UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

SISTEMA DE SEGURIDAD EN ALTA DISPONIBILIDAD PARA UNA RED CORPORATIVA DE DATOS Y SERVICIOS

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TITULO DE:

INGENIERO ELECTRICO ELECTRONICO

P R E S E N T A N :

EN EL AREA ELECTRONICA PARA C O M U N I C A C I O N E S :

HECTOR LEONARDO AGUILAR LARA

L E T I C I A A R V I Z U B A R B O S A

I S R A E L G O N Z A L E Z C R U Z

X I U H N E L H U I Z A R S A N C H E Z

EN EL AREA ELECTRONICA:

DAVID OCTAVIO SOLIS SANTANA

DIRECTOR DE TESIS: M. EN I. LAURO SANTIAGO CRUZ

MEXICO, D. F. 2004

Quiero agradecer:

A Dios,
Por permitirme realizar este sueño...

A mis padres,
Héctor Aguilar y Ma.Cristina Lara,
ya que gracias a sus valiosos consejos, amor, apoyo
y comprensión que me dieron en todo momento,
he podido cerrar este capítulo tan importante de mi vida.

A mis hermanas,
Fiorella y Valeria,
por todo su cariño que me han demostrado,
y por estar conmigo en los momentos buenos y malos.

A toda mi familia y Amigos,
con los que siempre he contado
y siempre seguirán apoyándome.

A Heather Anderson,
por todo el amor que me ha demostrado.

A la Universidad Nacional Autónoma de México,
por ser testigo de mi preparación profesional.

A la Facultad de Ingeniería,
Por los sólidos conocimientos que me ha transmitido.

A mi asesor Lauro Santiago,
Por sus invaluables consejos para realizar este trabajo.

Y a todos los que hicieron posible
que este trabajo fuera una realidad.

Gracias!

Héctor Leonardo Aguilar Lara

A MIS PADRES
Mi eterna gratitud...
Como justo reconocimiento a su honradez y fortaleza,
por la educación que me brindaron y cuyo apoyo fue invaluable.

A MIS HERMANOS
Por estar presentes durante todo el camino.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Mi gratitud por haberme dado la oportunidad de ingresar a una de sus facultades.

A LA FACULTAD DE INGENIERÍA
Mi sincero agradecimiento por las enseñanzas recibidas en sus aulas.

AL M. EN I. LAURO SANTIAGO CRUZ
Mi sincero reconocimiento por su valiosa orientación en la elaboración de esta tesis.

Con agradecimiento a la noble labor de todos mis maestros,
a partir de aquél que me enseño mis primeras letras.

Leticia

AGRADECIMIENTOS

Durante el desarrollo de la carrera y de la presente tesis, recibí el apoyo de varias personas a las que quisiera expresar mi gratitud:

A la Facultad de Ingeniería y en conjunto a la Universidad Nacional Autónoma de México, por la formación y enseñanza que me aportaron por medio de todos los profesores.

A M.I.Lauro Santiago Cruz por sus consejos, asesoría y contribución para elaborar la presente.

A mi mamá Amelia Cruz Hernández por darme lo mejor que puede recibir un hijo, apoyo, comprensión y sobre todo amor.

A mis hermanos Daniel e Iván que sin su compañía, no hubiera superado los momentos más difíciles que tuve.

A Ismael Nieto Alquicira por seguir mi trayectoria escolar y proporcionarme todo su apoyo moral.

Y por último, no por ser la menos importante al contrario, quiero agradecerle a mi esposa, por estar siempre a mi lado en los peores y en los mejores momentos, por comprenderme, por apoyarme en todos los aspectos, a ella que siempre creyó en mi y que es mi razón de ser, gracias Adriana López Vivero.

Israel González Cruz

A mis padres, a quienes debo todo el amor, ejemplo, consejos y apoyo recibidos a lo largo de mi vida. Gracias por estar siempre a mi lado.

A mis abuelitos, por ser una fuente de grandes ejemplos a seguir. Muchas gracias por el apoyo incondicional a toda la familia.

A mis hermanos, tíos y tías con quienes siempre he podido contar en cualquier momento.

A mis amigos, de quienes siempre escuche una palabra de aliento.

A nuestro director de tesis, M. en I. Lauro Santiago Cruz, por su paciencia y cooperación en la realización del presente trabajo.

A la Facultad de Ingeniería de la UNAM, por permitirme ser parte de ella.

Xiuhnel.

Agradecimientos

A mis padres, Jaime y Rosalinda, y mis hermanas, Norma y Mayra, quienes durante el transcurso de mi vida me han brindado su apoyo incondicional, amor y paciencia... porque este logro también es de ustedes... mi eterna gratitud por ayudarme a forjar lo mejor de mi persona.

A mis familiares y amistades, por su cariño y cercanía, por la convivencia de tanto tiempo, su compañerismo y afecto sincero.

A Isa y Magda, por su fraternidad tan próxima pese a la distancia.

Aquellos que no están, a quienes les habría sido grato ver este trabajo concluido y compartir el significado que tiene para mí.

A nuestro asesor, M. en I. Lauro Santiago, por sus comentarios, críticas y sugerencias a lo largo de la realización de este trabajo, así como su asesoría en el contenido y en la redacción del documento.

A mi Universidad y Alma Mater, porque seré un profesionista gracias a ella y al conocimiento y dedicación de sus profesores.

A todos los involucrados en la realización de este trabajo... especialmente a Héctor, Leti, Israel, Xiuhnel y a su generosa familia.

...David

CARPE DIEM

PRÓLOGO

Es importante recalcar que la mayoría de los daños que puede sufrir una red corporativa no será sobre los medios físicos sino contra su activo más importante: la información que posee. Así, la seguridad física sólo es una parte de un amplio espectro que se debe cubrir para obtener la mayor seguridad posible y por lo tanto deben existir técnicas que la aseguren.

Estas técnicas las brinda la seguridad informática con la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas". Hoy es imposible hablar de un sistema cien por cien seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen el riesgo de perder un negocio o ser vulnerables. La solución inmediata sería acotar todo el rango de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total.

En esta tesis se presenta el proceso involucrado en la elaboración de un sistema de seguridad informática, la cual surge como una herramienta organizacional para proteger la información importante y servicios críticos. Asimismo, permite a la red corporativa de la compañía desarrollarse y mantenerse en su sector de negocios.

La tesis está divida en cinco capítulos: en el primer capítulo presentamos conceptos teóricos, en los cuales se basa el resto del trabajo, entre ellos encontramos definiciones de topologías, dispositivos de interconexión, métodos de acceso y protocolos de red.

En el segundo capítulo presentamos las generalidades de seguridad en redes, así como definición de virus, posibles ataques y amenazas.

Posteriormente, en el tercer capítulo hacemos una referencia general del análisis del estado actual de la red corporativa, además de plantear recomendaciones de solución a la problemática de seguridad existente.

En el cuarto capítulo se lleva a cabo el diseño e implementación del sistema, basándose en la propuesta seleccionada. Esto involucra las etapas de planeación e ingeniería, instalación, configuración y pruebas de funcionamiento del sistema implementado, a fin de comprobar su eficiencia.

En el quinto capítulo se realiza la presentación de resultados y conclusiones sobre el trabajo. Finalmente se incluye la bibliografía utilizada y los apéndices, en los que se presentan los elementos que complementan la comprensión del material presentado en esta tesis, además de un glosario con los términos técnicos más utilizados.

