecnológica y son:

- Adquisición e implementación
- Entrega de Servicios y Soporte

Las amenazas son eventos que pueden crear situaciones de incertidumbre que pueden generar un hecho dañino sobre los recursos afectando directamente a sus vulnerabilidades, si una amenaza no afecta a las vulnerabilidades esta no se considera un riesgo.

El tercer paso de la evaluación de riesgos que corresponde a la identificación vulnerabilidades permite generar una lista de defectos y debilidades sobre los objetivos de control del modelo COBIT que puedan ser provocados intencionalmente o accidentalmente.

El objetivo del cuarto paso es identificar los controles existentes definidos por la organización para minimizar o eliminar la probabilidad de la incidencia de una amenaza sobre una vulnerabilidad.

Para determinar la probabilidad latente por la presencia de las amenazas que afectan a las vulnerabilidades se definen tres niveles de posibilidades. ( Tabla 1.2)

| Nivel | Descripción |
|---|---|
| Alta | Existen controles ineficientes para prevenir los efectos de las amenazas altamente motivadas |
| Media | Existen controles que pueden impedir los efectos de amenazas medianamente motivadas |
| Baja | Existen controles totalmente eficientes o no existen amenazas para los recursos |

*Tabla 1.2 Niveles de Vulnerabilidad*

*Fuente: NIST, Risk Management Guide for Information Technology Systems, USA, Julio 2002, Pag. 21*

Como sexto objetivo de esta metodología de evaluación del riesgo se centra en el análisis del impacto el que permite medir el nivel del riesgo que para sistemas de información puede generar pérdida de integridad, pérdida de disponibilidad y pérdida de confidencialidad los que pueden causar desembolsos para reparaciones de equipos, pérdidas de ingresos, para diferenciar el impacto de las amenazas sobre las vulnerabilidades de los activos se las puede clasificar en la Tabla 1.3:

| Nivel | Descripción |
|---|---|
| Alta | ▪ Cuando los daños generan grandes pérdidas económicas sobre los activos o recursos.<br>▪ Cuando los daños impiden a la organización cumplir sus objetivos.<br>▪ Cuando los daños pueden generar muertes de personas. |
| Media | ▪ Cuando los daños generan pérdidas económicas recuperables sobre los activos o recursos.<br>▪ Cuando los daños aplazan las metas de la organización.<br>▪ Cuando los daños pueden generar heridas a personas. |
| Baja | ▪ Cuando los daños generan pérdidas económicas casi imperceptibles sobre los activos o recursos.<br>▪ Cuando los daños no afectan a las metas de la organización. |

*Tabla 1.3 Niveles de Impacto de las amenazas*

*Fuente: NIST, Risk Management Guide for Information Technology Systems, USA, Julio 2002, Pag. 23*

Una vez identificadas las amenazas y vulnerabilidades ya se puede sustanciar el riesgo mediante una multiplicación simple entre la probabilidad de la ocurrencia de las amenazas y el impacto que estas pueden generar sobre los activos de la empresa, la NIST 800-30 propone la siguiente matriz de 3x3. (Ver Tabla 1.4).

| **Probabilidad** | **Impacto** | | |
|---|---|---|---|
| | Baja (10) | Media (50) | Alta (100) |
| Alta (1.0) | 10 | 50 | 100 |
| Media (0.5) | 5 | 25 | 50 |
| Baja (0.1) | 1 | 5 | 10 |

*Tabla 1.4 Matriz para la determinación del riesgo*
*Fuente: NIST, Risk Management Guide for Information Technology Systems, USA, Julio 2002, Pag. 25*

Alta (Entre 50 y 100; 50 no incluido),

Media (Entre 10 y 50; 10 no incluido),

Baja (Entre 1 y 10).

# 1.4 FUNDAMENTOS DE ISP´S Y SERVICIOS

## 1.4.1 EL PROVEEDOR DE SERVICIOS DE INTERNET

Antes de profundizar en el Proveedor de Servicios de Internet, es necesario determinar que papel juega con los demás participantes en la estructura de las telecomunicaciones, cómo está organizada la red Internet, qué organismos o autoridades la rigen y cómo se ve afectado por ellos.

### 1.4.1.1 Participantes de la Red Internet

Los participantes de la red Internet pueden clasificarse en varios grupos principales:

- Proveedores de Transporte de Telecomunicaciones (Telecomunications Carriers),

- Proveedores de Troncales Mayores de Internet (Network Service Providers),
- Proveedores de Enlaces Locales (Local Exchange Carriers),
- Proveedores de Servicios de Internet (Internet Service Providers),
- Servicios en-Línea (On - line Services),
- Proveedores de Contenido (Content Providers),
- Integradores de Sistemas,
- Diseñadores de Web,
- Consumidores finales.

#### 1.4.1.2 Proveedores de Transporte de Telecomunicaciones

Los Proveedores de Transporte de Telecomunicaciones (Telecommunications Carriers - TELCOs) operan la infraestructura de larga distancia que transporta transmisiones de voz y datos, tales como puntos de interconexión, líneas físicas de larga distancia, y enlaces de radiofrecuencia, como los son microondas de punto-a-punto, enlaces de Fibra Optica y transmisión satelital. En los EE.UU. se encuentran entre los TELCOs, las compañías AT&T, MCI, Sprint, Worldcom, GTE, Level 3 y un centenar de empresas de menor escala dedicadas a este servicio. Así mismo se encuentra en este género los operadores de sistemas satelitales y cable submarino.

#### 1.4.1.3 Proveedores de Troncales Mayores de Internet

Los Proveedores de Troncales Mayores de Internet (Network Service Providers - NSPs o también llamados Backbone Providers), proveen infraestructura de redes de datos, que transporta e intercambia tráfico de Internet en múltiples puntos de interconexión con otros proveedores similares. Es común entre los TELCOs y los utilizan para la transmisión de tráfico de Internet.

#### 1.4.1.4 Proveedores de Enlaces Locales

Los Proveedores de Enlaces Locales (Local Exchange Carriers - LECs) operan la infraestructura de acceso metropolitano y de última milla local entre la entidad comercial o usuario final y la red Internet. Hasta hace unos cuantos años, y después de la ruptura de AT&T en EE.UU. este papel era exclusivo de las compañías locales telefónicas llamadas "Bebés Bell" o formalmente Regional Bell Operating Companies (RBOCs). En otros países sigue siendo los PTTs mismos que actúan en este papel. Recientemente diversas entidades han instalado o adaptado infraestructura local alámbrica, de fibra óptica, y de radiofrecuencia para interconectar en un área metropolitana diferentes entidades comerciales. Entre ellas se encuentran compañías de televisión por cable, proveedores de energía eléctrica, operadoras de telefonía celular, y una gama de compañías de comunicaciones. Así alcanzan al consumidor residencial quien tiene necesidad de interconectarse con la red Internet y con otras aplicaciones de voz y datos digitales (Competitve Local Exchange Carriers - CLECs). En el Ecuador los Proveedores de Enlaces Locales son Andinadatos (redes con tecnología ATM y TDM), Suratel que es una empresa privada de enlaces dedicados por medio de un Back-Bone local de Fibra Optica, con la que pueden entregar circuitos con TDM, Frame-Relay y también con tecnologías de Cable MODEM, Pacifictel, TelcoCarrier, Impsat, Megadatos, Teleholding con pequeños anillos de Fibra y última de cobre, Ecutel y Puntonet con redes de acceso inalámbrico y las otras compañías que todavía no se encuentran operando ni reportadas en la SENATEL.

### 1.4.2 TOPOLOGIA DE INTERNET

La topología de la red Internet no es planeada ni tiene una forma predeterminada. Básicamente la red original NSFNET consistía en segmentos alámbricos que interconectaban a los NAPs (Network Access Point) originales, San Francisco, California, Chicago, Illinois, y Pennsauken, New Jersey. Estos NAPs a la vez interconectaban a las principales universidades. Más tarde se le añadieron las NAPs federales FIX-EAST y FIX WEST interconectando las agencias federales. Más tarde ya en forma comercial, se formaron los NAPs no oficiales como MAE-

EAST, MAE-WEST y los IXs, que proveen puntos de interconexión y agregación adicionales. La interconexión de tráfico se realiza por medio de redes privadas. La "telaraña" que forma el Internet entonces está compuesta de los NAPs, los MAEs, los IX, y las líneas troncales que los unen en forma redundante. Así mismo a cada NAP está interconectado un NSP, que a su vez es un proveedor de varios ISPs, y estos a su vez pueden alimentar a otros ISPs de menor tamaño, hasta llegar al usuario final. Para complicar aún más la tecnología, un ISP o un usuario final corporativo puede tener acceso a más de un ISP o NSP de más alto nivel. Por esta razón la topología de la red Internet es ilustrada como una nube sin forma específica, donde una entrada a la nube puede ser un acceso a cualquier nivel, ISP, NSP, IX, MAE, o NAP.

Debido a que el Internet no es planeado o coordinado centralmente, el encaminamiento de tráfico debe de realizarse en cada empalme de rutas. Para esto se requiere un equipo, llamado router. Un router con capacidad de encaminar entre dos o más redes se le llama "router de frontera" (Border Router). Los routers internos a un NSP se les llama "routers de núcleo" (Core Routers). Los routers de frontera requieren conocer gran parte de todas las rutas posibles que existen en el Internet. Hoy en día el número de rutas es directamente proporcional al número de redes definidas en forma de bloques de direcciones de Internet. Originalmente existían varias clases de direcciones, entre ellas las llamadas Clase A ( 127 redes de 16 millones de direcciones cada una), Clase B ( 16 mil redes de 65 mil direcciones cada una), y Clase C (2 millones de redes de 254 direcciones cada una).

La Fig. 1.6 muestra el Diagrama Jerárquico de Acceso a Internet.

**DIAGRAMA JERARQUICO DE ACCESO A INTERNET**

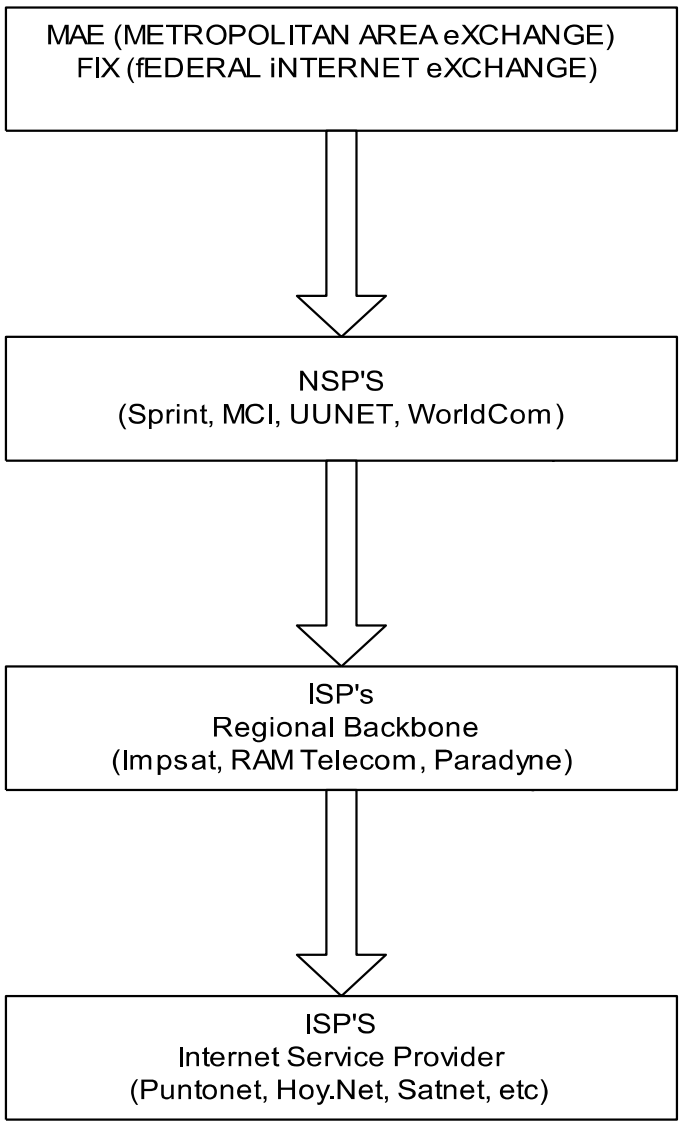



*Fig. 1.6 Diagrama Jerárquico de Acceso a Internet*
*Fuente: LACNIC www.lacnic.net*

### 1.4.2.1 Suministro y Asignación de Direcciones de Internet

Inicialmente el suministro de direcciones de Internet se realizó de una manera liberal justificada únicamente por el número de nodos planeados para una red. Tras el reto de una demanda cada vez mayor de direcciones y la explosión exponencial en el número de rutas (que impone requerimientos técnicos en los mismos routers), la diferencia entre clases de direcciones tipo A, B y C, fue eliminada con lo que se conoce como encaminamiento tipo CDIR (Classless Inter-Domain Routing).

El objetivo de CIDR es agregar múltiples rutas en una sola serie contigua, requiriendo una sola ruta. Para garantizar ruteo en toda la nube Internet, un bloque debe ser contiguo y asignado en forma jerárquica. Bajo el concepto de CIDR, las direcciones se asignan directamente por el InterNIC y LACNIC (exclusivo para Latinoamérica), a NSPs y ISPs que cumplen rigurosas condiciones, entre ellas que tengan acceso a NAPs o que tengan múltiples

accesos a la nube de Internet (multihomed). Para aquellos ISPs que no califican, deben forzosamente obtener sus direcciones y aquellas para sus clientes, directamente de su proveedor cuesta-arriba. Los bloques CDIR obtenidos del InterNIC-LACNIC son por lo general transportables, y aquellos suministrados por los ISPs de más alto nivel a sus clientes no lo son. El resultado es que si un ISP en particular, que no califique a obtener su propio bloque CDIR transportable del InterNIC, deseara cambiar de proveedor cuesta-arriba, requeriría renumerar su red y la de sus clientes, con considerable molestia y costo para todos los afectados.

Actualmente existen tecnologías como la traducción de direcciones dinámicas (Network Address Translation - NAT) que permiten utilizar bloques de direcciones no oficiales dentro de redes privadas (stub-networks), y mediante su implementación en routers y otros productos de software (Proxy Servers, IP Gateways, Firewalls) pueden ocultar las direcciones internas, minimizando el número de direcciones a renumerar. Sin embargo existe un costo de eficiencia por la utilización de NAT e incompatibilidad con ciertos protocolos presentes y en desarrollo. Por otro lado existen ventajas de seguridad del NAT ya que se oculta la topología de una red interna al exterior.

### 1.4.3 SERVICIOS EN LINEA

Un desarrollo que precede al Internet comercial, es el servicio en-línea (On-line Services). Su labor masiva de reclutamiento y enseñanza de usuarios ha contribuido a la expansión del Internet. A medida que las necesidades de acceso y nivel de sofisticación técnica de sus suscriptores han avanzado, una porción de éstos a emigrado hacia ISPs en busca de un menor costo de acceso o mejor desempeño.

#### 1.4.3.1 El Proveedor de Internet (Internet Service Provider - ISP)

Que es su denominación más común, pero en ocasiones también conocido como Proveedores de Acceso de Internet (Internet Access Providers), engloban a todos

aquellos que añaden a un producto o un servicio relacionado al acceso de Internet al consumidor, ya sea corporativo o residencial. El ISP provee puertos de acceso de Internet y otros servicios que apalancan su oferta, tales como hospedaje de contenido en servidores de alto desempeño, almacenamiento y direccionamiento de correo electrónico, servicios de configuración de equipo e instalación de programas, capacitación y apoyo técnico al usuario final. El papel de los ISPs es muy importante ya que gracias a ellos se ha alcanzado un nivel de penetración mucho mayor y más acelerado que el de los servicios en línea o el de los grandes operadores. Esto se debe a que este papel posee una cobertura muy amplia y abarca diversos mercados geográficos, y su rodaje paralelo, competitivo y de crecimiento acelerado, ha podido ofrecer sus servicios a los más diversos usuarios finales, con una atención al cliente personalizada.

El ISP como negocio ha sido motivo de gran propaganda ya que ha demostrado, que es posible tener un mercado competitivo servido por un gran número de jugadores, algunos de ellos de cobertura nacional, otros regionales, otros locales, cada tipo con diferente enfoque, fortalezas y debilidades. Existen diferentes fases en la vida del producto, desde su creación, crecimiento, madurez y decadencia. El mercado de Internet y sus productos son muy jóvenes y están en plena madurez. Sin embargo, como en otros mercados, siempre existen etapas de consolidación, y durante estas etapas, es común que los márgenes disminuyan, y haya gran competencia por un mercado de menor crecimiento o decreciente. El mercado de Internet para ISPs ha mostrado una gran capacidad de re-inventarse, como mercado corporativo, como mercado residencial, como mercado de entretenimiento, como reemplazo de otras tecnologías, etc.

### 1.4.3.2 Proveedores de Contenido

Dentro de los Proveedores de Contenido (Content Providers) se incluyen todos aquellos que crean, compilan y ensamblan contenido que se transmite a través de la red. Aunque en un inicio el material era principalmente de investigación y didáctico, hoy en día un gran número de participantes de Internet contribuye en todos los temas, de difusión pública y comercial. Más aún el Internet se está

convirtiendo en el medio preferido para difundir e intercambiar contenido en todos los géneros y en múltiples formatos de medios (texto, gráficos, sonido, video, realidad virtual, etc.), entre una multitud cada día mayor de participantes de la comunidad Internet al nivel mundial. Más recientemente vemos a editores, cadenas televisivas, y todo género de proveedores de contenido de otros medios, abordando el medio del Internet en forma estratégica en una carrera por atraer a la mayor audiencia posible.

### 1.4.3.3 Integradores de Sistemas

Dentro de este grupo se incluyen las firmas especializadas en la integración de sistemas de información, infraestructura de telecomunicaciones y de cómputo, necesarias para implantar las soluciones de acceso a Internet y de uso interno de las empresas. Incluimos también a aquellas firmas que ofrecen servicios de programación de software, asesoría y desarrollo de aplicaciones de proyecto específicos. Así mismo se encuentran aquellos que ofrecen entrenamiento técnico en las diferentes tecnologías, algunas veces como parte integral de su oferta. El integrador de sistemas usualmente ofrece sus servicios a los otros participantes de la red Internet, cuando carecen de la especialidad y conocimiento técnico suficiente. El integrador de sistemas por lo general mantiene estrechas relaciones con los fabricantes de hardware y software, algunas veces como distribuidor o revendedor de valor agregado. El ISP intenta mantener personal técnico especializado en los equipos más utilizados, sin embargo, con la proliferación de tecnologías es imposible mantener una cobertura amplia y el nivel de detalle necesario sobre las tecnologías Internet en la forma de Intranets y Extranets.

### 1.4.3.4 Diseñadores de Web

A pesar de que el diseño de páginas de Web está cada vez más al alcance del usuario final, de los Integradores de Sistemas, de los ISPs, de los Proveedores de Contenido, etc. Existe una gran diferencia entre el diseñador amateur y el artista especializado en el medio Web. Por lo general firmas o individuos con

capacidades existentes en diseño gráfico, producción y post-producción en otros medios como los son TV, video, gráficos impresos, etc., desarrollan el conocimiento suficiente y la especialización necesaria de este nuevo medio. Los diseñadores de Web crean así su propio nicho que complementa la oferta y las soluciones de los demás participantes. Es también común que los ISP y Proveedores de Contenido mantengan internamente departamentos en este género. Sin embargo siempre se beneficiarán de utilizar los servicios de las firmas especializadas, en las ocasiones que lo ameriten.

#### 1.4.3.5 Consumidores Finales

Empresas del sector público o privado, entidades gubernamentales, organizaciones sin fines de lucro, y en general cualquier individuo, forman la base de Consumidores Finales. Ejemplos de consumidores finales son: un individuo cualquiera averiguando las noticias de último momento, el clima y la situación del mercado bursátil. Un miembro de un equipo de trabajo participando en una discusión de un proyecto con otros miembros en varias ciudades del mundo, revisando las opiniones y comentarios de sus contrapartes, y añadiendo su contribución a los temas en común. En forma más sofisticada, un profesional respondiendo, en forma interactiva y mediante una interface audiovisual, una inquietud de un asociado o cliente.

### 1.4.4 PRINCIPALES SERVICIOS DE LA RED INTERNET

Los principales servicios disponibles de la red Internet incluyen un gran repertorio de recursos de comunicación e intercambio de objetos en múltiples medios (multimedios) como lo son todos aquellos compuestos de texto, gráficos, audio, video y programas de software. El éxito de la red Internet radica en la facilidad de ofrecer sus recursos y capacidades a un número cada vez mayor de usuarios, en una forma transparente de su localización geográfica, y de una manera cada vez más amigable, y al alcance de un mayor número de usuarios. La red Internet a menudo se encuentra rodeada de términos técnicos y configuraciones complejas necesarias para enlazar las PCs a la red. Esta complejidad es una

barrera temporal de utilización que está siendo simplificada a gran velocidad, gracias a los avances de nuevos programas de software y de nuevos equipos de hardware que son cada vez más baratos y más poderosos. A continuación se presenta el método universal de direccionamiento de las numerosas computadoras de Internet y los servicios más populares de esta red.

### 1.4.4.1 Direccionamiento en la Red Internet

Los recursos en el Internet se basan en el direccionamiento de las diversas computadoras entrelazadas en la red. El método de direccionamiento requiere de la individualidad de la dirección, igual que en el sistema telefónico. En su forma más fundamental, la dirección de Internet es un agregado numérico compuesto de cuatro cifras separadas por puntos. Por ejemplo 10.12.15.20. Cada cifra puede tener un valor entre 1 y 254 (el 0 y el 255 están reservados para direcciones de difusión). Este agregado de cifras presenta el mismo reto a la memoria humana que el sistema numérico telefónico. Pero a diferencia de su contraparte, la numeración de las direcciones de Internet no está organizada por país, región, ciudad o zona, sino que su asignación es organizacional. Aunque inicialmente el direccionamiento fue numérico, el Internet Assigned Numbers Authority (IANA) implantó el sistema de nombres de dominio (Domain Name System – DNS), el cual permite utilizar direcciones compuestas de términos alfanuméricos fácil de recordar. El sistema DNS traduce un nombre de dominio alfanumérico al equivalente numérico. Los nombres de dominio están compuestos por una serie de nombres separados por puntos. Por ejemplo: “pc1.puntonet.ec”. Esta representación es jerárquica, y empieza por un nombre de computadora, seguido por un nombre de dominio, el cual está compuesto de un nombre de organización, o término arbitrario, y un dominio de alto nivel (Top Level Domain-TLD) predefinido. Los TLDs están asociados con un país (“us” para EE.UU, “ec” para Ecuador, etc.) o un tipo de organización (“com” para el sector privado, “gov” para instituciones de gobierno, “org” para organismos sin fines de lucro, “mil” para la milicia, “net” para entidades de infraestructura de la red, etc.).

### 1.4.4.2 World Wide Web

La “telaraña global” o World Wide Web o (WWW) es el más popular de todos los servicios de Internet, ha integrado gran parte de los servicios originales. El WWW enlaza documentos de multimedia llamados páginas Web (Web pages) de una manera flexible y bajo control del autor de cada página. En contraste con un documento tradicional (en papel o electrónico) donde las páginas son secuenciales y localizadas en un mismo lugar (el libro o archivo mismo), las páginas Web se pueden encontrar hospedadas físicamente en diferentes computadoras alrededor del mundo en los llamados sitios de Web (Web sites).

El protocolo de transmisión de páginas Web, HTTP (Hyper Text Transmition Protocol) permite que diversos servidores alrededor del mundo, creados por diferentes fabricantes de hardware y software, puedan establecer enlaces (links) en común y responder a peticiones de diversos Visualizadores de Web. A diferencia de los documentos tradicionales, los documentos HTML (Hyper Text Mark-up Languaje) son multi-dimensionales – hypertextos – cuyas páginas entrelazadas se encuentran distribuidas en múltiples lugares del mundo. Adicionalmente el HTML permite extender la presentación más allá del texto y gráficos, añadiendo programas, video y audio.

### 1.4.4.3 Correo Electrónico

Este servicio es el más común y con mayor penetración de mercado. El correo electrónico está basado en el protocolo llamado SMTP (Simple Mail Transport Protocol). El direccionamiento del correo está basado en un nombre de usuario y en un nombre único de destino.

El correo electrónico es uno de los principales incentivos de conectarse al Internet. Mientras que el sistema postal tradicional fue apropiado en muchos casos, el correo electrónico reduce el tiempo de entrega de días a segundos. Inicialmente el correo electrónico se presentó como una forma informal de

comunicación, actualmente se ha convertido en un vehículo formal de negocios. Su bajo costo lo hace ideal para transmitir en forma de difusión (broadcast). Nuevo software se ha desarrollado que permite procesar el correo de manera automática y clasificarlo dependiendo de su origen y otras características. La comunicación con clientes, proveedores y demás asociados de negocios es fundamental. Hoy en día es común pedir la dirección electrónica de correo tal como lo fue en la década de los ochenta pedir el número de facsímil.

#### 1.4.4.4 Transferencia de Archivos y Programas

Desde los inicios del Internet, la transmisión de archivos y programas ha sido uno de los servicios más importantes de la red. El protocolo FTP (File Transfer Protocol) permite la transmisión confiable (sin errores) de diversos archivos y programas. Los detalles de interconexión y las eventualidades de la red que pueden causar errores en las transmisiones, son automáticamente corregidas. Esta corrección es posible ya que los archivos son transmitidos en pequeños fragmentos o paquetes, de tal manera que cada uno de ellos es direccionado individualmente. Aunque los paquetes transmitidos pueden llegar a su destino en forma desordenada, incompleta o inclusive perderse en tránsito, estos son retransmitidos si es necesario y re-ensamblados en el orden correcto, asegurando así la integridad del archivo o programa original.

#### 1.4.4.5 VoIP

Uno de los servicios de mayor crecimiento en el mercado de Internet es la transmisión de voz sobre la red IP, ya sea que las regulaciones de telecomunicaciones de cada uno de los países lo permite o no, este servicio tiende a ser uno de los de mayor aceptación a nivel corporativo o personal, debido a que los costos por llamadas son increíblemente bajos en comparación con los valores que actualmente usan los Proveedores de Transporte de Telecomunicaciones. A nivel local, este servicio es el que ha masificado el crecimiento del mercado de Cyber Cafés, ya que con valores de hasta un 200% más bajo que los de las operadoras locales, los usuarios prefieren perder calidad

por reducción de precio, sin embargo los permisos o concesiones que se han dado en nuestro país han permitido que empresas privadas entren a competir en este mercado con las PTTs estatales tradicionales.

#### 1.4.4.6 Video Conferencia

Con la implementación de servicios de Banda Ancha, se dio oportunidad al surgimiento de nuevas tecnologías y aplicaciones en línea, es así que servicios como los de Video Conferencia están siendo usados con gran demanda actualmente, ya que los riesgos y los costos que implican los viajes de ejecutivos se ven reducidos en un gran porcentaje, otro mercado que ha explotado este servicio es la educación y la telemedicina, que permite capacitación e incluso operaciones y diagnósticos que se realizan de forma remota.

## 1.5 SEGURIDAD EN INTERNET

Las organizaciones, para utilizar los servicios de Internet internamente y relacionarse con el exterior deben tomar medidas que permitan garantizar la confidencialidad, la integridad y la disponibilidad de la información. Para ello deben identificar las amenazas a las que se encuentran expuestos los citados servicios, cuáles son los requerimientos de proveedores, organizaciones y usuarios finales, identificar los servicios de seguridad que dan respuesta a las amenazas identificadas, las técnicas o mecanismos de seguridad necesarios para implementar los servicios de seguridad identificados y finalmente los productos que mediante la implementación de las técnicas de seguridad proporcionan los citados servicios.

Cuando hablamos de seguridad en una red, debemos determinar los elementos que están siendo parte de una red, y existen dos elementos de seguridad bien definidos:

**Seguridad en los servicios.-** Se refiere, a la seguridad que debemos implementar, en las diferentes capas que permiten que un servicio de aplicación este disponible en un servidor (hardware), los mismos que son:

- Sistema Operativo.
- Base de Datos.
- Aplicación.

**Seguridad en la comunicación.-** Involucra que toda la información que sale a través de una red, desde una computadora personal hacia otra, tenga las seguridades del caso.

El análisis que se realiza sobre amenazas, servicios de seguridad, técnicas de seguridad y productos es válido para los servicios de Internet. Se presta en algunos puntos especial atención a estos últimos por presentar mayores debilidades en el ámbito de la seguridad. Ver el Esquema de Seguridad Base en la Fig. 1.7.

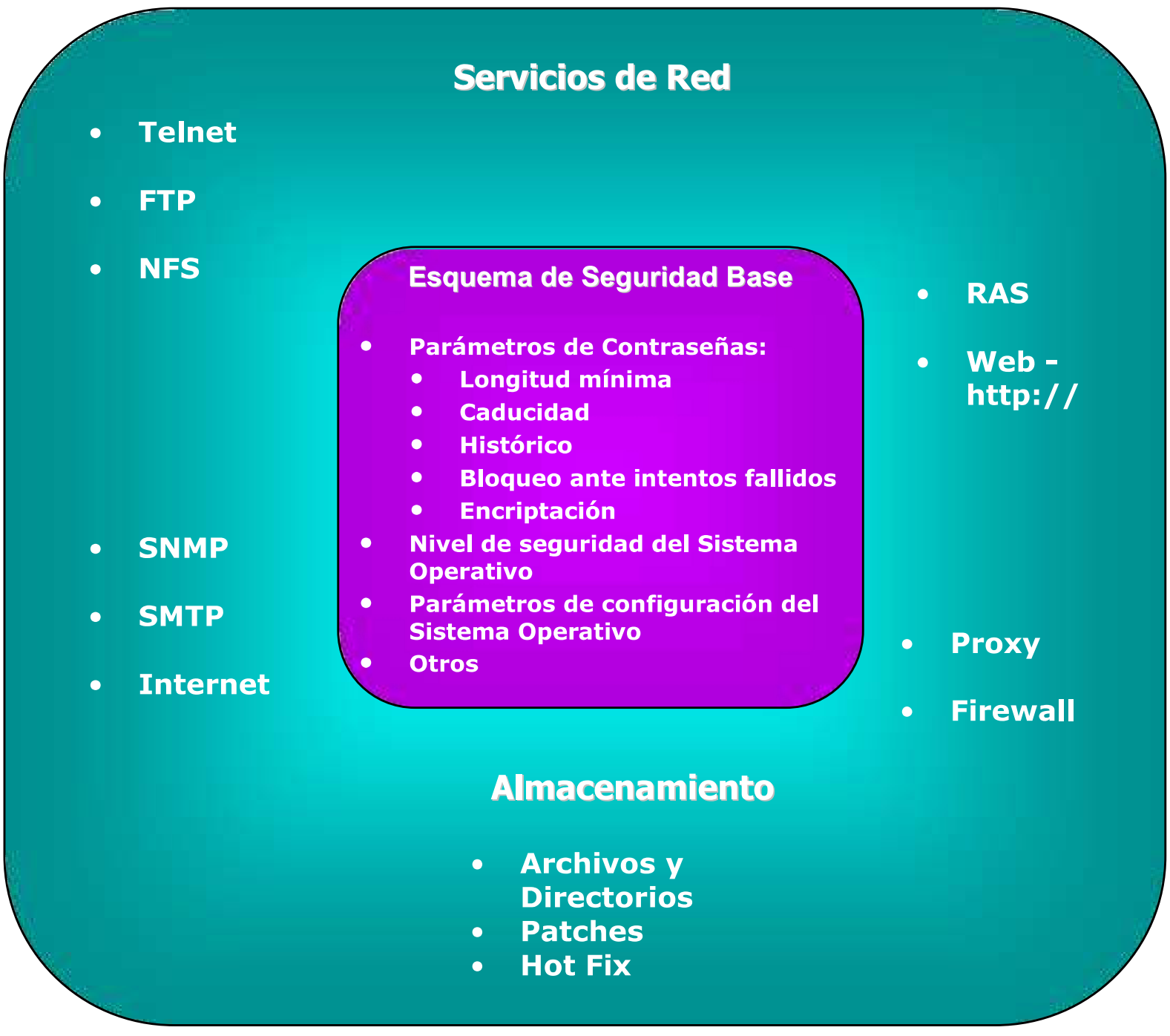



*Fig. 1.7 Esquema de Seguridad Base*

### 1.5.1 IDENTIFICACION Y DESCRIPCIÓN DE ATAQUES, VULNERABILIDADES Y AMENAZAS

#### 1.5.1.1 Definiciones y Términos

**Amenaza**. "Probabilidad de que un fenómeno, de origen natural o humano, se produzca en un determinado tiempo y espacio. Peligro potencial de que las vidas o bienes materiales humanos sufran un perjuicio o daño".[23]

**Amenazas naturales.** Eventos causados por la naturaleza que tiene el potencial para impactar una organización.

**Análisis de Riesgo.** "El análisis de riesgo involucra identificar las amenazas más probables y analizar las vulnerabilidades relacionadas con las amenazas en la organización". [24]

Para realizar el análisis del riesgo es necesario identificar: recursos, amenazas y las vulnerabilidades en el entorno informático del Área IT.

Para tratar de minimizar los efectos de un problema de seguridad, se realiza el análisis de riesgo, término utilizado para responder tres preguntas básicas sobre la seguridad de la organización.

- ¿Qué está bajo riesgo?
- ¿Cómo se puede producir?
- ¿Cuál es la probabilidad de que suceda?

**¿Qué está bajo riesgo?** Determinar todos los componentes del sistema susceptibles a ser dañados. Por ejemplo: pérdida de conexión, datos, etc.

---

[23] www.crid.or.cr, Material de capacitación conceptos básicos, http://www.crid.or.cr/crid/esp/conceptos_basicos.html
[24] www.drj.com, Risk analysis techniques, http://www.drj.com/new2dr/w3_030.htm

**¿Cómo se puede producir?** Los desastres más comunes son los desastres naturales, humanos o ambientales tales como: terremotos, inundaciones, incendios, sabotaje, etc.

**¿Cuál es la probabilidad de que suceda?** Es necesario seleccionar los tipos de desastres contra los que se intentará proteger al sistema, estos desastres serán los que posean la mayor probabilidad de afectar la continuidad del negocio.

En la práctica existen dos métodos para responder a estas preguntas: el método cuantitativo y el cualitativo.

El método cuantitativo, en base a la valoración cuantitativa es el menos usado en el análisis de riesgo, debido a que implica cálculos complejos o datos difíciles de estimar.

El método cualitativo es mucho más sencillo e intuitivo, porque no se utilizan probabilidades exactas sino simplemente una estimación de pérdidas potenciales.

**Evaluación de riesgos.** Lista de riesgos ordenados por su impacto y su probabilidad de ocurrencia.

**Identificación de las amenazas.** El proceso de identificar situaciones o condiciones que tiene el potencial de causar lesiones a personas, daños a la propiedad, o daños al ambiente.

**Riesgo.** Probabilidad de daños, sociales, ambientales y económicos en un lugar dado y durante un tiempo de exposición determinada.

**Vulnerabilidad.** Es la debilidad en el plan o aplicación del control dentro de un proceso, función, o facilidad que pueden promover o pueden contribuir a una ruptura.

### 1.5.1.2 Clases de amenazas:

Las amenazas pueden ser accidentales o intencionadas.

***ACCIDENTALES.-*** No son premeditadas y en ellas podemos incluir los posibles fallos del hardware y software de nuestra instalación.

***INTENCIONADAS.-*** Por medio de algo o de alguien se produce un ataque a nuestra información para fines distintos de los que fueron creados.

Nos centraremos por razones obvias en las amenazas intencionadas a las que pueden estar expuestos los servicios de la Internet. Ver Tabla 1.5:

| ***Amenaza*** |
|---|
| Divulgación no autorizada de la información |
| Modificación no autorizada de la información |
| Enmascaramiento |
| Repudio del mensaje, del origen o del acuse de recibo |
| Acceso no autorizado a recursos |
| Denegación de servicio |

*Tabla 1.5 Amenazas en los servicios de la Internet*

*Elaborado por: Los Autores*

### 1.5.1.3 Ataques a la Información

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas se puede utilizar para la defensa, ya que es tan importante conocer los diferentes tipos de ataques así como las soluciones para prevenir, detectar y reparar un siniestro de este tipo.

EAVESDROPPING Y PACKET SNIFFING: En Internet esto es realizado por analizadores de paquetes (packet sniffers), que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

SNOOPING Y DOWNLOADING: Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

TAMPERING O DATA DIDDLING: Se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos.

SPOOFING: Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

JAMMING o FLOODING: Este tipo de ataques saturan y desactivan los recursos del sistema. Un atacante puede consumir toda la memoria o espacio en disco disponible.

CABALLOS DE TROYA: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones no autorizadas y que la persona que lo ejecuta no conoce.

BOMBAS LOGICAS: Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un

programa o rutina que en una fecha determinada destruirá, modificará la información o provocará la caída del sistema.

DIFUSION DE VIRUS: Si bien es un ataque de tipo “tampering”, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no está instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

SPAMMING, JUNK MAIL: Se denomina junk mail o garbage mail, al correo basura, que por lo general no tiene carácter comercial, pero si es una "baratija" (la traducción literal de junk es baratija), es decir son mensajes que llenan el buzón.

EXPLOTACIÓN DE ERRORES DE DISEÑO, IMPLEMENTACIÓN U OPERACIÓN: Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje.