ÍNDICE

APÉNDICES

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las redes por naturaleza son inseguras, ya que la mayor parte del tráfico no viaja encriptado, y para muchas aplicaciones se mandan contraseñas sin protección a través de la red. Actualmente la información privilegiada y las aplicaciones de misión crítica están cada día más expuestas a accesos no autorizados, como son los *hackers*, empleados, competidores, etc.

La amenaza evaluada lleva a la necesidad de una política de seguridad confiable, ya que los ataques han aumentado en 498% desde 1991, de los cuales el 90% pasan sin ser detectados, y los *hackers* adivinan entre el 10% y 20% de las contraseñas[1].

La integridad de la red y de la información, el buen funcionamiento de los sistemas operativos, la preservación de la confidencialidad de las comunicaciones y de los datos, corporativos y comerciales, la seguridad física, jurídica y mercantil, son ya, y lo serán cada vez más, elementos fundamentales para el desarrollo de la Sociedad de la Información.

La cultura de la seguridad está lejos de alcanzar la extensión que sería necesaria, sobre todo para facilitar el financiamiento de dispositivos costosos y de medidas que requieren pautas de comportamiento generalizadas, como en el caso de la intervención de comunicaciones, el acceso no autorizado a ordenadores o redes, la saturación malintencionada de las mismas o los ataques a los servidores de nombres de dominio, situaciones que se multiplican enormemente con la interconexión creciente de las redes.

El término "seguridad de la red" se ha desarrollado para abarcar muchas y diversas cosas. Puesto que las redes han llegado a ser más penetrantes y la red corporativa se ha abierto al exterior a través del Internet, la necesidad de una fuerte seguridad ha llegado a ser evidente. Pero en la mayoría de los casos, asegurar la Intranet corporativa ha sido una tarea enormemente difícil, requiriendo equipo altamente especializado y personal entrenado. La "seguridad de la red" ha creado toda una gama de conceptos nuevos y todo un objeto de estudio, generando un área nueva dentro de los sistemas de información.

Con el crecimiento rápido del interés en Internet, la seguridad de la red corporativa se ha convertido en una preocupación importante para la compañía Ledaxis. El simple hecho de que la información y las herramientas necesarias para penetrar la seguridad de la misma estén disponibles en Internet, ha ocasionado extensamente la preocupación de sus administradores.

La red corporativa proporciona servicios de correo electrónico, servidor de páginas WWW (World Wide Web, Red Mundial de Redes), servidor de archivos, servidor de dominios y servidores de FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos), por mencionar los más importantes. Al encontrarse estos disponibles dentro de la red pública, nos enfrentamos a constantes ataques en nuestros servidores, debidos a usuarios que poseen herramientas gratuitas por Internet y que perjudican la disponibilidad de los servicios usando la red pública como medio.

[1] CSI/DOD (Computer Security Institute/Department of Defense).
Fuente: http://pronad.uson.mx/docs/acapulco/eventogro.ppt

Actualmente existen varias herramientas con las cuales un usuario de Internet, con un poco de conocimiento en redes, puede usar para perpetrar en algún sistema o darse cuenta de qué vulnerabilidades existen en algún equipo dentro la red, incluso tiene la posibilidad de lanzar un ataque de negación de servicio o robar una contraseña con algún programa que le permita adivinarlo, por citar algún ejemplo. Es decir, con las herramientas que existen actualmente en Internet se puede fácilmente vulnerar cualquier elemento que se encuentre en ella.

El problema que la compañía Ledaxis enfrenta, son los ataques cada vez mayores a causa de las vulnerabilidades propias de nuestros sistemas, aun cuando estos tengan las últimas versiones de software proporcionadas por el fabricante. El número creciente y la gravedad de estas amenazas requieren de una vigilancia renovada por parte del responsable de la seguridad de la red para bloquear tales ataques con inteligencia.

Debido al riesgo inherente de la conexión permanente de la red corporativa con Internet, se han registrado amenazas que pueden dar como resultado alteraciones e incluso pérdidas de información, así como caída de servidores, robo de información (contraseña, nombre de usuario, etc.), bloqueo de puertos, intrusiones o accesos no autorizados, entre otros.

Ante esta problemática la compañía Ledaxis requiere de un sistema de seguridad que nos permita la disponibilidad, la confiabilidad y la seguridad de los servicios para que el acceso a estos opere de forma continua y segura.

El sistema de seguridad en alta disponibilidad que se desea desarrollar permitirá la protección de la red a ataques, tales como:

- Ataques de denegación de servicio.
- Ataques de direcciones de red IP (Internet Protocol, Protocolo de Internet)
- Disfraz de IP.
- Ataques mediante fragmentación de IP.
- Paquetes ilegales y malformados.
- Puntos vulnerables de la Web y las aplicaciones.
- Ataques a servidores de dominio.
- Incumplimiento de protocolos.
- Vulnerabilidades específicas de aplicaciones.
- Troyanos.
- Puertas traseras y administración remota.
- Código móvil (Java Script, ActiveX).
- Extensión de archivos oculta.
- Exploración de puertos.
- Exploración de servicios.
- Gusanos de HTTP (Hiper Text Transfer Protocol, Protocolo de Transferencia de Hipertexto).
- Código rojo.

- Nimda.

Ledaxis es una compañía de servicios de red que proporciona a sus clientes sistemas inalámbricos, utilizando la tecnología más innovadora del mercado, fabricada por sus socios tecnológicos.

Desde su fundación en el año 1998, los logros alcanzados le han permitido ubicarse en el mercado mexicano de los segmentos de redes, sistemas inalámbricos y soluciones de Internet alrededor del país.

Hoy en día, Ledaxis posee una red privada tipo WAN (Wide Area Network, Red de Área Amplia) con 1 enlace E1 hacia Internet y 10 DS0 para la interconexión con sus oficinas remotas. Cuenta con aproximadamente 1000 empleados dentro de la misma, repartidos a lo largo del territorio nacional. Además, las áreas de Recursos Humanos, Finanzas, Ventas y Mercadotecnia, Soporte Técnico y Sistemas, se encuentran segmentadas con direccionamientos privados.

Nuestro objetivo en este trabajo será desarrollar un sistema de seguridad en alta disponibilidad para una red corporativa de datos y servicios, que garantice a los usuarios la continuidad y la seguridad de la información.

CAPÍTULO 1

GENERALIDADES DE REDES

En este capítulo estudiaremos las generalidades que se refieren a las redes de datos, es decir, los tipos y topologías de las mismas, así como de los dispositivos de interconexión, métodos de acceso y protocolos de red.

En las décadas de los 60s y 70s la información, los cálculos, etc., de cualquier empresa ya comenzaban a ser gestionados y administrados por sistemas centralizados desde una computadora principal, y eran manejados por niveles superiores, por lo que muchos no se veían beneficiados por estos sistemas, además que su almacenamiento y procesamiento eran altos.

En sus inicios las redes estaban conformadas por terminales "tontas" conectadas a una macrocomputadora mediante líneas telefónicas privadas, como se muestra en la figura 1.1.

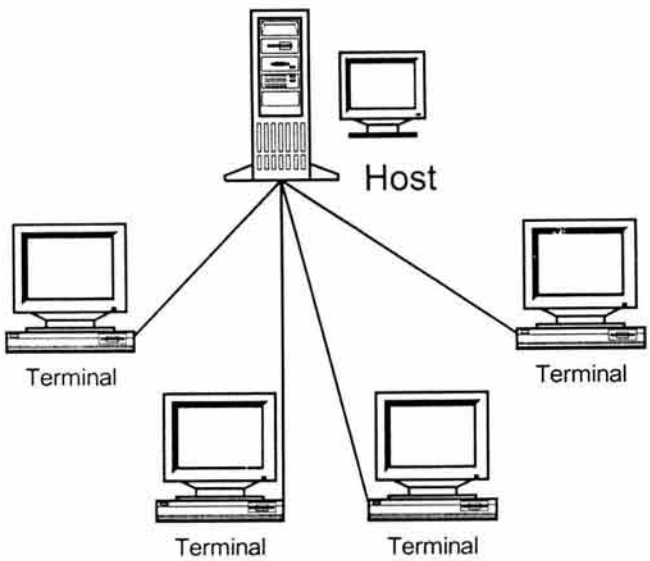

Figura 1.1. Host con terminales tontas.

Una terminal "tonta" es una terminal donde no se realizaba ningún procesamiento en ella, sino que sólo se utilizaba para enviar la información por medio del teclado al *host* o anfitriona y recibirla mediante la pantalla.

Trabajaban por procesamiento en lotes, lo cual se fue modificando y se tuvo la capacidad para procesar la información en tiempo real, lo que permitió que se pudiera acceder a la información en cuanto se tecleaba. Puesto que cada red se comunicaba de forma diferente a las demás, se vio la necesidad de establecer estandares de comunicación.

Con el avance de la tecnología evolucionó la manera de acceder a los servicios de las redes con una mayor capacidad y menor costo; las microcomputadoras por ser menos costosas, aunque menos poderosas que las macrocomputadoras, fueron adquiridas por varias empresas, con la ventaja de que con los estándares en la comunicación, con una sola terminal podían acceder a muchos tipos de computadoras anfitriones y servicios.

Desde 1980, las computadoras lograron un cambio muy importante en el mundo de las empresas, negocios e industria, proporcionando a los usuarios el acceso a recursos de información que les eran ajenos.

Al aparecer la PC (Personal Computer, Computadora Personal), los departamentos pudieron tener su propio sistema con costos menores. Se fue descentralizando el manejo de la información hasta llegar a los puestos de trabajo de los usuarios, pero surgió el problema de que la información se fue diseminando por varias estaciones de trabajo; es por ello que a mitad de la década de los 80s se vió la necesidad de integrar la información en un lugar central. Se comenzaron a conectar las computadoras en las llamadas redes de información y el almacenamiento de los archivos era centralizado de tal forma que los archivos podían ser accedidos con facilidad por otros usuarios.

La necesidad de compartir la información de una PC da origen a las redes. Hoy día la probabilidad de que una PC no esté conectada o una red es baja; podemos conectarnos a una red, y esa a otra, y a otra, para compartir recursos.

Una vez establecida una red, ésta trae consigo una serie de beneficios que se traducen en eficiencia y eficacia dentro de la empresa; estos beneficios son:

- Uso compartido de programas y archivos.
- Uso compartido de los recursos de la red.
- Utilización de *software* de red.
- Correo electrónico.
- Creación y manejo de grupos de trabajo.
- Gestión centralizada.
- Seguridad.
- Acceso a otros sistemas operativos.
- Mejoras y actualización continua en la empresa.

Una red es un sistema de comunicación entre computadoras y otros equipos, que está integrada por un conjunto de computadoras con las cuales se puede acceder a los archivos, programas y recursos de un servidor central. Además de que cada computadora ejecuta sus propios procesos.

El principal objetivo de las redes de computadoras es el poder conectarse con otros equipos de información, de la misma forma en como se conectan dos personas mediante un teléfono, no importando que se encuentren en el mismo edificio o del otro lado del mundo.

Los componentes principales que conforman una red de computadoras son el servidor y las estaciones de trabajo.

- El servidor es el que ejecuta el sistema operativo de red y ofrece los servicios a las estaciones de trabajo; dichos servicios pueden ser: almacenamiento de archivos, gestión de usuarios, seguridad, órdenes de red generales, órdenes del responsable de red, etc.

- Las estaciones de trabajo pueden ser computadoras personales con sistemas operativos como DOS, Macintosh, OS/2, etc.

Otros componentes importantes son:

- NIC (Network Interfase Card, Tarjeta de Interface de Red). Puede venir ya integrada, o puede ser un elemento opcional y debe ser del tipo de red que se desea utilizar. El cable de red se conecta a la parte trasera de la NIC.

- El sistema de cableado o conexión lo constituye el cable de conexión de las terminales entre sí y con el servidor; puede ser cable coaxial, par trenzado o fibra óptica.

- Recursos compartidos y periféricos son los dispositivos de almacenamiento del servidor, las unidades de disco óptico, impresoras, los trazadores y demás equipos que puedan ser utilizados por cualquiera en la red.

1.1. TIPOS DE REDES

Las redes locales se dividen por su extensión en: LAN (Local Area Networks, Redes de Área Local), MAN (Metropolitan Area Networks, Red de Área Metropolitana) y WAN. La otra clasificación la encontramos con las redes *Enterprise Network*, que se clasifica como una red corporativa en grupos de trabajos de organizaciones o de campus.

De los vocablos red y local, diremos que el primero se asocia a la conexión entre equipos de cómputo y el segundo a la característica física de la conexión entre estos, en cuanto a la distancia de conexión va desde unos cuantos metros hasta unos cuantos kilómetros; se sabe que a veces hasta 10 km., distancia que ya más bien es un parámetro de enlace remoto. El vocablo área amplia se refiere a la característica física de conexión y comunicación, que surge de la necesidad de comunicar las redes locales entre sí, en una misma ciudad, o en ciudades distintas. Dentro de estas mismas características pueden entrar las redes MAN, de acuerdo al punto de vista del diseñador, tomando en cuenta la extensión geográfica.

1.1.1. Redes de Área Local

Una LAN es un sistema de comunicaciones de alta velocidad, que consta de varias microcomputadoras o PCs que se encuentran cercanas; cubre un área geográfica limitada, normalmente localizada dentro de un edificio o grupo de edificios que pertenecen a una organización. Esto da la posibilidad de que las PCs compartan entre ellas programas, información y recursos, como se muestra en la figura 1.2. Las redes LAN pueden ser capaces de enlazar cientos de sistemas y de dar servicio a varios miles de usuarios.

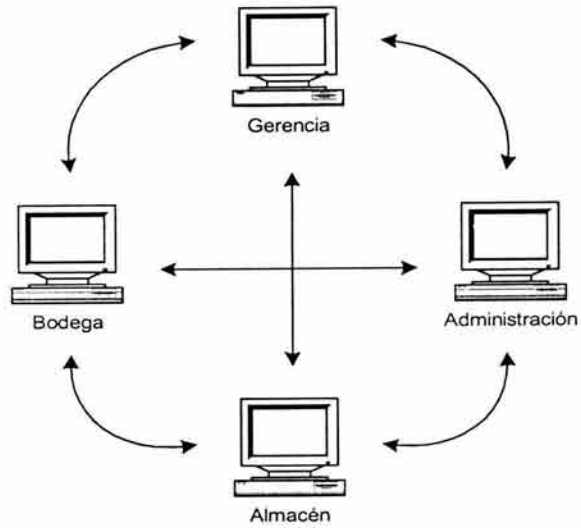

Figura 1.2. Red de Área Local.