### 1.5.2 SERVICIOS DE SEGURIDAD

#### 1.5.2.1 Requerimientos de servicios seguridad

Los servicios de seguridad que implementados van a permitir contrarrestar las amenazas previamente identificadas, son los siguientes:

*a) Confidencialidad de datos.*
*b) Integridad del mensaje y del contenido.*
*c) Autenticación de entidades, firma digital.*
*d) No repudio - acuse de recibo.*
*e) Control de acceso*

En la tabla 1.6 siguiente se relacionan las amenazas y los servicios de seguridad.

| ***Amenaza*** | ***Servicio de Seguridad*** |
|---|---|
| Divulgación no autorizada de la información | *Confidencialidad de datos* |
| Modificación no autorizada de la información | *Integridad del mensaje y del contenido* |
| Enmascaramiento | *Autenticación de entidades* |
| Repudio del mensaje de origen o del acuse de recibo | *No repudio* |
| Acceso no autorizado a recursos | *Control de acceso* |
| Denegación de servicio | *Control de acceso* |

*Tabla 1.6 Amenazas y servicios de seguridad*

*Elaborado por: Los Autores*

***a) CONFIDENCIALIDAD DE LOS DATOS***

Su propósito es impedir que alguien, que no sea el receptor, pueda leer el contenido de un mensaje y, por lo tanto, tener la disponibilidad de divulgarlo. Hablando de un sistema de transmisión de mensajes, se trata de impedir que la información transmitida sea interceptada (leída) por persona no autorizada, y por lo tanto conocer su contenido. Se trata en definitiva de garantizar que la información sólo pueda ser leída por el usuario o usuarios a quienes va dirigida. La confidencialidad por tanto, se puede aplicar en:

- Información del destinatario.
- Texto completo.
- Parte del texto.

La técnica más moderna existente hoy en día que se puede aplicar como una solución muy eficaz, es la **CRIPTOGRAFÍA**, que mediante algoritmos matemáticos y aplicación de claves o contraseñas, y utilizando medios de software o hardware, permite transformar el contenido del texto en un conjunto de caracteres no entendibles. La seguridad se tiene en que se requiere el conocimiento y acuerdo mutuo entre el receptor del mensaje y el emisor, de las

claves y utilizar el mismo medio software o hardware para poder cifrar y descifrar el mensaje. Se puede decir entonces que se ha establecido una comunicación segura.

***b) INTEGRIDAD DEL MENSAJE Y DEL CONTENIDO***

Se garantizará a la entidad receptora que el mensaje o información que está recibiendo es exactamente el mismo que le envió la entidad origen. Al mismo tiempo, el receptor tendrá la seguridad de que no ha habido, sobre la información original emitida, ninguna modificación, ni pérdida, ni contenido adicional antes de su recepción.

Para poder lograrlo, nos basamos igualmente en la tecnología de la **CRIPTOGRAFÍA**, pero pudiendo usar esta vez la clave pública y/o la clave privada. Con la utilización de la clave pública, basta que emisor y receptor la conozcan. Si utilizamos ambas, la clave pública y privada, deberá existir algún mecanismo adicional que permita a la entidad origen transferir la clave secreta al receptor. Ver Fig. 1.8:

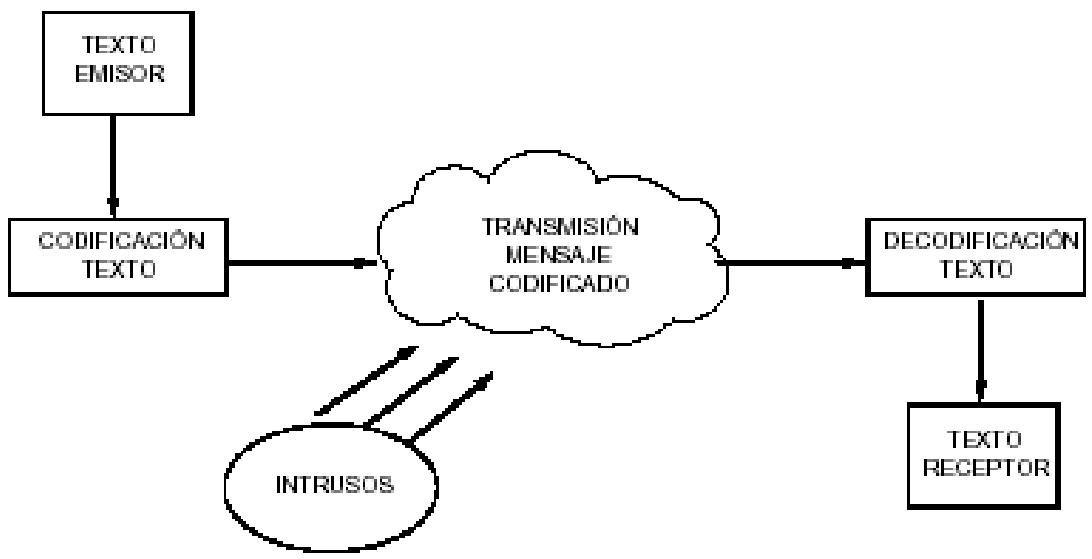



*Fig. 1.8 Integración del mensaje del contenido*

Podemos decir que aparte de una comunicación segura, hemos logrado que no haya manipulación del texto en el trayecto emisor - receptor.

*c) AUTENTICACION DE ENTIDADES – FIRMA DIGITAL*

Garantizará a la entidad receptora que el mensaje que llegó de la entidad emisora, pertenece a quién dice ser. Esto lo podemos realizar mediante lo siguiente:

- **AUTENTICACION DE ENTIDAD SIMPLE**: Puede tratarse de la entidad origen de los datos o de la entidad destino.
- **AUTENTICACION DE ENTIDADES MUTUA:** Ambas entidades comunicantes se autentican una a la otra.

La autenticación debe realizarse por medio de mecanismos de cifrado y de firma digital, no por un simple mecanismo de intercambio de 'passwords' o de mensajes cifrados del tipo pregunta / respuesta, que son más vulnerables.
El empleo de este mecanismo de intercambio de autenticación con tecnologías de certificados puede utilizarse para proporcionar una capacidad de autenticación distribuida de modo que sea posible un tratamiento seguro de la información y una mayor seguridad en la conectividad entre emisor / receptor.

Pueden utilizarse diversos mecanismos conjuntamente, que garanticen la Integridad, Confidencialidad, Autenticación y No Repudio en la transmisión de mensajes en la Internet.

*d) NO REPUDIO - ACUSE DE RECIBO*

Proporcionará al emisor/receptor de un mensaje, una prueba irrefutable de que el contenido recibido fue el mismo que el del mensaje enviado por el emisor, y que por lo tanto no ha habido modificación del mismo desde el emisor, y se aceptará el mensaje. Para poder proporcionar una confirmación de NO REPUDIO, el procedimiento sería el siguiente:

I. El **emisor del mensaje** solicita notificación afirmativa o negativa de la recepción con autenticación no repudiable.
II. El **receptor del mensaje**, emite notificación afirmativa o negativa con no repudio, utilizando el procedimiento de autenticación.
III. El **emisor del mensaje**, cuando recibe la notificación, utiliza los procedimientos de verificación para asegurarse que el emisor de la notificación es el deseado.

La presencia de un **CERTIFICADO DE NO REPUDIO**, prueba que el receptor aceptó la notificación de no repudio solicitado por el emisor.

Este servicio protege al emisor/receptor de un documento, de cualquier intento por parte del origen/destino de negar su envío/recepción en su totalidad o en parte del contenido del mismo.

Asimismo pretende dar una validez legal a un documento, ya que requiere que una persona se responsabilice de contenido del documento estampando su firma digital en él. Estos servicios pueden ser de dos clases:

- Con **PRUEBA DE ORIGEN**. El receptor tiene prueba, demostrable ante terceros, del origen de los datos recibidos.

- Con **PRUEBA DE ENTREGA**. El emisor tiene prueba de que los datos han sido entregados al receptor deseado.

***Acuse de recibo***

Todas las funciones descritas anteriormente, están dentro de la confirmación de entrega extremo a extremo. Su propósito es poder probar que el contenido del mensaje enviado por la entidad origen fue recibido por la entidad destino.

Esta función es similar al concepto de acuse de recibo.

***La necesidad del acuse de recibo***

La posición del emisor puede resultar difícil ya que el receptor puede alegar que no recibió mensaje alguno o lo que es lo mismo, negar su existencia.
Al emisor sólo le puede quedar la seguridad de que el receptor no le puede alterar el contenido del mensaje.

Para que el emisor esté seguro de que el mensaje ha llegado a su destino, aparece la figura del acuse de recibo. Este se produce en un mensaje del receptor al emisor, de haberlo recibido.

Para que el acuse de recibo sea operativo, se debe establecer un plazo de tiempo mínimo en que se produzca el envío del mismo.

Es en este punto cuando se invierten las posiciones, pues el receptor no puede justificar que envió el acuse de recibo, estaríamos dentro de un círculo cerrado de envíos y contra envíos de acuses de recibo.

Para solucionar este problema, se impone la figura de una tercera parte, siendo a través de su actuación la forma de que se logre que todas las partes tengan prueba plena del origen, contenido y destino de cualquier mensaje que se haya emitido o recibido.

***e) CONTROL DE ACCESO***

Los servicios de seguridad de control de acceso tienen por objeto garantizar que sólo acceden a la información y a los diversos recursos del sistema aquellos usuarios que tienen los derechos para ello. Los mecanismos a utilizar van desde una adecuada gestión de claves de acceso (*passwords)* hasta las más complejas técnicas de cortafuegos (*firewall)* como se verá más adelante.

### 1.5.3 TECNICAS Y MECANISMOS DE SEGURIDAD

Los servicios de seguridad constituyen el ***qué***, mientras que las técnicas y mecanismos de seguridad constituyen el ***cómo*** en la implantación de la

seguridad, así una técnica o mecanismo de seguridad es la lógica o algoritmo que implementa un servicio de seguridad particular en  hardware y software.

La tabla 1.7 expresa la relación entre los servicios de seguridad y las técnicas o mecanismos de seguridad aplicables.

| ***Servicio de Seguridad*** | ***Técnica/Mecanismo de Seguridad*** |
|---|---|
| Autenticación de entidad | *Intercambio de autenticaciones* |
| Autenticación de datos de origen | *Cifrado*<br>*Firma digital*<br>*Función de comprobación criptográfica* |
| Control de acceso | *Lista de control de acceso*<br>*Cortafuegos* |
| Confidencialidad orientada a la conexión | *Cifrado*<br>*Etiquetas de seguridad* |
| Confidencialidad no orientada a la conexión | *Cifrado*<br>*Etiquetas de seguridad* |
| Confidencialidad del flujo de tráfico | *Cifrado*<br>*Relleno del tráfico*<br>*Etiquetas de seguridad* |
| Integridad orientada a la conexión | *Función de comprobación criptográfica*<br>*Funciones hash y cifrado* |
| Integridad no orientada a la conexión | *Función de comprobación criptográfica*<br>*Funciones hash y cifrado*<br>*Firma digital* |
| No repudio, origen | *Firma digital*<br>*Terceras Partes de Confianza* |
| No repudio, destino | *Firma digital*<br>*Terceras Partes de Confianza* |

*Tabla 1.7 Servicios de Seguridad y Técnicas de Seguridad*
*Elaborado por: Los Autores*

# CAPITULO 2

# ETAPA 1: EVALUACION DE LA SEGURIDAD DEL ISP

## 2.1 SITUACION ACTUAL DEL ISP

Es importante iniciar este capítulo con una idea global de cómo se encuentra actualmente el mercado de Proveedores de Servicios de Internet en el Ecuador,

de tal forma que se conozca quienes son los integrantes principales con los que se tiene relación o competencia.

### 2.1.1 INTERNET EN EL ECUADOR

Dentro del universo de usuarios latinoamericanos, el Ecuador se presenta dentro de los países menos desarrollados en Latinoamérica, existiendo alrededor de 200.000 conexiones contratadas actualmente, lo que nos debería dar un total aproximado de 700,000 usuarios en el país. Esto, no solo obedece a que tenemos un sistema de telecomunicaciones estatal que se encuentra precariamente desarrollado, sino también al hecho de que ha existido muy poca difusión sobre este fenómeno, a excepción de este último año en el cual las compañías establecidas han visto la ventaja competitiva de atraer clientes por medio de la publicidad.

Esta situación, sin lugar a dudas, presenta una excelente oportunidad para quien tome la iniciativa de manera agresiva y masiva para proveer servicios por medio de Internet, y lograr un fuerte posicionamiento dentro de los actuales y potenciales usuarios del país, que ha experimentado un crecimiento superior al 60% anual en los últimos tres años. Adicionalmente, hay que resaltar que el Ecuador cuenta con un alto nivel de profesionales preparados en las áreas de informática y tecnología, que constituyen un excelente respaldo para el desarrollo de proyectos regionales desde esta localidad.

## 2.1.2 PROVEEDORES AUTORIZADOS

Datos a Septiembre del 2004

| PROVEEDORES DE INTERNET EN EL ECUADOR | |
|---|---|
| AÑO | CANTIDAD |
| 1998 | 14 |
| 99 | 18 |
| 2000 | 39 |
| 2001 | 72 |
| 2002 | 96 |
| 2003 | 107 |
| 2004 (Sep) | 126 |

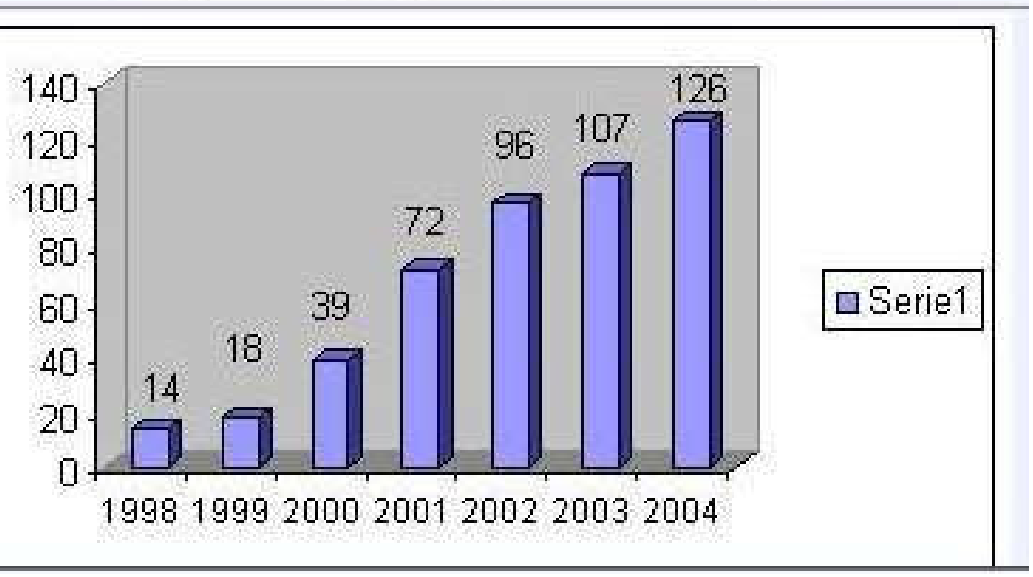



*Fig. 2.1 Proveedores de Internet a nivel nacional*
*Fuente: Dirección General de Gestión de los Servicios de Telecomunicaciones (CONATEL) 20/01/2005*

Sin embargo el principal problema para poder operar como Proveedores de Servicios de Internet en nuestro país (Ver Fig. 2.1) se presenta el momento de obtener una licencia para la prestación de Servicios de Valor Agregado, en la actualidad en el Ecuador existen 150 empresas que tienen su permiso aprobado y podríamos decir que están operando "legalmente" (Tabla 2.1), sin embargo existen muchos más proveedores que se encuentran operando y sus licencias no han sido tramitadas por la lentitud y deficiencia de los trámites burocráticos que se deben realizar tanto en la Secretaría Nacional de Telecomunicaciones (SENATEL) como en el Consejo Nacional de Telecomunicaciones (CONATEL), adicionalmente la inestabilidad económica y política de los últimos cuatro años ha provocado que estos organismos de control no tengan personal fijo en cargos de Superintendencia y Dirección de Areas, lo cual ha motivado una mayor demora en la aprobación o negación de dichas licencias, se estima que son alrededor de 50

empresas que han presentado su solicitud y que están en espera de su aprobación.

| No | OPERADORA | | COBERTURA |
|---|---|---|---|
| 1 | MEGADATOS | | Quito, Guayaquil, Cuenca |
| 2 | ANDINATEL | | De acuerdo al contrato de concesión |
| 3 | AT&T GLOBAL NS | | Quito, Guayaquil |
| 4 | BARAINVER | | Quito |
| 5 | BISMARK | | Quito, Guayaquil, Cuenca, Machala |
| 6 | CONECEL | | Quito, Guayaquil |
| 7 | COSINET S.A. | | Quito, Guayaquil |
| 8 | CONSULSYSNET ECUADOR S.A. | | Quito |
| 9 | ECUAFAST (TICSA) | | Quito |
| 10 | ECUANET – INFORNETSA | | Quito, Guayaquil, Libertad, Cuenca, Ambato, Puerto Ayora, Machala, Manta, Sto. Domingo, Portoviejo, Ibarra, Riobamba. |
| 11 | ESPOLTEL | | Guayaquil |
| 12 | ETAPA | | |
| 13 | FIBROPTEL S.A. | | Machala, Puerto Bolívar, Santa Rosa |
| 14 | GEVETE S.A. | | Guayaquil, Quito, Machala, Manta, Esmeralda, Bahía de Caráquez y Cuenca. |
| 15 | GRUPO BRAVCO | | Quito, Guayaquil |
| 16 | GRUPO MICROSISTEMAS JOVICHSA S.A. | | Quito |
| 17 | IMBANET S.A. | | Ibarra |

| No | OPERADORA | | COBERTURA |
|---|---|---|---|
| 18 | INFONET | | Quito |
| 19 | INTELLICOM INFORMÁTICA | | Guayaquil |
| 20 | JAIME BEJAR FEIJOO | | Guayaquil |
| 21 | LUTROL S.A. INTERACTIVE | | Guayaquil, Quito, Cuenca, Machala, Ambato, Manta |
| 22 | ONNET S.A. | | Quito, Guayaquil, Cuenca, Manta, Esmeraldas, Machala, Libertad, Bahía de Caráquez |
| 23 | OTECEL | | Tulcán, Ibarra, Cayambe, Quito y valles, Guayaquil, Salinas, Ambato, Latacunga, Riobamba, Cuenca, Esmeraldas, Manta, Portoviejo, Machala, Loja, carretera Santo Domingo-Guayaquil. |
| 24 | PACIFICTEL | | De acuerdo al contrato de concesión. |
| 25 | PANCHONET | | Quito, Guayaquil |
| 26 | PARADYNE (Ecuador On Line) | | Quito, Guayaquil, Cuenca, Ambato, Machala, Manta, Portoviejo |
| 27 | PUNTONET | | Quito, Guayaquil, Ambato, Riobamba, Santo Domingo, Machala, Manta, Cuenca |
| 28 | PRODATA (HOY NET) | | Quito |
| 29 | READYNET | | Quito |
| 30 | SATEFAR | | Quito, Guayaquil, Ambato |
| 31 | SATNET | | Quito, Guayaquil, Cuenca, Ambato, Machala, Manta |
| 32 | SITA | | Quito, Guayaquil, Cuenca, Manta, Machala, Ambato, Santo Domingo, Latacunga, Riobamba, Ibarra, Otavalo, Loja, Milagro, Salcedo, Azogues, Santa Rosa, Huaquillas, Cayambe, Portoviejo. |
| 33 | SYSTRAY S.A. | | Manta |

| No | OPERADORA | | COBERTURA |
|---|---|---|---|
| 34 | TELCONET | Telconet Acelera a fondo...! | Guayaquil, Quito, Loja |
| 35 | TELEFÓNICA LINK DEL ECUADOR | TELEFONICA LINK DEL ECUADOR S.A. | Cuenca |
| 36 | TERREMARKDEL ECUADOR | | Guayaquil |
| 37 | TESAT S.A. | TESAT | Quito Guayaquil |
| 38 | UNIVER. TÉCNICA PARTICULAR DE LOJA | utpl.net | Loja, Zamora, Chinchipe, El Oro |

*Tabla 2.1 ISP's Aprobados por la SENATEL*
*Fuente: SENATEL*

"Empresas SVA autorizadas que no operan o no remiten datos: A.A Producciones Filmar CIA. LTDA., Admistelsa S.A., Ajelcorp, Americatel, Casver S.., Ciencompu S.A. Colegio del Pacifico S.A., Compin S.A., Consulsysnet Ecuador S.A., Comuninsa S.A., Diana Soft S.A.,DigilinK S.A, Econophone S.A, Ecuaonline S.A., Eficensa S.A.,Escuela Politécnica Javeriana, Frimen S.A., Estatel S.A,Globatel S.A., Infratel Cia. Ltda., Interloop S.A., Intec S.A., Interfot S.A., Internetsa, Intergeos Internacional Trade, Latinbell S.A., Lucent Ecuador Corp. S.A., Ludeña Espit Telecomp Cia., Mconis Empresa de Computo Comunicaciones, Internet y Sistemas Quirola S.A., Medios Interactivos Miwebwor, Metrocable S.A., Medamac S.A., Mundodigital S.A., Nexatel, Octonet S.A., Opnet S.A., Patricio Ivan Lalama Salas, Privanet, Richard Gonzalo Espinoza Guzmán, Raquilsa S.A., Rimex, RDH Asesoria y Sistemas S.A., Saril S.A., Satlink S.A., Servicios Netsec S.A.,Speednet S.A., Suramericana de Telecomunicaciones S.A., Systelecom, Systemdosmil S.A., Techsoftnet S.A., Telecomunicaciones Knowledgment S.A., Terremark del Ecuador S.A., Teleaxxis Telecomunicaciones Cia. Ltda., Telinet S.A., Unisolutions Informatica S.A., Univisa S.A.,Virtual Team Entreprises Ecuador S.A., Wexcom S.A."[25]

### 2.1.3 EMPRESAS PORTADORAS AUTORIZADAS POR LA SENATEL

Dentro del ámbito de las comunicaciones Carriers o Portadores, existen en el país diez y nueve empresas que pueden prestar este tipo de servicio según la

[25] Información proporcionada por el SENATEL

legislación ecuatoriana y las cuales están debidamente aprobadas por la Secretaría Nacional de Telecomunicaciones. Ver Tabla 2.2:

| # | Empresas Concesionarias Portadores | |
|---|---|---|
| **1** | QUICKSAT S.A. (CLASESAT ) | Servicios Portadores Satelitales |
| **2** | ANDINATEL S.A. | Servicios Finales y Portadores |
| **3** | PACIFICTEL S.A. | Servicios Finales y Portadores |
| **4** | IMPSATEL S.A. | Servicios Portadores |
| **5** | MEGADATOS S.A. | Servicios Portadores |
| **6** | CONECEL S.A. | Servicios Portadores |
| **7** | SURATEL S.A. | Servicios Portadores |
| **8** | TELCONET S.A. | Servicios Portadores |
| **9** | OTECEL S.A. | Servicios Portadores |
| **10** | GILAUCO S.A. | Servicios Portadores |
| **11** | NEDETEL S.A. | Servicios Portadores |
| **12** | TRANSNEXA S.A. | Servicios Portadores |
| **13** | TRANSELECTRIC S.A | Servicios Portadores |
| **14** | GRUPO BRAVCO CIA. LTDA. | Servicios Portadores |
| **15** | ECUADOR TELECOM | WLL (Servicios Finales y Portadores ) |
| **16** | SETEL | WLL (Servicios Finales y Portadores) |
| **17** | ETAPATELECOM S.A. | Servicios Finales y Portadores |
| **18** | TELEHOLDING S.A. | Servicios Portadores |
| **19** | PUNTONET S.A. | Servicios Portadores |

*Fuente: Dirección General de Gestión de los Servicios de Telecomunicaciones 20/01/2005*

*Tabla 2.2 Operadoras aprobadas por la SENATEL*
*(*) El número de usuarios a través de la empresa TELEHOLDING no forma parte de este informe*

### 2.1.4 MERCADO ACTUAL DE PROVEEDORES

Tal como habíamos mencionado anteriormente existe en el país un número cercano a 210.000 conexiones de Internet, los cuales se distribuyen entre los ISP's que actualmente se encuentran operando en el país, como se presenta en la Tabla 2.3, esto nos da una muy buena fuente de información sobre la distribución del mercado e incluso la forma en que se han distribuido de acuerdo a la ubicación geográfica, sin lugar a dudas los centros de mayor concentración de usuarios son las ciudades de Quito y Guayaquil, como se presenta en la Tabla 2.4 Número de Conexiones por Ubicación Geográfica.

| No | OPERADORA | | CUENTAS DIAL UP | | CUENTAS CORPORATIVAS | | TOTAL USUARIOS | |
|---|---|---|---|---|---|---|---|---|
| 1 | MEGADATOS | | 2.265 | 2.41% | 414 | 6.35% | 2.679 | 2.66% |
| 2 | ANDINATEL | | 24.001 | 25.52% | 2.615 | 40.09% | 26.616 | 26.46% |
| 3 | AT&T GLOBAL NS | | 181 | 0.19% | 10 | 0.15% | 191 | 0.19% |
| 4 | BARAINVER | | 127 | 0.14% | 9 | 0.14% | 136 | 0.14% |
| 5 | BISMARK | | | 0.00% | 679 | 10.41% | 679 | 0.68% |
| 6 | CONECEL | | 3.524 | 3.75% | 30 | 0.46% | 3.554 | 3.53% |
| 7 | COSINET S.A. | | 184 | 0.20% | 2 | 0.03% | 186 | 0.18% |
| 8 | CONSULSYSNET ECUADOR S.A. | | 2.687 | 2.86% | 35 | 0.54% | 2.722 | 2.71% |
| 9 | ECUAFAST (TICSA) | | 274 | 0.29% | 8 | 0.12% | 282 | 0.28% |
| 10 | ECUANET – INFORNETSA | | 8.490 | 9.03% | 312 | 4.78% | 8.802 | 8.75% |
| 11 | ESPOLTEL | | 1.315 | 1.40% | 10 | 0.15% | 1.325 | 1.32% |
| 12 | ETAPA | | 4.400 | 4.68% | 330 | 0.51% | 4.433 | 4.41% |
| 13 | FIBROPTEL S.A. | | | 0.00% | 6 | 0.09% | 6 | 0.01% |
| 14 | GEVETE S.A. | | | 0.00% | 16 | 0.25% | 16 | 0.02% |
| 15 | GRUPO BRAVCO | | | 0.00% | 50 | 0.31% | 20 | 0.02% |
| 16 | GRUPO MICROSISTEMAS JOVICHSA S.A. | | | 0.00% | 150 | 0.23% | 15 | 0.01% |
| 17 | IMBANET S.A. | | 330 | 0.35% | 6 | 0.09% | 336 | 0.33% |
| 18 | INFONET | | | 0.00% | 22 | 0.34% | 22 | 0.02% |
| 19 | INTELLICOM INFORMÁTICA | | 373 | 0.40% | | 0.00% | 373 | 0.37% |
| 20 | JAIME BEJAR FEIJOO | | 59 | 0.06% | | 0.00% | 59 | 0.06% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 21 | LUTROL S.A. INTERACTIVE | | 11.917 | 12.67% | 200 | 0.00% | 11.917 | 11.85% |
| 22 | ONNET S.A. | | 2.895 | 2.01% | 241 | 0.63% | 1.936 | 1.92% |
| 23 | OTECEL | | 148 | 0.05% | 192 | 2.94% | 240 | 0.24% |
| 24 | PACIFICTEL | | 16823 | 7.25% | 881 | 13.51% | 7704 | 7.66% |
| 25 | PANCHONET | | 1.680 | 1.79% | 100 | 0.15% | 1.690 | 1.68% |
| 26 | PARADYNE (Ecuador On Line) | | 71 | 0.08% | 88 | 1.35% | 159 | 0.16% |
| 27 | PUNTONET | | 7.077 | 5.50% | 625 | 1.92% | 5.302 | 5.27% |
| 28 | PRODATA (HOY NET) | | 1.033 | 1.10% | 377 | 5.78% | 1.410 | 1.40% |
| 29 | READYNET | | 412 | 0.23% | 21 | 0.32% | 233 | 0.23% |
| 30 | SATEFAR | | 69 | 1.56% | | 0.00% | 1.469 | 1.46% |
| 31 | SATNET | | 11.461 | 13.25% | 612 | 6.32% | 12.873 | 12.80% |
| 32 | SITA | | | 0.00% | 74 | 1.13% | 74 | 0.07% |
| 33 | SYSTRAY S.A. | | 232 | 0.25% | 6 | 0.09% | 238 | 0.24% |
| 34 | TELCONET | | 2.600 | 1.70% | 830 | 0.51% | 1.633 | 1.62% |
| 35 | TELEFÓNICA LINK DEL ECUADOR | | 976 | 1.04% | 6 | 0.09% | 982 | 0.98% |
| 36 | TERREMARKDEL ECUADOR | | | 0.00% | 14 | 0.21% | 14 | 0.01% |
| 37 | TESAT S.A. | | 125 | 0.13% | | 0.00% | 125 | 0.12% |
| 38 | UNIVER. TÉCNICA PARTICULAR DE LOJA | | 130 | 0.14% | 1 | 0.02% | 131 | 0.13% |
| TOTAL : | | | 164.059 | | 46.523 | | 210.382 | |

*Tabla 2.3 Número de Conexiones por ISP.*

*Fuente: SENATEL*

| CIUDAD | # Conexiones Dial Up | # Conexiones Coorporativas | % Mercado Dial Up | % Mercado Coorporativas |
|---|---|---|---|---|
| QUITO | 109861 | 8963 | 53.01% | 45.42% |
| GUAYAQUIL | 91368 | 4467 | 22.72% | 22.49% |
| CUENCA | 18330 | 586 | 12.05% | 5.92% |
| PORTOVIEJO | 1850 | 138 | 0.90% | 2.12% |
| RIOBAMBA | 2270 | 409 | 1.35% | 6.27% |
| AMBATO | 3005 | 189 | 2.13% | 2.90% |
| IBARRA | 1888 | 167 | 0.94% | 2.56% |
| MACHALA | 6187 | 207 | 2.33% | 3.17% |
| MANTA | 2560 | 118 | 2.72% | 1.81% |
| STO. DOMINGO | 1677 | 138 | 0.72% | 2.12% |
| OTRAS | 3063 | 341 | 1.13% | 5.23% |
| **TOTAL** | **232061** | **15523** | **100.00%** | **100.00%** |

*Tabla 2.4 Conexiones por Ubicación Geográfica*
*Fuente: SENATEL*

De acuerdo a la legislación en el área de comunicaciones de nuestro país se debe presentar el Anteproyecto Técnico a la Secretaría Nacional de Telecomunicaciones, previó a la obtención de la Licencia para prestación de Servicios de Valor Agregado.

Luego de revisado como se encuentra actualmente el mercado de Carriers e ISPs en el Ecuador, vamos a continuar con la revisión de la situación actual del ISP caso de estudio (Punto Net).

### 2.1.5 INFRAESTRUCTURA TECNOLÓGICA DE PUNTO NET

La Plataforma tecnológica se divide en equipamiento de Telecomunicaciones (Border-Routers, Access-Servers, Switchs de Core, Packet Shapper, DSLAMs, Redes inalámbricas, etc.), y equipamiento de Servidores (Correo, DNS, Autenticación, Monitoreo, Web, FTP, Antivirus, AntiSpam, etc.), los mismos que se detallan a continuación:

El ISP cuenta con los siguientes equipos (Ver Fig. 2.2 *Diagrama de Red del ISP*)

- **Ruteadores:**
  - **Cisco 7206 VXR IOS 12.2 (17a) (2 equipos), con interfaces seriales, GigaEthernet y HSSI – BORDER ROUTER**
  - Cisco 7304 VXR IOS 12.3 (1a) (2 equipos), con interfaces seriales, Gigabit Ethernet, STM-1 y E3

- **Access-Servers:**
  - **Cisco AS5300 IOS 12.3 (3) 8 E1s 240 modems digitales MICA (2 equipos) – ENLACES DIAL-UP**
  - **Cisco AS5300 IOS 12.3 (3) 4 E1s 120 modems digitales MICA (1 equipo) – ENLACE CORPORATIVOS, ADSL, CLEAR CHANNEL**
  - **Cisco AS5300 IOS 12.3 (3) 4E1s (2 equipos) – ENLACES SDSL, CLEAR CHANNEL**
  - Cisco 3640 IOS 12.1 (9) 4 puertos seriales V.35
  - Cisco 3640 IOS 12.1 (9) 2 puertos seriales, 96 puertos async (1 equipo)
  - Cisco 3620 IOS 12.1 (5 T12) 4 puertos seriales (1 equipo)
  - Cisco 2511 IOS 12.1 (12b) 2 puertos seriales, 16 puertos async (2 equipos)

- **Servidores:**
  - **HP Proliant DL380 (2 equipos), 3 Discos Hot Swap, Linux 9.0, RAID 5. – SERVIDOR DNS Y CORREO ELECTRONICO**
  - **Compaq Proliant ML370, 3 Discos Hot Swap, Windows 2000, RAID 5. – SERVIDOR DE AUTENTICACION, MONITOREO DE ENLACES Y WEB MAIL**
  - **Compaq Proliant ML330, 2 Discos SCSI, Windows 2000. – SERVIDOR DE FACTURACION**
  - **Clon Pentium IV, 3 discos IDE, Linux 9.0 – SERVIDOR DNS SECUNDARIO, WEB SERVER Y RESPALDOS**
  - **Clon Pentium IV, 1 disco IDE, Windows 2000 – SERVIDOR MONITOREO ANCHO DE BANDA DE CLIENTES**

- **Modem Pools:**
  - 8 Total Control MP16 USRobotics, 16 puertos análogos cada uno.

- **Switchs y Hubs:**
  - Cisco 3750 (2 equipos), 24 puertos puertos FE, IOS 12.3 (ISP)
  - Cisco 2950T, 24 puertos puertos FE, IOS 12.3 (ISP)
  - Cisco 2924, 24 puertos puertos FE, IOS 12.3 (ISP)
  - 3COM 3300 Super Stack 12 puertos FE (LAN)
  - **Packet-Shapper, Packeteer 4500 ISP (2 equipos). LINUX – ADMINISTRACION ANCHO DE BANDA**

- **Cisco Cache Engine CE590, IOS ACNS 4.1:**
  - **Servidor Web CACHE**

### 2.1.5.1 Diagrama de Red del ISP

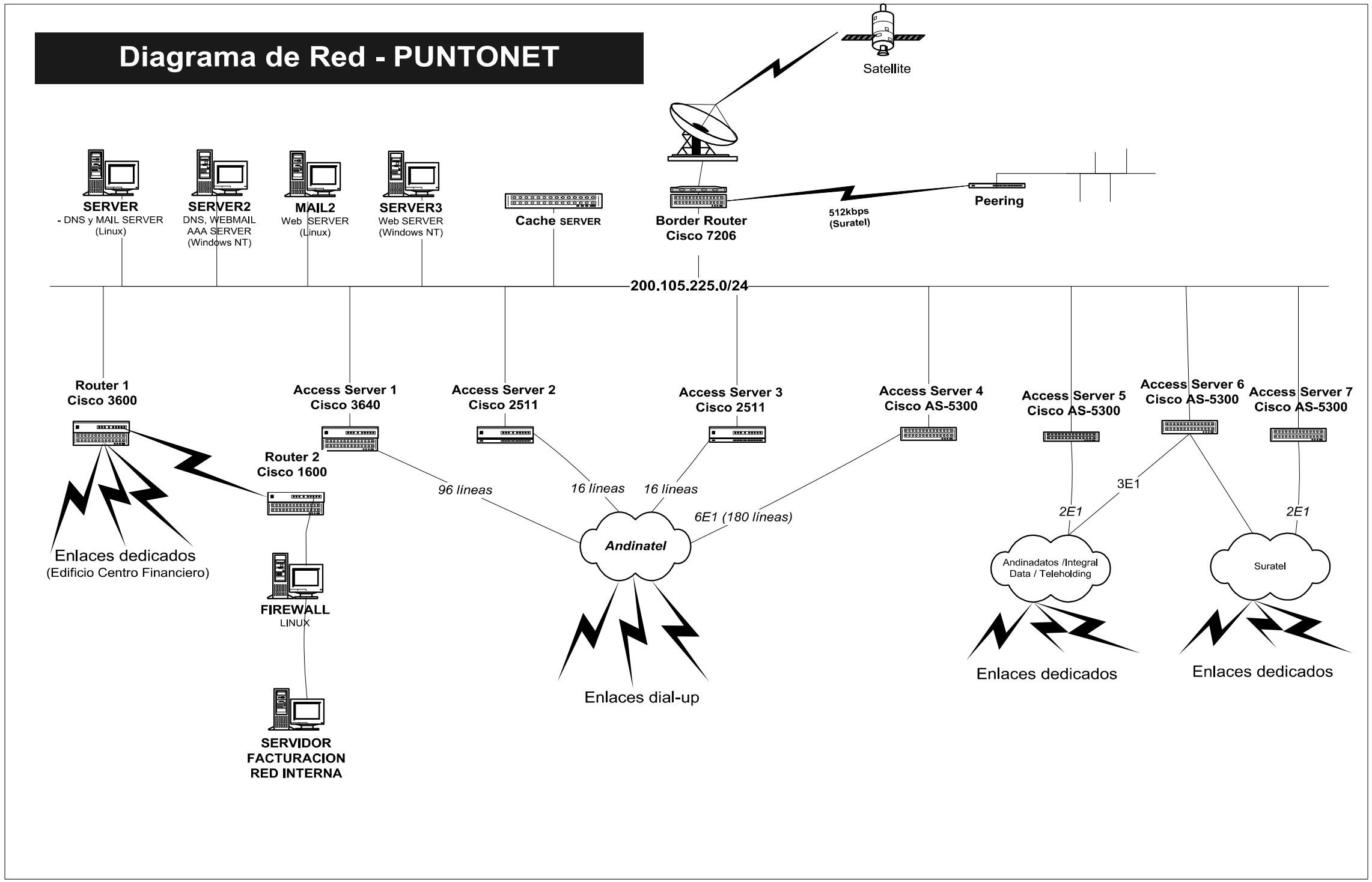



*Fig. 2.2 Diagrama de Red del ISP*

### 2.1.6 SERVICIOS OFRECIDOS POR EL ISP

El ISP caso de estudio tiene servicios dentro del campo corporativo y dentro del campo individual o personal, a continuación se detallan los servicios de cada uno:

#### 2.1.6.1 Corporativo

Actualmente se trabaja con las empresas de última milla Andinadatos y Suratel, además de contar una red de acceso inalámbrico en modo bridge, en cada caso se tiene diferentes opciones de servicio de conexión, para facilitar la diferenciación de los servicios a continuación se detallan por empresa.