1.1.2. Redes de Área Metropolitana

Es un conjunto de redes de área local interconectadas dentro de un área específica, como un campus, un polígono industrial o una ciudad. Se utiliza una base de cableado o sistemas de conexión especiales a alta velocidad para conectar las redes en un sistema interconectado. Una MAN puede ser propiedad de de una sola organización, aunque generalmente es usada por muchos individuos y organizaciones. La figura 1.3 muestra un ejemplo.

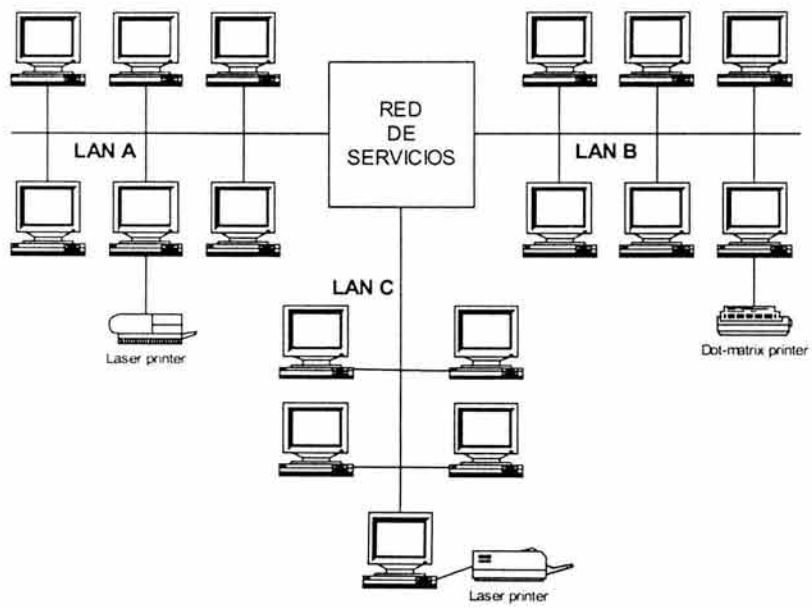

Figura 1.3. Red de Área Metropolitana.

1.1.3. Redes de Área Amplia

Se trata de redes que cubren varios países, incluso el mundo (un ejemplo puede ser el sistema de reservas de las líneas aéreas). Las LANs pueden conectarse para formar una WAN, como se muestra en la figura 1.4; éstas no están limitadas geográficamente en tamaño. Las WAN necesitan de un *software* especial para conectar las LANs, así como líneas telefónicas proporcionadas por una compañía telefónica, este *software* se puede usar para incluir mini y microcomputadoras como elementos de red. El *hardware* para crear una WAN también puede incluir enlaces de satélite, fibras ópticas, aparatos de rayos infrarrojos y de láser. Internet está conectada para formar una WAN.

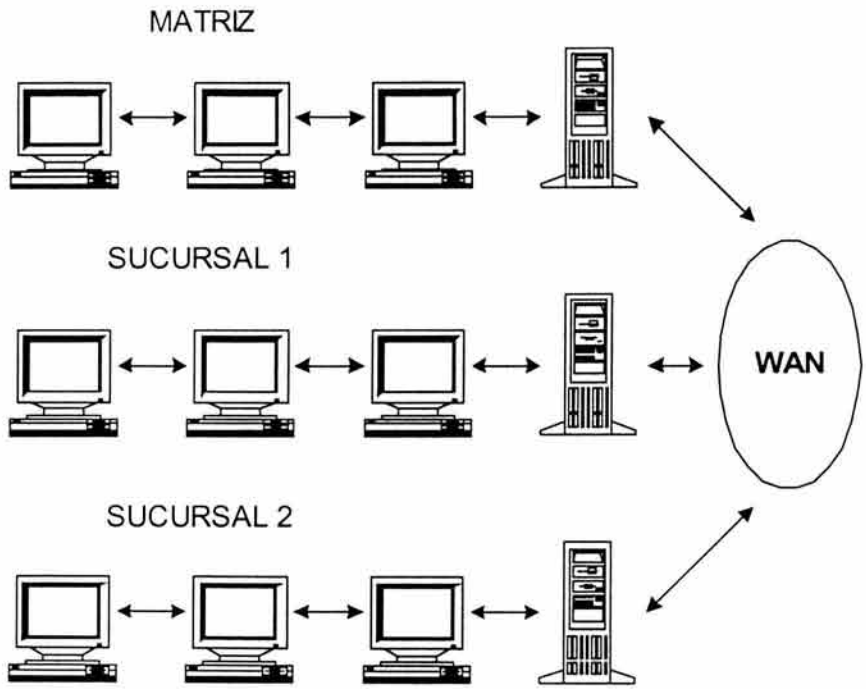

Figura 1.4. Red de Área Amplia.

1.2. TOPOLOGÍAS DE RED

La arquitectura de una red define la estructura del sistema de cableado y de estaciones de trabajo conectadas a éste, además de las reglas que se usan para la transferencia de señales de una estación a otra. La estructura física del sistema de cableado se llama topología. Para establecer comunicación entre nodos, se debe hacer uso de protocolos de comunicación y de un método de acceso al cable para enviar señales sobre éste.

La topología de una red es la descripción de cómo va el cable de un nodo a otro. Una red tiene dos diferentes topologías, física y lógica:

- Física: es la disposición física actual de la red, la manera como los nodos están conectados unos con otros.

- Lógica: es el método usado para la comunicación entre los nodos, la ruta de los datos dentro de la red.

Las topologías de red típicas son: horizontal, en estrella, en anillo, jerárquica y en malla. La compañía básicamente trabaja con dos de ellas: horizontal y en estrella.

1.2.1. Topología horizontal

La topología horizontal es también conocida como de *bus*. En esta topología cada nodo está conectado a un segmento continuo de cable que es común a todos. El segmento se coloca como un *bus* lineal, de lado a lado de la red al que se conectan los nodos. No requiere de una computadora central, además una terminal no depende de otra para que la información sea continua, como se muestra en la figura 1.5.

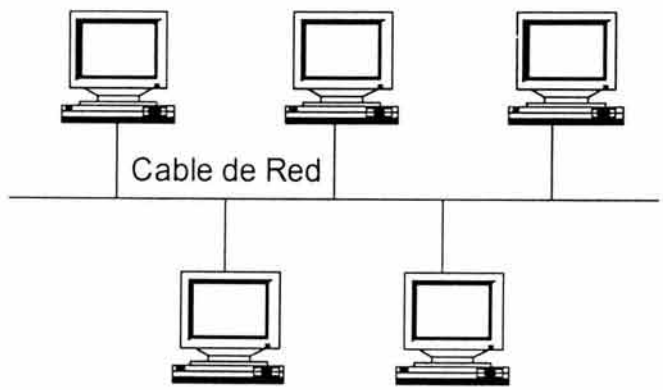

Figura 1.5. Topología física de bus.

Ventajas:

- No requiere de un controlador central.
- Es adaptable fácilmente a voz, video y datos.
- El manejo de la comunicación de nodos es sencillo.
- Es fácilmente expandible.
- Es factible de ser usada en edificios de varios pisos.

Desventajas:

- El uso de repetidores para amplificar las señales sobre largas distancias.
- Una falla en el *bus* afectará a la red completa.

1.2.2. Topología en estrella

En una topología de estrella, cada nodo se conecta a un concentrador o *hub* ubicado centralmente. El concentrador es un dispositivo de *hardware* con varios puertos a los cuales va conectada cada computadora. Es muy usada en redes privadas, debido a lo indispensable del servidor para establecer un enlace, bajo la confiabilidad del sistema y el rendimiento es directamente proporcional al volumen de información. En la figura 1.6 se muestra un ejemplo.

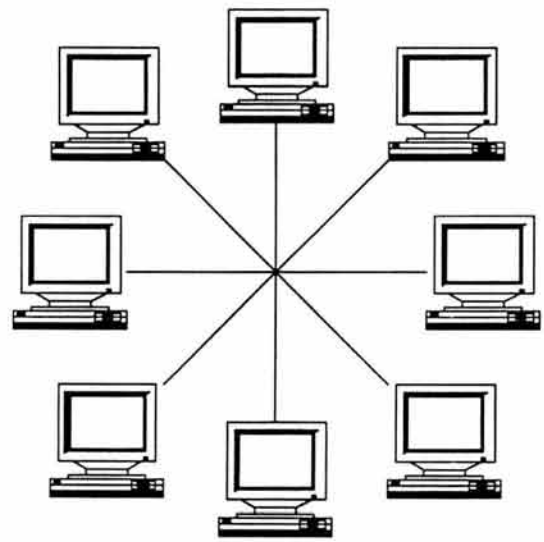

Figura 1.6. Topología física de estrella.

Ventajas:

- Existe una buena comunicación entre nodos.
- Manejo eficiente de la base de datos compartida.
- Fácil expansión (depende de la capacidad de la computadora).
- Fácil acceso a otras redes.

Desventajas:

- Un tráfico pesado puede causar una caída del sistema.
- Cuando el concentrador falla, todos los nodos dejan de funcionar.

1.3. DISPOSITIVOS DE INTERCONEXIÓN

Cuando se diseña una red de datos se desea sacar el máximo de sus capacidades, para conseguirlo la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar sus características.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de ésta. Las ventajas que nos ofrece la interconexión son:

- Uso compartido de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

Para superar las limitaciones físicas de los elementos básicos de una red, existen equipos cuyas funciones son las de extender las topologías de red. Los equipos de interconexión proporcionan alguna de las siguientes funciones:

- Extensión de la red.
- Permiten ampliar el rango de distancia que puede alcanza una red.
- Definición de segmentos dentro de la red.
- Al dividir la red en segmentos se consigue aumentar las prestaciones de la red, ya que cada tramo soporta sólo su propio tráfico y no los otros segmentos.
- Separación entre redes.
- Mediante estos equipos las grandes redes se pueden componer de otras más pequeñas, interconectadas entre sí, de forma transparente para el usuario. Varias redes físicas pueden combinarse para formar una única red lógica.
- Cada uno de los equipos usados para expandir la red tiene un propósito específico; sin embargo, muchos equipos incorporan las características de otros tipos de equipos para aumentar la flexibilidad y el valor.

Entre los principales equipos de interconexión se encuentran: los repetidores, concentradores, *switches*, puentes, ruteadores y compuertas.

1.3.1. Repetidores

El repetidor es un elemento que permite la conexión de dos tramos de red, teniendo como función principal regenerar eléctricamente la señal, para alcanzar distancias mayores, manteniendo el mismo nivel de la señal a lo largo de la red. Interconecta múltiples segmentos de red en el nivel físico del modelo de referencia OSI (Open System Interconection, Interconexión de Sistemas Abiertos). Sólo se pueden utilizar para unir dos redes que tengan los mismos protocolos de nivel físico. Los repetidores no discriminan entre los paquetes generados en un segmento y los que son generados en otro segmento, por lo que los paquetes llegan a todos los nodos de la red. Se pueden clasificar en:

- Locales: cuando enlazan redes próximas.
- Remotos: cuando las redes están alejadas y se necesita un medio de comunicación entre ellas.

Normalmente la utilización de repetidores está limitada por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados. En las redes Ethernet, por problemas de gestión de tráfico en la red, no deben existir más de dos repetidores entre dos equipos terminales de datos, lo que limita la distancia máxima entre los nodos más lejanos de la red a 1,500 metros.

Los repetidores son utilizados para interconectar LANs que estén muy próximas, cuando se quiere una extensión física de la red. La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal manera que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), *ThickEthernet* (10Base5), *ThinEthernet* (10Base2), *Token Ring*, fibra óptica, etc.

1.3.2. Concentradores

El término concentrador o *hub* describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en un único dispositivo. Normalmente los concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de encaminamiento filtrado y conexión de diferentes medios de transmisión (por ejemplo Ethernet y *Token Ring*).

Los primeros concentradores o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión a varios puntos. Los concentradores avanzados de "segunda generación" basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (*Token Ring* y Ethernet). Los nuevos concentradores de "tercera generación" ofrecen un proceso basado en arquitectura del tipo RISC (Reduced Instruction Set Computer, Computadoras con Conjunto Reducido de Instrucciones) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios *buses* independientes Ethernet, *Token Ring*, FDDI (Fiber Distributed Data Interface, Interfaz de Distribución de Datos de Fibra Óptica) y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación.

1.3.3. *Switches*

Los *switches* tienen la funcionalidad de los concentradores, a los que añaden la capacidad de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos, esto se consigue debido a que el *switch* no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos. Esto es posible debido a que los equipos configuran unas tablas de encaminamiento con las direcciones de medio de control de acceso MAC (Medium Access Control) asociadas a cada una de sus puertas.

Esta tecnología logra que cada una de las puertas disponga de una totalidad de ancho de banda para su utilización. Habitualmente trabajan con anchos de banda de 10 y 100 Mbps, pudiendo coexistir puertas con diferentes anchos de banda en el mismo equipo.

1.3.4. Puentes

Los puentes o *bridges* son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y los no locales, estos elementos disminuyen el número total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a una congestión en la red.

Operan en el nivel de enlace del modelo de referencia OSI, en el nivel de trama MAC y se utilizan para conectar o extender redes similares, de protocolos idénticos en los dos niveles inferiores OSI, y conexiones a redes de área amplia.

Se encargan de filtrar el tráfico que pasa de una red a otra red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas. Las redes conectadas a través de un puente aparentan ser una única red, ya que realizan su función de forma transparente, es decir, las estaciones no necesitan saber de la existencia de los dispositivos.

Un puente ejecuta tres tareas básicas:

- Aprendizaje de las direcciones de nodos en cada red.
- Filtrado de las tramas destinadas a la red local.
- Envío de las tramas destinadas a la red remota.

Existen dos tipos de puentes:

- Locales: sirven par enlazar directamente dos redes físicamente cercanas.
- Remotos o de área amplia: se conectan en parejas, enlazando dos o más redes locales, formando una red de área amplia, a través de líneas telefónicas.

1.3.5. Ruteadores

Los ruteadores son equipos inteligentes que trabajan en el nivel de red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.

Los ruteadores convierten los paquetes de información de la LAN en paquetes capaces de ser enviados mediante redes de área amplia. Durante el envío, el ruteador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual actualiza por medio de intercambio de información con otros ruteadores para establecer rutas de enlace que los interconectan. Este intercambio de información se realiza mediante protocolos de gestión de propietarios.