- **Andinadatos:**
  - Clear-Channel, los mismos que son basados en una red TDM, se cuenta con un canal de conexión E1 para este tipo de servicios y la división se lo hace por time-slots, de esta forma se garantiza el acceso de cada cliente de forma individual, el Ancho de Banda es incremental en Nx64 de acuerdo a las necesidades del cliente.
  - xDSL, se basan en una red ATM como transporte y como enlace se utiliza xDSL (actualmente solo ADSL o SDSL), se cuenta con canales E1 independientes para cada tipo de servicio.
- **Suratel:**
  - Clear-Channel, los mismos que son basados en una red TDM, se cuenta con dos canales de conexión E1 para este tipo de servicios y la división se lo hace por time-slots, de esta forma se garantiza el acceso de cada cliente de forma individual, el Ancho de Banda es incremental en Nx64 de acuerdo a las necesidades del cliente.
  - Frame-Relay, es una red de acceso compartido y que se define el usuario de acuerdo a PVCs individuales por cada usuario de conexión, se cuenta con una matriz Frame-Relay que soporta un Ancho de Banda de 2Mbps, los canales virtuales se los puede configurar en velocidades de Nx64kbps de acuerdo a las necesidades del cliente.
  - IP Connect, es una tecnología basada en Bridge, lo que emula una extensión de la LAN, se tiene una matriz de IP Connect, la misma que se configura por medio de PVCs contra el cliente remoto que tiene un

MODEM con un puerto LAN (Ethernet) para la conexión de las oficinas del cliente contra la matriz ubicada en el ISP, las velocidades que se manejan son de Nx64.

- **PUNTONET:**
  - Circuitos Simétricos, los mismos que son basados en una red FDM, se cuenta con seis nodos de acceso en Quito, cuatro en Guayaquil, dos en Santo Domingo y dos en Cuenca para este tipo de servicios, la distribución se lo hace mediante el acceso punto-multipunto y la seguridad viene dada nivel de VLANs exclusivas para cada cliente, las mismas que son generadas en un router Cisco 3750, de esta forma se garantiza el acceso de cada cliente de forma individual, el Ancho de Banda es incremental en Nx64 de acuerdo a las necesidades del cliente.

### 2.1.6.2 Personal – DialUp

Para la conexión de usuarios de forma conmutada se cuenta con canales de conexión tanto analógicos como digitales y la forma de conexión se detalla a continuación:

- Digital, se cuenta con canales E1 de conexión para usuarios conmutados, los mismos que se interconectan a la Central Telefónica del PTT por medio de Fibra Optica, las velocidades de conexión pueden llegar a velocidades de 56kbps por cada una.
- Analógica, se cuenta con líneas de conexión individual que vienen desde la central del PTT por medio de cobre, estas líneas forman PBXs de acceso, los cuales pueden llegar a velocidades máximas de conexión de 38.8kbps.

### 2.1.6.3 Alojamiento de Servidores

Se ofrece servicios de colocation o housing de servidores en las instalaciones del ISP, este servicio está orientado a clientes que desean alojar Sistemas de Bases de Datos relacionados con páginas Web y de contenido. El Ancho de Banda del cliente es garantizado por medio de conexiones Back-to-Back entre el Access-Server del lado del ISP y un router del lado del servidor del cliente.

### 2.1.6.4 Alojamiento de Web-Sites

Si el cliente no desea tener un Ancho de Banda independiente y tiene aplicaciones de menor tamaño, se le ofrece la publicación de sus Web-Sites en los servidores de Web del ISP.

### 2.1.6.5 Sistemas de Real Audio y Real Video

Se trabaja en modalidad similar a la del Alojamiento de Servidores, pero el servicio es el de publicación en línea de contenido de Audio o de TV, los clientes de este tipo de servicio son las radios y las estaciones de TV, este mercado es muy apreciado en inmigrantes que por medio de conexiones a Internet pueden escuchar emisoras de su país o incluso mirar TV si ese fuera el caso.

## 2.1.7 ESQUEMA DE SEGURIDAD DE LA RED DE DATOS DEL ISP

La red del ISP se encuentra actualmente protegida desde el Border-Router Cisco 7304, en el cual se tiene Listas de Acceso y filtrado de paquetes con restricción de direcciones IP, subredes y redes de direcciones dudosas o reconocidas como SPAM o de Hackers, adicionalmente se tiene cerrado acceso a los routers y access-servers desde direcciones externas y bloqueo de puertos (sockets) para ciertas aplicaciones críticas del ISP.

La red del sistema de facturación es independiente del nodo principal y esta protegido por listas de acceso en un router Cisco 1601 que esta conectado Back-to-Back a uno de los Access-Servers, luego existe una PC con Linux e implementado Firewall para protección de la red LAN de posibles ataques.

Todos los servidores cuentan con Sistemas Antivirus, AntiSpam y políticas AntiHacking en la parte de Correo y de datos.

## 2.2 APLICACIÓN DE METODOLOGIAS DE EVALUACION DE SEGURIDADES PARA EL ISP

En esta fase es necesario partir con el enfoque de COBIT para la Administración del Servicio de Infraestructura Tecnológica y sus objetivos de control específicos relacionados a Seguridades. (Ver Anexo C). Para ello vamos a considerar la importancia de los objetivos de control general relacionados con el tema de seguridades, siguiendo las recomendaciones del documento Security Baseline de COBIT (Ver Anexo I)que fue publicado a inicios del 2005. Este documento expone los objetivos de control detallados de COBIT que tienen relación con la seguridad en un ambiente de TI. Del estudio de estos, se han seleccionado aquellos que tienen relación con la gestión de la seguridad de la red informática que sean aplicables a la naturaleza del negocio y que contribuyen a alcanzar los objetivos del negocio.

En efecto podemos indicar que se debe revisar los siguientes objetivos de control a nivel general:

1. Proporcionar las plataformas apropiadas para soportar las aplicaciones del negocio.
2. Proporcionar un entorno físico adecuado que proteja el equipo de TI y a la gente contra peligros artificiales y naturales.
3. Salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o pérdida.

De acuerdo a la selección de los objetivos de control general podemos asociar según las Guías de Auditoría de COBIT los objetivos de control específicos para realizar la evaluación de riesgo, los mismos que detallamos en la Tabla 2.5 y 2.6:

| Objetivo de Control General | Objetivos de Control Específicos |
|---|---|
| **Proporcionar las plataformas apropiadas para soportar las aplicaciones del negocio** | **AI3.3** La gerencia de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse atención especial a la instalación y mantenimiento de los parámetros del software del sistema. |

*Tabla 2.5 Objetivos de Control General a evaluar 1*

*Fuente: Los Autores*

| Objetivo de Control General | Objetivos de Control Específicos |
|---|---|
| **Proporcionar un entorno físico adecuado que proteja el equipo de TI y a la gente contra peligros artificiales y naturales** | **DS12.1** Establecimiento de medidas apropiadas de seguridad física y control de accesos, protección contra factores ambientales y prácticas de salud para las instalaciones de tecnología informática |

| Objetivo de Control General | Objetivos de Control Específicos |
|---|---|
| **Salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o perdida** | **DS5.1** Administrar medidas de seguridad |
| | **DS5.2** Identificación, autenticación y acceso lógico |
| | **DS5.3** Garantizar el control de la seguridad de acceso (permisos) |
| | **DS5.4** Administración de cuentas de usuario (emisión, suspensión y cierre) |
| | **DS5.5** Revisión gerencial de cuentas de usuario (dueños de la información) |
| | **DS5.6** Control de usuarios sobre cuentas de usuario (registro de actividades inusuales) |
| | **DS5.7** Registrar toda actividad de seguridad y cualquier indicación de una inminente violación a la seguridad (notificación y consecuencias) |
| | **DS5.8** Clasificación de datos por propietario mediante una decisión formal y explícita de acuerdo con el esquema de clasificación de datos definido por la Gerencia |
| | **DS5.9** Administración centralizada de los derechos de acceso de los usuarios, identidad del sistema y propiedad de los datos |
| | **DS5.11** Manejo de incidentes de seguridad |
| | **DS5.16** Asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales seguros (protocolos, encriptación de datos) |
| | **DS5.19** Prevención, detección y corrección de software malicioso (virus) |
| | **DS5.20** Arquitectura de firewalls y conexión a redes públicas |

*Tabla 2.6 Objetivos de Control General a evaluar 2*

*Fuente: Los Autores*

### 2.2.1 IDENTIFICACIÓN DE OBJETIVOS DE CONTROL PARA EL CASO DE ESTUDIO

Previo a la ejecución del trabajo de evaluación de seguridades se debe realizar un análisis de riesgo para determinar las vulnerabilidades más significativas para la revisión de los objetivos de control propuestos por COBIT en la sección anterior, para esto aplicamos el método más difundido a nivel mundial para la evaluación de riesgo y publicado por la NITS "National Institute of Standards and Technology" en su publicación número 800-30.

#### 2.2.2.1 Identificación del Riesgo e Identificación de objetivos de Control a ser evaluados

Con la aplicación del modelo de valoración del riesgo NIST 800-30 determinamos la evaluación de riesgos tecnológicos del ISP. En la matriz de riesgo propuesta (Ver Tabla 2.7) se identifican cuales son las principales amenazas que afectan a cada uno de los objetivos de control propuestos por COBIT para nuestra evaluación, una vez identificadas las amenazas se procede a cuantificar el riesgo para determinar el nivel de riesgo sobre el objetivo de control, lo que más adelante será la base para el desarrollo de la evaluación de seguridades, Ver Tabla 2.8.

## MATRIZ DE RIESGO

**Empresa: Proveedor de Servicios de Internet**

| Objetivo de Control de Alto Nivel | Caracterización del Sistema | Identificación de Amenazas | Identificación de Vulnerabilidades | Controles Existentes | Determinación de Probabilidad | Valor Prob. | Análisis del Impacto | Valor Imp. | Determi-nación del Riesgo | Valor Riesgo |
|---|---|---|---|---|---|---|---|---|---|---|
| **AI3** | **Adquisición e implementación -** Proporcionar las plataformas apropiadas para soportar las aplicaciones de negocios | El desempeño de las actividades de la organización se vea afectado a causa de las debilidades en la configuración e implantación de la infraestructura tecnológica, incidentes continuos con las principales aplicaciones del negocio a causa de los problemas en la plataforma de soporte. Daños en los equipos servidores. | Ausencia de Planes y procedimientos de mantenimiento preventivo y correctivo de problemas encontrados a nivel de plataforma. | Revisiones de los equipos servidores a cargo del personal técnico responsable del ISP. | Media | 0.5 | Alta | 100 | Media | 50 |

## MATRIZ DE RIESGO (Continuación)

### Empresa: Proveedor de Servicios de Internet

| Objetivo de Control de Alto Nivel | Caracterización del Sistema | Identificación de Amenazas | Identificación de Vulnerabilidades | Controles Existentes | Determinación de Probabilidad | Valor Prob. | Análisis del Impacto | Valor Imp. | Determi-nación del Riesgo | Valor Riesgo |
|---|---|---|---|---|---|---|---|---|---|---|
| **DS5** | **Entrega de Servicios y Soporte -** Salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida | Robo de información para fines no autorizados, no mantener un rastro de posibles accesos no autorizados, que la información no se encuentre clasificada de manera adecuada y no se pueda identificar cual es la información que debe ser restringida y protegida, accesos no autorizados al sistema | Ausencia de pistas de Auditoría<br>Falta de una política de administración de la seguridad.<br>Falta de Aprobaciones formales en las solicitudes de acceso de usuarios.<br>Ausencia de políticas para el manejo y prevención de virus<br>Hackeos<br>Ataques de DOS | Políticas de acceso configuradas a nivel de dominio.<br>Controles automáticos a nivel de BDD y aplicaciones.<br>Antivirus activados.<br>Configuración del Firewall de software | Alta | 1 | Alta | 100 | Alta | 100 |

**MATRIZ DE RIESGO (Continuación)**

**Empresa: Proveedor de Servicios de Internet**

| Objetivo de Control de Alto Nivel | Caracterización del Sistema | Identificación de Amenazas | Identificación de Vulnerabilidades | Controles Existentes | Determinación de Probabilidad | Valor Prob. | Análisis del Impacto | Valor Imp. | Determi-nación del Riesgo | Valor Riesgo |
|---|---|---|---|---|---|---|---|---|---|---|
| **DS12** | **Entrega de Servicios y Soporte -** Proporcionar un ambiente físico conveniente que proteja los equipos y al personal de IT contra peligros naturales o fallas humanas | Poca protección de los recursos de IT, siendo el recurso humano el más importante, inseguridad del personal lo que conlleva a un mal desempeño de actividades, pérdida de equipos y de información. | El área de IT no posee el equipo necesario para la protección en caso de una contingencia (extinguidores, salidas de emergencia)<br>Falta de Planes de contingencia y capacitación a los usuarios de las actividades a realizar en caso de un desastre natural o contingente<br>Poca protección de los equipos, equipos no asegurados. | Protecciones Físicas al área de servidores. Guardias en los ingresos. UPS en sala de servidores, ventanas amplias. Sistemas de control de incendios y alarmas. | Baja | 0.1 | Alta | 100 | Baja | 10 |

*Tabla 2.7 Matriz de Evaluación de Riesgos Tecnológicos del ISP*

*Fuente: Los Autores*

### 2.2.2.2 Concentración del Riesgo en los Objetivos de Control General COBIT

Aplicada la metodología NIST 800-30 para la evaluación de los riesgos tecnológicos del ISP, que permite determinar los riesgos que se encuentran categorizados por Bajos, Medios y Altos, en la Tabla 2.8 se detallan los resultados de la evaluación y se facilita el análisis de concentración de riesgos por los objetivos de control general de COBIT.

| Objetivos de Control General de COBIT | | Riesgos | | |
|---|---|---|---|---|
| | | Baja | Media | Alta |
| AI3 | Proporcionar las plataformas apropiadas para soportar las aplicaciones de negocios | | 1 | |
| DS5 | Salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida | | | 13 |
| DS12 | Proporcionar un ambiente físico conveniente que proteja los equipos y al personal de IT contra peligros naturales o fallas humanas | 1 | | |
| | **Subtotales** | 1 | 1 | 13 |
| | **Total** | **15** | | |

*Tabla 2.8 Concentración del Riesgo por Objetivos de control General*
*Fuente: Los Autores*

La mayor concentración de riesgos después del análisis realizado se establece en el dominio de Entrega de Servicios y Soporte “DS”, resultante por los pocos procedimientos de control asociados a los 13 objetivos de control específicos que generarían un alto impacto en la organización.

De manera global el riesgo tiene una concentración en el nivel alto para los 15 objetivos de control totales de alto nivel de COBIT relacionados con seguridades de la infraestructura tecnológica, se lo puede visualizar en la siguiente tabla y figura. Tabla 2.9, Fig. 2.3

| Riesgo | | |
|---|---|---|
| Bajo | 1 | |
| Medio | 1 | |
| Alto | 13 | |
| Total | 15 | Objetivos de control |

*Tabla 2.9 Concentración total de riesgo por Objetivos de Control*
*Fuente: Los Autores*

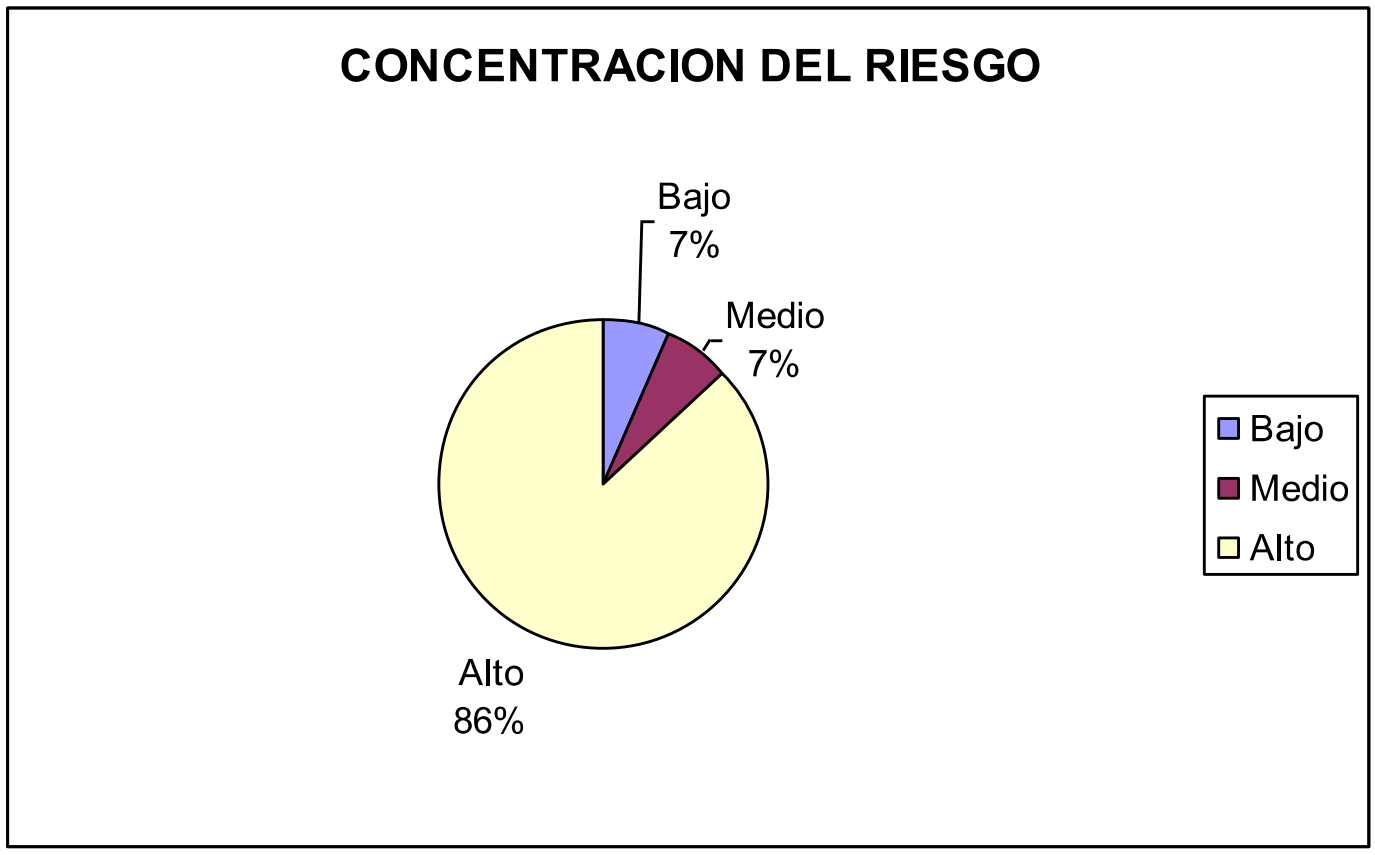



*Fig. 2.3 Concentración del Riesgo*
*Fuente: Los Autores*

### 2.2.2 DIAGNOSTICO DE CONTROL IT

Una vez identificado el ambiente de IT, riesgos altos, medios y bajos, controles existentes, se define la siguiente tabla de diagnóstico de control que nos permitirá estructurar el plan de evaluación a los objetivos de control definidos por COBIT.

| Objetivos de Control | Evaluado | | Controles | | Riesgo |
|---|---|---|---|---|---|
| | SI | NO | SI | NO | |
| **Adquisición e Implementación** | | | | | |
| AI3 Adquisición y mantenimiento de infraestructura tecnológica | | x | x | | Medio |
| | | | | | |
| **Entrega de Servicios y Soporte** | | | | | |
| DS5 Garantizar la seguridad de los sistemas | | x | x | | Alto |
| D12 Administración de Instalaciones | | x | x | | Bajo |

*Tabla 2.10 Diagnóstico de Control de IT*
*Fuente: Los Autores*

Nuestra evaluación se enfoca en los objetivos de control cuyo riesgo se ha determinado como alto y medio, resumiendo en la Tabla 2.11:

| DOMINIO | PROCESO | | Criterios de Información | Recursos de TI |
|---|---|---|---|---|
| | | | Efectividad<br>Eficiencia<br>Confidencialidad<br>Integridad<br>Disponibilidad<br>Cumplimiento<br>Confiabilidad | Recursos<br>Sist. Aplicación<br>Tecnología<br>Instalaciones<br>Datos |
| **Adquisición e Implementación** | **AI3** | Adquirir y mantener la arquitectura tecnológica | P P S | X |
| **Entrega de Servicios y Soporte** | **DS5** | Garantizar la seguridad de sistemas | P P S S S | X X X X X |

*Tabla 2.11 Objetivos de Control Cobit – Criterios y Recursos TI afectados*
*Fuente: Marco Referencial COBIT*

#### 2.2.2.1 Dominio: Adquisición e Implementación

***AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica***

Se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.

El objetivo de control detallado a ser considerado es:

AI3.3 Seguridad de Software del sistema

#### 2.2.2.2 Dominio: Entrega de Servicios y Soporte

***DS5 Garantizar la Seguridad de Sistemas***

Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.

Los objetivos de control detallados a ser considerados son:

DS5.1 Administrar medidas de Seguridad

DS5.2 Identificación, autenticación y acceso

DS5.3 Seguridad de acceso a datos en línea

DS5.4 Administración de cuentas de usuario

DS5.5 Revisión gerencial de cuentas de usuario

DS5.6 Control de usuarios sobre cuentas de usuario

DS5.7 Vigilancia de seguridad

DS5.8 Clasificación de Datos

DS5.9 Administración de derechos de acceso e identificación centralizada

DS5.11 Manejo de incidentes

DS5.16 Sendero Seguro

DS5.19 Prevención, detección y corrección de software malicioso

DS5.20 Arquitectura de Firewalls y conexión a redes públicas

## 2.2.3 DISEÑO DEL PLAN DE EVALUACION PARA EL CASO DE ESTUDIO

### 2.2.3.1 Alcance de la Evaluación

De entre los 15 objetivos de control específicos nivel se identificaron que 86% de los objetivos de control tienen amenazas consideradas como riesgo alto, 7% de amenazas son riesgo medio, y 7% de riesgo bajo.

En el presente trabajo de evaluación nos enfocamos en todos los objetivos de control que implican riesgo alto es decir que la probabilidad de que la amenaza afecte las vulnerabilidades de los activos es alta y provoca un impacto considerable en la organización, y en el objetivo de control de riesgo medio, para la selección del objetivo de control de riesgo medio a ser evaluado se consideró el nivel de impacto alto de las amenazas sobre los activos y el nivel de probabilidad medio de ocurrencia.

"Este criterio es adoptado debido a que la auditoría propuesta en la presente Tesis es realizada por primera vez en la entidad caso de estudio"[25], el plan de auditoría propuesto cubre los objetivos de control específicos que han sido analizados por su riesgo e incidencia en la organización y son: 13 objetivos con riesgo Alto, y 1 objetivo con riesgo medio. Ver Anexo D (Selección de Sub. Objetivos de Control).

#### *2.2.3.1.1 Diseño de Matrices de trabajo*

La primera matriz considerada para realizar la Evaluación de Seguridades es la matriz de "Programa de auditoría" (Tabla 2.12), la matriz es aplicable a los objetivos de control específicos que serán cubiertos por el trabajo de auditoría. Los objetivos de control específicos se definen en base a los criterios de selección de sub-objetivos de control, también se define el factor de riesgo identificado en base a la evaluación de riesgos preliminar que permite definir los principales puntos de enfoque del trabajo de auditoría.

---

[25] Criterio de selección en base a la experiencia de auditoría en estos temas de evaluación

| PROGRAMA DE AUDITORÍA<br>DOMINIO COBIT<br>Objetivo de Control | | |
|---|---|---|
| **OBJETIVOS DE CONTROL GENERAL** | **OBJETIVOS DE CONTROL ESPECÍFICOS** | **FACTOR DE RIESGO** |
| | | |

*Tabla 2.12 Matriz Programa de Auditoría*
*Fuente: www.isaca.org*

Una vez definido el programa de auditoría se elabora la "Matriz de Pruebas" (Tabla 2.13) en la cual que se incluyen las pruebas a realizar, basadas en las "Guías de Auditoría de COBIT", que aplican a los objetivos de control específicos seleccionados para la prueba, en la matriz elaborada se incluyen los objetivos de control específicos seleccionados en base a los criterios de selección de objetivos de control específicos o sub-objetivos, las pruebas de auditoría propuestas por COBIT y el detalle de la prueba aplicable a la entidad a ser analizada.

| MATRIZ DE PRUEBAS<br>DOMINIO COBIT<br>Objetivo de Control General | | | |
|---|---|---|---|
| **#** | **OBJETIVOS DE CONTROL ESPECÍFICOS** | **REVISIÓN A TRAVÉS DE:** | **DESCRIPCIÓN DE LA PRUEBA** |
| | | | |

*Tabla 2.13 Matriz de Pruebas*
*Fuente: www.isaca.org*

Para obtener los resultados de las pruebas de los controles a auditar se propone la matriz "Evaluación de Control" (Tabla 2.14), en la que se amplía información sobre el detalle de la prueba realizada incluyendo: las personas entrevistadas, los resultados obtenidos, y en base a la evaluación de las pruebas propuestas por las "Guías de Auditoría de COBIT" obtener la evaluación final de los objetivos de control dando únicamente dos calificativos "Efectivo" o "Inefectivo" en la columna de referencia se indica el anexo en el que se encuentra la evidencia obtenida durante el trabajo de campo, en el caso de que la evaluación sea inefectiva proponemos una recomendación que se detalla en la Etapa 2: Emisión de Recomendaciones.

| EVALUACIÓN DE CONTROL<br>DOMINIO<br>Objetivo de Control General<br>Objetivo de Control Específico | | | | |
|---|---|---|---|---|
| **REVISION A TRAVES DE** | **DESCRIPCIÓN DE LA PRUEBA** | **EVALUACIÓN** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| | | | | |

*Tabla 2.14 Matriz de Evaluación de Control*
*Fuente: www.isaca.org*

Para la obtención de la evidencia de auditoría para los objetivos y sub-objetivos de control seleccionados para el presente trabajo se efectuaron propiamente las pruebas respectivas en función del "Cronograma de Auditoría", realizadas en conjunto con el personal técnico del ISP. Dichas pruebas se realizaron con la finalidad de evidenciar toda la información posible que permita emitir una opinión acerca de la eficiencia de los controles implantados para cada uno de los objetivos de control de COBIT a ser auditados. Las técnicas de auditoría informática utilizadas serán las sugeridas por las guías de auditoría de COBIT que incluyen la observación, las entrevistas y los Penetration Testing.

Para la etapa de evaluación de seguridad se considerará las Matrices de Evaluación de Control de cada uno de los objetivos de control específicos seleccionados en las Matrices de Pruebas de Auditoría.

Se revisará la información relacionada con las pruebas realizadas y su análisis será calificado como "EFECTIVO" cuando las pruebas demuestren el cumplimiento y logro de los objetivos de control propuestos; y será calificado como "INEFECTIVO" cuando no se logren los objetivos de control.

Posteriormente se mostrarán y analizarán las diferentes vulnerabilidades relacionadas a la evaluación realizada por las herramientas tecnológicas como parte del Penetration Testing.

Las Matrices de Evaluación de Control direccionarán a la sección 2.5 Emisión de Recomendaciones que servirán para completar esta etapa.

# CRONOGRAMA DE AUDITORIA

| | | por fecha de inicio de semana | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Abril - 05 | | | Mayo - 05 | | | | Junio - 05 | | | | |
| Actividades | | 11 | 18 | 25 | 2 | 9 | 16 | 23 | 6 | 13 | 20 | 27 | |
| ETAPA 1: EVALUACION DE LA SEGURIDAD DEL ISP | | | | | | | | | | | | | |
| 2.1 | Situación actual del ISP | | | | | | | | | | | | |
| 2.2 | Aplicación de Metodologías de Evaluación de Seguridades para el ISP | | | | | | | | | | | | |
| 2.2.1 | Evaluación de Parámetros de Configuración de equipos críticos (Dispositivos de Comunicación) | | | | | | | | | | | | |
| 2.2.2 | Evaluación de Parámetros de Configuración de equipos críticos (Servers) | | | | | | | | | | | | |
| 2.3 | Diagnóstico de Huecos y Vulnerabilidades de Seguridad - Aplicación de Test de Penetración | | | | | | | | | | | | |
| 2.3.1 | Aplicación de Nessus, NMAP | | | | | | | | | | | | |
| 2.3.2 | Aplicación de Retina y otros | | | | | | | | | | | | |
| 2.3.3 | Documentación de la evaluación | | | | | | | | | | | | |
| ETAPA 2: EMISION DE RECOMENDACIONES | | | | | | | | | | | | | |
| 2.4 | Análisis del Diagnóstico de Huecos y Vulnerabilidades de Seguridad | | | | | | | | | | | | |
| 2.5 | Recomendaciones de Seguridad | | | | | | | | | | | | |
| 2.6 | Documentación de Recomendaciones | | | | | | | | | | | | |

# CRONOGRAMA DE AUDITORIA (Continuación)

| | | por fecha de inicio de semana | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Abril - 05 | | | Mayo - 05 | | | | Junio - 05 | | | | |
| Actividades | | 11 | 18 | 25 | 2 | 9 | 16 | 23 | 6 | 13 | 20 | 27 | |
| ETAPA 3: IMPLANTACION DEL ESQUEMA DE SEGURIDAD DEL ISP | | | | | | | | | | | | | |
| 3.1 | Análisis de Requerimientos de Seguridad del ISP | | | | | | | | | | | | |
| 3.2 | Diseño del Esquema de Seguridad del ISP | | | | | | | | | | | | |
| 3.3 | Implantación del Esquema de Seguridad del ISP | | | | | | | | | | | | |
| 3.3.1 | Implantación de Recomendaciones | | | | | | | | | | | | |
| 3.4 | Pruebas de funcionamiento del Esquema de Seguridad del ISP | | | | | | | | | | | | |
| 3.5 | Afinamiento del Esquema de Seguridad | | | | | | | | | | | | |
| 3.5.1 | Documentación de la implantación | | | | | | | | | | | | |
| ETAPA 4: REEVALUACION DEL NIVEL DE RIESGO Y EXPOSICION | | | | | | | | | | | | | |
| 3.6 | Seguimiento a la implantación de las recomendaciones de Auditoría de Seguridades | | | | | | | | | | | | |
| 3.7 | Reevaluación del nivel de riesgo y exposición ante ataques al ISP | | | | | | | | | | | | |
| 3.7.1 | Aplicación de Nessus, NMAP | | | | | | | | | | | | |
| 3.7.2 | Aplicación de Retina y otros | | | | | | | | | | | | |
| 3.8 | Documentación de Reevaluación | | | | | | | | | | | | |

*Fig. 2.4 Cronograma de Auditoría*
*Fuente: Los Autores*

### 2.2.3.2 Programa de Auditoría Objetivos de Control con riesgo Alto

| **PROGRAMA DE AUDITORÍA**<br><br>**DOMINIO COBIT ENTREGA DE SERVICIOS Y SOPORTE**<br>**DS5: Garantizar la seguridad de los sistemas** | | |
|---|---|---|
| **OBJETIVOS DE CONTROL GENERAL** | **OBJETIVOS DE CONTROL ESPECÍFICOS DS5 COBIT** | **FACTOR DE RIESGO** |
| **Salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o perdida** | DS5.1 Administrar medidas de seguridad | • Violación de información sensible<br>• Incumplimientos con estándares de seguridad<br>• Afectación a la Integridad de Datos<br>• Altos costos<br>• Falta de políticas<br>• Falta de compromiso de usuarios<br>• Problemas de control de acceso<br>• Fuga de datos confidenciales<br>• Accesos no autorizados a la red y datos |
| | DS5.2 Identificación, autenticación y acceso lógico | |
| | DS5.3 Garantizar el control de la seguridad de acceso (permisos) | |
| | DS5.4 Administración de cuentas de usuario (emisión, suspensión y cierre) | |
| | DS5.5 Revisión gerencial de cuentas de usuario (dueños de la información) | |
| | DS5.6 Control de usuarios sobre cuentas de usuario (registro de actividades inusuales) | |
| | DS5.7 Registrar toda actividad de seguridad y cualquier indicación de una inminente violación a la seguridad (notificación y consecuencias) | |
| | DS5.8 Clasificación de datos por propietario mediante una decisión formal y explícita de acuerdo con el esquema de clasificación de datos definido por la Gerencia | |
| | DS5.9 Administración centralizada de los derechos de acceso de los usuarios, identidad del sistema y propiedad de los datos | |
| | DS5.11 Manejo de incidentes de seguridad | |

| **PROGRAMA DE AUDITORÍA**<br><br>**DOMINIO COBIT ENTREGA DE SERVICIOS Y SOPORTE**<br>**DS5: Garantizar la seguridad de los sistemas** | | |
|---|---|---|
| **OBJETIVOS DE CONTROL GENERAL** | **OBJETIVOS DE CONTROL ESPECÍFICOS DS5 COBIT** | **FACTOR DE RIESGO** |
| | DS5.16 Asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales seguros (protocolos, encriptación de datos) | • Pérdida de información<br>• Pérdidas económicas<br>• Ausencia de monitoreo |
| | DS5.19 Prevención, detección y corrección de software malicioso (virus) | |
| | DS5.20 Arquitectura de firewalls y conexión a redes públicas | |

*Tabla 2.15 Programa de Auditoría Objetivo de Control DS5*
*Fuente: Los Autores*

### 2.2.3.3 Programa de Auditoría Objetivos de Control con riesgo Medio

| **PROGRAMA DE AUDITORÍA**<br><br>**DOMINIO COBIT ADQUISICIÓN E IMPLEMENTACIÓN**<br>**AI3: Adquisición y mantenimiento de infraestructura tecnológica** | | |
|---|---|---|
| **OBJETIVOS DE CONTROL GENERAL** | **OBJETIVOS DE CONTROL ESPECÍFICOS AI3 COBIT** | **FACTOR DE RIESGO** |
| **Proporcionar las plataformas apropiadas para soportar las aplicaciones del negocio** | AI3.3 La gerencia de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse atención especial a la instalación y mantenimiento de los parámetros del software del sistema. | • Inadecuadas configuraciones de los sistemas operativos<br>• Ausencia de control de cambios de parámetros de configuraciones<br>• Ausencia de monitoreo a eventos de seguridad |

*Tabla 2.16 Programa de Auditoría Objetivo de Control AI3*
*Fuente: Los Autores*

# 2.3 DIAGNÓSTICO DE HUECOS Y VULNERABILIDADES DE SEGURIDAD

## 2.3.1 MATRICES DE PRUEBAS OBJETIVOS DE CONTROL CON RIESGO ALTO

| **MATRIZ DE PRUEBAS**<br>**DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE** | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.1 Administrar Medidas de Seguridad**<br><br>La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye:<br><br>• Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI;<br>• Implementar el plan de seguridad de TI;<br>• Actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI;<br>• Evaluar el impacto de las solicitudes de cambio en la seguridad de TI;<br>• Monitorear la implementación del plan de seguridad de TI; y<br>• Alinear los procedimientos de seguridad de TI a otras políticas y procedimientos | *Evaluación de controles:*<br><br>Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte<br><br>*Probando que:*<br><br>Los parámetros de seguridad del sistema tienen como base estándares locales/del proveedor | Solicitar documento de políticas de seguridad.<br><br>Entrevista al Gerente de TI.<br><br>Revisión del Plan de Contingencia. |

*Tabla 2.17 Matriz de Pruebas DS5.1*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.2 Identificación, Autenticación y Acceso**<br><br>El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso.<br><br>Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas por marcado 25 y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo.<br><br>Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords). | *Evaluación de controles:*<br><br>Se cuenta con perfiles de seguridad de usuario que representen “los menos accesos requeridos” y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.<br><br>Los mecanismos de autenticidad en uso proveen las siguientes facilidades:<br>• uso individual de datos de autenticación<br>• autentificación múltiple<br>• autenticación basada en políticas<br>• Autenticación por demanda<br><br>La política de password incluye:<br>• Forzar el cambio inicial de password la primera vez de uso<br>• longitud adecuada mínima del password<br>• la frecuencia obligada mínima de cambio de password<br>• verificación del password en la lista de valores no permitidos<br>• protección adecuada para los passwords de emergencia<br><br>Los procedimientos de marcación telefónica incluyen autenticación basada en token o dial-back, cambios frecuentes del número telefónico, firewalls de hardware y software para restringir el acceso a los activos y cambios frecuentes de las claves de acceso y desactivación de las claves de acceso de los empleados temporales. | Entrevista al Gerente de TI.<br><br>Correr herramienta que ayude a detectar problemas con claves y vulnerabilidades de seguridad en los servidores de aplicación. |