1.3.6. Compuertas

Estos equipos están pensados para facilitar el acceso entre sistemas y entornos soportando distintos protocolos. Operan en los niveles más altos de los modelos de referencia OSI y realizan conexiones de protocolos de alto nivel diferentes. Incluyen 7 niveles del modelo OSI, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos.

Tienen mayores capacidades que los anteriores, porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que sus dispositivos puedan comunicarse con los de otro tipo de red.

Para acceder a una red se requieren de métodos de acceso.

1.4. MÉTODOS DE ACCESO

Es la manera como un nodo accede al sistema de cableado, se puede utilizar un método de detección de portadora o uno de pase de testigo.

Detección de Portadora. En este método el nodo comprueba si el cable está siendo utilizado antes de transmitir, a través de todo el cable y los demás nodos escuchan y determinan si la transmisión está dirigida a ellos, si no lo está la rechazan. Si dos nodos transmiten a la vez, se produce una colisión y se eliminan las dos colisiones, después de un tiempo aleatorio los nodos vuelven a transmitir. El método más usado de detección de portadora es el CSMA/CD (Carrier Sense Multiple Access / Collision Detection, Acceso Múltiple por Percepción de Portadora / Detección de Colisiones).

Pase de Testigo. El pase de testigo se utiliza más frecuentemente en las redes de anillo. El "testigo" define cuándo un nodo puede acceder al cable. Una estación de trabajo que está lista para transmitir, debe esperar a que esté disponible un testigo y tomar posesión de él, entonces puede empaquetar y enviar la información a otra estación de la red. Una vez realizada la transmisión libera el testigo. Cada estación debe revisar el paquete para determinar si va dirigido a él.

1.4.1. Ethernet

Se le conoce como el estándar IEEE 802.3, emplea una topología lógica de bus y una topología física de estrella o de bus; usa un método de acceso CSMA/CD.

En las redes de tipo Ethernet la utilización de cable coaxial fue lo más empleado y actualmente es reemplazado por el par trenzado. El cable coaxial se emplea tanto con

transmisión en banda de base como con transmisión en banda ancha, si bien el primer tipo es el más utilizado.

La arquitectura Ethernet maneja una nomenclatura que la distingue, y que está definida por los siguientes elementos:

<velocidad en Mbps><tipo de transmisión><distancia en centenares de metros>

Ejemplos de esta nomenclatura son 10Base2, 10Base5, 10BaseT y 10BaseF, que además tienen una relación directa con el tipo de cableado. Las redes Ethernet pueden utilizar diferentes tipos de cableado, cada uno con sus beneficios y problemas. Los tres cableados más comunes son *Thinnet* o 10Base2, *Thicknet* o 10 Base5 y *Twisted Pair* (Par trenzado) o 10 BaseT.

10Base2

Puede transmitir datos a 10 Mbps por Banda Base (señales digitales), pudiendo llegar el cableado hasta 185 metros. Es el más utilizado y recomendado para redes pequeñas. Utiliza la topología local bus. Especifica el uso de cable coaxial de 50 ohms.

10 Base5

Transmite datos a 10 Mbps por Banda Base en un cableado que puede alcanzar 500 metros. El cableado es grueso y es utilizado principalmente para oficinas. La longitud de la red se puede ampliar mediante el empleo de repetidores. Un repetidor es transparente al nivel MAC y dado que no gestiona memoria temporal, no aísla un segmento del otro. Así, si dos estaciones en diferentes segmentos intentan transmitir al mismo tiempo, sus transmisiones se colisionarán.

Para evitar la aparición de *bucles* sólo se permite un camino de segmentos y repetidores entre cualesquiera de las dos estaciones, ampliando la longitud efectiva del medio hasta de 2.5 km.

Es posible mezclar en la misma red segmentos 10Base2 y 10Base5, la única restricción consiste en que el segmento 10Base2 no se debería usar para conectar dos segmentos 10Base5, ya que un segmento "central" debería ser tan inmune al ruido como lo son los segmentos que conecta.

10BaseT

Este arreglo consiste en varias estaciones conectadas a un punto central, denominado repetidor multipuerto, mediante pares trenzados. El punto central acepta la entrada a través de una línea, y la repite en todas las otras líneas.

En la especificación 10BaseT, la longitud máxima de un segmento es de 100 m y se define una topología en estrella. Sacrificando la distancia se puede desarrollar una LAN a 10 Mbps haciendo uso de cable UTP (Unshielded Twisted Pair, Par Trenzado sin Blindaje)

o STP (Shielded Twisted Pair, Par Trenzado Blindado). El cable blindado está recubierto por una malla conductora que actúa de pantalla frente a interferencias y ruido eléctrico generado por motores, luces fluorescentes, generadores, compresores de aire acondicionado, etcétera. Su impedancia característica típica es de 120 a 150 ohms, mientras que el cable no blindado no cuenta con ningún tipo de pantalla adicional y con una impedancia característica típica de 100 ohms. Por su menor sensibilidad a las interferencias y menor atenuación el cable STP es más adecuado para mayores distancias y velocidades de transmisión, así como para operación en entornos con interferencias. Si bien la tendencia es utilizar cable UTP, siempre que sea posible, por su bajo costo, sencillez de instalación y su utilización en tendido telefónico. Tanto el cable UTP como STP se utilizan actualmente a velocidades muy elevadas, incluso a 150 Mbps, con longitudes de cable no superiores a 100 m. Los cables UTP se fabrican frecuentemente con 4 pares y los cables STP con dos pares. Los conectores utilizados se denominan RJ45 y RJ11. El medio generalmente determina si los cables deben ser blindados o no.

10BaseF

La especificación 10BaseF permite a un usuario aprovechar la característica de interferencia nula disponible con el uso de fibra óptica, para transmitir datos a velocidades superiores a 10 Mbps. La longitud máxima de segmento es de 1 km. Las normalizaciones contienen tres especificaciones:

- 10BaseFP (pasivo): topología en estrella pasiva para interconectar estaciones y repetidores con 1 km por segmento como máximo.

- 10BaseFL (enlace): define un enlace punto a punto que puede ser usado para conectar estaciones o repetidores en una distancia máxima de 2 km.

- 10BaseFB (núcleo): define un enlace punto a punto que puede usarse para conectar repetidores en 2 km como máximo. Se puede usar en cascada con un número máximo de 15 repetidores en secuencia para conseguir longitudes superiores.

Las tres especificaciones utilizan un par de fibras ópticas para cada enlace de transmisión, cada una para transmitir en una dirección.

10BaseFL y 10BaseFP definen conexiones punto a punto que pueden emplearse para ampliar la longitud de una red. La principal diferencia entre ellas es que 10BaseFP hace uso de transmisión síncrona, mientras que en 10BaseFL no tiene lugar esa sincronización, de manera que cualquier variación en ésta se propaga a través de varios repetidores.

Ethernet Rápido

El concepto principal en el que se basa el Ethernet Rápido es sencillo: mantener todos los formatos de paquete, interfaces y reglas de procedimiento anteriores, y simplemente reducir el tiempo de bit de 100 nseg. a 10 nseg. Los sistemas Ethernet Rápido

usan concentradores; no se permiten cables de derivación múltiple con derivaciones vampiro o conectores BNC.