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.2 Identificación, Autenticación y Acceso *(Continuación)***<br><br>El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso.<br><br>Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas por marcado 25 y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo.<br><br>Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords). | *Probando que:*<br><br>TI cumple con los estándares de seguridad relacionados con:<br>• autenticación y acceso<br>• administración de perfiles de usuario y clasificación de la seguridad de datos<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema | |

*Tabla 2.18 Matriz de Pruebas DS5.2*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.3 Seguridad de Acceso a Datos en Líneas**<br><br>En un ambiente de tecnología de información en línea, la Gerencia de TI deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos. | *Evaluación de controles:*<br><br>Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de re-acreditación.<br><br>*Probando que:*<br><br>Accesos inapropiados por parte de los usuarios a los recursos del sistema. | Revisión de log's de aplicaciones del servidor. |

*Tabla 2.19 Matriz de Pruebas DS5.3*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.4 Administración de cuentas de usuario**<br><br>La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario.<br><br>Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.<br><br>La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación.<br><br>Los acuerdos de outsourcing deben considerar los riesgos, los controles sobre seguridad y los procedimientos para los sistemas de información y las redes en el contrato que se establece entre las partes. | *Evaluación de controles*:<br><br>El número de sesiones concurrentes correspondientes al mismo usuario están limitadas.<br><br>La política de password incluye:<br>Forzar el cambio inicial de password la primera vez de uso - longitud adecuada mínima del password sistemas –la frecuencia obligada mínima de cambio de password.<br>Verificación del password en la lista de valores no permitidos (Ej., verificación de diccionario).<br><br>Protección adecuada para los passwords de emergencia.<br><br>*Probando que:*<br>Cumple con los estándares de seguridad relacionados con:<br>- Autenticación de usuarios.<br>- Administración de perfiles de usuario y clasificación de la seguridad de datos.<br>- Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.<br>- Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad. | Revisión de Parámetros de Cuentas de Usuario.<br><br>Solicitar documento de políticas de seguridad.<br><br>Reporte de Languard.<br><br>Entrevista al Gerente de TI. |

*Tabla 2.20 Matriz de Pruebas DS5.4*

*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.5 Revisión Gerencial de Cuentas de Usuario**<br><br>La Gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.<br><br>Se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental. | *Evaluación de controles:*<br><br>Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.<br>Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.<br><br>Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir:<br>• intentos no autorizados de acceso al sistema (sign on)<br>• intentos no autorizados de acceso a los recursos del sistema<br>• privilegios de acceso a recursos por ID de usuario<br>• modificaciones autorizadas a las definiciones y reglas de seguridad<br>• accesos autorizados a los recursos<br>• cambio de estatus de la seguridad del sistema<br><br>*Probando que:*<br>TI cumple con los estándares de seguridad relacionados con reportes y revisión gerencial de las violaciones e incidentes de seguridad | Aplicación de las herramientas LANGUARD y RETINA. Ver Anexos E y F<br><br>Revisión de los archivos Log para revisión de accesos a los recursos. |

*Tabla 2.21 Matriz de Pruebas DS5.5*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.6 Control de Usuarios sobre Cuentas de Usuario**<br><br>Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta (s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales. | *Evaluación de controles:*<br><br>Al ingresar al sistema, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.<br><br>Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales.<br><br>Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario.<br><br>*Probando que*<br>TI cumple con los estándares de seguridad relacionados con la administración de perfiles de usuario y clasificación de la seguridad de datos<br><br>Existen procedimientos para el mantenimiento del acceso de usuarios al sistema<br><br>Existen procedimientos de “logon” vigentes para sistemas y usuarios | Entrevista al Gerente de TI.<br><br>Aplicar pruebas específicas sobre los controles de usuarios en el acceso a aplicaciones. |

*Tabla 2.22 Matriz de Pruebas DS5.6*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.7 Vigilancia de seguridad**<br><br>La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectados, tanto interna como externamente y se debe actuar de una manera oportuna. | *Evaluación de controles*:<br><br>Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas.<br>Estos reportes deberán incluir:<br>- Intentos no autorizados de acceso al sistema (sign on).<br>- Intentos no autorizados de acceso a los recursos del sistema.<br>- Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.<br>- Privilegios de acceso a recursos por ID de usuario.<br>- Modificaciones autorizadas a las definiciones y reglas de seguridad de TI.<br>- Accesos autorizados a los recursos (seleccionados por usuario o recurso).<br>- Cambio de estatus de la seguridad del sistema.<br>- Accesos a las tablas de parámetros de seguridad del sistema operativo.<br><br>*Probando que*:<br>TI cumple con los estándares de seguridad relacionados con: reportes y revisión gerencial de las violaciones e incidentes de seguridad. Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. | Revisión de manuales de procedimientos y plan de seguridad IT y de Logs de seguridad del sistema.<br><br>Entrevista al Gerente de TI. |

*Tabla 2.23 Matriz de Pruebas DS5.7*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.8 Clasificación de datos**<br><br>La Gerencia deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación de datos.<br><br>Aún los datos que "no requieren protección" deberán contar con una decisión formal que les asigne dicha clasificación.<br>Los dueños deben determinar la ubicación o disposición de sus datos y determinar quienes pueden compartir los datos aun si y cuando los programas y archivos sean mantenidos, archivados o borrados.<br><br>Debe quedar evidencia de la aprobación del dueño y de la disposición del dato. Se deben definir políticas para soportar la reclasificación de la información, basados sobre cambios en la sensitividad.<br><br>El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones. | *Evaluación de controles:*<br><br>Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.<br><br>*Probando que:*<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.<br><br>Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad.<br><br>El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante. | Revisión de manuales de procedimientos y funciones.<br><br>Entrevista al Gerente de TI. |

*Tabla 2.24 Matriz de Pruebas DS5.8*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.9 Administración de Derechos de Acceso e Identificación Centralizada**<br><br>Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control de acceso global. | *Evaluación de controles:*<br><br>Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.<br><br>*Probando que:*<br><br>T.I. cumple con los estándares de seguridad relacionados con:<br><br>- Administración de perfiles de usuario y clasificación de la seguridad de datos.<br>- Reportes y revisión gerencial de las violaciones e incidentes de seguridad.<br>- Clasificación y propiedad de datos<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema. | Revisión de documentos de soporte para creación de usuarios.<br><br>Entrevista al Gerente de TI.<br><br>Revisión de derechos de usuarios, grupos, perfiles creados en sistemas. |

*Tabla 2.25 Matriz de Pruebas DS5.9*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.11 Manejo de Incidentes**<br><br>La Gerencia deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras.<br><br>Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad. | *Evaluación de controles:*<br><br>Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte.<br><br>Se utilizan rutas confiables para transmitir información sensitiva.<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br>Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. | Revisión del plan de seguridad IT respecto del manejo de incidentes.<br><br>Entrevista al Gerente de TI. |

*Tabla 2.26 Matriz de Pruebas DS5.11*
*Fuente: Los Autores*

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.16 Sendero Seguro**<br><br>Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (*trusted paths*). La información sensitiva incluye información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas.<br><br>Para lograr esto, se pueden establecer canales confiables utilizando encripción entre usuarios, entre usuarios y sistemas y entre sistemas. | *Evaluación de controles:*<br><br>Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión.<br><br>El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas se limita a la base de la “necesidad de conocer”.<br><br>Se utilizan rutas confiables para transmitir información sensitiva no encriptada.<br><br>*Probando que:*<br><br>T.I. cumple con los estándares de seguridad relacionados con:<br><br>- Autenticación y acceso<br>- Estándares de administración de llaves criptográficas<br><br>Existen llaves secretas para la transmisión. | Entrevista al Gerente de TI.<br><br>Recopilar información sobre las transacciones sensitivas que se realicen. |

*Tabla 2.27 Matriz de Pruebas DS5.16*
*Fuente: Los Autores*

| **MATRIZ DE PRUEBAS**<br><br>**DOMINIO: ENTREGA DE SERVICIO Y SOPORTE** | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.19 Prevención, detección y corrección de software malicioso**<br><br>Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas y responder y reportar su presencia.<br><br>Las Gerencias de TI y de negocios deben asegurar que se establezcan procedimientos a través de toda la organización para proteger los sistemas de información contra virus computacionales.<br><br>Los procedimientos deben incorporar protección contra virus, detección, respuesta ante su presencia y reporte. | *Evaluación de controles:*<br><br>El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br><br>Los procedimientos para la protección contra software malicioso incluyen:<br><br>• todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso.<br><br>• existe una política por escrito sobre descargue de archivos, aceptación y uso de software, freeware y shareware y esta política está vigente. | Revisión de manuales de manejo y uso de los recursos de TI para los empleados.<br><br>Revisión de software antivirus instalado en servidores y estaciones de trabajo. |

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | |
|---|---|---|
| *DS5 Garantizar la seguridad de Sistemas* | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.19 Prevención, detección y corrección de software malicioso** | • el software para aplicaciones altamente sensibles está protegido por MAC (Messsage Authentication Code- Código de Autentificación de Mensajes) o firma digital, y se utilizan mecanismos, fallas de verificación para evitar el uso del software.<br><br>• los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos.<br><br>• existe una política y un procedimiento vigente para la verificación de disquetes obtenidos por fuera del programa de compra normal de la organización. | |

*Tabla 2.28Matriz de Pruebas DS5.19*
*Fuente: Los Autores*

| **MATRIZ DE PRUEBAS**<br><br>**DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE** | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **DS5.20 Arquitectura de Firewalls y conexión a redes públicas**<br><br>La organización deberá contar con *Firewall* adecuados para proteger contra negación de servicios y cualquier acceso no autorizado a los recursos internos si existe conexión con Internet u otras redes públicas, se deberá controlar en ambos sentidos cualquier aplicación y el flujo de administración de infraestructura y se deberá proteger contra ataques de negación del servicio. | *Evaluación de controles:*<br><br>El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la "necesidad de conocer".<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br><br>Los firewalls poseen por lo menos las siguientes propiedades:<br><br>- Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles lógicos, debe reforzarse físicamente).<br>- Sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local.<br>- Los firewalls por sí mismo es inmune a la penetración.<br>- El tráfico de intercambio en el firewall se lleva a cabo en la capa de aplicación únicamente.<br>- La arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación.<br>- La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte. | Entrevista al Gerente de T.I.<br><br>Aplicar una herramienta para detectar las vulnerabilidades de la red.<br><br>Identificar la existencia de un Firewall y sus reglas definidas actualmente.<br><br>Evaluar la arquitectura de seguridad del Firewall para el ISP. |

| MATRIZ DE PRUEBAS<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | |
|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| | - La arquitectura del firewall debe estar configurada de acuerdo a la “filosofía de arte mínimo”.<br>- La arquitectura del firewall debe desplegar sólida autenticación para la administración y sus componentes.<br>- La arquitectura del firewall oculta la estructura de la red interna.<br>- La arquitectura del firewall provee una auditoria de todas las comunicaciones hacia o a través del sistema del firewall y activara alarmas cuando se detecte alguna actividad sospechosa.<br>- El host de la organización, que provee el soporte para las solicitudes de entrada al servicio e las redes públicas, permanece fuera del firewall.<br>- La arquitectura del firewall se defiende de los ataques directos (ej. A través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico).<br>- Todo código ejecutable se explora en busca de códigos maliciosos (ej. virus, applets dañinos) antes de introducirse. | |

*Tabla 2.29 Matriz de Pruebas DS5.20*
*Fuente: Los Autores*

## 2.3.2 MATRICES DE PRUEBAS OBJETIVOS DE CONTROL CON RIESGO MEDIO

| **MATRIZ DE PRUEBAS**<br><br>**DOMINIO: ADQUISICION E IMPLEMENTACION** | | |
|---|---|---|
| ***AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica*** | | |
| **OBJETIVO DE CONTROL ESPECIFICO** | **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** |
| **AI3.3 Seguridad de Software del sistema**<br><br>La Gerencia de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo.<br><br>Deberá prestarse gran atención a la instalación y mantenimiento de los parámetros del software del sistema. | *Evaluación de controles:*<br><br>Existen políticas y procedimientos que aseguran que:<br>- la posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de información operativa está limitada<br>- la preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema.<br>- se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema.<br><br>*Probando que:*<br>Existen las declaraciones de aseguramiento de la integridad del software del sistema entregados por los proveedores para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema.<br><br>Los parámetros del software del sistema aseguran que el personal apropiado de TI seleccionó los correctos con el fin de asegurar la integridad de los datos y los programas almacenados en el sistema. | Revisión de parámetros de seguridad de los sistemas operativos, bases de datos en servidores principales y revisión de la aplicación de Facturación. |

*Tabla 2.30 Matriz de Pruebas Objetivo de Control A13*

*Fuente: Los Autores*

## 2.3.3 EVALUACION DE PRUEBAS DE OBJETIVOS DE CONTROL CON RIESGO ALTO

| **EVALUACION DE CONTROL**<br><br>**DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE** | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.1 Administrar Medidas de Seguridad** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte<br><br>*Probando que:*<br><br>Los parámetros de seguridad del sistema tienen como base estándares locales/del proveedor. | Solicitar documento de políticas de seguridad.<br><br>Entrevista al Gerente de TI.<br><br>Revisión del Plan de Contingencia. | NO EFECTIVO | Plan de Contingencia. | Ver **Recomendación DS5.1** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.31 Evaluación de Pruebas DS5.1*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.2 Identificación, Autenticación y Acceso** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Se cuenta con perfiles de seguridad de usuario que representen “los menos accesos requeridos” y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.<br>Los mecanismos de autenticidad en uso proveen las siguientes facilidades:<br>• uso individual de datos de autenticación<br>• autentificación múltiple<br>• autenticación basada en políticas<br>• Autenticación por demanda<br><br>La política de password incluye:<br>• Forzar el cambio inicial de password la primera vez de uso<br>• longitud adecuada mínima del password<br>• la frecuencia obligada mínima de cambio de password<br>• verificación del password en la lista de valores no permitidos<br>• protección adecuada para los passwords de emergencia | Entrevista al Gerente de TI.<br><br>Correr herramienta que ayude a detectar problemas con claves y vulnerabilidades de seguridad en los servidores de aplicación. | NO EFECTIVO | Reporte emitido por software Languard y Retina.<br><br>Ver Anexos E y F | Ver **Recomendación DS5.2** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.2 Identificación, Autenticación y Acceso** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| Los procedimientos de marcación telefónica incluyen autenticación basada en token o dial-back, cambios frecuentes del número telefónico, firewalls de hardware y software para restringir el acceso a los activos y cambios frecuentes de las claves de acceso y desactivación de las claves de acceso de los empleados temporales<br><br>*Probando que:*<br><br>TI cumple con los estándares de seguridad relacionados con:<br>• autenticación y acceso<br>• administración de perfiles de usuario y clasificación de la seguridad de datos<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema | | NO EFECTIVO | | |

*Tabla 2.32 Evaluación de Pruebas DS5.2*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.3 Seguridad de Acceso a Datos en Líneas** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de re-acreditación.<br><br>*Probando que:*<br><br>Accesos inapropiados por parte de los usuarios a los recursos del sistema. | Revisión de log's de aplicaciones del servidor. | EFECTIVO | | |

*Tabla 2.33 Evaluación de Pruebas DS5.3*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.4 Administración de cuentas de usuario** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles*:<br>El número de sesiones concurrentes correspondientes al mismo usuario están limitadas.<br><br>La política de password incluye:<br>- Forzar el cambio inicial de password en el primer uso – longitud mínima de password -frecuencia obligada de cambio de password.<br>- Verificación del password en la lista de valores no permitidos (Ej., verificación de diccionario).<br>- Protección adecuada de passwords de emergencia.<br><br>*Probando que:*<br>IT cumple con los estándares de seguridad en:<br>- Autenticación de usuarios.<br>- Administración de perfiles de usuario y clasificación de la seguridad de datos.<br>- Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.<br>- Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad. | Revisión de Parámetros de Cuentas de Usuario.<br><br>Solicitar documento de políticas de seguridad.<br><br>Reporte de Languard.<br><br>Entrevista al Gerente de TI. | EFECTIVO | Solicitudes de creación de usuarios en diferentes sistemas.<br><br>Documentos de entrega de claves para usuarios. | |

*Tabla 2.34 Evaluación de Pruebas DS5.4*

*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.5 Revisión Gerencial de Cuentas de Usuario** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br>Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.<br>Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.<br>Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir:<br>• intentos no autorizados de acceso al sistema (sign on)<br>• intentos no autorizados de acceso a los recursos del sistema<br>• privilegios de acceso a recursos por ID de usuario<br>• modificaciones autorizadas a las definiciones y reglas de seguridad<br>• accesos autorizados a los recursos<br><br>*Probando que:*<br>TI cumple con los estándares de seguridad relacionados con reportes y revisión gerencial de las violaciones e incidentes de seguridad. | Aplicación de las herramientas LANGUARD y RETINA.<br><br>Revisión de los archivos Log para revisión de accesos a los recursos. | NO EFECTIVO | Reporte de LANGUARD y RETINA<br>Ver Anexos E y F. | Ver **Recomendación DS5.5** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.35 Evaluación de Pruebas DS5.5*

*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.6 Control de Usuarios sobre Cuentas de Usuario** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Al ingresar al sistema, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.<br><br>Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales.<br><br>Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario.<br><br>*Probando que:*<br>TI cumple con los estándares de seguridad relacionados con la administración de perfiles de usuario y clasificación de la seguridad de datos<br><br>Existen procedimientos para el mantenimiento del acceso de usuarios al sistema y existen procedimientos de “logon” vigentes para sistemas y usuarios. | Entrevista al Gerente de TI.<br><br>Aplicar pruebas específicas sobre los controles de usuarios en el acceso a aplicaciones. | NO EFECTIVO | Pantallas de acceso a aplicaciones | Ver **Recomendación DS5.6** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.36 Evaluación de Pruebas DS5.6*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.7 Vigilancia de seguridad** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles*:<br>Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas.<br><br>Estos reportes deberán incluir:<br>- Intentos no autorizados de acceso al sistema (sign on).<br>- Intentos no autorizados de acceso a los recursos del sistema.<br>- Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.<br>- Privilegios de acceso a recursos por ID de usuario.<br>- Modificaciones autorizadas a las definiciones y reglas de seguridad de TI.<br>- Accesos autorizados a los recursos (seleccionados por usuario o recurso).<br>- Cambio de estatus de la seguridad del sistema.<br>- Accesos a las tablas de parámetros de seguridad del sistema operativo.<br><br>*Probando que*:<br>TI cumple con los estándares de seguridad relacionados con: reportes y revisión gerencial de las violaciones e incidentes de seguridad. Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. | Revisión de manuales de procedimientos y plan de seguridad IT y de Logs de seguridad del sistema.<br><br>Entrevista al Gerente de TI. | NO EFECTIVO | Manuales de procedimientos existentes. | Ver **Recomendación DS5.7** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.37 Evaluación de Pruebas DS5.7*

*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.8 Clasificación de datos** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.<br><br>*Probando que:*<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.<br><br>Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad.<br><br>El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante. | Revisión de manuales de procedimientos y funciones.<br><br>Entrevista al Gerente de TI. | NO EFECTIVO | | Ver **Recomendación DS5.8** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.38 Evaluación de Pruebas DS5.8*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.9 Administración de Derechos de Acceso e Identificación Centralizada** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.<br><br>*Probando que:*<br><br>T.I. cumple con los estándares de seguridad relacionados con:<br><br>- Administración de perfiles de usuario y clasificación de la seguridad de datos.<br>- Reportes y revisión gerencial de las violaciones e incidentes de seguridad.<br>- Clasificación y propiedad de datos<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema. | Revisión de documentos de soporte para creación de usuarios.<br><br>Entrevista al Gerente de T.I.<br><br>Revisión de derechos de usuarios, grupos, perfiles creados en sistemas. | EFECTIVO | Documentos de respaldo sobre solicitudes de creación de usuarios, documentos de entrega de identificación de usuarios y passwords. | |

*Tabla 2.39 Evaluación de Pruebas DS5.9*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.11 Manejo de Incidentes** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte.<br><br>Se utilizan rutas confiables para transmitir información sensitiva.<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br><br>Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. | Revisión del plan de seguridad IT respecto del manejo de incidentes.<br><br>Entrevista al Gerente de TI. | NO EFECTIVO | | Ver **Recomendación DS5.11** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.40 Evaluación de Pruebas DS5.11*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.16 Sendero Seguro** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión.<br><br>El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas se limita a la base de la "necesidad de conocer".<br><br>Se utilizan rutas confiables para transmitir información sensitiva no encriptada.<br><br>*Probando que:*<br>T.I. cumple con los estándares de seguridad relacionados con:<br>- Autenticación y acceso<br>- Estándares de administración de llaves criptográficas<br><br>Existen llaves secretas para la transmisión. | Entrevista al Gerente de TI.<br><br>Recopilar información sobre las transacciones sensitivas que se realicen. | EFECTIVO | Pruebas de conexión a información sensible a través de https:// | |

*Tabla 2.41 Evaluación de Pruebas DS5.16*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.19 Prevención, detección y corrección de software malicioso** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br><br>Los procedimientos para la protección contra software malicioso incluyen:<br><br>– Todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso.<br><br>– Existe una política por escrito sobre descargue de archivos, aceptación y uso de software, freeware y shareware y esta política está vigente.<br><br>- El software para aplicaciones altamente sensibles está protegido por MAC (Messsage Authentication Code-Código de Autentificación de Mensajes) o firma digital, y se utilizan mecanismos, fallas de verificación para evitar | Revisión de manuales de manejo y uso de los recursos de TI para los empleados.<br><br>Revisión de software antivirus instalado en servidores y estaciones de trabajo. | EFECTIVO | Documento de Políticas de TI. | |

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | | | |
|---|---|---|---|---|
| *DS5 Garantizar la seguridad de Sistemas* | | | | |
| **DS5.19 Prevención, detección y corrección de software malicioso** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| el uso del software.<br><br>- Los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos.<br><br>- Existe una política y un procedimiento vigente para la verificación de disquetes obtenidos por fuera del programa de compra normal de la organización. | | | | |

*Tabla 2.42 Evaluación de Pruebas DS5.19*
*Fuente: Los Autores*

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.20 Arquitectura de Firewalls y conexión a redes públicas** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br><br>El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la "necesidad de conocer".<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br>Los firewalls poseen por lo menos las siguientes propiedades:<br>- Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles lógicos, debe reforzarse físicamente).<br>- Sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local.<br>- Los firewalls por sí mismo es inmune a la penetración.<br>- El tráfico de intercambio en el firewall se lleva a cabo en la capa de aplicación únicamente. | Entrevista al Gerente de T.I.<br><br>Aplicar una herramienta para detectar las vulnerabilidades de la red.<br><br>Identificar la existencia de un Firewall y sus reglas definidas actualmente.<br><br>Evaluar la arquitectura de seguridad del Firewall para el ISP. | NO EFECTIVO | Vulnerabilidades del Firewall y Reportes de Nessus en la red.<br><br>Ver Información Adicional de Soporte en CD – Reportes Nessus. | Ver **Recomendación DS5.20** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

| EVALUACION DE CONTROL<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.20 Arquitectura de Firewalls y conexión a redes públicas** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| - La arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación.<br>- La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte.<br>- La arquitectura del firewall debe estar configurada de acuerdo a la "filosofía de arte mínimo".<br>- La arquitectura del firewall debe desplegar sólida autenticación para la administración y sus componentes.<br>- La arquitectura del firewall oculta la estructura de la red interna.<br>- La arquitectura del firewall provee una auditoria de todas las comunicaciones hacia o a través del sistema del firewall y activará alarmas cuando se detecte alguna actividad sospechosa.<br>- El host de la organización, que provee el soporte para las solicitudes de entrada al servicio e las redes públicas, permanece fuera del firewall.<br>- La arquitectura del firewall se defiende de los ataques directos (ej. A través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico).<br>- Todo código ejecutable se explora en busca de códigos maliciosos (ej. virus, applets dañinos) antes de introducirse. | | | | |

*Tabla 2.43 Evaluación de Pruebas DS5.20*

*Fuente: Los Autores*

## 2.3.4 EVALUACION DE PRUEBAS DE OBJETIVOS DE CONTROL CON RIESGO MEDIO

| **EVALUACION DE CONTROL**<br>**DOMINIO: ADQUISICION E IMPLEMENTACION** | | | | |
|---|---|---|---|---|
| ***AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica*** | | | | |
| **AI3.3 Seguridad de Software del sistema** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **DOCUMENTOS DE SOPORTE** | **RECOMENDACIÓN** |
| *Evaluación de controles:*<br>Existen políticas y procedimientos asegurando que:<br>- la posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de información operativa está limitada<br>- la preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados.<br>- se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema.<br><br>*Probando que:*<br>Existen las declaraciones de aseguramiento de la integridad del software del sistema entregados por los proveedores para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema.<br><br>Los parámetros del software del sistema aseguran que el personal apropiado de TI seleccionó los correctos con el fin de asegurar la integridad de los datos y los programas almacenados en el sistema. | Revisión de parámetros de seguridad de los sistemas operativos, bases de datos en servidores principales y revisión de la aplicación de Facturación. | NO EFECTIVO | | Ver **Recomendación AI3.3** en sección 2.5.1 **RECOMENDACIO-NES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** |

*Tabla 2.44 Evaluación de Pruebas DS5.1*
*Fuente: Los Autores*

### 2.3.5 UTILIZACION DE PENETRATION TESTING PARA IDENTIFICACION DE VULNERABILIDADES

Para realizar el análisis de las vulnerabilidades de los distintos sistemas operativos y servicios de red del ISP, esta Tesis se apoyó en las algunas de las mejores prácticas y herramientas que cumplen con los estándares ISO17799[15], SANS[16], NIST[17], ITIL[18], orientados al descubrimiento de la red, escaneadores de puertos y escaneadores de vulnerabilidades, como los siguientes:

- WS Ping ProPack
- Sniffer Pro - NAI
- Nmap
- Nessus
- Microsoft Baseline Security Analyzer
- Retina Network Security Scanner
- LANguard Network Security Scanner

#### 2.3.5.1 WS Ping ProPack

Es un conjunto de herramientas para descubrimiento de información de red. Incluye ping, tracertoute, data troughput, dns lookup, whois, finger, SNMP, Navegación a través de Dominios Windows y herramientas de navegación LDAP.

#### 2.3.5.2 Sniffer Pro - NAI

Es el mejor analizador de red del mercado (Network Associates INC.) que permite realizar ataques pasivos en la red para descubrir todo el tráfico que esté en ese momento pasando por la red. Sirve para redes LAN y WAN. A la vez es una herramienta para gestión de la red.

---

[15] ISO 17799 - Estándar Internacional de Gestión de Seguridad de la Información.
[16] SANS - SysAdmin, audit., Network, Security Institute
[17] NIST – National Institute of Standards and Technology
[18] ITIL – IT Infrastructure Library

#### 2.3.5.3 Nmap

Es una poderosa herramienta para escanear puertos e identifica dispositivos de red, sistemas operativos y potenciales vulnerabilidades. Existe en versiones Windows y Unix.

#### 2.3.5.4 Nessus

Es el mejor escaneador de vulnerabilidades de código abierto que permite personalizar los puertos y servicios a ser escaneados. Genera reportes de vulnerabilidades detallados con sus recomendaciones para solucionarlas y cubre las plataformas Windows, Linux, AIX, AS/400, Netware, CISCO, Checkpoint, entre las principales.

#### 2.3.5.5 Microsoft Baseline Security Analyzer (MBSA)

Es un producto de Microsoft que analiza las vulnerabilidades de cada computadora. MBSA examina las computadoras que están corriendo Microsoft Windows Server 2003, Windows XP, Windows 2000, o Windows NT 4.0. Se deben tener privilegios de administrador para que se examine el computador o si se va a examinar de manera remota a un grupo de equipos se lo debe hacer como administrador del Dominio.

#### 2.3.5.6 Retina Network Security Scanner

Este producto es ideal para un administrador de red Windows ya que identifica vulnerabilidades, puertos abiertos, cuentas de usuario, recursos compartidos y servicios levantados, esta herramienta permite realizar un análisis avanzado de seguridades. Identifica el nivel de riesgo de las vulnerabilidades encontradas y emite las respectivas medidas correctivas

#### 2.3.5.7 LANguard Network Security Scanner

Similar al Retina identifica vulnerabilidades, puertos abiertos, cuentas de usuario, recursos compartidos, hot fix y patches implantados. Permite obtener información detallada de las diferentes unidades de disco y un reporte global de cada una de las cuentas de usuario del Active Directory en ambientes Windows.

## 2.3.6 VULNERABILIDADES OBTENIDAS

### 2.3.6.1 Período de pruebas

Se realizaron pruebas iniciales independientes en un ambiente de pruebas en las siguientes fechas: 5, 6, 12, 14 y 24 de Abril del 2005.

Estas pruebas se realizaron en horario nocturno a fin de no comprometer ningún servicio de Punto Net.

Posteriormente, una vez identificado que no existían riesgos de afectar la disponibilidad de los elementos críticos se realizó una prueba integral el 4 de Mayo del 2005.

### 2.3.6.2 Resultados de pruebas

En la evaluación inicial de huecos y vulnerabilidades de seguridad realizada sobre 16 equipos críticos de la red global de Punto Net, utilizado el Nessus, identificamos que:

**Existen 47 debilidades de nivel alto de seguridad**
**Existen 188 debilidades de nivel medio de seguridad**
**Existen 273 debilidades de nivel bajo de seguridad**

Correspondiente a los siguientes equipos:

| Dirección IP | Descripción | Vulnerabilidades |
|---|---|---|
| 200.105.225.1 | Access Server1 Cisco 3640 | (**Existen 8 debilidades de nivel medio de seguridad**) |
| 200.105.225.2 | DNS Primario /Linux | (**Existen 3 debilidades de nivel alto de seguridad**) |
| 200.105.225.4 | Autent., DNS Secund/WIN2K | (**Existen 3 debilidades de nivel alto de seguridad**) |
| 200.105.225.5 | Border Router Cisco 7206 | (**Existen 9 debilidades de nivel medio de seguridad**) |
| 200.105.225.6 | Servidor Monitoreo/WIN2K | (**Existen 5 debilidades de nivel alto de seguridad**) |
| 200.105.225.7 | Access Server2 Cisco 2511 | (**Existen 10 debilidades de nivel medio de seguridad**) |
| 200.105.225.8 | Access Server3 Cisco 2511 | (**Existen 10 debilidades de nivel medio de seguridad**) |
| 200.105.225.9 | Access Server4 Cisco AS5300 | (**Existen 3 debilidades de nivel medio de seguridad**) |

| Dirección IP | Descripción | Vulnerabilidades |
|---|---|---|
| 200.105.225.10 | Router1 Cisco AS3620 | (**Existen 8 debilidades de nivel medio de seguridad**) |
| 200.105.225.11 | Web Server /WIN2K | (**Existen 4 debilidades de nivel alto de seguridad**) |
| 200.105.225.14 | Web Server /Linux | (**Existen 29 debilidades de nivel alto de seguridad**) |
| 200.105.225.17 | Access Server5 Cisco AS5300 | (**Existen 5 debilidades de nivel medio de seguridad**) |
| 200.105.225.18 | Access Server8 Cisco AS3640 | (**Existen 8 debilidades de nivel medio de seguridad**) |
| 200.105.225.19 | Access Server6 Cisco AS5300 | (**Existen 5 debilidades de nivel medio de seguridad**) |
| 200.105.225.22 | Caché Server – Cisco CE590 | (**Existen 3 debilidades de nivel alto de seguridad**) |
| 200.105.225.23 | Access Server7 Cisco AS5300 | (**Existe 1 debilidad de nivel medio de seguridad**) |

*Tabla 2.45 Resultados iniciales de vulnerabilidades*
*Fuente: Los Autores*

Ver información adicional de soporte en CD – Reporte Nessus

Por otro lado identificamos las siguientes debilidades de seguridad en la red interna y en el Sistema de Facturación de Punto Net:

***RED INTERNA DE PUNTO NET:***

En la red actual de punto net, encontramos las siguientes debilidades de seguridad:

- No existe ninguna política de seguridad para accesos de red. Si bien existe un servidor con Windows 2000 central que además da soporte al Sistema de Facturación, no tiene activado Active Directory con políticas de seguridad para control de accesos en red desde las estaciones de trabajo hacia este servidor y sus recursos.

- Adicionalmente, las claves no cuentan con un adecuado esquema de seguridad en red que les provea de confidencialidad a los usuarios, pues no tienen definidos elementos de control como bloqueo por intentos fallidos en inicios de sesión, caducidad para un intervalo de tiempo, registro de contraseñas anteriores y longitud de clave, entre los principales.

- No posee mecanismos de Auditoría sobre el Sistema Operativo, tampoco sobre archivos y objetos.

- Los recursos compartidos en algunos casos tienen los permisos de compartición “Acceso Total” para todos los usuarios.

***SISTEMA DE FACTURACION:***

El actual sistema de facturación que utiliza Punto Net se encuentra desarrollado en Visual Basic 6.0 como front-end y SQL Server 7.0 como back-end. En este sistema encontramos las siguientes debilidades de seguridad:

- Las claves no cuentan con un adecuado esquema de seguridad en red que les provea de confidencialidad a los usuarios, pues no tienen definidos elementos de control como bloqueo por intentos fallidos en inicios de sesión, caducidad para un intervalo de tiempo, registro de contraseñas anteriores y longitud de clave, entre los principales.

- La base de datos no tiene activada la opción de Auditoría que permita identificar accesos fuera de la aplicación por parte del operador/administrador.

- La cuenta de administrador de la base de datos “sa” no tiene password.

- Si bien el sistema contempla la utilización de auditoría sobre planes, activaciones y promociones, no existe un mecanismo de reporte proactivo ante cambios en el sistema. De lo que nos informaron, sólo revisan los logs de auditoría las áreas usuarias a fines de mes y como parte del proceso de prefacturación, existiendo el riesgo de que existan cambios durante el mes que no sean detectados.

Finalmente, al realizar el análisis de las vulnerabilidades de los sistemas operativos y los servicios de red que están presentes en la red Windows se determina las siguientes vulnerabilidades a nivel general en la tabla 2.46 y a continuación se lo detalla por cada una de las plataformas.

Apoyados por las herramientas de análisis Languard y Retina, se pudo identificar problemas en la plataforma Microsoft que se utiliza en la red.

| Problema | Windows 9.X | Windows 2000 Server | Windows 2003 Server | Windows 2000 Professional | Windows XP Professional | Total equipos con problemas | Porcentaje |
|---|---|---|---|---|---|---|---|
| **Total de equipos** | **6** | **2** | **2** | **15** | **22** | | |
| LSASS | 6 | 2 | 2 | 14 | 18 | 42 | 89 % |
| Sesión Nula | 6 | 2 | 0 | 0 | 0 | 8 | 17 % |
| Agente de Antivirus | 3 | 0 | 0 | 0 | 0 | 3 | 6 % |
| FAT 32 | 6 | 0 | 0 | 0 | 0 | 6 | 13 % |
| Internet Explorer | 3 | 1 | 1 | 13 | 10 | 28 | 60 % |
| Regedit: LanMan | 0 | 0 | 0 | 0 | 11 | 11 | 23 % |
| Servicio de terminal Service | 0 | 0 | 2 | 0 | 6 | 8 | 17 % |
| El calendarizador de tareas de Windows | 0 | 0 | 2 | 6 | 18 | 26 | 55 % |
| **Porcentaje total de equipos con vulnerabilidades en los sistemas operativos** | | | | | | | **35 %** |
| **Servicios** | | | | | | | |
| Servicio WINS | 0 | 2 | 2 | 15 | 22 | 41 | 87 % |
| Servicio de mensajería de Windows | 0 | 0 | 1 | 8 | 12 | 21 | 45 % |
| Servicio Rpc: DCOM Habilitado | 1 | 0 | 1 | 9 | 14 | 25 | 53 % |
| Netbios: Wins puede permitir ejecutar código | 3 | 2 | 2 | 11 | 19 | 37 | 79 % |
| Servicio SNMP | 0 | 0 | 1 | 17 | 18 | 36 | 77 % |
| **Porcentaje total de equipos con vulnerabilidades en los servicios de red** | | | | | | | **68 %** |
| **Puertos Abiertos** | | | | | | | |
| TCP 21 FTP | 0 | 2 | 1 | 3 | 0 | 6 | 13 % |
| TCP 25 SMTP | 0 | 2 | 2 | 13 | 17 | 34 | 72 % |
| TCP 110 POP3 | 0 | 2 | 2 | 13 | 17 | 34 | 72 % |
| TCP 135 EPMAP | 0 | 0 | 0 | 11 | 0 | 11 | 23 % |
| **Porcentaje total de equipos con vulnerabilidades en puertos abiertos** | | | | | | | **45 %** |

| Problema | Windows 9.X | Windows 2000 Server | Windows 2003 Server | Windows 2000 Professional | Windows XP Professional | Total equipos con problemas | Porcentaje |
|---|---|---|---|---|---|---|---|
| **Total de equipos** | **6** | **2** | **2** | **15** | **22** | | |
| **Recursos compartidos preestablecidos** | | | | | | | |
| ADMIN$ | 6 | 2 | 2 | 15 | 22 | 47 | 100 % |
| C$ | 6 | 2 | 2 | 15 | 22 | 47 | 100 % |
| **Porcentaje total de equipos con vulnerabilidades en recursos compartidos preestablecidos** | | | | | | | **100%** |
| **Porcentaje total de equipos con vulnerabilidades** | | | | | | | **62 %** |

*Tabla 2.46 Vulnerabilidades en la plataforma Microsoft*
*Fuente: Los Autores*

Ver Detalle de Vulnerabilidades Plataforma Microsoft. Reportes de Vulnerabilidades de Languard y Retina – Anexos E y F.

# ETAPA 2: EMISION DE RECOMENDACIONES

## 2.4 ANÁLISIS DEL DIAGNÓSTICO DE HUECOS Y VULNERABILIDADES DE SEGURIDAD

Al realizar el análisis del Diagnóstico de huecos y vulnerabilidades de Seguridad, identificamos el siguiente nivel de exposición y riesgos de seguridad inicial del ISP:

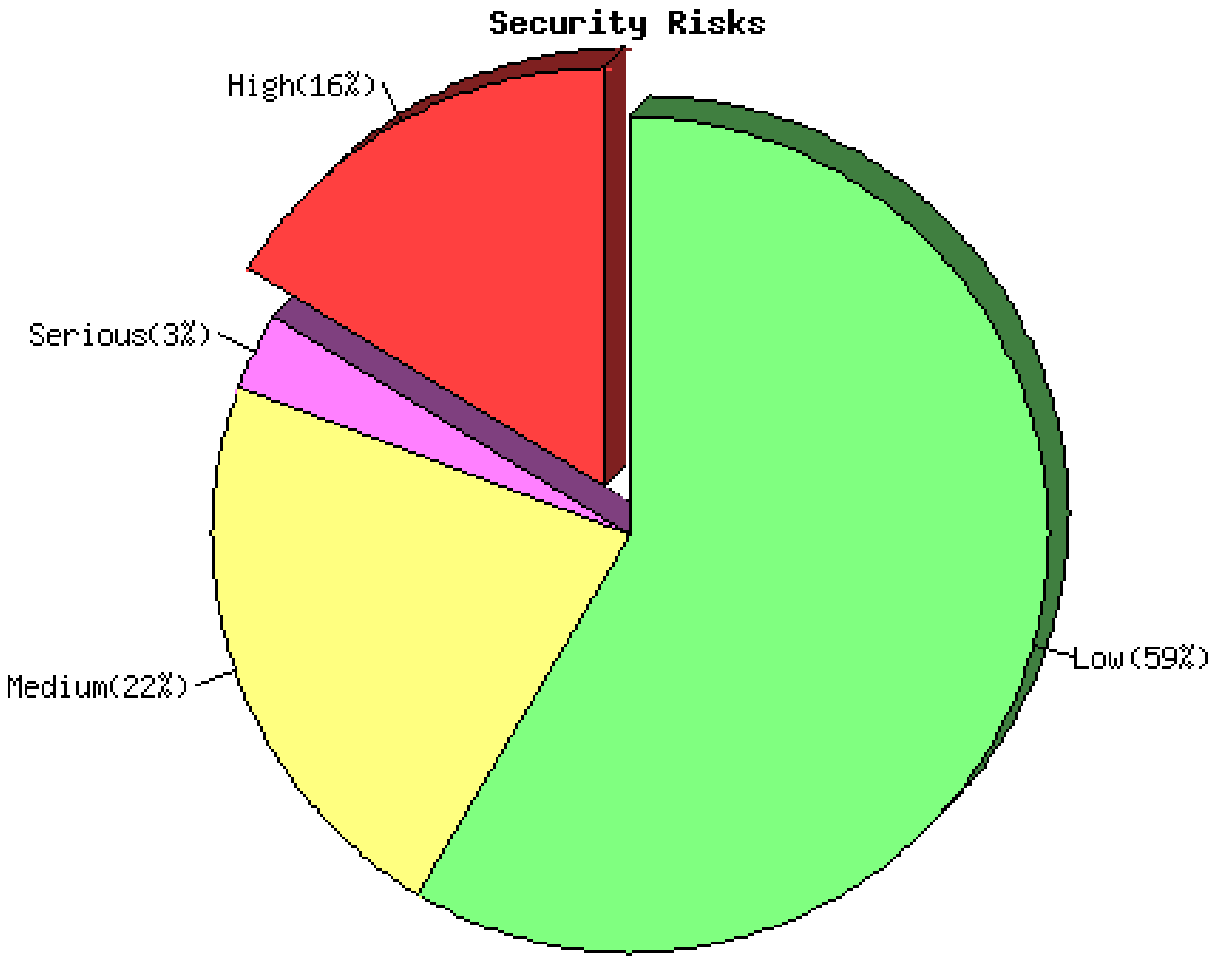



*Fig. 2.5 Nivel de exposición y riesgos de seguridad inicial del ISP*
*Fuente: Diagnóstico inicial de vulnerabilidades con NESSUS*

De la globalidad (16 elementos críticos evaluados), identificamos que el Servidor Web sobre Linux es el que posee mayor cantidad de vulnerabilidades. Ver en página siguiente Fig. 2.6.

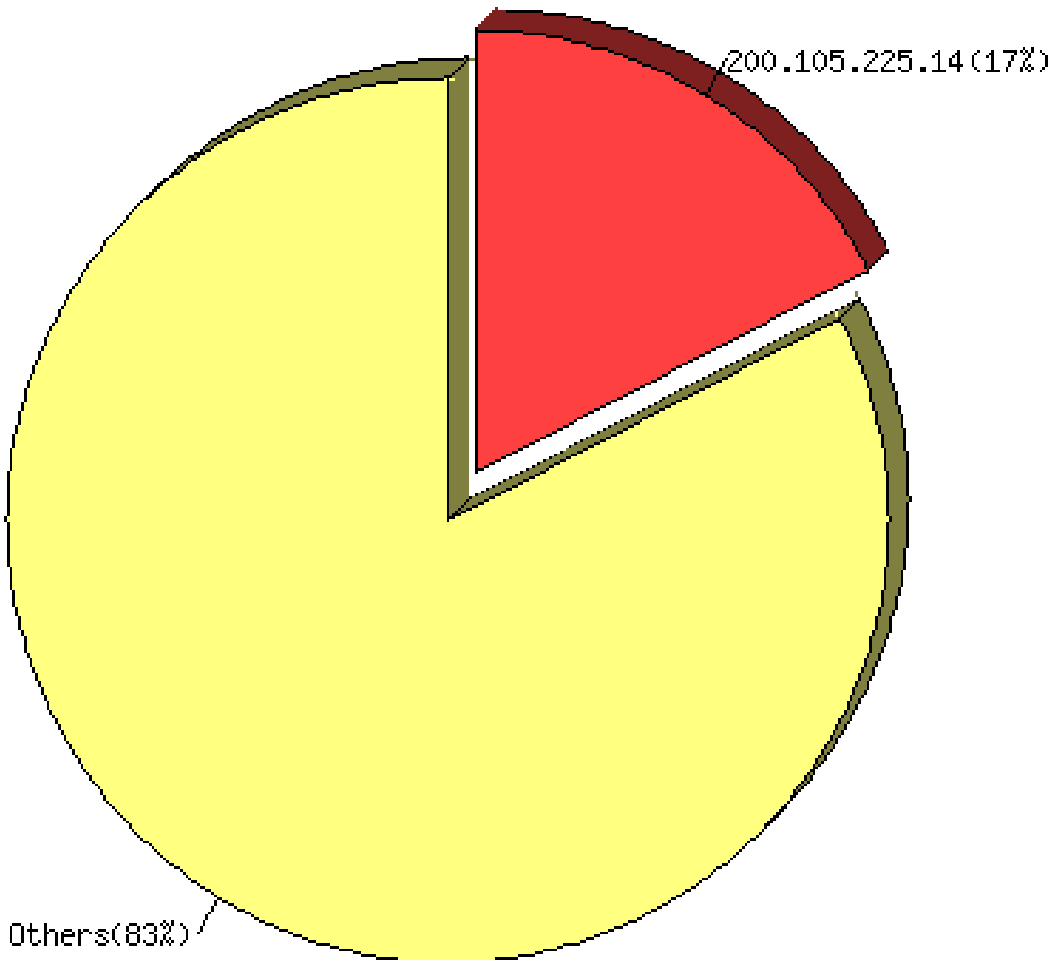



*Fig. 2.6 Mayor incidencia de exposición y riesgos de seguridad del servidor Web*
*Fuente: Diagnóstico inicial de vulnerabilidades con NESSUS*

Adicionalmente, identificamos que la mayor cantidad de problemas de seguridad se debe a los protocolos “ssh” y “http”, tal como se indica a continuación:

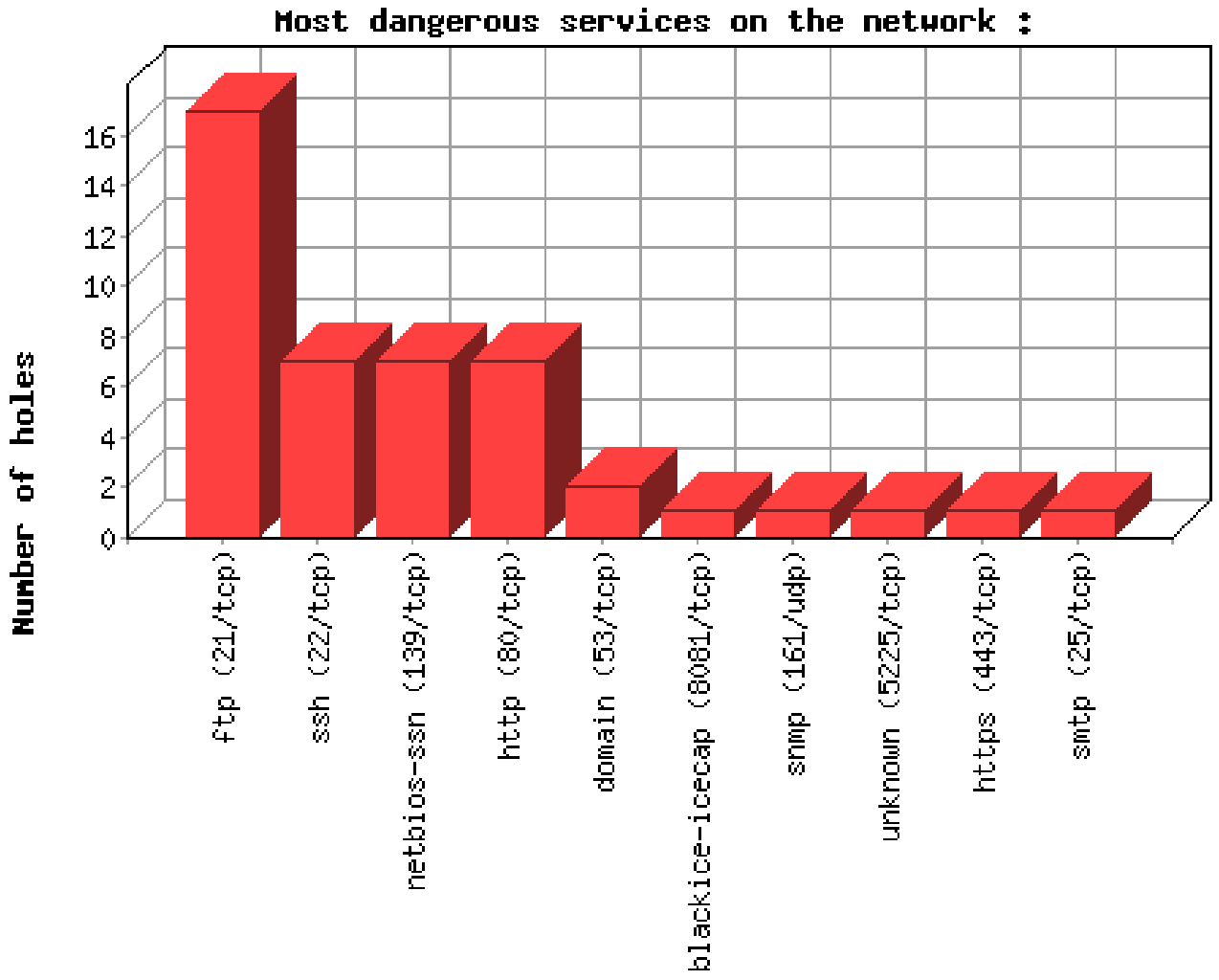



*Fig. 2.7 Servicios de red con mayor nivel de riesgos de seguridad del ISP*
*Fuente: Diagnóstico inicial de vulnerabilidades con NESSUS*

## 2.5 RECOMENDACIONES DE SEGURIDAD

A continuación indicamos las recomendaciones de seguridad sobre el cumplimientos de los objetivos de control específicos:

### A1.3.3 Seguridad de Software del Sistema

- Contar con un sistema alterno en el cual se apliquen las modificaciones, actualizaciones, parches y verificar que estos no afecten los datos almacenados y el comportamiento en sí del sistema para luego ser aplicado en el sistema que se encuentra en producción.

- Corregir las vulnerabilidades indicadas en la plataforma Microsoft según la tabla 2.6

- Implantar las recomendaciones técnicas detalladas para los diferentes elementos críticos de la red y analizar la posibilidad de cerrar puertos y servicios peligrosos en los equipos públicos. Ver Información adicional de soporte en CD – Reportes vulnerabilidades identificadas en el servidor Windows 2000 soporte al Sistema de Facturación y servidor Web sobre Linux, con las respectivas recomendaciones.

### DS5.1 Administrar Medidas de Seguridad

- Establecer un plan específico de seguridad de TI aplicado a los sistemas y los usuarios.

### DS5.2 Identificación, Autenticación y Acceso

- Implantar políticas de seguridad para la red Windows 2000 de Punto Net basadas en Active Directory, para controlar el acceso desde estaciones de trabajo a los recursos de red.

- Considerar la revisión de permisos sobre los recursos compartidos en el servidor y en la red en general.

- Definir nuevas políticas de creación y mantenimiento de passwords y controlar su cumplimiento.

- Proveer más seguridades al Sistema de Facturación a través de las cuentas de usuario y protección a la cuenta “sa” de administración de la base de datos SQL Server 7.0.

**DS5.5 Revisión Gerencial de Cuentas de Usuario**

- Revisar las debilidades de cuentas de usuario de los reportes LANGUARD y RETINA y tomar acciones correctivas por parte de la Gerencia. Ver Anexo E y Anexo F.

**DS5.6 Control de Usuarios sobre Cuentas de Usuario**

- Implementar scripts en los servidores y aplicaciones de red para autenticación del ingreso.

**DS5.7 Vigilancia de seguridad**

- Definir un procedimiento y responsable para revisar posibles incidentes de violación de seguridad.

- Analizar el costo beneficio de activar la opción de Auditoría en Windows 2000 Server y en la Base de Datos SQL Server 7.0 soporte a la información del Sistema de Facturación.

**DS5.8 Clasificación de datos**

- Crear un procedimiento para la clasificación y responsabilidad de datos según la criticidad e importancia.

**DS5.11 Manejo de Incidentes**

- Elaborar y definir en los planes de seguridad lo referente al manejo de incidentes de seguridad.

- Definir un procedimiento para la elaboración de reportes de los incidentes de seguridad.

**DS5.20 Arquitectura de Firewalls y conexión a redes públicas**

- Implantar un firewall a nivel de hardware y software más robusto mediante la aplicación de DMZ´s para acceso a red interna, servicios de acceso remoto para clientes corporativos y clientes dial-up según la definición del "Esquema de Seguridad para Punto Net" basado en el Firewall Checkpoint.

# CAPITULO 3

# ETAPA 3: IMPLANTACION DEL ESQUEMA DE SEGURIDAD DEL ISP

## 3.1 ANALISIS DE REQUERIMIENTOS DE SEGURIDAD DEL ISP

### 3.1.1 ANALISIS DE LOS REQUERIMIENTOS DE SERVICIO QUE BRINDA UN ISP

Para definir los diferentes requerimientos que tiene un Proveedor de Servicios de Internet para brindar servicios y acceder a la Internet, es necesario que tomemos en cuenta cada uno de los factores de acuerdo a su servicio. Para nosotros poder realizar un estudio más veraz de cuál es la realidad, en las diferentes conexiones que un ISP tiene, hemos tomado como caso de estudio, la red de "Punto Net",

por ser uno de los ISP más importantes del país, y por tener la facilidad de estudio.

Los servicios más importantes que al momento mantiene el ISP provee hacia la red Internet son:

- Web Hosting.
  - Publicitario.
- Servicio de correo entrante y saliente.
- Servicio de Acceso Remoto.
- Servicio de Resolución de Nombres (DNS)
- Servicio de Transferencia de Archivos (FTP).

### 3.1.1.1 Web Hosting

**Publicitario** .- El ISP brinda el servicio publicitario a través de su página WEB de presentación, en donde expone su logotipo. Tiene una serie de hipervínculos hacia una descripción de los servicios, ofrece el acceso para el uso de consultas en sus cuentas corporativas a nivel de enlaces.

### 3.1.1.2 Servicio de correo entrante y saliente

Este servicio se brinda a los usuarios corporativos mediante la asignación de una cuenta de correo para que puedan enviar y recibir correo electrónico de una forma más rápida, efectiva y sin costo.

### 3.1.1.3 Servicio de acceso remoto

Los servidores de acceso remoto permiten a los usuarios dial-up y corporativos conectarse por este medio al Servicio de Internet.

### 3.1.1.4 Servicio de resolución de nombres (DNS)

Este es un servicio de resolución de nombres de alto dominio a direcciones IP y se provee de este servicio a los usuarios corporativos a través del registro de sus dominios en Internic.

#### 3.1.1.5 Servicio de transferencia de archivos (FTP)

Este servicio puede ser de entrada y de salida, para el efecto existe un servidor Linux con el servicio de FTP Server para que los usuarios externos depositen en el directorio asignado de este servidor la información que necesite intercambiar con otros usuarios.

El servicio de salida sirve para transferir archivos hacia el exterior del ISP y es necesario tener un software cliente de FTP y para una mayor seguridad se puede hacer uso del servicio de SOCKS, el mismo que permite enviar y traer archivos de servidores de FTP externos de una manera segura y controlada.

Otro de los análisis que permitirá dimensionar las políticas de seguridad y las herramientas que permitirán ejecutar dichas políticas son las siguientes:

- Cuántas Sesiones de FTP tenemos.
- Cuáles son las direcciones FTP más visitadas.
- Cuál es la dimensión de los archivos a bajarse.
- Cuántos clientes existen en nuestra página WEB.
- Cuál es el tiempo de respuesta de una consulta en Hora Pico.
- Cuáles son los usuarios de los servidores de Acceso Remoto.
- Cuántos clientes dial-up con acceso remoto existen.
- Cuántos clientes corporativos existen.

### 3.1.2 REQUERIMIENTOS POR PARTE DEL PROVEEDOR DE SERVICIOS.

- Disponer de personal que administre la seguridad. Informes de seguridad.
- Efectuar con regularidad pruebas del sistema de seguridad implantado.

- Máquinas gestionadas, operativas 24 horas.
- Seguimientos y anuncios del CERT (Computer Emergency Response Team).
- Conocimiento y soluciones dadas por el Centro Alarmas de INTERNET.
- Detección temprana de intentos de ataque. Seguridad ante la intrusión.
- Uso de criptografía para el transporte seguro de datos.
- Asegurar la privacidad en:
    - Transacciones comerciales, financieras y comercio electrónico.
    - Transporte seguro de información confidencial. Firma Digital.
    - Confidencialidad en la transferencia de ficheros.
- Asegurar integración con sistemas existentes.

### 3.1.3 REQUERIMIENTOS POR PARTE DEL USUARIO DEL ISP

- Disponer del acceso seguro y sin virus para los siguientes servicios:

    - *Correo electrónico*. Utilizar tanto las herramientas estándar del mercado, como el protocolo de comunicaciones TCP/IP estándar.
    - *Transferencia de ficheros*. Permite dentro de un ordenador remoto, mirar directorios, seleccionar ficheros y transferirlos por las líneas de comunicación a otro ordenador externo.
    - *Telnet*. Un terminal con un programa de emulación de pantallas, puede establecer sesiones de trabajo con otros ordenadores situados en la red INTERNET. Los usuarios deben facilitar la dirección o el nombre del ordenador remoto a TELNET.
    - *List server*. Directorio automatizado de direcciones que acepta los mensajes enviados a él y los distribuye a sus suscriptores. Este directorio permite ver cada mensaje que le ha sido enviado solamente a los usuarios suscritos.
    - *WEB.* Utilizar los estándares de seguridad como es el HTTPS.

### 3.1.4 CASO DE ESTUDIO – ISP PUNTO NET

La red del ISP se encuentra actualmente protegida desde el Border-Router Cisco 7304, en el cual se tiene Listas de Acceso y filtrado de paquetes con restricción de direcciones IP, subredes y redes de direcciones dudosas o reconocidas como SPAM o de Hackers, adicionalmente se tiene cerrado acceso a los routers y access-servers desde direcciones externas y bloqueo de puertos (sockets) para ciertas aplicaciones críticas del ISP.

Los servicios provistos por el ISP básicamente son de conexión individual o dial-up y corporativo por medio de líneas dedicadas, en los dos casos se entrega navegación y correo, no se restringe el uso a cualquiera de las aplicaciones del suite de protocolos TCP/IP que el cliente desee usar. En la parte corporativa se da el servicio de instalación de Linux o Windows y la configuración de servicios como, Correo, Web, seguridad, restricción de Ancho de Banda y seguridad global de la red.

Como la empresa de estudio es Punto Net, se realizará un análisis en las cuatro áreas de seguridad que debe tener una empresa al conectarse a la Internet como son:

- Seguridad de Perímetro (Firewall)
- Seguridad de canal (encripción).
- Seguridad de Acceso (autenticación)
- Seguridad Interna.

**3.1.4.1 Seguridad de Perímetro**.- El ISP Punto Net, al momento tiene un firewall basado en Linux, este firewall solamente permite el filtrado de paquetes, a nivel de capa IP y de Transporte, bloqueando puertos. Es bastante limitado, en la conexiones Físicas, ya que está ubicado en el backbone principal de la red sin ninguna protección de red perimetral basada en DMZ.

**3.1.4.2 Seguridad de Canal**.- La empresa financiera, no tiene ningún método de encripción para enviar y recibir archivos de la Internet, debido a que los usuarios

pueden enviar y recibir su información desde y hacia cualquier parte del Internet sin ninguna restricción de seguridad.

**3.1.4.3 Seguridad de Acceso**.- Este tipo de seguridad está orientado a los usuarios del servicio corporativo y dial-up, en donde tenemos:

**PROXY SERVER.-** Este servidor es un PROXY a través del servicio de APACHE, de Linux con Red-Hat 9.0, se tiene alrededor de 400 usuarios, para que los usuarios salgan directamente, al WEB no tiene ningún tipo de Autenticación, solamente es restringido por la dirección IP Interna.

Otro servicio que se tiene en este servidor es el reenvío de correo a los servidores de correo de la red Interna, este servicio no dispone de un control ANTI-SPAM.

El sistema operativo esta configurado de tal manera que acepte conexiones TELNET, y FTP por motivo de administración, sin ningún tipo de encripción.

**DNS SERVER.-** Este servidor tiene como función principal tener el servicio de resolución de nombres (DNS), es el servidor primario y de correo electrónico.

También se tiene un servicio de correo a través de SENDMAIL, este servicio tiene el antivirus MailScanner, y un servicio de ANTI-SPAM.

Finalmente su sistema operativo tiene abierto los puertos de Telnet y FTP para que usuarios del departamento técnico puedan hacer gestión en los mismos sin ningún tipo de seguridad.

**WEB SERVER.-** Este servidor está encargado de alojar la página WEB de Punto Net, este no tiene un mecanismo de autenticación a través de una página segura, maneja certificados digitales emitidos por el propio servidor para el caso de que se requieran utilizar Web Mail.

**SERVIDORES DE ACCESO REMOTO.-** Estos son siete dispositivos de comunicación que entregan el servicio de navegación en la Internet para los usuarios dial-up y corporativos que necesiten acceder a Internet.

Tienen el servicio de RADIUS para la autenticación y restricción de usuarios que ingresan a través de los servidores de Acceso Remoto.

**3.1.4.4 Seguridad Interna.-** En el ISP no se dispone de un esquema seguro para accesos a Internet desde la red Interna.
No existe una zona Desmilitarizada o DMZ que protega a la red interna. Sin embargo, existen Listas de Acceso y denegación de servicios por IP o por puerto.

Existe una VPN interna para acceso a la red LAN desde estaciones que se encuentran fuera y que son de los Administradores del Sistema, básicamente son 3 personas con Acceso, la VPN esta implementada sobre Linux 9.0.

A nivel general en todos los equipos del nodo ISP tienen acceso con su respectivo username y password.

Existen 3 personas responsables de la administración y seguridad de los servicios que presta el ISP (Gerente Técnico, Supervisor Técnico1, Supervisor Técnico2). Estas tres personas manejan las claves de administrador de todos los equipos.

Los técnicos tienen acceso a los Access-Servers con su respectivo username y password para ejecutar comandos de operador o de monitoreo, no pueden cambiar nada, ni ver las configuraciones, no tienen acceso a los servidores.

*3.1.4.4.1 Sistema de Facturación:*

La red del sistema de facturación es independiente del nodo principal y esta protegido por listas de acceso en un router Cisco 1601 que esta conectado Back-to-Back a uno de los Access-Servers, luego tenemos una PC con Linux e implementado Firewall para protección de la red LAN de posibles ataques.

En el sistema de facturación, tienen acceso adicionalmente a los 3 administradores con acceso total, personal de soporte como desarrollador del aplicativo con acceso a nivel general para mantenimiento y modificación del Sistema.

El Presidente Ejecutivo, Gerente Técnico y los Gerentes de Ventas Dial-Up y Cobranzas tienen accesos con opción de modificación.

Los usuarios del área de Cobranzas pueden realizar ingresos y modificaciones de planes y valores de pagos
Finalmente, los técnicos tienen acceso a ver la información de estado y pagos del cliente e ingreso de datos de Servicio al Cliente.

El servidor de facturación tiene el dominio GNTQ, el mismo que no tiene nada compartido, incluso no pueden autenticar en el servidor y tener acceso a las aplicaciones del Sistema de Facturación, ya que estos accesos están controlados en los routers.

### 3.1.5 CONSIDERACIONES PARA SELECCIONAR EL FIREWALL

Para el efecto se han analizado los dos Firewalls líderes en el tema de seguridades del mercado, esto es CISCO PIX y CHECK POINT.

**STATEFULL INSPECTION (TERCERA GENERACION)**

Este es un módulo de software que funciona sobre los sistemas operativos Windows o Unix, e inspecciona los paquetes que ingresan a nivel de capa de enlace de datos.

La tabla 3.1.a determina desde qué capa se realiza la revisión de contenido con la Inspección de paquetes, tanto del modelo OSI como del TCP/IP. La tabla 3.1.b

muestra una comparación de las capas del modelo OSI, con el modelo TCP/IP, y donde se realiza el análisis con cada uno de los firewalls CISCO PIX y CHECKPOINT.

**Firewall, Capas y Modelos**

| Modelo de 7 capas ISO | Modelo de 5 capas Internet | Firewalls |
|---|---|---|
| Aplicación (7) | Aplicación (5) | Servicio de Proxy |
| Transporte (4) | TCP/DP (4) | Filtrado de paquete<br>Ruteo de paquetes |
| Red (3) | IP/ICMP (3) | Sreening Router<br>Stateful Inspection |
| Enlace (2)<br>Física (1) | Enlace (2)<br>Sistema de Interfase (1) | Nada |

*Tabla 3.1-a Cuadro comparativo capas del modelo OSI vs. TCP/IP y análisis con Firewall*
*Fuente: Los Autores*

Statefull Inspection es una tecnología Firewall de tercera generación, cuya tecnología mantiene un alto nivel de seguridad. Para ello el Firewall debe registrar y controlar el flujo de información que pasa a través de este, debe tomar decisiones en los servicios referentes al conjunto de protocolos de TCP/IP, como aceptar, rechazar, eliminar, autenticar, encriptar, y registrar pistas de auditoría de los requerimientos de comunicación. Además, un Firewall debe tener la capacidad de obtener, guardar, recuperar, y manipular la información de todas las capas de comunicación y de otras aplicaciones.

### 3.1.5.1 Cuadro de las Características Básicas de los Firewalls a analizar

| NOMBRE | CARACTERISTICA | SOFTWARE Y HARDWARE |
|---|---|---|
| **CISCO PIX** | Es una caja Cerrada con Hardware especializado con software propietario de CISCO. | S.O. : Cisco IOS 12.xx<br>Hardware : Cisco 515<br>Soft. Firewall : PIX |
| **CHECK POINT** | El software de Firewall Check Point se soporta en un Hardware de NOKIA, CROSSBEAM, INTEL, SOLARIS | S.O. : IPSO<br>Hardware : NOKIA IPxxx, CROSSBEAM, INTEL, SOLARIS<br>Soft. Firewall: CheckPoint |

*Tabla 3.1-b Características básicas de los Firewalls*

*Fuente: Los Autores*

### 3.1.5.2 Características Mínimas que debe cumplir un Firewall

Las mínimas propiedades que un Firewall debe tener en hardware y software, son las siguientes:

**Hardware**

- Alto Rendimiento
- Número de paquetes procesados por segundo (throughputs)
- Mínimo 4 Interfaces de red Ethernet 10/100 PCI

- Procesador mínimo Pentium IV de 1.2 GHz
- Memoria RAM mínimo 512 MB.
- Disco duro mínimo de 10 GB

**Software**

- Tecnología de Firewall Statefull Inspection
- Soporte de VPN (DES, 3DES, IPSEC, MD5)
- Listas de control de acceso (ACL)
- Traslación de direcciones (NAT)
- Herramientas de Administración (Management, GUI)
- Generación de logs de acceso
- No permitir enmascaramiento de direcciones permitidas (Anti Spoofing)
- Sistema Operativo robusto (Basado en Unix)
- Modularidad en software base
- Debe Soportar herramientas de Gestión

### 3.1.5.3 Revisión de las Características de cada una de las marcas de Firewalls

En esta parte se presentan las características técnicas que permitirán descubrir cada una de las funcionalidades de los Firewalls a ser analizados en las páginas siguientes, ver tabla 3.2 y tabla 3.3:

*3.1.5.3.1 Cisco Pix:*

| Hardware | CISCO PIX 515 | CISCO PIX 525 |
|---|---|---|
| Rendimiento | 50.000 conexiones simultáneas | 280.000 conexiones simultaneas |
| Throuthputs | 170 Mbps | 370 Mbps |
| Tarjeta red | 6 10/100BaseT Fast Ethernet, RJ-45 | 4 10/100BaseT Fast Ethernet, RJ-45 |
| VPN Accelerator Card (VAC) Support | SI | SI |
| Procesador | 200 MHz Intel Pentium II | 600 MHz Intel Pentium III |
| Memoria RAM | 32 MB or 64 MB | Up to 256 MB |
| Disco Duro | 10 GB. | 10 GB. |
| Flash Memory | 16 MB | 16 MB |
| Port consola | RJ-45 | RJ-45 |
| **Software** | | |
| Tecnología de Firewall | State-of-the-art Adaptive Security Algorithm (ASA) and stateful inspection firewalling | State-of-the-art Adaptive Security Algorithm (ASA) and stateful inspection firewalling |
| Soporte de VPN | 56-bit DES IPsec<br>168-bit 3DES IPsec | 56-bit DES IPsec<br>168-bit 3DES IPsec |
| Detector de Intrusos | Integration with Cisco Intrusion Detection Systems for shunning connections of known malicious IP addresses | Integration with Cisco Intrusion Detection Systems for shunning connections of known malicious IP addresses |
| Traslación de direcciones | True Network Address Translation (NAT) as specified in RFC 1631 | True Network Address Translation (NAT) as specified in RFC 1631 |
| Generación de logs de acceso | Enhanced customization of syslog messages | Enhanced customization of syslog messages |
| Anti Spoofing | SI | SI |
| Sistema Operativo | PIX 6.2 | PIX 6.2 |
| Modularidad | NO | NO |
| Debe Soportar herramientas de Gestión | SI | SI |

*Tabla 3.2 Características Firewall CISCO PIX*

*Fuente: http://www.cisco.com/*

### *3.1.5.3.2 CHECK POINT sobre Nokia IPXX:*

| **Hardware** | **NOKIA IP 440** | **NOKIA 330** |
|---|---|---|
| Rendimiento | 128,000 Conexiones simultáneas. | 64,000 conexiones simultaneas. |
| Throuthputs | 176 Mbps | 176 Mbps |
| Tarjeta red | 4 PCI SLOT x 4 10/100BaseT Fast Ethernet. | 4 PCI SLOT x 4 10/100BaseT Fast Ethernet. |
| VPN Accelerator Card (VAC) Support | 1 10/100 non-accelerated Ethernet ports for HA, management, etc | 1 10/100 non-accelerated Ethernet ports for HA, management, etc |
| Procesador | 600 MHz. | 600 MHz. |
| Memoria RAM | 256 MB | 256 MB |
| Disco Duro | 10 GB. | 10 GB. |
| Flash Memory | | |
| Port consola | 1 serial console port | 1 serial console port |
| **Software** | | |
| Tecnología de Firewall | Statefull Inspection Check-point | Statefull Inspection Check-point |
| Soporte de VPN | DES, 3DES | DES, 3DES |
| Detector de Intrusos | SI | SI |
| Traslación de direcciones | Státics, Hiden | Statícs, Hiden. |
| Generación de logs de acceso | Personalizado Log | Personalizado Log |
| Anti Spoofing | SI | SI |
| Sistema Operativo | IPSO 3.4 | IPSO 3.4 |
| Modularidad | NO | NO |
| Debe Soportar herramientas de Gestión | SI | SI |

*Tabla 3.3 Características Firewall CHECK POINT sobre Nokia IPXX*

*Fuente: http://www.checkpoint.com/*

### 3.1.5.4 Selección del Firewall

Debido al análisis anterior se puede observar que existen sistemas de firewalling, en cajas cerradas como es CISCO o sistemas modulares con software independiente como es el caso de CheckPoint sobre diferentes tipos de Hardware tales como NOKIA IPSeries, blades CROSSBEAM, cajas INTEL, cajas SOLARIS y otros, sobre Sistemas Operativos robustos.

La ventaja de los sistemas modulares, es que son independientes del Hardware y el sistema operativo, este permite armar soluciones caras o baratas dependiendo de la importancia de la información y el rendimiento de la plataforma.

El software que se encuentra en estudio y permite tener la característica de modularidad es CheckPoint a nivel de sotware. Debido a limitantes en costos para su adquisición con la plataforma de Hardware marca NOKIA IPXX, así como para proveerle mayor desempeño a nivel de procesamiento central, se instalará el Checkpoint NG sobre un servidor con Sistema Operativo Windows 2003 Enterprise Edition.

Se ha escogido como sistema de Firewall el software CheckPoint debido a:

- El software incorpora la tecnología de Firewalling Statfull Inspection (tercera generación), lo que permite tener un control a partir de la capa de enlace.
- Permite tener un esquema modular y portable, en el caso de falla nosotros podemos levantar nuestro Firewall sobre cualquier plataforma de Hardware y sobre sistemas operativos como son LINUX, WINDOWS 2000/2003, SUN, HP-AUX.
- Permite implementar niveles de seguridad hasta a nivel de aplicación en los protocolos más utilizados como son FTP, HTTP, SMTP.
- Permite implementar soluciones de envió de información seguros como es el caso de la encriptación.

- Permite tener niveles de autenticación con niveles de seguridad altos, aplicando tecnologías de punta como es el caso de Certificado digitales.
- Esta plataforma soporta todos los requerimientos básicos detallados en este capítulo.
- Administra y controla toda la seguridad basada en objetos de red.

### 3.1.6 POLITICAS DE SEGURIDAD DE ACCESO A LA INTERNET

Una política de seguridad no es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que deseamos proteger y el por qué de ello.

Implementar políticas de seguridad que gobiernen el acceso a los recursos de información de las empresas es, actualmente, la única manera de obtener esa privacidad e integridad de las comunicaciones a través del Internet, Intranet o Extranet.

Entendemos que el ISP caso de estudio debe establecer políticas de seguridad que le permita prevenirse de los peligros de pérdida o robo de su información crítica y es necesario diseñar una arquitectura Segura y Confiable.

El desarrollo de las diferentes políticas de seguridad se ha realizado en base del análisis de las vulnerabilidades identificadas en el Capítulo 2 de esta Tesis y de acuerdo a las necesidades de protección de información reflejadas en el análisis de requerimientos de seguridad del ISP, como es: la seguridad de perímetro, seguridad de canal, seguridad de acceso y seguridad interna.

Para la implementación de estas políticas de seguridad se ha visto la necesidad de dividir las áreas de acción y de acuerdo a éstas aplicar las políticas.

Estas áreas tienen las siguientes políticas que se van a aplicar en los diferentes componentes, las mismas que han sido acopladas al ISP en estudio, y son:

#### 3.1.6.1 Conectividad

Del análisis realizado sobre los requerimientos que tiene el ISP se proponen las siguientes políticas.