1.4.2. Token Ring

Token Ring, también llamado IEEE 802.5, fue ideado por IBM y algunos otros fabricantes, con operación a una velocidad de 4 Mbps o 16 Mbps. *Token Ring* emplea una topología física de estrella. La tarjeta interfaz (NIC) de cada computadora se conecta a un cable que a su vez se enchufa a un *hub* central llamado MAU (Multiple Access Unit, Unidad de Acceso Múltiple). Se pueden conectar MAUs de diferentes anillos de tal modo que los anillos que están en forma separada aparezcan como una sola red. Ver la figura 1.7.

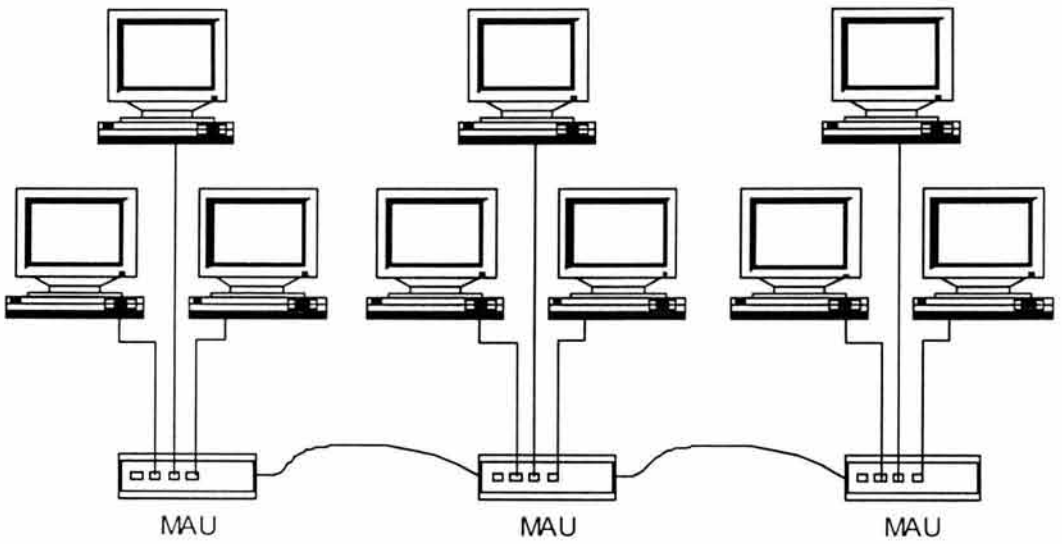

Figura 1.7. Estándar de red Token Ring.

Token Ring se basa en un esquema de paso de testigo (*Token Passing*), tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes de poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, Token Ring llega a ser más eficiente. Esto se debe a que evita las colisiones comunes en el esquema CSMA/CD y que dan como resultado tener que volver a enviar los datos.

1.4.3. Interfaz de Distribución de Datos de Fibra Óptica

La FDDI (Fiber Distributed Data Interface, Interfaz de Distribución de Datos de Fibra Óptica), es una LAN *Token Ring* de fibra óptica de alto desempeño, que opera a 100 Mbps y distancias de hasta 200 km, con un máximo de 1000 estaciones conectadas. Otro

uso común es como *Backbone* para conectar varias LANs de cobre, como se muestra en la figura 1.8.

El cableado de la FDDI consiste en dos anillos de fibra, uno que transmite en dirección de las manecillas del reloj y otro en dirección contraria. Si se rompe cualquiera de ellos, se puede usar el otro como respaldo. Si ambos se rompen en el mismo punto, como por ejemplo, debido a un incendio u otro accidente en el conducto del cable, pueden unirse los dos anillos en uno solo de aproximadamente el doble de longitud.

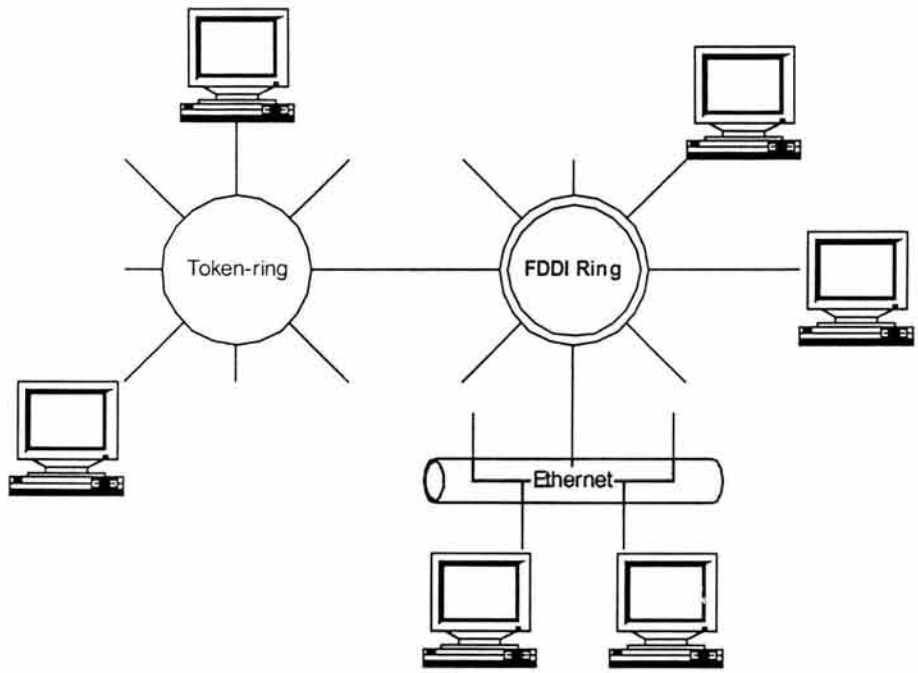

Figura 1.8. Anillo FDDI.

Se suponía que la FDDI debería ser la LAN de la siguiente generación pero realmente nunca se extendió su uso más allá del mercado del *Backbone* (donde sigue desempeñándose bien). La administración de estaciones era demasiado complicada, lo que condujo a *chips* complejos y altos precios. El costo considerable de los *chips* FDDI evitó que los fabricantes de estaciones de trabajo se prestaran a hacer de la FDDI la red estándar, por lo que la producción en volumen jamás se dió y la FDDI nunca entró al mercado de masas.

1.4.4. X.25

Muchas redes públicas antiguas siguen un estándar llamado X.25 que el CCITT (Comité Consultatif International de Télégraphique et Téléphonique, Comité Consultor

Internacional de Telegrafía y Telefonía) desarrolló durante la década de los 70s para proveer una interfaz entre las redes públicas de conmutación de paquetes y sus clientes.

X.25 está orientado a la conexión y trabaja con circuitos virtuales tanto conmutados como permanentes. Un circuito virtual conmutado se crea cuando una computadora envía un paquete a la red y pide que se haga una llamada a una computadora remota. Una vez establecida la conexión, los paquetes se pueden enviar por ella y siempre llegarán en orden. X.25 proporciona control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento u ocupado.

Un circuito virtual permanente se usa de la misma forma que uno conmutado pero se establece previamente por un acuerdo entre el cliente y la portadora; siempre está presente y no se requiere una llamada que lo establezca para poder usarlo. Un circuito de este tipo es semejante a una línea rentada.

1.4.5. *Frame relay*

Este es un servicio para las personas que quieren una forma lo más austera posible, orientada a la conexión, para mover bits a una velocidad razonable y bajo costo. En estos tiempos las líneas telefónicas rentadas son rápidas, digitales y confiables, y las computadoras son rápidas y baratas. Esto sugiere el uso de protocolos simples, con la mayor parte del trabajo realizado por las computadoras de los usuarios en vez de la red. Este es el ambiente para el que está pensado *frame relay*.