- Toda Red que se conecta a la Internet debe tener un Firewall.
- Todo Firewall debe tener por lo menos 3 Interfaces LAN, y una interfase para conectarse el router de salida a la WAN o Internet.
- Todo Firewall en una de sus Interfaces debe configurar por lo menos una red desmilitarizada (DMZ).
- No se puede tener un servidor de Acceso Remoto dentro de una red donde se tengan servidores sean estos BASTION o Internos.
- El Hardware dedicado a controlar el acceso de paquetes debe estar independiente del dispositivo que se encargue de rutear paquetes.
- Todo servicio de Acceso Remoto debe ser controlado por un servicio de autenticación como es RADIUS.
- Cualquier usuario que desee salir a la Internet debe hacer uso de PROXYS que se encuentran en la red desmilitarizada.
- Nunca un usuario debe salir a la red externa directamente.
- Un usuario interno nunca debe hacer uso de una conexión DIAL-UP hacia un proveedor de Internet si está conectado a la red Interna.
- Todo servidor de servicio debe estar siempre tras del Firewall.
- En la red desmilitarizada debe existir un equipo que permita ver el acceso de intrusos.
- Un equipo no puede estar conectado con una Interfaz a la red desmilitarizada y con otra a la red Interna realizando un puente.
- Todo usuario externo que desee ingresar a la red Internet debe estar controlado por Firewall.
- El servicio de correo debe tener un servidor de Relay en la red desmilitarizada.
- Todo servidor que tenga Sistema Operativo Windows y trabajando con el servicio de correo, debe estar dentro de la red Interna

### 3.1.6.2 Políticas de software base

El software base está compuesto por los diferentes Sistemas Operativos que se implementan en los servidores de la red desmilitarizada

**Las políticas son:**

- Todo Sistema Operativo debe ser instalado con los últimos parches que el fabricante haya publicado.
- Todo Sistema Operativo debe tener abierto solamente el puerto del servicio que va a brindar como puede ser: ftp puerto21, http puerto 80, etc.
- Todo Sistema Operativo debe hacer uso de niveles de acceso de usuario a través de perfiles de usuario.
- Todo Sistema Operativo debe llevar un Log de acceso de usuarios.
- Todo Sistema Operativo debe llevar un registro de los comandos ejecutados.
- El Sistema Operativo que se instale en la red desmilitarizada, debe ser robusto y bien estructurado, de preferencia basado bajo Unix/Linux.
- El password de administrador debe ser cambiado cada mes.
- El password de administrador no debe tener caracteres alfanuméricos.
- Todo servidor Bastion debe tener habilitado el servicio SSH2 para su propia gestión.

### 3.1.6.3 Políticas para los servicios TCP/IP

Debido a que tenemos gran variedad de servicios basados sobre el protocolo orientado a la conexión como es TCP/IP, las políticas que definamos se irán describiendo por cada servicio, como se presenta a continuación:

*3.1.6.3.1 Políticas para Correo:*

- El servidor de correo debe tener en el Firewall una regla donde cualquier IP de inicio se conecte a la IP del servidor como IP destino con el puerto 25 (smtp).
- En el Firewall de todo servidor de correo que esté en la red Interna y tenga salida a la Internet, se debe realizar un NAT.
- Todo servidor de correo que esté en la red Interna y tenga salida a la Internet, en el Firewall debe tener una regla en donde la dirección IP de inicio se conecte a la dirección IP destino. Donde la dirección IP destino es la dirección del servidor Bastión de Relay de correo.
- En el Firewall debe existir una regla de POP3 que permita al usuario de Acceso Remoto bajarse los correos del servidor respectivo.
- Todo usuario remoto que se conecte desde la Internet a un servidor de correo que se encuentre en la red Interna debe tener una regla en el Firewall que nos permita formar una VPN.
- El Firewall debe tener la regla que permita reservar el 40% del canal para el servicio de correo de Internet.
- Todo servidor de correo que tenga el software de Microsoft Exchange en el Firewall se debe habilitar los puertos necesarios para bajarse los correos.
- Debe existir el servicio de antivirus para correo electrónico.
- El servicio de correo no dejará pasar archivos con extensiones jpg, mp3, gif, exe.
- El servicio de correo podrá enviar mensajes con archivos anexos de máximo 1024 bytes.

*3.1.6.3.2 Políticas para FTP:*

- El Firewall debe tener dos reglas que permitan a los usuarios internos conectarse a los servidores FTP externos. La primera regla permite que el usuario, que se encuentra en la red interna, se conecte al servidor bastión

que tenga el servicio de socks4 (puerto 1080), la segunda regla permite al servidor bastión conectarse al servidor FTP correspondiente.

- El Firewall debe tener la regla que permita reservar el 20% del canal para el servicio de FTP hacia la Internet.
- El Firewall debe tener la regla que permita que los usuarios externos se conecten a nuestro servidor de FTP por el puerto 21.
- El Firewall debe tener la regla de restringir los verbos de FTP, entre los cuales tenemos: PORT, PASV, MGET, MPUT, LS, etc.
- El Firewall debe tener la regla que permita que los administradores ingresen a los servidores bastión por el puerto 22 que es ssh2 y en el momento de su ejecución deben autenticarse tanto en el Firewall como en el servidor bastión.

#### *3.1.6.3.3 Políticas para Web:*

- El Firewall debe tener la regla para que cualquier persona ingrese a nuestra página web por el puerto 80 y 443.
- El Firewall debe tener la regla para que nuestro servidor Proxy salga hacia cualquier servidor Web de la Internet por el puerto 80 y 443.
- El Firewall debe tener la regla que permita que los usuarios internos se conecten al servidor Proxy por el puerto 80.

#### *3.1.6.3.4 Políticas para DNS:*

- Debe existir la comunicación de los puertos domain UDP y domain TCP (53), solamente entre el servidor primario y secundario de DNS.
- El servidor DNS primario debe salir por el puerto domain UDP hacia todos los servidores DNS de la Internet.
- Todos los servidores DNS de la Internet deben ver al servidor DNS primario del ISP con el puerto domain UDP.
- Todo servidor DNS primario debe tener registrado al menos un servidor DNS secundario para mejor su disponibilidad.

- Toda Empresa que requiera registrar un dominio en la Internet necesita de un servidor DNS primario.
- Todo servidor bastión debe tener configurado el servicio de DNS.

#### 3.1.6.4 Políticas para análisis de LOGS de los Servidores

- Todo servicio instalado en un servidor bastión debe generar un archivo de Log que permita entregar la información de los clientes que ingresan.
- Todo registro grabado en un Log debe permitir determinar la hora de acceso al servidor y la salida del mismo.
- Los servidores bastión deben disponer de una herramienta que permita sacar de forma estadística los datos generados por el Log.
- Se debe realizar un análisis del crecimiento en el tamaño del archivo de Log en MB para determinar la frecuencia de respaldo del archivo.
- Se debe presentar un documento del análisis del Log una vez a la semana al departamento de control del ISP.

#### 3.1.6.5 Políticas para análisis del LOG del FIREWALL

- El Firewall debe ser capaz de generar archivo de log, el mismo que debe reflejar todo el flujo de paquetes que lleguen al Firewall.
- El log del Firewall debe ser capaz de reflejar toda la información que contiene la cabecera TCP/IP, como también la fecha y hora en que un paquete ha llegado al Firewall.
- El Firewall debe disponer de una herramienta que permita recuperar, analizar y mostrar en cuadros estadísticos toda la información que se encuentra en el log.
- Los logs del Firewall deberán ser analizados y organizados en forma estadística cada semana.
- Los logs del Firewall deberán ser respaldados de forma diaria por la importancia de la información que se genera.

### 3.1.6.6 Políticas para controlar el Ancho de Banda

- Los ruteadores que tienen salida a la Internet deben ser capaces de controlar el ancho de banda por servicio, esto de manera dinámica.
- Se debe implementar una herramienta que permita restringir el ancho de banda de acuerdo a los servicios implementados en el ISP para la Internet .

### 3.1.6.7 Políticas para bloqueo de páginas Web

- El servicio de salida al Internet para los usuarios internos debe estar restringido por una base jerárquica de páginas Web.
- En el servicio de Web no se dejará pasar páginas Web con código html que contengan strings malicioso (applets, scripts, etc.)
- Todo usuario que tenga acceso a servidores de páginas Web debe estar consciente de que el sitio Web que visita debe ser productivo para la Empresa.
- Se debe implementar una herramienta que permita restringir el acceso por parte de los usuarios a sitios Web improductivos para la Empresa.
- El Administrador de la Internet, debe realizar un análisis de los sitios Web visitados por los usuarios de la empresa para determinar si estos sitios son productivos o no para la empresa.
- La herramienta de restricción de páginas Web debe tener las siguientes características:
  - Una base de datos categorizada de acuerdo a los sitios Web improductivos para la Empresa.
  - Debe tener un motor que permita actualizar desde la Internet, la base de datos categorizada de páginas Web improductivas.
  - La herramienta debe permitir agregar en la base de datos categorizada sitios Web improductivos.
  - La herramienta debe permitir generar reporte detallado de los sitios Web visitados por lo usuarios.
  - La herramienta debe disponer de un motor promiscuo para la captura de paquetes TCP/IP de forma autónoma.

#### 3.1.6.8 Políticas de Antivirus

- Debe instalarse una herramienta que permita detectar y notificar los virus, troyanos y spyware embebidos en el correo electrónico. La misma que debe disponer de un motor que permita actualizar desde la Internet, la base de datos de antivirus.

#### 3.1.6.9 Políticas de detector de Intrusos

- Debe instalarse una herramienta que permita detectar el acceso de código malicioso embebido en páginas Web, correo electrónico, etc.

## 3.2 DISEÑO DEL ESQUEMA DE SEGURIDAD DEL ISP

El diseño del Esquema de Seguridad propuesto se lo ha enfocado desde una óptica de reorganización de infraestructura, a fin de establecer los requerimientos de seguridad de perímetro, seguridad de canal, seguridad de acceso y seguridad interna.

Debemos indicar que complementariamente para garantizar un Esquema de Seguridad completo, se ha tomado en cuenta las diferentes recomendaciones específicas de seguridad emitidas en la sección 2.3.6.2 “Resultados de Pruebas” sobre los 16 elementos críticos del ISP.

Partiendo desde el núcleo de seguridad a nivel de infraestructura y del análisis de los cortafuegos del mercado, el ISP tomó la decisión de utilizar las mejores prácticas de seguridad según el Firewall Checkpoint, el mismo que se muestra en la Fig. 3.1.

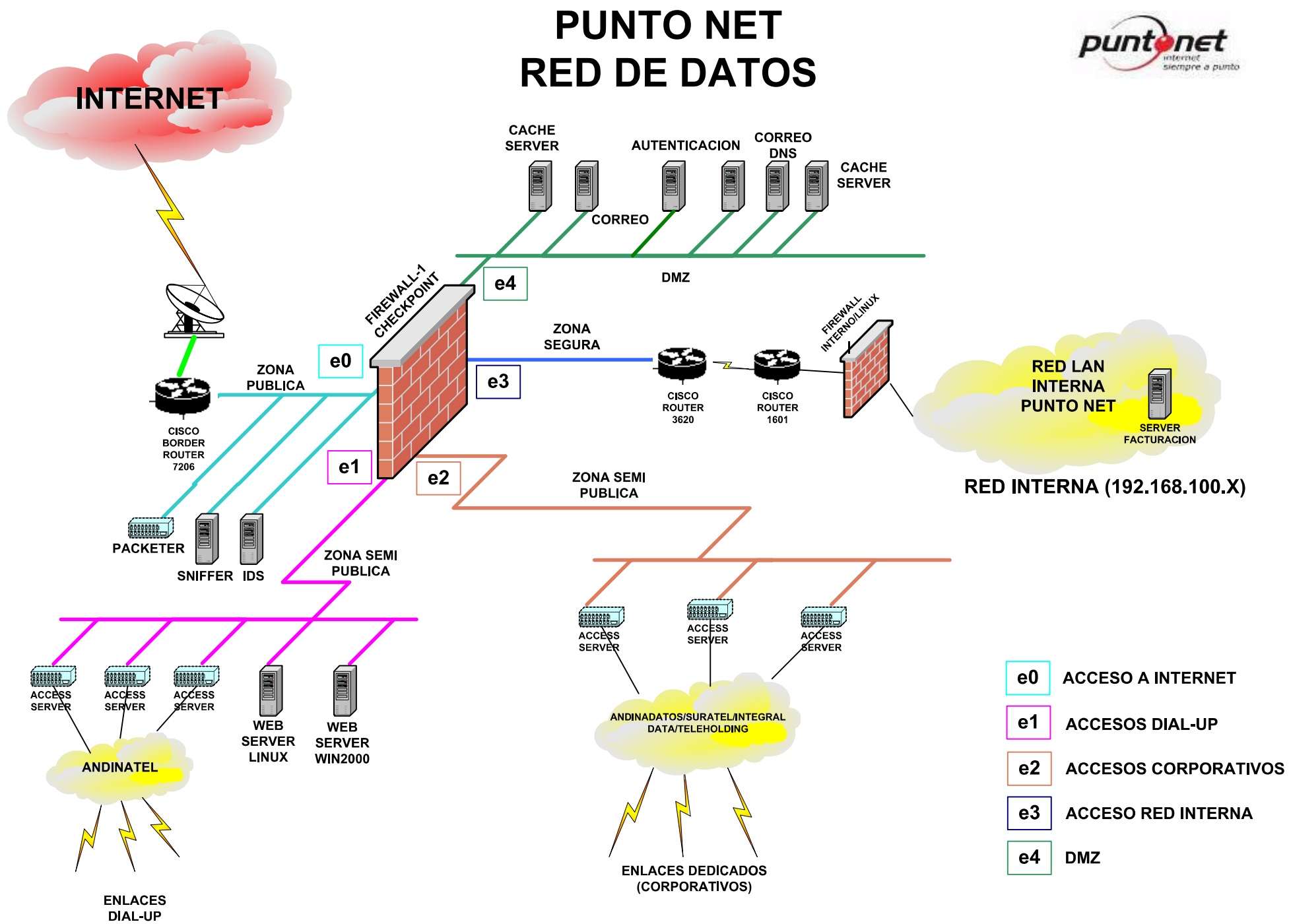



*Fig. 3.1 Esquema de Seguridad propuesto para el ISP*

*Fuente: Los Autores*

Como primer paso se ha visto la necesidad de implementar un Firewall central basado en Checkpoint, el cual será el administrador de seguridad de todo el ISP.

Como punto de convergencia de todo flujo de información que sale y entra desde la red interna hacia la Internet es el Firewall, el mismo que debe tener varias interfaces LAN de conexión, esto permitirá direccional el flujo de paquetes entre los diferentes segmentos de red que estén conectados en el Firewall. La forma como sea configurado el Firewall y el nivel de conocimiento de la persona sobre el producto determinará la fortaleza de la seguridad de la red interna.

Una característica importante en este esquema es tener los servicios de acceso a la Internet organizados de tal manera que no atenten contra la seguridad de los mismos, como es el caso de los servidores de Acceso Remoto y los servidores de Web Hosting, los mismos que deben ser separados por segmentos de red independientes, es decir que cualquier usuario que ingrese a través de una conexión Dial UP tendrá el mismo nivel de restricción que si se conectara desde la Internet hacia los servidores bastión que se encuentran en un segmento de red diferente, y más aún hacia la red interna, e incluso podemos incrementar un nivel de la confidencialidad de la información entre cualquier usuario de la red desmilitarizada y el Firewall aplicando una conexión a través de VPN.

### 3.2.1 ZONA PUBLICA

Se ha definido una zona pública a través de la interfase “e0” y el Border Router 7206 a través de la cual todos los usuarios internos y clientes dial-up y corporativos saldrán al Internet. En esta zona se recomienda instalar el Administrador del Ancho de Banda para los clientes del ISP, así como Herramientas de Monitoreo (Sniffer) y Sistema de Detección de Intrusos (IDS).

### 3.2.2 ZONA SEMIPUBLICA ENLACES DIAL-UP

A través de la interfaz “e1” se ha diseñado una zona semipública, en la cual estarán conectados 3 Access Server para los enlaces de los clientes dial-up del ISP que utilizan la red de Andinatel para su conexión. En esta zona se han

definido ubicar también a los servidores Web en Linux y Windows 2000 que proveen el servicio de Hosting a los clientes del ISP.

### 3.2.3 ZONA SEMIPUBLICA ENLACES CORPORATIVOS

A través de la interfaz “e2” se ha diseñado una zona semipública, en la cual estarán conectados 3 Access Server para los enlaces dedicados de los clientes corporativos del ISP que utilizan la red de Andinadatos, Suratel, Integral Data y Teleholding como última milla.

### 3.2.4 ZONA SEGURA RED INTERNA

Por medio de la interfaz “e3” se ha diseñado una zona segura, la cual permite restringir el acceso a la red interna del ISP mediante una conexión back to back entre 2 routers Cisco y un Firewall en software (Linux) adicional. En esta red interna se encuentra el Servidor de Facturación de Consumos Dial-up y las estaciones de trabajo administrativas del ISP.

Mediante esta configuración se pretende proteger toda la red interna del ISP y tener un esquema de conectividad que sea escalable, como es el caso de conectarse a ubicaciones WAN (Guayaquil y Santo Domingo).

### 3.2.5 ZONA DESMILITARIZADA DMZ

Finalmente se ha definido una zona desmilitarizada o DMZ mediante la interfaz “e4” a fin de albergar servidores Bastión para los servicios de Correo Electrónico, Autenticación (AAA), DNS y Cache Server.

A esta zona puede acceder cualquier usuario de Internet externamente por medio de la interfaz “e0” y cualquier cliente dial-up o corporativo del ISP a través de las interfases “e1” y “e2”.

# 3.3 IMPLANTACION DEL ESQUEMA DE SEGURIDAD DEL ISP

## 3.3.1 INSTALACION Y CONFIGURACION DEL SOFTWARE CHECKPOINT

Previamente se instaló un servidor Windows 2003 Enterprise Edition con el Service Pack 1 y se configuró todas las medidas de seguridad recomendadas por Microsoft para el efecto en un servidor HP Proliant ML350 con procesador Intel Xeon de 3.2 GHz, 1 GB de RAM y 36 GB de capacidad de almacenamiento.

Luego se procedió a instalar el Software Chekpoint NG en este servidor, ver Fig. 3.2.

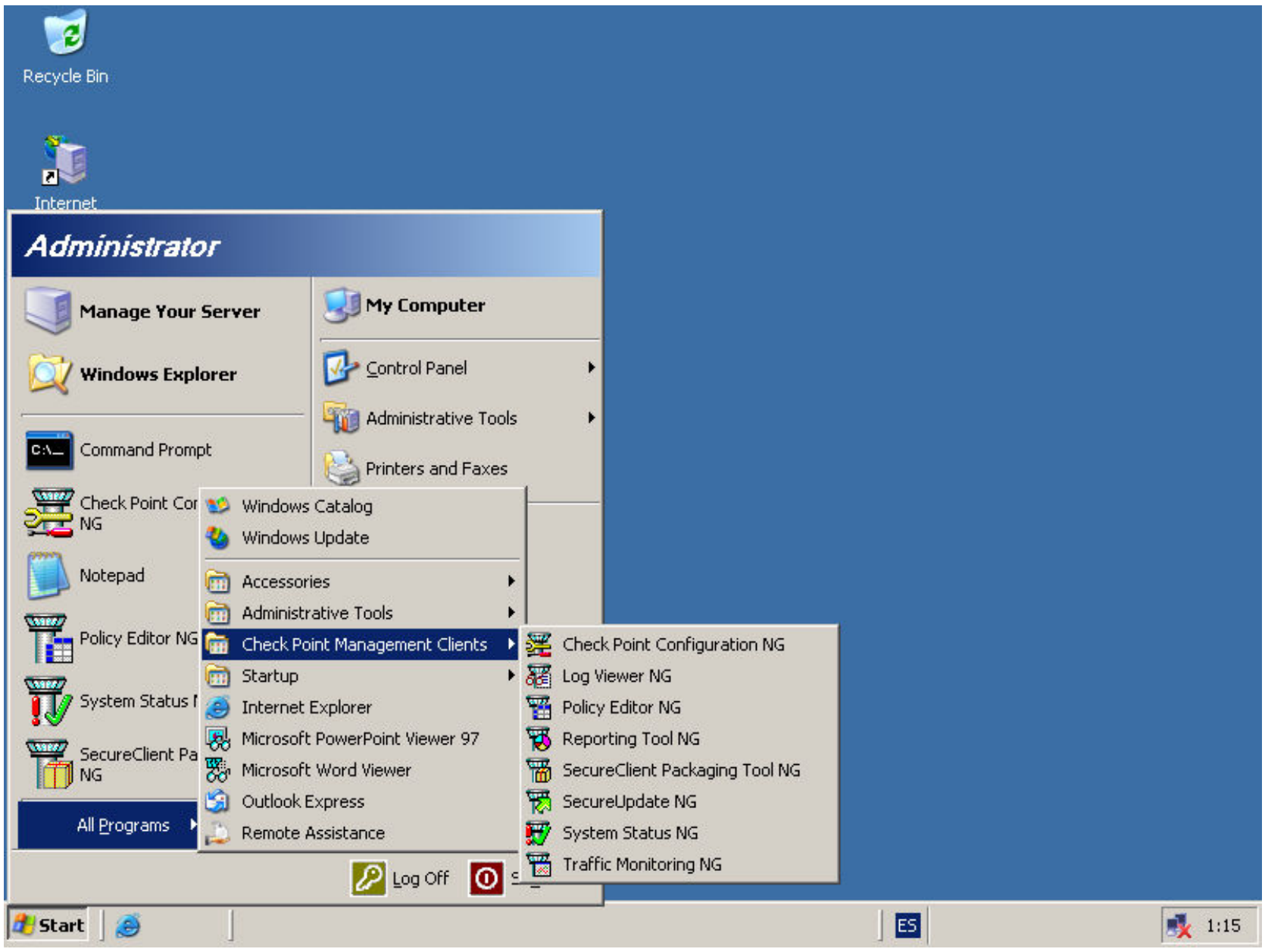



*Fig. 3.2 Firewall CheckPoint instalado en servidor Windows 2003*

A continuación presentamos las principales pantallas de configuración de CheckPoint NG:

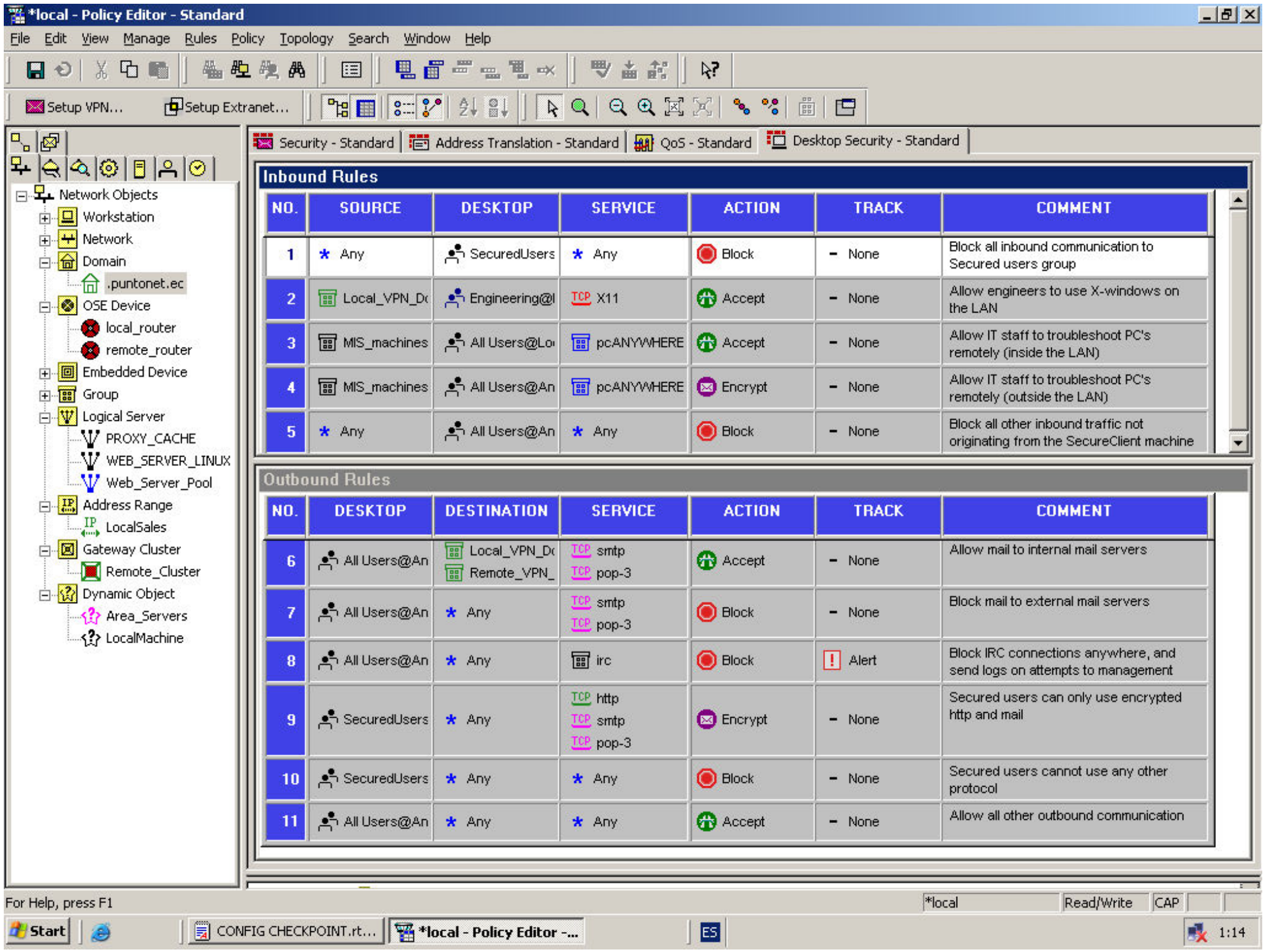



*Fig. 3.3 Firewall CheckPoint Desktop Security*

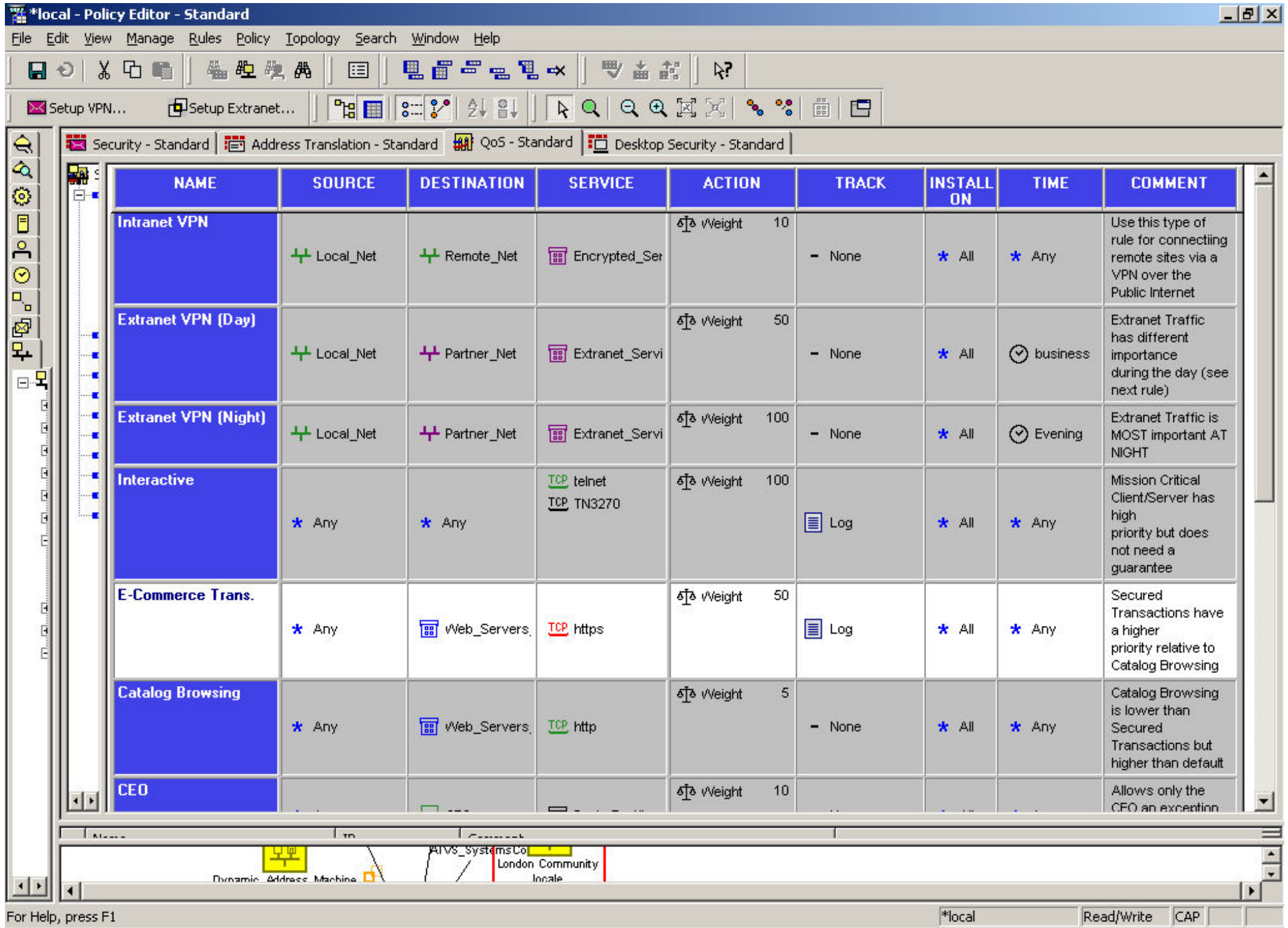



*Fig. 3.4 Firewall CheckPoint QoS standar1*

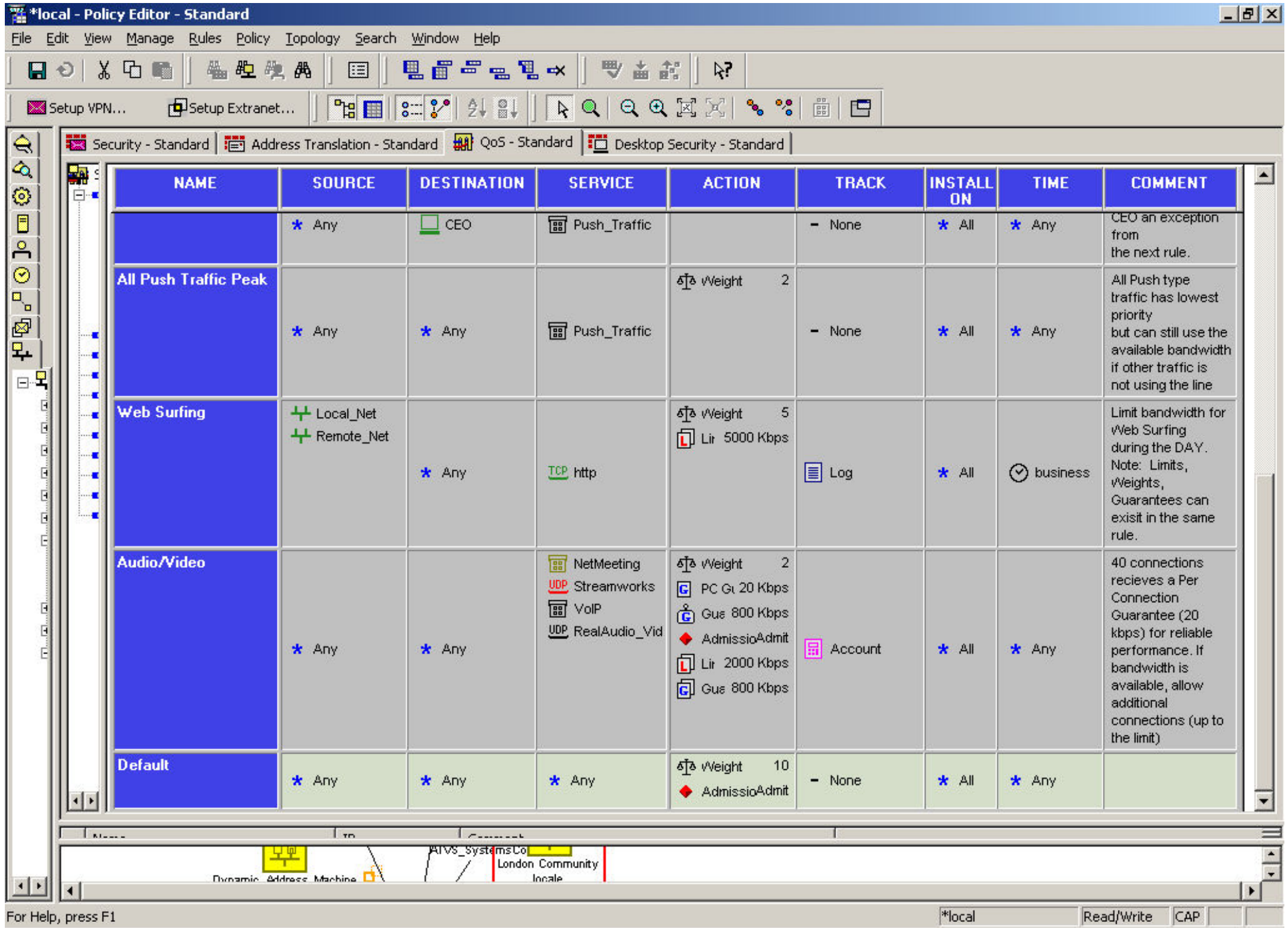



*Fig. 3.5 Firewall CheckPoint QoS standar2*

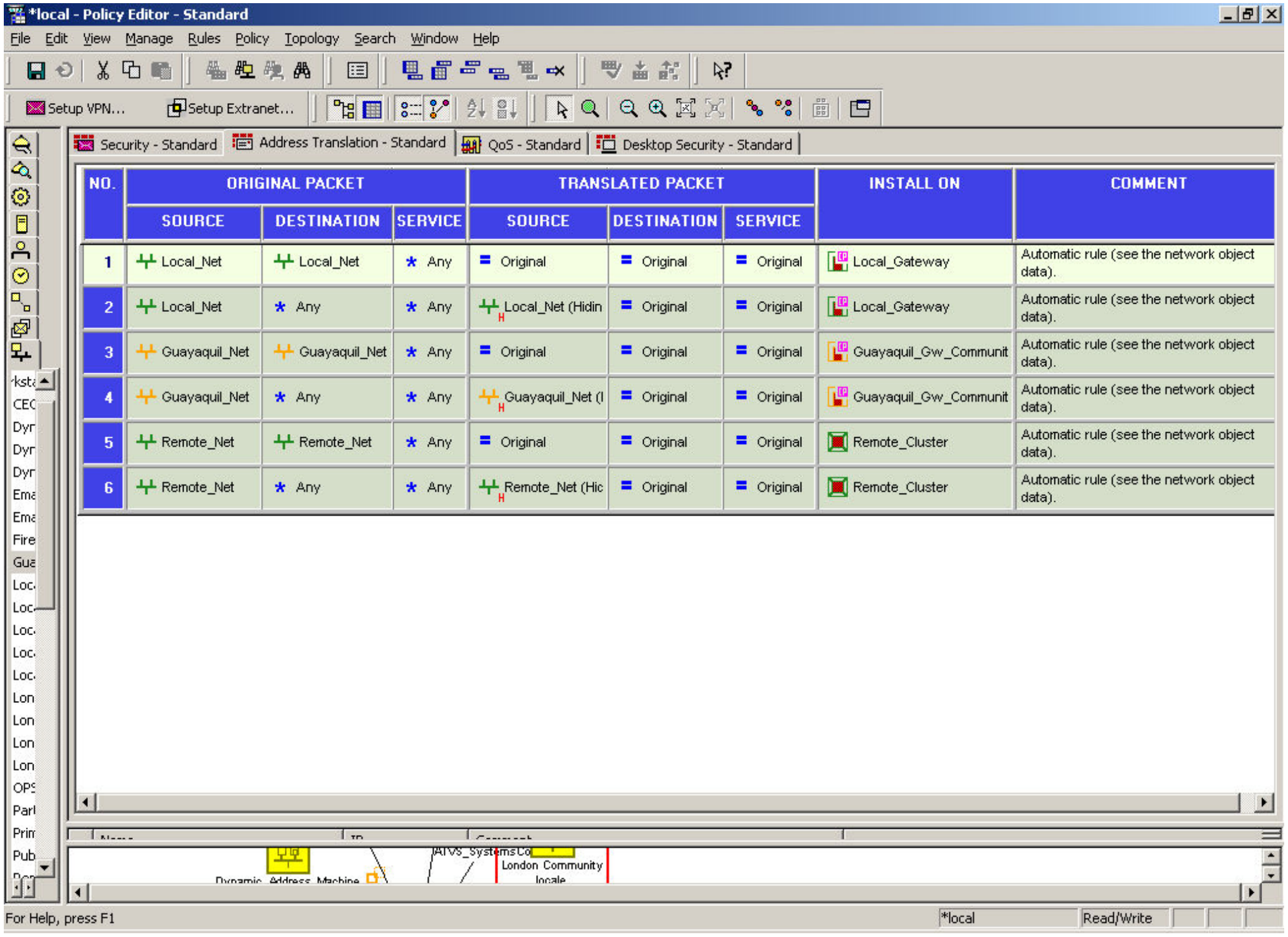



*Fig. 3.6 Firewall CheckPoint Address Translation - Standar*

En el Anexo G se encuentra de forma detallada toda la configuración principal del software de CheckPoint NG a través del utilitario Policy Editor NG.

### 3.3.2 CREACION DE LAS POLÍTICAS EN EL FIREWALL CHECKPOINT

Para instalar las diferentes políticas que van a ser aplicadas al tráfico que fluye desde o hacia la Internet es necesario conocer, cual es el tráfico que más circula por el canal, este análisis fue realizado al inicio de este capítulo, con estos antecedentes se debe escoger el lugar en done ubicar una política dependiendo de los servicios, es decir si hay un servicio que tiene el mayor tráfico, la política debe estar al principio de la reglas. Considerar que el Firewall filtra las políticas desde arriba hacia abajo.

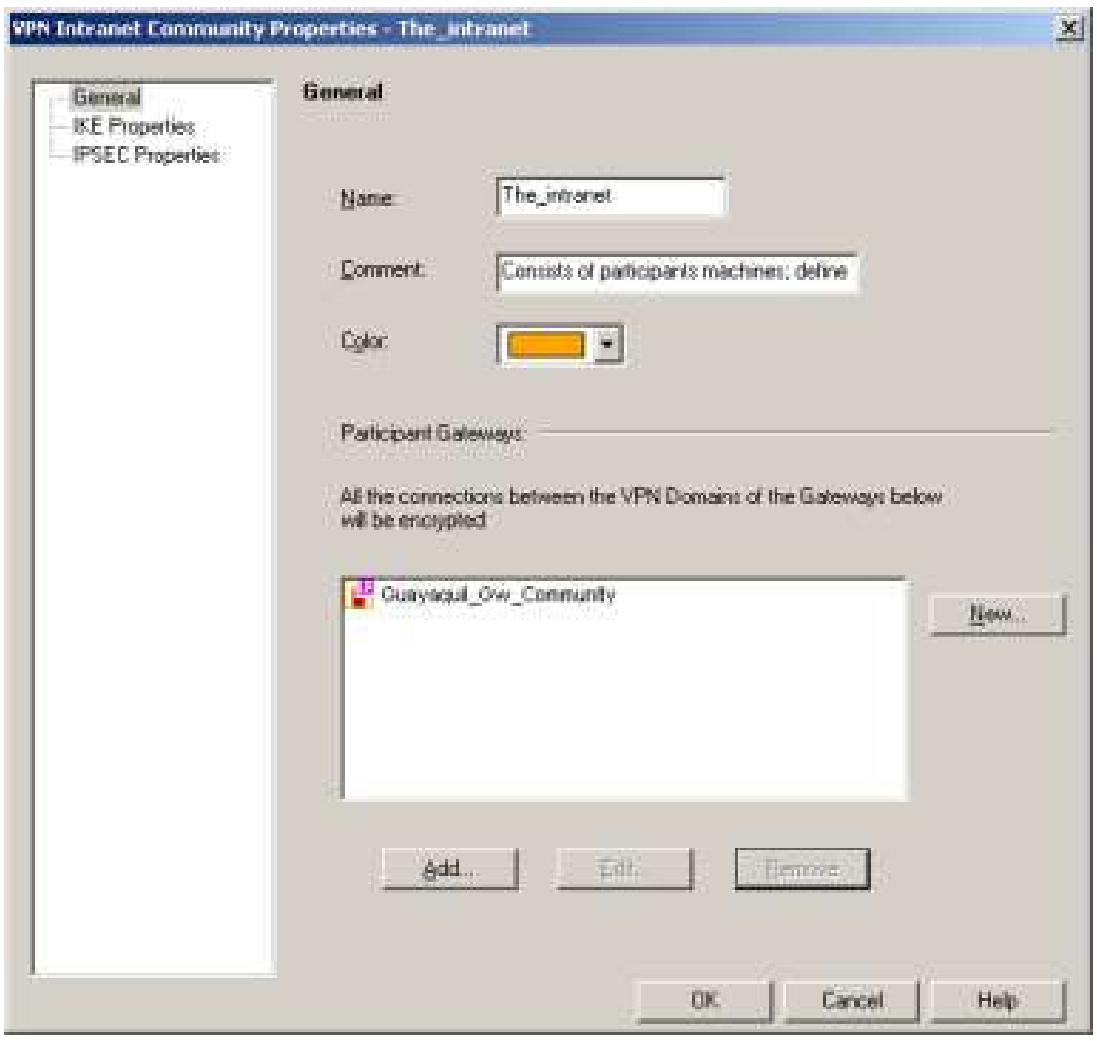
Entre las reglas más importantes que se han configurado se tiene:

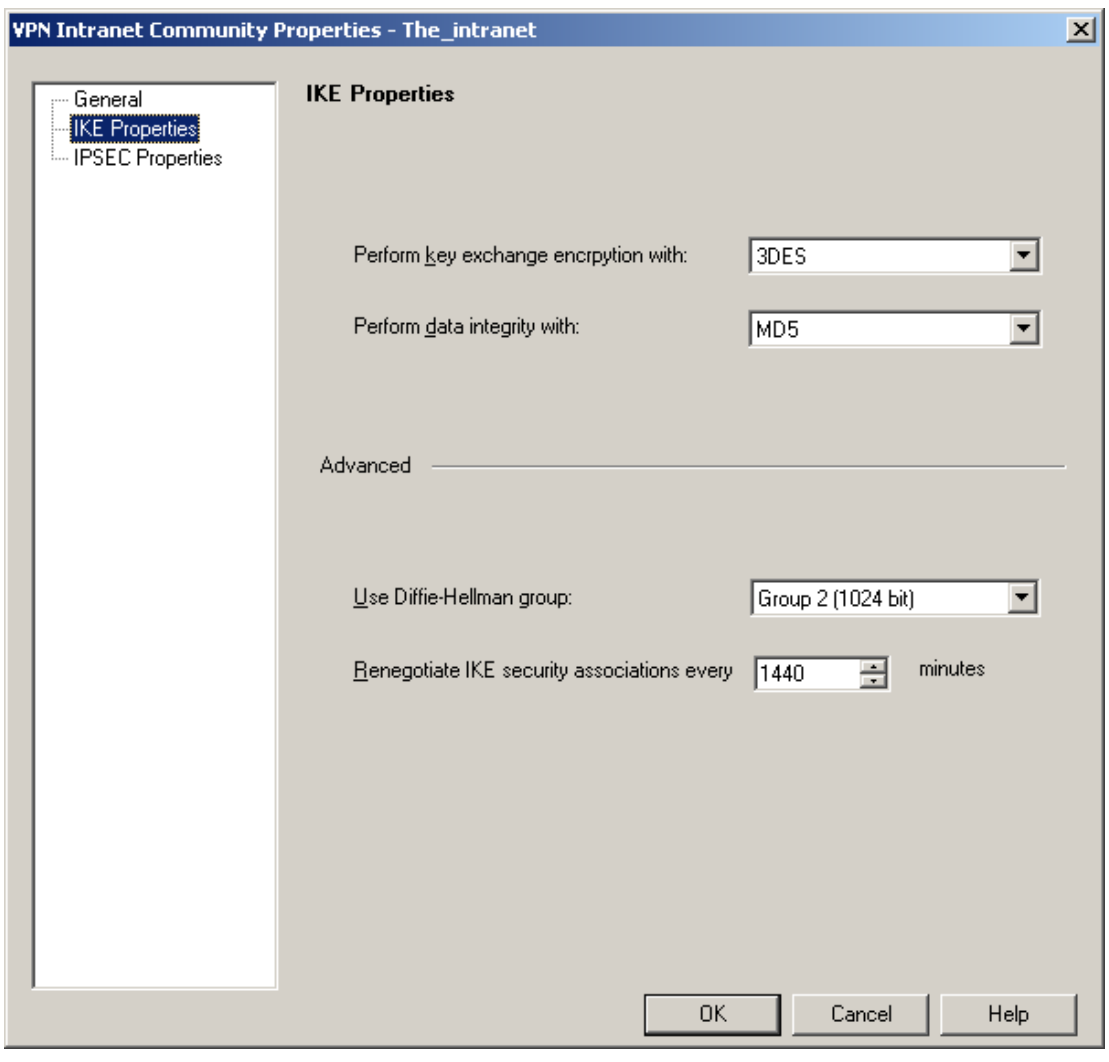
- **Regla de configuración de la VPN entre Oficina Matriz y Oficina Sucursal Mayor.**

  Como requerimiento básico toda regla que permite el paso de información a través de una VPN debe estar al principio de todas las reglas, sea ésta sitio a sitio o desde un cliente hacia la red Interna.

  La VPN es desde la red de la Oficina Matriz de Quito a la red de la Oficina Sucursal Mayor de Guayaquil, con un protocolo estándar como es IPSEC, con algoritmo de encripción 3DES y método hash MD5, la configuración de la VPN se muestra en la página siguiente:

## CONFIGURACION VPN ENTRE MATRIZ Y GUAYAQUIL



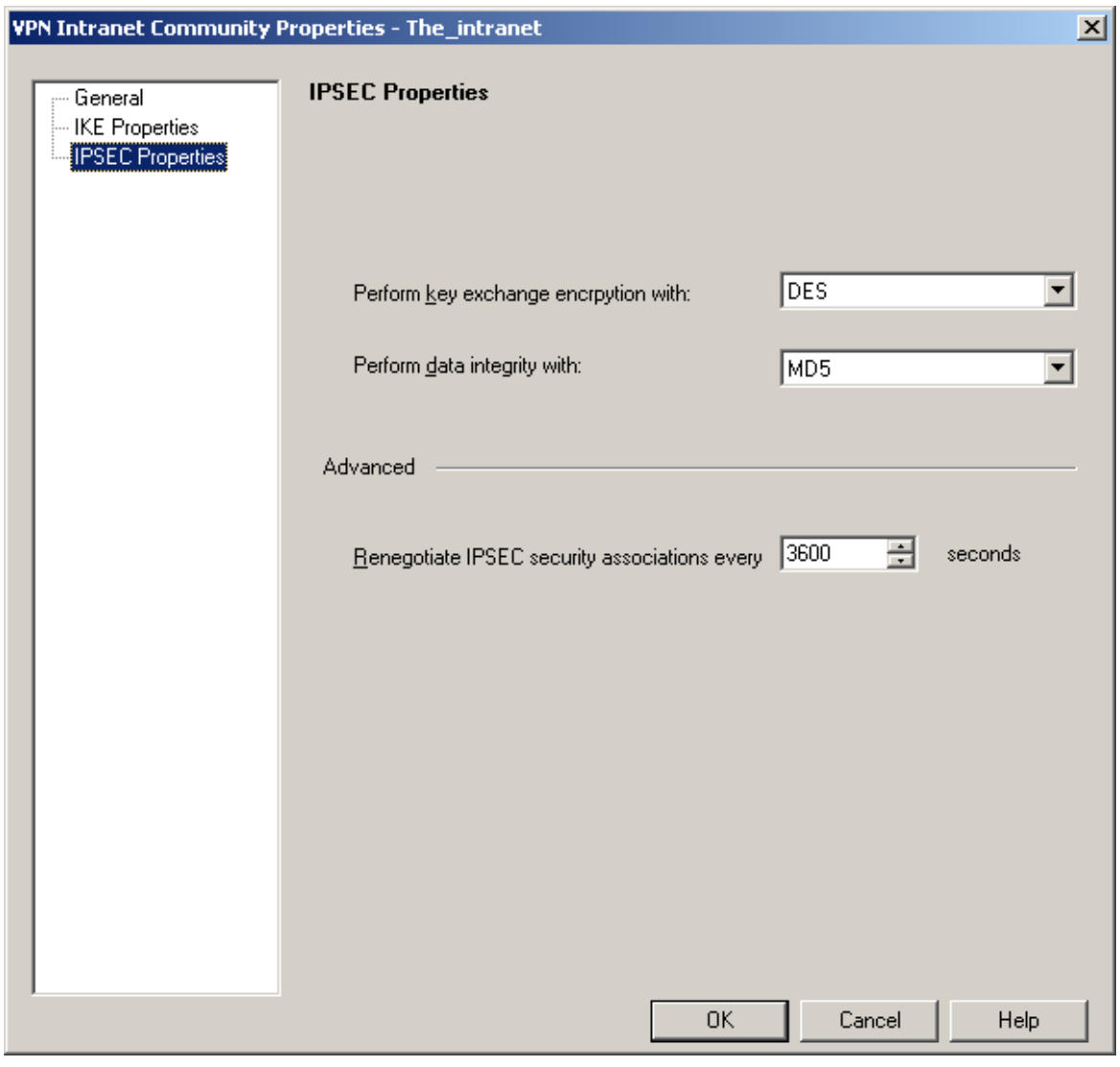



*Fig. 3.7 Configuración VLAN entre Matriz y Sucursal de Punto Net*

La VPN se configura con el módulo de Encripción IKE y IPSEC.

El objetivo de esta VPN es que el tráfico que circula desde la red Matriz hacia la Sucursal pase encriptada y segura y viceversa.

En la Fig. 3.8, regla 2 se presenta la configuración del CheckPoint para la VPN.

- **Regla de bloqueo del protocolo Netbios**

  Esta regla permite bloquear todo el tráfico Netbios entre las diferentes interfases que tiene el Firewall, en la Fig. 3.8, regla 3 se encuentra explicado esta configuración.

- **Regla para administración del Firewall**

  Mediante esta regla, solamente las computadoras que tengan los permisos correspondientes pueden tener acceso a la administración del Firewall, en la Fig. 3.8, regla 4 se encuentra la forma de tener estos permisos.

- **Regla de bloqueo de tráfico hacia el Firewall**

  A través de esta regla ninguna computadora de cualquiera de las sub redes podrán ver las interfaces del Firewall con ningún servicio, esto permite trabajar al Firewall en modo escondido, la Fig. 3.8, regla 5 se encuentra el proceso para realizar implementar esta tarea.

- **Regla para permitir acceso al tráfico de Web**

  Esta regla permitirá acceder al Internet a las diferentes páginas Web, siempre que los usuarios tengan los permisos correspondientes, a través de un servidor proxy que realiza las funciones de proxy_cache, en la Fig. 3.8, regla 6 se implementa las reglas necesarias.

- **Regla para permisos de funcionamiento del correo**

  Como plataforma de correo se tiene Sendmail 9.0, sobre la plataforma Linux, este servidor para sacar tráfico desde la red interna hacia el exterior, se conecta a un servidor proxy que hace las funciones de mail relay, por este motivo como regla principal se tiene la regla entre el servidor proxy y el servidor de relay y con servicio de SMPT, en la Fig. 3.8 regla 7 se encuentra la forma de agregar los permisos para esta regla.

- **Regla para el servicio de DNS**

  Este servicio de DNS permite comunicar entre el DNS primario que se encuentra en el proveedor de Internic y el DNS secundario que se encuentra en el ISP, esta regla ayuda a controlar los puertos de acceso hacia este servicio, en la Fig. 3.8 regla 8 se encuentra los pasos para la creación de dicha regla.

- **Regla para la conexión de los servicios de la página WEB del ISP**

  Esta regla permite tener acceso a los servidores de Web tanto para los usuarios internos como para los clientes externos con las debidas seguridades, en la Fig. 3.8 regla 9 está la forma de configurar esta regla.

- **Regla de administración de los servidores bastión**

  Para la administración de los servidores bastión es necesario que los usuarios ingresen a estos servidores a través de autenticación y utilizando el puerto seguro con encripción SSH2, para esto se generan los usuarios que van a ingresar a través de la base de datos, en la Fig. 3.8 regla 10 se encuentra detallada dicha configuración

- **Regla de acceso a FTP**

  Este servicio es importante para el ISP ya que existen usuarios clientes corporativos que utilizan software de ftp cliente y se conectan a diferentes instituciones externas como son Mastercard, Super Intendencia de Bancos, Banco Central del Ecuador, etc, para este servicios se tiene un servidor proxy habilitado el puerto 1080, los usuarios se conectan a este servidor y por medio de este puerto tienen el servicio de ftp, en la Fig. 3.8 regla 11 se encuentra la configuración para este servicio.

- **Regla de acceso remoto**

  El servicio de acceso remoto se utiliza para la navegación a Internet de los clientes dial-up y corporativos de Punto Net, la autenticación de los usuarios es a través de radius, y en el Firewall se ponen los filtros específicos, en la Fig. 3.8 regla 12 se encuentra la implementada dicha regla.

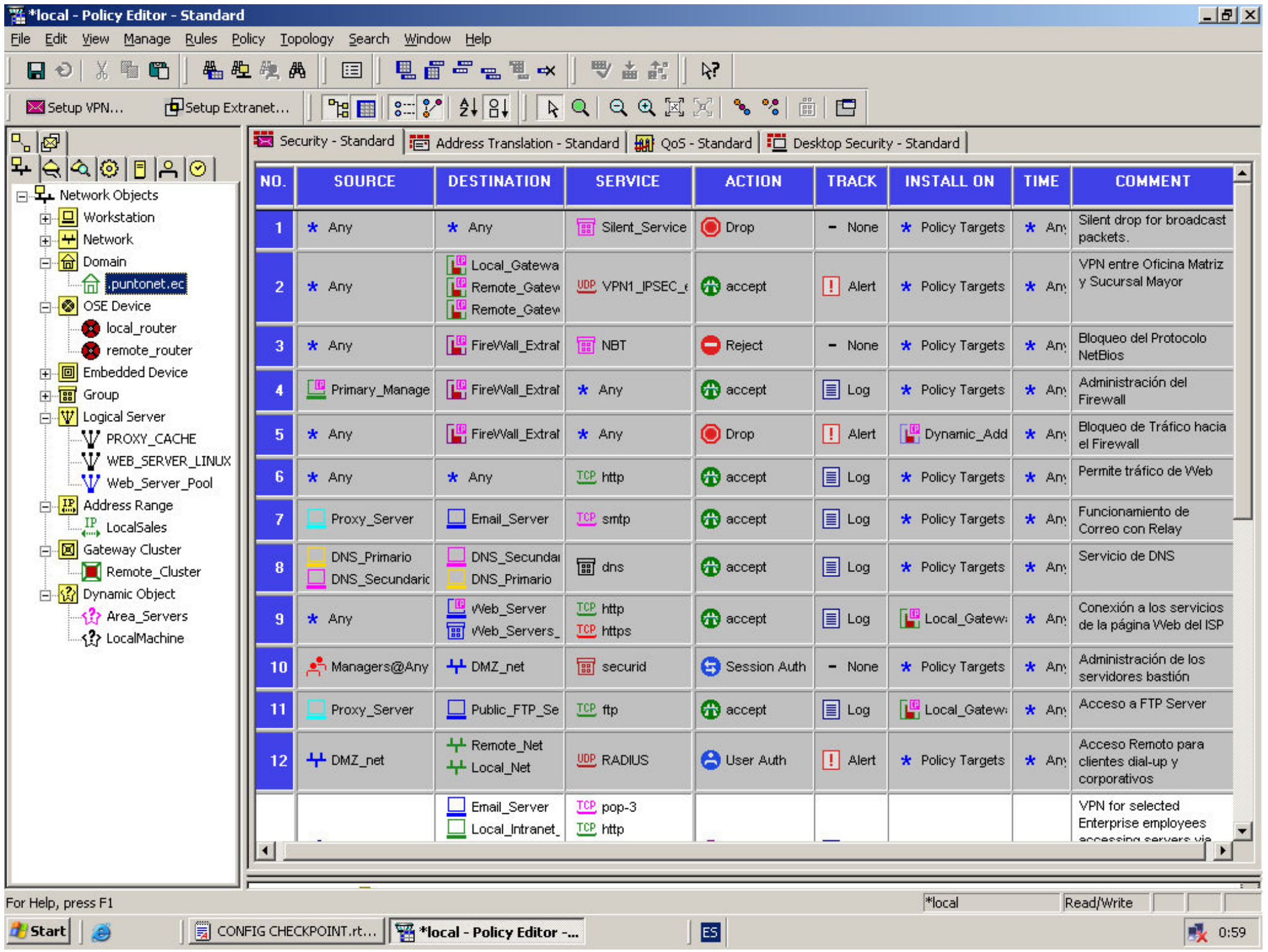



Fig. 3.8 Firewall CheckPoint – Reglas de Seguridad Iniciales

# 3.4 PRUEBAS DE FUNCIONAMIENTO DEL ESQUEMA DE SEGURIDAD DEL ISP

## 3.4.1 VULNERABILIDADES ENCONTRADAS

Luego de la implantación del Esquema de Seguridad basado en el Firewall Check Point, así como de las recomendaciones específicas dadas a cada una de las vulnerabilidades dadas en la sección 2.3.6.2 “Resultados de Pruebas”, se volvió a evaluar el nivel de riesgo y exposición de los 16 elementos críticos del ISP.

### 3.4.1.1 Período de pruebas

Se realizaron pruebas sobre el esquema de seguridad implantado en las siguientes fechas: 18, 25 y 29 de Junio del 2005.

Estas pruebas se realizaron en horario nocturno a fin de no comprometer ningún servicio de Punto Net.

Posteriormente, una vez identificado que no existían riesgos de afectar la disponibilidad de los elementos críticos se realizó una prueba integral el 2 de Julio del 2005.

### 3.4.1.2 Resultados de pruebas

Al realizar las pruebas de seguridades luego de implantar las recomendaciones dadas por el reporte de Nessus para corregir las vulnerabilidades detectadas y aplicar los patches respectivos a los 16 equipos críticos del ISP, identificamos que:

**Existen 24 debilidades de nivel alto de seguridad**

**Existen 161 debilidades de nivel medio de seguridad**

**Existen 215 debilidades de nivel bajo de seguridad**

Correspondiente a los siguientes equipos:

| Dirección IP | Descripción | Vulnerabilidades |
|---|---|---|
| 200.105.225.1 | Access Server1 Cisco 3640 | (**Existen 7 debilidades de nivel medio de seguridad**) |
| 200.105.225.2 | DNS Primario /Linux | (**Existen 2 debilidades de nivel alto de seguridad**) |
| 200.105.225.4 | Autent., DNS Secund/WIN2K | (**Existen 2 debilidades de nivel alto de seguridad**) |
| 200.105.225.5 | Border Router Cisco 7206 | (**Existen 9 debilidades de nivel medio de seguridad**) |
| 200.105.225.6 | Servidor Monitoreo/WIN2K | (**Existen 4 debilidades de nivel alto de seguridad**) |
| 200.105.225.7 | Access Server2 Cisco 2511 | (**Existen 10 debilidades de nivel medio de seguridad**) |
| 200.105.225.8 | Access Server3 Cisco 2511 | (**Existen 10 debilidades de nivel medio de seguridad**) |
| 200.105.225.9 | Access Server4 Cisco AS5300 | (**Existen 3 debilidades de nivel medio de seguridad**) |
| 200.105.225.10 | Router1 Cisco AS3620 | (**Existen 8 debilidades de nivel medio de seguridad**) |
| 200.105.225.11 | Web Server /WIN2K | (**Existen 3 debilidades de nivel alto de seguridad**) |
| 200.105.225.14 | Web Server /Linux | (**Existen 11 debilidades de nivel alto de seguridad**) |
| 200.105.225.17 | Access Server5 Cisco AS5300 | (**Existen 3 debilidades de nivel medio de seguridad**) |
| 200.105.225.18 | Access Server8 Cisco AS3640 | (**Existen 8 debilidades de nivel medio de seguridad**) |
| 200.105.225.19 | Access Server6 Cisco AS5300 | (**Existen 3 debilidades de nivel medio de seguridad**) |
| 200.105.225.22 | Caché Server – Cisco CE590 | (**Existen 2 debilidades de nivel alto de seguridad**) |
| 200.105.225.23 | Access Server7 Cisco AS5300 | (**Existe 1 debilidad de nivel medio de seguridad**) |

*Tabla 3.4 Resultados de vulnerabilidades luego de implantar el esquema de seguridad*
*Fuente: Los Autores*

Por otro lado identificamos las siguientes debilidades de seguridad en la red interna y en el Sistema de Facturación de Punto Net que aún se mantenían:

***RED INTERNA DE PUNTO NET:***

En la red interna de Punto Net, encontramos las siguientes debilidades de seguridad:

- No posee mecanismos de Auditoría sobre el Sistema Operativo, tampoco sobre archivos y objetos.

- Los recursos compartidos en algunos casos tienen los permisos de compartición “Acceso Total” para todos los usuarios.

***SISTEMA DE FACTURACION:***

En las pruebas del sistema de facturación que utiliza Punto Net se encuentra desarrollado en Visual Basic 6.0 como front-end y SQL Server 7.0 como back-end, encontramos las siguientes debilidades de seguridad:

- Las claves no cuentan con un adecuado esquema de seguridad en red que les provea de confidencialidad a los usuarios, pues no tienen definidos elementos de control como bloqueo por intentos fallidos en inicios de sesión, caducidad para un intervalo de tiempo, registro de contraseñas anteriores y longitud de clave, entre los principales.

- La base de datos no tiene activada la opción de Auditoría que permita identificar accesos fuera de la aplicación por parte del operador/administrador.

Adicionalmente en estas pruebas se evaluó las vulnerabilidades de la Plataforma Microsoft, considerando la implantación de recomendaciones realizadas hasta esta fecha, obteniéndose que el porcentaje total de equipos con vulnerabilidades disminuyó al 12%.  (Ver Anexo J).

# 3.5 AFINAMIENTO DEL ESQUEMA DE SEGURIDAD DEL ISP

## 3.5.1 AFINAMIENTO DEL FIREWALL

Una vez que se ha realizado la revisión de las recomendaciones de seguridad implantadas en los 16 elementos críticos y la verificación de la corrección de las vulnerabilidades en los equipos de la plataforma Microsoft, así como las pruebas al Esquema de Seguridad del ISP implantado, es necesario afinar la seguridad del ISP mediante la revisión de las reglas del Firewall, a fin de estar acorde a las políticas de seguridad requeridas y definidas para Punto Net. Ver Fig. 3.9 en página siguiente:

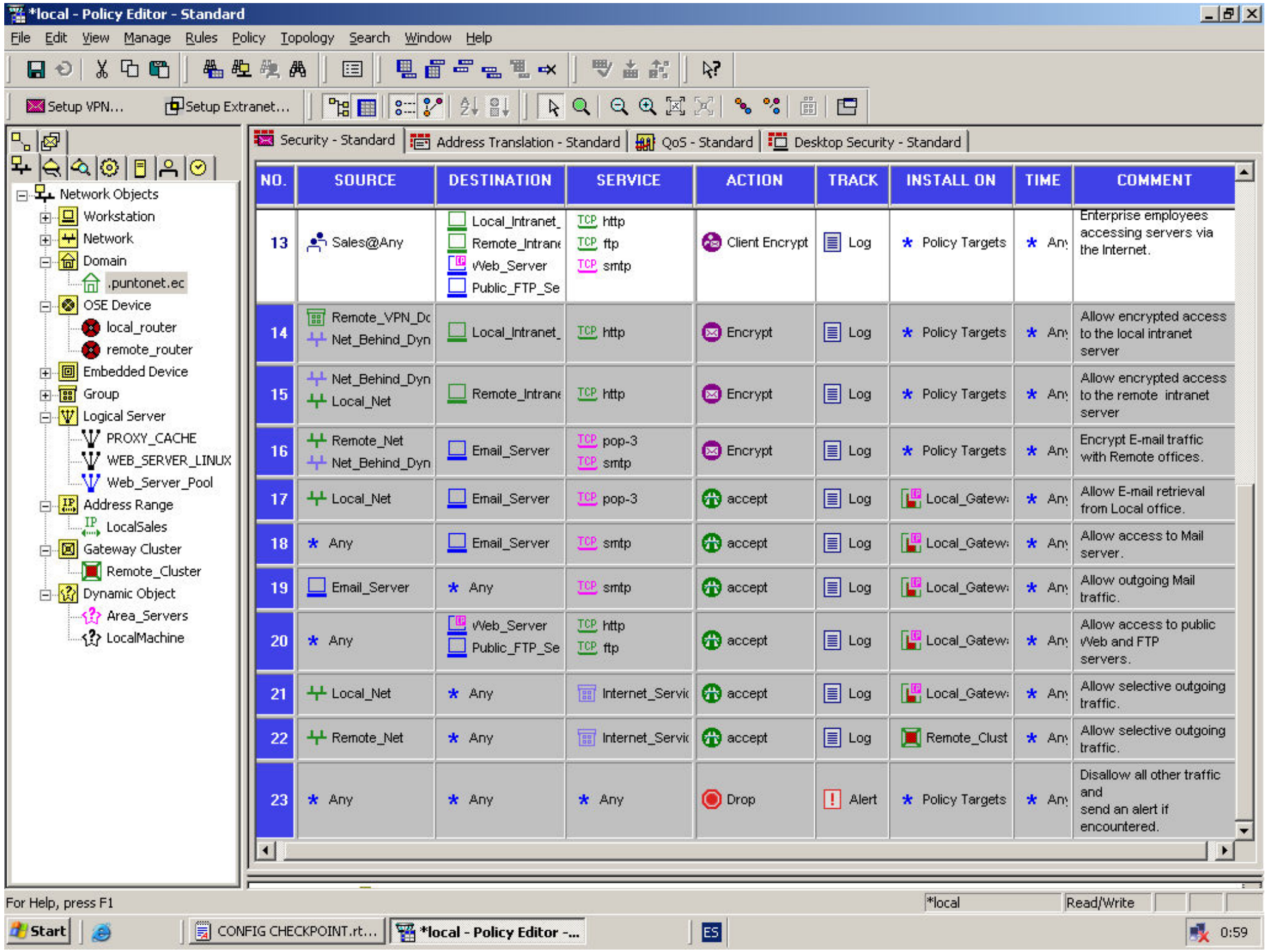



*Fig. 3.9 Firewall CheckPoint – Reglas de Seguridad Complementarias*

### 3.5.2 AFINAMIENTO DEL SERVIDOR DE FACTURACION

***SISTEMA DE FACTURACION:***

A fin de mejorar el ambiente de control y seguridades en la red interna de Punto Net, se procedió a afinar el servidor soporte a la aplicación de Facturación de Consumos en conjunto con el personal técnico del ISP.

- Se implantó un adecuado esquema de seguridad para las cuentas de usuario y sus contraseñas a fin de proveerles de confidencialidad a los usuarios y un mejor nivel de seguridad, mediante las definición de políticas locales en el servidor Windows 2000 como son: definición de elementos de control para cuentas de usuario a través del bloqueo por intentos fallidos en inicios de sesión, caducidad para un intervalo de tiempo, registro de contraseñas anteriores y longitud de clave, entre los principales.

- En la base de datos se activó la opción de Auditoría que permitirá identificar accesos fuera de la aplicación por parte del operador/administrador.

- Se complementó las seguridades mediante la instalación del Antivirus McAfee con las últimas actualizaciones SDAT.

- Se implantó el Service Pack 6 para Windows 2000 y se aplicaron todos los patches y hot fix recomendados según los reportes de Retina y Languard.

- Finalmente, se instaló una unidad de CD-ROM reescribible para la obtención de backups de la base de datos de forma local.

# ETAPA 4: REEVALUACION DEL NIVEL DE EXPOSICION Y RIESGO

## 3.6 SEGUIMIENTO A LA IMPLANTACION DE LAS RECOMENDACIONES DE AUDITORIA DE SEGURIDADES

Como en toda fase de Auditoría si no se realiza un seguimiento a las recomendaciones dadas, no se podrá garantizar un adecuado nivel de control de las empresas.

De ahí la necesidad de realizar este seguimiento a la implantación de las recomendaciones.

Al respecto debemos manifestar de manera general que prácticamente todas las recomendaciones emitidas en la sección “2.5 RECOMENDACIONES DE SEGURIDAD” de esta TESIS han sido implantadas y reevaluadas a fin de minimizar el nivel de riesgo y exposición ante ataques al ISP que podrían surgir como fruto de las vulnerabilidades y huecos de seguridad identificados.

Para clarificar más esta situación, mostramos a continuación las Matrices de Seguimiento respectivas asociadas por el objetivo de control específico y su nivel de riesgo identificado.

En páginas siguientes se mostrarán solo aquellos objetivos de control que fueron evaluados como “NO EFECTIVOS” en su cumplimiento.

### 3.6.1 MATRIZ DE SEGUIMIENTO DE OBJETIVOS DE CONTROL CON RIESGO ALTO

| **MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES**<br><br>**DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE** | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.1 Administrar Medidas de Seguridad** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br><br>Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte<br><br>*Probando que:*<br><br>Los parámetros de seguridad del sistema tienen como base estándares locales/del proveedor. | Solicitar documento de políticas de seguridad.<br><br>Entrevista al Gerente de TI.<br><br>Revisión del Plan de Contingencia. | NO EFECTIVO | Ver **Recomendación DS5.1** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACION IMPLANTADA** |

*Tabla 3.5 Matriz de Seguimiento DS5.1*
*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.2 Identificación, Autenticación y Acceso** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br><br>Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.<br>Los mecanismos de autenticidad en uso proveen las siguientes facilidades:<br>• uso individual de datos de autenticación<br>• autentificación múltiple<br>• autenticación basada en políticas<br>• Autenticación por demanda<br><br>La política de password incluye:<br>• Forzar el cambio inicial de password la primera vez de uso<br>• longitud adecuada mínima del password<br>• la frecuencia obligada mínima de cambio de password<br>• verificación del password en la lista de valores no permitidos<br>• protección adecuada para los passwords de emergencia | Entrevista al Gerente de TI.<br><br>Correr herramienta que ayude a detectar problemas con claves y vulnerabilidades de seguridad en los servidores de aplicación. | NO EFECTIVO | Ver **Recomendación DS5.2** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACION IMPLANTADA** |

*Tabla 3.6 Matriz de Seguimiento DS5.2*
*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.5 Revisión Gerencial de Cuentas de Usuario** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br>Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.<br>Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.<br>Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir:<br>• intentos no autorizados de acceso al sistema (sign on)<br>• intentos no autorizados de acceso a los recursos del sistema<br>• privilegios de acceso a recursos por ID de usuario<br>• modificaciones autorizadas a las definiciones y reglas de seguridad<br>• accesos autorizados a los recursos<br><br>*Probando que:*<br>TI cumple con los estándares de seguridad relacionados con reportes y revisión gerencial de las violaciones e incidentes de seguridad. | Aplicación de las herramientas LANGUARD y RETINA. Ver anexos E y F.<br><br>Revisión de los archivos Log para revisión de accesos a los recursos. | NO EFECTIVO | Ver **Recomendación DS5.5** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACION IMPLANTADA** |

*Tabla 3.7 Matriz de Seguimiento DS5.5*

*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.6 Control de Usuarios sobre Cuentas de Usuario** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br><br>Al ingresar al sistema, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.<br><br>Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales.<br><br>Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario.<br><br>*Probando que:*<br>TI cumple con los estándares de seguridad relacionados con la administración de perfiles de usuario y clasificación de la seguridad de datos<br><br>Existen procedimientos para el mantenimiento del acceso de usuarios al sistema y existen procedimientos de “logon” vigentes para sistemas y usuarios. | Entrevista al Gerente de TI.<br><br>Aplicar pruebas específicas sobre los controles de usuarios en el acceso a aplicaciones. | NO EFECTIVO | Ver **Recomendación DS5.6** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACION IMPLANTADA** |

*Tabla 3.8 Matriz de Seguimiento DS5.6*
*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br><br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.7 Vigilancia de seguridad** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles*:<br>Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas.<br><br>Estos reportes deberán incluir:<br>- Intentos no autorizados de acceso al sistema (sign on).<br>- Intentos no autorizados de acceso a los recursos del sistema.<br>- Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.<br>- Privilegios de acceso a recursos por ID de usuario.<br>- Modificaciones autorizadas a las definiciones y reglas de seguridad de TI.<br>- Accesos autorizados a los recursos (seleccionados por usuario o recurso).<br>- Cambio de estatus de la seguridad del sistema.<br>- Accesos a las tablas de parámetros de seguridad del sistema operativo.<br><br>*Probando que*:<br>TI cumple con los estándares de seguridad relacionados con: reportes y revisión gerencial de las violaciones e incidentes de seguridad. Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. | Revisión de manuales de procedimientos y plan de seguridad IT y de Logs de seguridad del sistema.<br><br>Entrevista al Gerente de TI. | NO EFECTIVO | Ver **Recomendación DS5.7** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACION IMPLANTADA** |

*Tabla 3.9 Matriz de Seguimiento DS5.7*

*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.8 Clasificación de datos** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br><br>Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.<br><br>*Probando que:*<br><br>Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.<br><br>Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad.<br><br>El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante. | Revisión de manuales de procedimientos y funciones.<br><br>Entrevista al Gerente de TI. | NO EFECTIVO | Ver **Recomendación DS5.8** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACIÓN IMPLANTADA** |

*Tabla 3.10 Matriz de Seguimiento DS5.8*
*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br>DOMINIO: ENTREGA DE SERVICIO Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.11 Manejo de Incidentes** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br><br>Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte.<br><br>Se utilizan rutas confiables para transmitir información sensitiva.<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br><br>Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. | Revisión del plan de seguridad IT respecto del manejo de incidentes.<br><br>Entrevista al Gerente de TI. | NO EFECTIVO | Ver **Recomendación DS5.11** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACIÓN IMPLANTADA** |

*Tabla 3.11 Matriz de Seguimiento DS5.11*
*Fuente: Los Autores*

| MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES<br>DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE | | | | |
|---|---|---|---|---|
| ***DS5 Garantizar la seguridad de Sistemas*** | | | | |
| **DS5.20 Arquitectura de Firewalls y conexión a redes públicas** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br><br>El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la "necesidad de conocer".<br><br>Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.<br><br>*Probando que:*<br>Los firewalls poseen por lo menos las siguientes propiedades:<br>- Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles lógicos, debe reforzarse físicamente).<br>- Sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local.<br>- Los firewalls por sí mismo es inmune a la penetración.<br>- El tráfico de intercambio en el firewall se lleva a cabo en la capa de aplicación únicamente. | Entrevista al Gerente de T.I.<br><br>Aplicar una herramienta para detectar las vulnerabilidades de la red.<br><br>Identificar la existencia de un Firewall y sus reglas definidas actualmente.<br><br>Evaluar la arquitectura de seguridad del Firewall para el ISP. | NO EFECTIVO | Ver **Recomendación DS5.20** en sección 2.5.1 **RECOMENDA-CIONES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACIÓN IMPLANTADA** |

*Tabla 3.12 Matriz de Seguimiento DS5.20*
*Fuente: Los Autores*

## 3.6.2 EVALUACION DE PRUEBAS DE OBJETIVOS DE CONTROL CON RIESGO MEDIO

| **MATRIZ DE SEGUIMIENTO A LA IMPLANTACION DE RECOMENDACIONES**<br><br>**DOMINIO: ADQUISICION E IMPLEMENTACION** | | | | |
|---|---|---|---|---|
| ***AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica*** | | | | |
| **AI3.3 Seguridad de Software del sistema** | | | | |
| **REVISION A TRAVES DE:** | **DESCRIPCION DE LA PRUEBA** | **EVALUACION** | **RECOMENDACIÓN** | **SEGUIMIENTO** |
| *Evaluación de controles:*<br>Existen políticas y procedimientos asegurando que:<br>- la posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de información operativa está limitada<br>- la preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados.<br>- se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema.<br><br>*Probando que:*<br>Existen las declaraciones de aseguramiento de la integridad del software del sistema entregados por los proveedores para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema.<br>Los parámetros del software del sistema aseguran que el personal apropiado de TI seleccionó los correctos con el fin de asegurar la integridad de los datos y los programas almacenados en el sistema. | Revisión de parámetros de seguridad de los sistemas operativos, bases de datos en servidores principales y revisión de la aplicación de Facturación. | NO EFECTIVO | Ver **Recomendación AI3.3** en sección 2.5.1 **RECOMENDACIO-NES SOBRE EL CUMPLIMIENTO DE LOS OBJETIVOS DE CONTROL ESPECIFICOS.** | **RECOMENDACIÓN IMPLANTADA** |

*Tabla 3.13 Matriz de Seguimiento AI3.3*
*Fuente: Los Autores*

# 3.7 REEVALUACION DEL NIVEL DE RIESGO Y EXPOSICION ANTE ATAQUES AL ISP

A fin de identificar el nivel de riesgo y exposición ante ataques que podría tener el ISP, luego del afinamiento al Esquema de Seguridad implantado, hemos reevaluado las vulnerabilidades en los 16 elementos críticos de la red del ISP, obteniendo lo siguiente:

## 3.7.1 VULNERABILIDADES OBTENIDAS

Las pruebas finales fueron coordinadas con el Gerente Técnico de Punto Net, y se generó un ambiente de pruebas a fin de prevenir cualquier eventualidad que podría suceder en los equipos reales.

Se coordinó la preparación de las configuraciones de prueba en los elementos críticos de comunicaciones de manera similar al ambiente de operación real.

Se realizaron pruebas de vulnerabilidades desde el Internet y el interior de la red sobre 16 elementos críticos de la infraestructura de Punto Net como son: Routers, Access Servers, Servidores Windows 2000 y Servidores Linux; y servicios de red: Web, FTP, e-mail, autenticación, etc.

Adicionalmente, se han realizado las pruebas al Sistema de Facturación, a la base de datos SQL Server, al servidor de la red Interna de Punto Net y al Firewall Interno.

### 3.7.1.1 Período de pruebas:

Se realizaron pruebas independientes sobre los sistemas en un ambiente de pruebas en las siguientes fechas:  9, 10, 18 y 19 de Julio del 2005.

Estas pruebas se realizaron en horario nocturno a fin de no comprometer ningún servicio de Punto Net.

Posteriormente, una vez identificado que no existían riesgos de afectar la disponibilidad de los elementos críticos se realizaron pruebas globales el 29 y 30 de Julio del 2005.

### 3.7.1.2 Resultados de pruebas:

De acuerdo a las últimas pruebas realizadas sobre 16 equipos críticos de la red global de Punto Net, identificamos que el nivel de riesgo y exposición de seguridad ha disminuido considerablemente, ya que:

**Existen 13 debilidades de nivel alto de seguridad**

**Existen 37 debilidades de nivel medio de seguridad**

**Existen 137 debilidades de nivel bajo de seguridad**

Correspondiente a los siguientes equipos:

| Dirección IP | Descripción | Vulnerabilidades |
|---|---|---|
| 200.105.225.1 | Access Server1 Cisco 3640 | **(Existe 1 debilidad de nivel medio de seguridad)** |
| 200.105.225.2 | DNS Primario /Linux | **(Existe 1 debilidad de nivel medio de seguridad)** |
| 200.105.225.4 | Autent., DNS Secund/WIN2K | **(Existen 3 debilidades de nivel medio de seguridad)** |
| 200.105.225.5 | Border Router Cisco 7206 | **(Existe 1 debilidad de nivel alto de seguridad)** |
| 200.105.225.6 | Servidor Monitoreo/WIN2K | **(Existe 1 debilidad de nivel alto de seguridad)** |
| 200.105.225.7 | Access Server2 Cisco 2511 | **(Existe 1 debilidad de nivel medio de seguridad)** |
| 200.105.225.8 | Access Server3 Cisco 2511 | **(Existen 2 debilidades de nivel medio de seguridad)** |
| 200.105.225.9 | Access Server4 Cisco AS5300 | **(Existen 3 debilidades de nivel medio de seguridad)** |
| 200.105.225.10 | Router1 Cisco AS3620 | **(Existen 3 debilidades de nivel medio de seguridad)** |
| 200.105.225.11 | Web Server /WIN2K | **(Existe 1 debilidad de nivel medio de seguridad)** |
| 200.105.225.14 | Web Server /Linux | **(Existen 6 debilidades de nivel alto de seguridad)** |
| 200.105.225.17 | Access Server5 Cisco AS5300 | **(Existen 2 debilidades de nivel medio de seguridad)** |
| 200.105.225.18 | Access Server8 Cisco AS3640 | **(Existen 3 debilidades de nivel medio de seguridad)** |
| 200.105.225.19 | Access Server6 Cisco AS5300 | **(Existen 2 debilidades de nivel medio de seguridad)** |
| 200.105.225.22 | Caché Server – Cisco CE590 | **(Existen 4 debilidades de nivel alto de seguridad)** |
| 200.105.225.23 | Access Server7 Cisco AS5300 | **(Existe 1 debilidad de nivel medio de seguridad)** |

*Tabla 3.14 Resultados finales de vulnerabilidades*
*Fuente: Los Autores*

En forma global, identificamos el siguiente nivel de riesgos de seguridad:

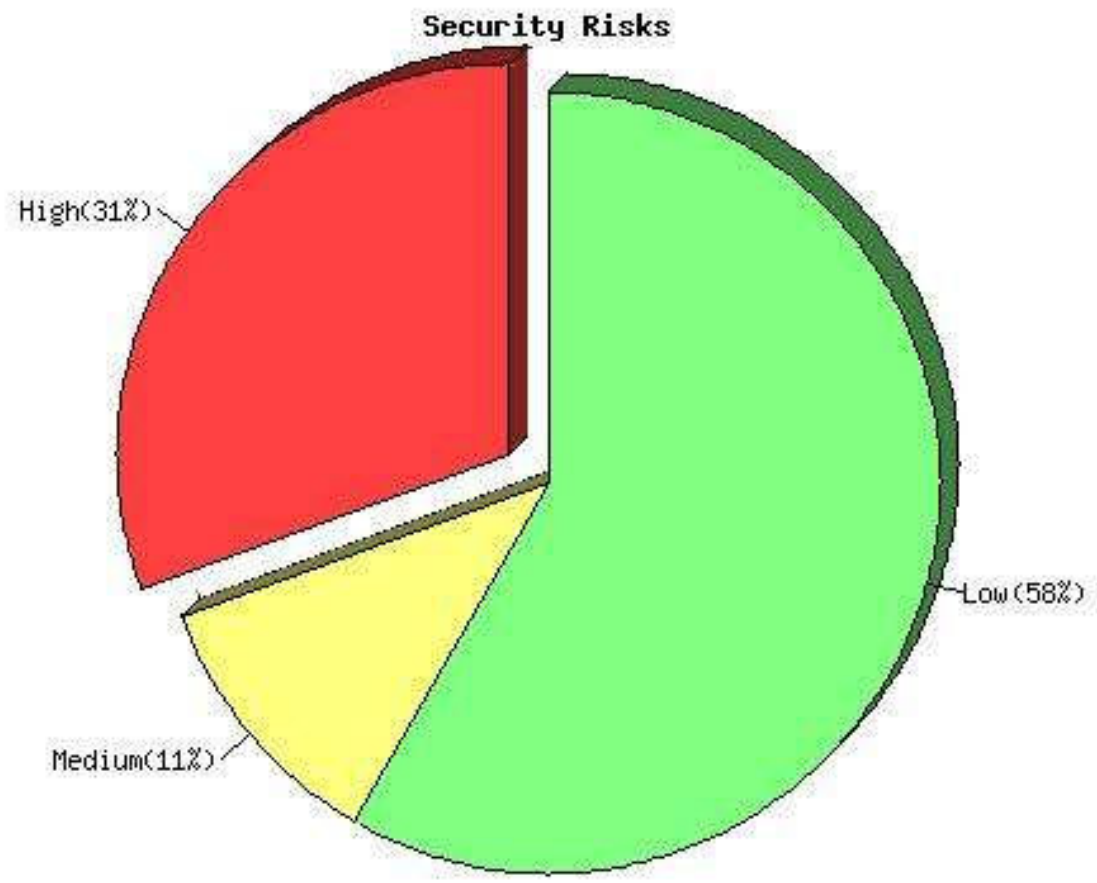



*Fig. 3.10 Nivel de exposición y riesgos de seguridad final del ISP*
*Fuente: Diagnóstico final de vulnerabilidades con NESSUS*

De la globalidad (16 elementos críticos evaluados), identificamos que el Servidor Web sobre Linux es el que posee mayor cantidad de vulnerabilidades, esta situación existe ya que este servidor es público y tiene el servicio de Hosting de los clientes de Punto Net.

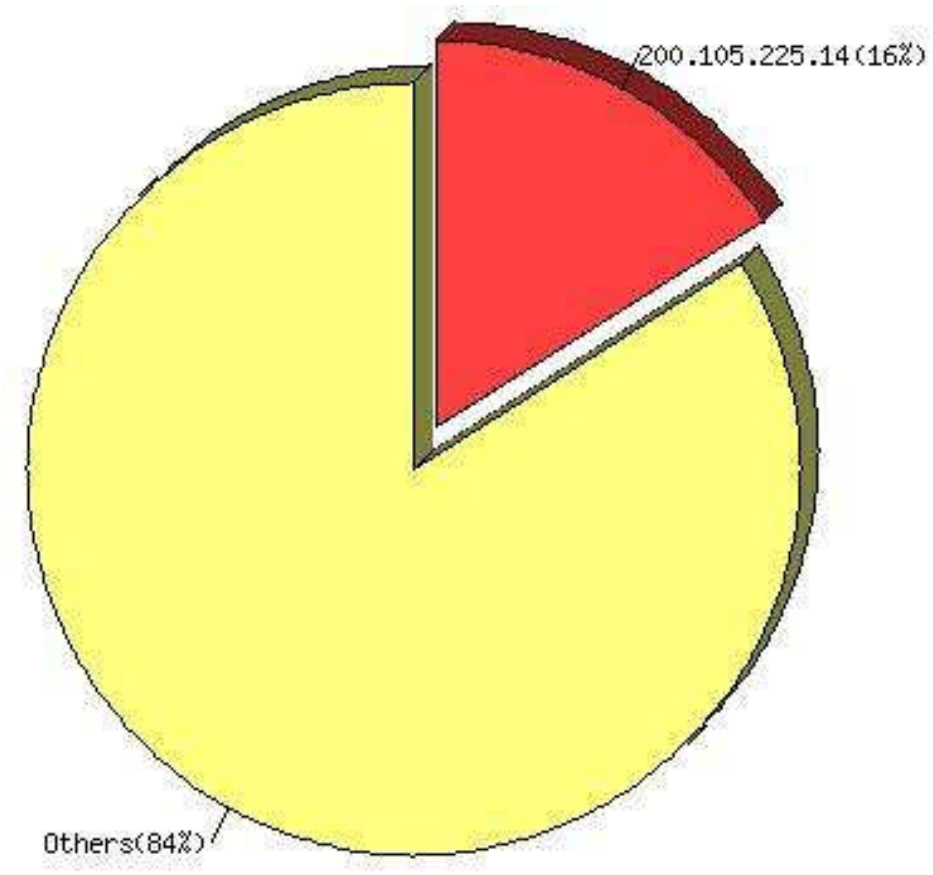



*Fig. 3.11Mayor incidencia de exposición y riesgos de seguridad del servidor Web*
*Fuente: Diagnóstico final de vulnerabilidades con NESSUS*

Adicionalmente, identificamos que la mayor cantidad de problemas de seguridad se debe a los protocolos “ssh” y “ftp”, tal como se indica a continuación:

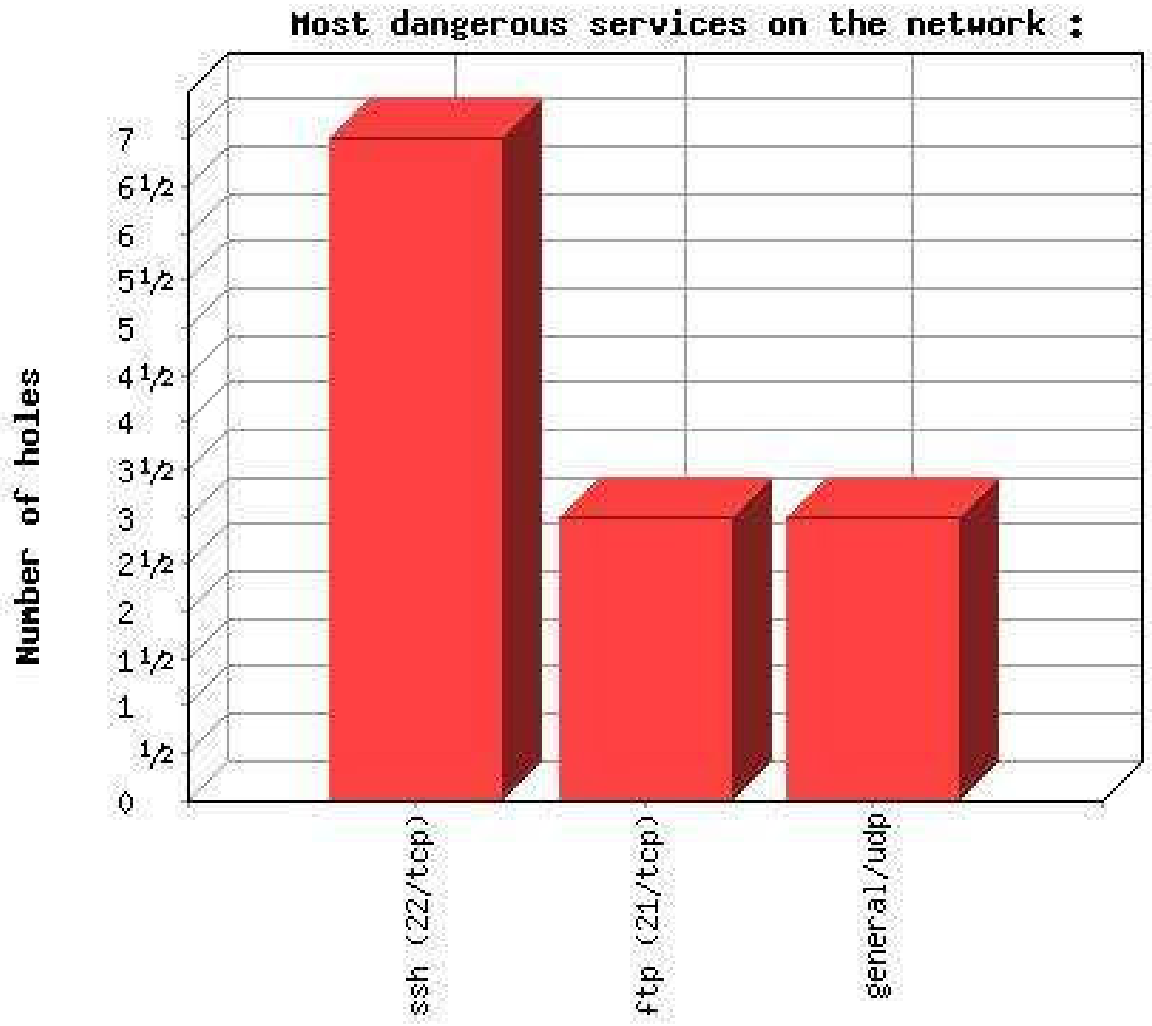



*Fig. 3.12 Servicios de red con mayor nivel de riesgos de seguridad de ISP*
*Fuente: Diagnóstico final de vulnerabilidades con NESSUS*

Se debe indicar que como conclusión general de esta etapa de reevaluación del nivel de exposición y riesgo ante ataques al ISP, podemos decir que es necesaria la evaluación permanente de las seguridades del ISP debido a que día a día aparecen nuevas vulnerabilidades y cambios al software, razón por la cual si el personal técnico del ISP no tiene una cultura de seguridad informática que le permita establecer un adecuado y permanente nivel de control de los recursos y servicios que se proveen a los usuarios finales, entonces el negocio del ISP puede fracasar.

# CAPITULO 4

# CONCLUSIONES Y RECOMENDACIONES

## 4.1 CONCLUSIONES

**a)** La utilización del marco de referencia de COBIT a través de sus guías de Auditoría, nos ha permitido enfocar efectivamente sobre los controles requeridos de tecnología que requiere el ISP para brindar un ambiente seguro para la transmisión de información a través del Internet.

**b)** Hemos podido apreciar que en este tipo de empresas, como son los ISP, el enfoque de seguridad tiene una restricción de seguridad en especial al contenido de la misma, debido a que la mayoría de los clientes del ISP utilizan el servicio de Internet como medio de navegación y emisión de correo electrónico, sin requerir altos niveles de confidencialidad ni encriptación.

**c)** De la evaluación inicial de vulnerabilidades a los 16 equipos críticos del ISP caso de estudio, se identificó principalmente que existían 47 debilidades de un nivel alto de seguridad y 188 debilidades de nivel medio. Sin embargo, al finalizar esta TESIS, luego de implantar las recomendaciones de seguridad e implantar el esquema de seguridad para el ISP, se identificó que aún existían 13 debilidades de un nivel alto de seguridad y 37 debilidades de nivel medio. Todo esto indica que no existe una seguridad absoluta en la que se mitigen todos los riesgos y se eliminen las vulnerabilidades, por lo que el tema de seguridad informática es un tema de evaluación permanente en una organización.

**d)** Una importante conclusión es el hecho de que generalmente se toma en consideración todas las medidas preventivas y controles de acceso a las aplicaciones críticas, como es el caso de la aplicación “Facturación” en el ISP caso de estudio, sin embargo, el administrador de la base de datos donde reside toda la información, no tiene clave y tampoco está habilitada la opción de auditoría.

**e)** El implantar un Esquema de Seguridad en el ISP caso de estudio, involucra no sólo configurar adecuadas políticas en un Firewall, sino también corregir todas las vulnerabilidades detectadas durante un proceso de evaluación de seguridades, pero quizás lo más importante es generar una concientización en

los usuarios y Gerencia, para que las políticas que se adopten puedan garantizar el cumplimiento de los objetivos organizacionales.

**f)** Una baja inversión económica en recursos y componentes tecnológicos asociada a la falta de un perfil con capacidades de administración de seguridad tecnológica no permite centralizar la administración y limita la implantación de controles a nivel de tecnología que aporten el mejoramiento del ambiente de control interno del caso de estudio, ISP.

**g)** Es necesario siempre realizar un análisis de riesgo en la etapa preliminar del trabajo de auditoría, a fin de conocer la organización objeto de estudio, ISP. Con la selección de los objetivos de control a auditar de acuerdo al nivel de riesgo alto y medio se puede enfocar mejor el trabajo de evaluación.

**h)** Para asegurar la integridad, completitud y exactitud de la información que es analizada por la gerencia y entregada para la toma de decisiones del directorio del ISP, se debe crear políticas con un criterio maduro sobre control y niveles de seguridad que se proyecten desde la cúspide del plano organizacional (Gerencias, Comités Generales, Directorios Ejecutivos) hacia los niveles administrativos y operativos.

**i)** Mediante un análisis de riesgos realizado para el ISP, hemos conocido las vulnerabilidades de la red y su infraestructura de telecomunicaciones, así como las posibles soluciones de control, en función de la evaluación del cumplimiento los objetivos de auditoría y su verificación con las estrategias del negocio.

**j)** Las guías de auditoria COBIT fueron utilizadas en la elaboración de las matrices de pruebas lo cual nos permitió obtener un plan de auditoría efectivo.

**k)** En una arquitectura de conexión hacia la Internet, se deben implementar dispositivos que garanticen la seguridad de la red Interna y de la información que fluya por esta, estos dispositivos son: Firewall, Detector de Intrusos,

Ruteadores, Switch de capa 2, Servidores bastión (Proxy), servidores de acceso remoto, etc.

**l)** Los dispositivos de seguridad que desee adquirir una empresa y el tipo de características que este tenga, depende del nivel de importancia del negocio, es decir si se trata de un proveedor de servicios de Internet, como fue el caso de estudio, es importante la implementación de productos que permitan monitorear, detectar y bloquear cualquier acceso indebido de intrusos en los servidores de la red. Esto de una manera rápida y efectiva, sin importar el costo de los mismos.

**m)** Toda herramienta o dispositivo que se instale como un elemento de seguridad debe tener la facultad de generar logs que registren las diferentes sesiones de conexión que atraviesen o acceden a él, es importante que todo dispositivo de seguridad genere un Log, que permita a futuro, a través de una herramienta o manualmente, realizar un análisis del mismo con el fin de detectar el intento de intrusos a nuestra red interna, y además poder detectar problemas de huecos de seguridad, como de configuración de los propios dispositivos.

**n)** Separar las redes DMZ, a nivel de funcionalidad y acceso, esto es, redes de pruebas y redes de producción. Además, la arquitectura de red de conexión hacia la Internet, debe estar contemplada con planes de contingencia, toda conexión hacia la Internet desde la red interna debe pasar a través de los servidores bastión o proxy, con el fin de que cualquier control de ataques lo podamos hacer en esta red desmilitarizada.

**o)** Todos los servidores que disponen de una base de datos donde se encuentre la información importante de una organización debe ser protegida de la red Interna como de la red externa, con un esquema de dos firewall consecutivos como se muestra en el diagrama propuesto.

**p)** Es necesario la implementación de filtros en los diferentes servidores de acceso remoto, y la realización del CALLBACK utilizando métodos de

autenticación seguros como CHAP, o PAP, el servidor de acceso remoto, vía dial-up se recomienda separarlo de la red servidores de la DMZ y colocarlo en otra red DMZ adyacente, con el fin de evitar el acceso indebido a los servidores bastión a intrusos.

**q)** En todo Sistema operativo sea este Linux o Windows es importante, tener actualizado sus parches o actualizaciones de software, de manera periódica, es importante realizar una prueba de escaneo de puertos a los servidores para verificar si tienen puertos abiertos, que no pertenecen al servicio que este presta.

**r)** Al realizar la selección de un Firewall, es importante tomar en cuenta la modularidad que presta las herramientas de firewalling, que se van a instalar, con el fin de poder implementar planes de contingencia rápidos y a un menor costo.

## 4.2 RECOMENDACIONES

**a)** Se recomienda un monitoreo continuo de las vulnerabilidades de seguridad sobre los elementos críticos y generar un plan de capacitación y concientización permanente a los usuarios del ISP.

**b)** Se recomienda para iniciar el camino de la mejora del ambiente de control interno del caso de estudio ISP, realizar análisis de riesgo aplicando la metodología propuesta por la NIST en su publicación 800.30 para identificar los riesgos existentes con su impacto alto, medio o bajo sobre los activos de la empresa, estas tareas pueden ser ejecutadas departamento de auditoría interna o contraloría con una sección específica para la evaluación de control en los sistemas tanto a nivel de aplicaciones y procesos a nivel de gestión.

**c)** Se recomienda que antes de implementar un proyecto de conexión hacia la Internet, se realice un análisis técnico de que servicios necesita la empresa por departamento, adicionalmente, qué políticas de seguridad son necesarias para el perfil de esa empresa e implementarlos en todos los niveles que ameriten seguridad.

**d)** Se recomienda crear un departamento de Seguridad, el mismo que se encargará de formar un comité de seguridad donde estén involucradas todas las áreas o departamentos de la institución, estos departamentos tendrán un representante dentro del comité, todo esto con el fin de generara un documento donde refleje las políticas de seguridad en todos los ambientes sean estos de carácter físico, de sistemas, de Internet. Este departamento de seguridad se encargará de aplicar las diferentes políticas a través de herramientas tecnológicas, y velar por su cumplimiento realizando auditorias periódicas, adicionalmente este departamento tiene que hacer un análisis del costo beneficio que representa aplicar políticas de seguridad en una empresa, y finalmente dictar charlas de concientización al personal.

**e)** Se recomienda contratar una empresa especializada en realizar pruebas de penetración (Ethical Hacking) para evaluar las seguridades de conexión y servicios de la empresa, con la finalidad de aplicar los correctivos del caso a las seguridades y minimizar los riesgos de ataques externos, esto se lo debe realizar de forma periódica.

**f)** Se recomienda implementar una arquitectura de detección de virus con el fin de evitar que la red interna sea infectada, y los servicios que ésta brinda no sean afectados, de esta manera minimizar la pérdida de información de los equipos.

**g)** En lo que se refiere al sistema operativo se recomienda que este sea lo más robusto posible y que permita aplicar niveles de seguridad, adicionalmente que permitan un buen rendimiento a las herramientas que trabajan sobre ellos.

**h)** Se recomienda utilizar Firewalls que tenga tecnología Statefull Inspection, con el fin de poder aumentar la seguridad y rapidez en el análisis de paquetes.

**i)** El Firewall no debe tener conexiones de salida hacia la WAN, es conveniente instalar una red independiente y con ruteador para acceso hacia el Internet, para combinar las diferentes tecnologías de Firewaling, todo servicio masivo que necesite de proxyficación debe realizarlo en un equipo que sea independiente del Firewall, con el fin de poder ganar rendimiento en cada dispositivo y distribuir los servicios, mejorando la administración, es importante que cada acceso a la Internet disponga de su equipo de ruteo, con el fin de poder filtrar el tráfico, no deseable en el canal, y además poder dejar las funciones de ruteo a este dispositivo, es importante implementar una red pública con el fin de poder instalar dispositivos de pruebas y sniffer que se permita hacer pruebas externas sin ningún tipo de restricción, esto puede ayudar a determinar daños en los equipos de seguridad o problemas de acceso para determinados servicios.

# GLOSARIO

| | |
|---|---|
| **A** | |
| ***Auditoría*** | Consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar ó cumple las condiciones que le han sido prescritas. |
| ***Autenticación*** | Comprobar que la persona es quien dice ser por medio de diferentes métodos |
| **B** | |
| ***Bomba lógica*** | Son códigos adicionados a los programas que ante ciertas fechas o tiempo de ejecución ejecutan acciones perjudiciales para el sistema. |
| ***Barrido de puertos*** | Es un escaneo que se realiza para identificar qué puertos están abiertos en un servidor |
| **C** | |
| ***Caballos de Troya (Troyanos)*** | Es un software que contiene una parte “invisible” de código, la cual cuando es ejecutada compromete la seguridad del sistema. |
| ***Cracker*** | Es una persona que accede a un sistema informático por lo general en forma no autorizada, para perjudicar el sistema y su información |
| ***Cracking de Contraseñas*** | Es una de las técnicas más utilizadas por los atacantes de un sistema, se usa herramientas que realizan combinaciones de letras y números en poco tiempo y crean diccionarios de contraseñas que sirven para ingresar a un sistema como si fuera un usuario autorizado del mismo |
| ***Control*** | Se puede definir como: “las políticas, estructuras y prácticas que están diseñadas para verificar de forma razonable que los objetivos del negocio están siendo alcanzados, y también para identificar, prevenir y corregir eventos no deseables” |
| ***Control Interno*** | Es una actividad o acción realizada manual y/o automáticamente que se realiza en el interior de una organización diseñada para cubrir los riesgos identificados en los procesos ejecutados de manera continua. |

| | |
|---|---|
| **D** | |
| ***Denegación de Servicio*** | Este tipo de ataques tiene por objeto inutilizar momentáneamente el ordenador atacado, de forma que deje de responder o haya que reiniciarlo. |
| ***Dirección MAC*** | Es un número hexadecimal de 6 dígitos generalmente presentado de esta forma: 00:11:22:33:44:55. Es único para cada interfaz de red. |
| ***DNS (Domain Name System)*** | Sistema de nombres de dominio, nos permite traducir las direcciones IP de las maquinas en nombres fácilmente entendibles para los humanos y viceversa |
| **E** | |
| ***E-mailing bombing*** | Consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario. |
| **F** | |
| ***FTP (File Transfer Protocol)*** | Protocolo de transferencia de archivos, trabaja con el modelo cliente servidor y permite enviar o recibir ficheros de una máquina a otra |
| **G** | |
| ***Gobierno de TI*** | “la estructura de procesos y relaciones encargada de dirigir a la organización con el fin de obtener los objetivos del negocio añadiéndole valor al balancear los riesgos con el retorno de IT y sus procesos” |
| ***Gusanos*** | Son programas similares a los virus, que se autoreplican sin necesidad de infectar a otros archivos, de tal manera que solo realizan copias de si mismos en una máquina dejándola sin recursos |
| **H** | |
| ***Hacker*** | Es una persona que disfruta ingresando a sistemas informáticos para probar sus capacidades y explotarlas, no es malintencionado |
| **I** | |
| ***IP Spoofing*** | Tomar un IP ajeno sin autorización, para realizar un ataque a otra maquina |
| **N** | |

| | |
|---|---|
| ***NAT (Network Address Translation)*** | Es el elemento encargado de transformar las direcciones IP empleadas en la red local en una sola que es la que se ve desde el exterior. Básicamente es un sistema de encapsulación de IP de terminales de LAN en los paquetes enviados |
| ***NETBIOS/NETBEUI*** | Conjunto de protocolos de aplicación para compartir recursos en red utilizados por los sistemas operativos de Microsoft para permitir una comunicación transparente entre sus estaciones y permitir la transferencia de archivos de una manera más sencilla. Se encarga de establecer la sesión y mantener las conexiones |
| ***NIS (Network Information Service)*** | Proporciona un servicio simple de las operaciones de búsqueda y consiste en bases de datos y procesos de red. Es quien proporciona los nombres y contraseñas de usuarios a un cliente que así lo requiera. |
| **O** | |
| ***Objetivo de Control*** | Un procedimiento resultante que se desea alcanzar aplicando procedimientos de control a una actividad de IT en particular |
| ***Operatividad*** | Posibilidad y facilidad de uso que tiene un usuario para realizar sus funciones en un sistema. |
| **P** | |
| ***Puerta trasera*** | Característica incorporada en un SW que ante un evento o entrada ejecuta acciones que pueden comprometer la seguridad del sistema. |
| ***Programas conejo o programas bacteria*** | Programas que no hacen nada útil, simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio. |
| **R** | |
| ***Proxy*** | Sistema de software que permite la conexión de una red de área local (LAN) entera al exterior con sólo una dirección IP de salida. |
| ***RAS (Remote Access Server)*** | Servidor de acceso remoto, permite acceder remotamente a una red, mediante dispositivos de comunicación como pueden ser los módems. |
| ***RADIUS*** | Servidor para autenticación remota de usuarios. Se lo utiliza principalmente en ISP, sin embargo puede ser utilizado en cualquier |

| | |
|---|---|
| | red que necesite una autenticación o manejo de cuentas centralizado para sus estaciones de trabajo. |
| **S** | |
| ***Shell*** | El Shell es el intérprete de comandos, a pesar de no ser parte del sistema operativo, hace un uso intenso de muchas características del sistema operativo. |
| ***Sniffer*** | Programa que captura el tráfico que circula en una red, si este viaja sin encriptar, lo podrá leer sin problemas. |
| ***Spamming*** | Es una variante del e-mail bombing, se refiere a enviar el mensaje a una gran cantidad de usuarios e, inclusive, a listas de interés. |
| **T** | |
| ***TCP/IP*** | Es una familia de protocolos, su objetivo fue que computadoras cooperativas compartieran recursos mediante una red de comunicaciones. |
| ***Telnet*** | Servicio que permite establecer una conexión remota y trabajar en una consola simulando estar trabajando directamente en el servidor. |
| **V** | |
| ***Virus*** | Son programas que se autoreplican y afectan principalmente los archivos ejecutables, a veces llegan a afectar a miles de computadoras. |

# REFERENCIAS BIBLIOGRAFICAS

## LIBROS


a. ISACA, COBIT Executive Summary, 3ra edición, Rolling Meadows, USA, 2000.

b. ISACA, COBIT Framework, 3ra edición, Rolling Meadows, USA, 2000.

c. ISACA, COBIT Control Objectives, 3ra edición, Rolling Meadows, USA, 2000.

d. ISACA, COBIT Audit Guidelines, 3ra edición, Rolling Meaddows, USA, 2000.

e. ISACA, COBIT Managment Guidelines, 3ra edición, Rolling Meaddows, USA, 2000.

f. American Institute of Certified Accountants, Committee of Sponsoring Organisations of the Treadway Commission. Internal Control – Integrated Framework. 2 Vols, USA - New Jersey, 1994.

*g.* National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, USA, Julio 2002.

h. SAC Systems Auditability and Control Report, the Institute of Internal Auditors Research Foundation, 1991 y 1994.

i. Mantilla Guayasamin Salome – Pazos Constante Xavier, Guías Para la Implantación de las Técnicas de Auditoría Informática en las Empresas de Quito, Escuela Politécnica Nacional, Quito – Ecuador, 2003.

j. Adam Qwiggle, "Osborne/Mc Graw. Hill", IMPLEMENTING CISCO VPN´S: A HANDS-ON GUIDE. 1999

k. Check Point 2000, J. 2000, "CheckPoint", Administraction Guide VPN-1/FIREWALL-1.

l. Manual de CCSA (CheckPoint Certification Security Administration) y el CCSE (CheckPoint Certification Security Engeneering). 1999

m. Guía del administrador de software detector de intrusos eTrust, versión 1.5; editado por: Computer Associates International, Inc. Agosto - January 2001.

n. Manual de las Redes Privadas Virtuales de CheckPoint. Part No.: 700350. Nov. 2001.

o. Guía de configuración de CISCO IOS.Customer Order Number: DOC-7811739. Text Part Number: 78-11739-01. Nov. 2001.

## DIRECCIONES ELECTRONICAS:

a. http://csrc.nist.gov/publications/nistpubs/, NIST Special Publications, 2002
b. http://www.isaca.org/, Information Systems Audit and Control Association, 2002
c. http://www.security-risk-analysis.com/ Introducción al Análisis de Riesgos de Seguridad
d. http://www.coresecurity.com/products/coreimpact/CI01.php Test de Penetración y Evaluación de Riesgos.
e. http://www.riskworld.net/7799.htm Mejores prácticas de seguridad de la información
f. https://portal.sans.org/login.php Portal de Seguridad Computacional
g. http://www.nessus.org Herramienta para Scaneo de Vulnerabilidades en TCP/IP
h. http://www.eeye.com Herramienta para Scaneo de Vulnerabilidades en Windows
i. http://www.tippingpoint.com/ Site con Herramientas para prevención de Intrusos
j. http://www.staysafeonline.info/index.adp Tips de Seguridad en Redes
k. http://www.cybsec.com/ Empresa de soluciones de seguridad para empresas
l. http://www.securityspace.com Ultimas vulnerabilidades de seguridad
m. http://www.verisign.com Autoridad Certificadora y emisión de bugs de seguridad
n. http://www.qualys.com Líder como empresa para Auditorías de Seguridad de Redes y Administración de Vulnerabilidades.
o. http://www.lafacu.com/apuntes/informatica/segu_sist_infor/default.htm- Evaluación seguridad de un sistema de información
p. http://www.iec.csic.es/criptonomicon/articulos Políticas de seguridad.
q. http://www.symantec.com/region/mx/enterprisesecurity/content/ Prevención de intrusos

r. http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO Políticas de seguridad

s. http://www.codetel.net.do/politicas/ Política de uso aceptable del servicio Internet

t. http://www.correomemo.com.co/politicas_de_seguridad.htm Seguridad en e-mail

u. www.checkpoint.com, Información del Firewall.

v. www.nokia.com, Información del hardware del Firewall.

w. www.rapidstream.com, Características sobre el Firewall rapadstream.

x. www.cisco.com, Información de los router CISCO y Firewall

y. www.ca.com, Documentación sobre el software detector de intrusos eTrust.