Se puede pensar en el *frame relay* como una línea virtual rentada. El cliente renta un circuito virtual permanente entre dos puntos y entonces puede enviar marcos o *frames* (es decir, paquetes) de hasta 1600 bytes entre ellos. También es posible rentar circuitos virtuales permanentes entre un lugar determinado y muchas otras localidades, de modo que cada marco lleve un número de 10 bits que le diga cual circuito virtual utilizar.

La diferencia entre una línea rentada real y una virtual es que, con una real, el usuario puede enviar tráfico durante todo el día a máxima velocidad. Con una línea virtual se pueden enviar ráfagas de datos a toda velocidad, pero el uso promedio a largo plazo deberá ser inferior a un nivel predeterminado. A cambio, la portadora cobra mucho menos por una línea virtual que por una física. Además de competir con las líneas rentadas, el *frame relay* también compite con los circuitos virtuales permanentes de X.25, excepto que opera a grandes velocidades, usualmente a 1.5 Mbps y ofrece menos funciones.

El *frame relay* proporciona un servicio mínimo que básicamente es una forma de determinar el inicio y el fin de cada marco y de detectar errores de transmisión. Si se recibe un marco defectuoso, el *frame relay* simplemente lo descarta. Corresponde al usuario descubrir que se perdió el bloque y emprender la acción necesaria para recuperarlo. A diferencia de X.25, *frame relay* no proporciona acuses de recibo ni control de flujo normal. Sin embargo, tiene un bit en el encabezado que un extremo de la conexión puede encender para indicar al otro que hay problemas, el uso de este bit es opcional para los usuarios.

1.4.6. Modo de Transferencia Asíncrono

El nuevo servicio de área amplia se llama B-ISDN (Broadband Integrated Services Digital Network, Red Digital de Servicios Integrados de Banda Ancha); ésta ofrecerá video sobre pedido, televisión en vivo de muchas fuentes, correo electrónico en multimedia de movimiento total, música con calidad de disco compacto, interconexión de LAN, transporte de alta velocidad para datos científicos e industriales y muchos otros servicios en los que ni siquiera se ha pensado, todo por la línea telefónica.

La tecnología subyacente que hace posible la B-ISDN se llama ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) debido a que no es síncrono (atado a un reloj maestro), como lo está la mayor parte de las líneas telefónicas de larga distancia.

La idea en que se basa la ATM consiste en transmitir toda la información en paquetes pequeños de tamaño fijo llamados celdas. Las celdas tienen una longitud de 53 bytes, de los cuales cinco son de encabezado y 48 de carga útil. ATM es tanto una tecnología (oculta a los usuarios) como un servicio potencial (visible a los usuarios). A veces se llama al servicio *cell relay*, como analogía con *frame relay*.

Las redes ATM son orientadas a la conexión. Para hacer una llamada primero se debe enviar un mensaje para establecer la conexión. Después, todas las celdas subsecuentes siguen la misma trayectoria al destino. La entrega de celdas no esta garantizada, pero si su orden. Las redes ATM se organizan como las WAN tradicionales, con líneas y conmutadores (enrutadores). Las velocidades pretendidas para las redes ATM son de 155 Mbps y 622 Mbps, con la posibilidad de tener velocidades de Giga bits.

Para conseguir que computadoras de diferentes tipos compartan recursos cuando dispongan de una conexión entre ellas, es necesario seguir el criterio descrito por el modelo OSI.

1.5. MODELO OSI

El modelo conceptual OSI (Open System Interconection, Interconexión de Sistema Abierto) es utilizado por prácticamente la totalidad de las redes del mundo. Este modelo fue creado por el ISO (International Standard Organization, Organización Internacional de Estándares), y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas.

Esta clasificación permite que cada protocolo fuera desarrollado con una finalidad determinada, lo cual simplifica el proceso de implementación. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores.

Los siete niveles del modelo OSI son los siguientes: capa de aplicación, capa de presentación, capa de sesión, capa de transporte, capa de red, capa de enlace y capa física.

Capa de Aplicación. En esta capa se encuentran las aplicaciones de red que permiten explotar los recursos de otros nodos. Dicha explotación se hace, por ejemplo, a través de una emulación de una terminal que trabaja en un nodo remoto, interpretando una gran variedad de secuencias de caracteres de control que permiten desplegar en la terminal local los resultados, aún cuando éstos sean gráficos. Otra forma de explotación se da cuando se transmite desde una computadora origen que almacena sus archivos en un formato distinto al del destino. Es posible que el programa de transferencia realice las conversiones necesarias de manera que el archivo puede usarse inmediatamente bajo alguna aplicación.

Capa de Presentación. Esta provee las facilidades para transmitir datos con la sintaxis propia de las aplicaciones o el nodo. En esta capa es posible convertir los datos a un formato independiente de los nodos que intervienen en la transmisión.

Capa de Sesión. Esta capa ofrece el servicio de establecer sesiones de trabajo entre nodos diferentes de una red, sincroniza y establece puntos de chequeo. Por ejemplo, si se hace necesario transferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que una transmisión ordinaria nunca terminaría porque algún interlocutor perderá la conexión. La solución es que se establezcan puntos de chequeo cada pocos minutos de manera que, si la conexión se rompe, más tarde se pueda reiniciar a partir del punto de chequeo, lo cual ahorra tiempo y permite la finalización de la transferencia.

Capa de Transporte. El objetivo de esta capa es el de tomar datos de la Capa de Sesión y asegurarse que dichos datos llegan a su destino. En ocasiones los datos que vienen de la Capa de Sesión exceden el tamaño del MTU (Maximum Transmission Unit, Unidad Máxima de Transmisión) de la interfaz de red, por lo cual es necesario particionarlos y enviarlos en unidades más pequeñas, lo cual da origen a la fragmentación y ensamblado de paquetes cuyo control se realiza en esta capa.

La última labor importante de la Capa de Transporte es ofrecer un mecanismo de nombrado que sirva para identificar y diferenciar las múltiples conexiones existentes, así como determinar en qué momento se inician y se terminan las "conversaciones"; es decir, en esta capa hay un mecanismo de control de flujo. Por ejemplo, si el usuario "a" en el nodo (A) quiere iniciar una sesión de trabajo remoto en un nodo (B), existirá una conexión que debe ser diferenciada de la conexión que el usuario "b" necesita para transferir un archivo del nodo (B) al nodo (A).

Capa de Red. Se encarga de controlar la operación de la subred (medios físicos y dispositivos de enrutado). Una tarea primordial es decidir cómo hacer que los paquetes lleguen a su destino desde su origen en el formato predefinido por un protocolo. Otra función importante en este nivel es la resolución de "cuellos de botella". En estos casos se pueden tener varias rutas para dar salida a los paquetes y con base en algunos parámetros de

eficiencia o disponibilidad se eligen rutas dinámicas de salida. Para efectos de la obtención de estadísticas, se registra el tipo y cantidad de paquetes que circulan.

Capa de Enlace. En esta capa se toman los bits a transmitir y se agrupan para formar marcos de bits (*frames*). Se realiza un chequeo de errores sobre cada *frame*. Si un marco se pierde o se daña en el medio físico esta capa se encarga de retransmitirlo, aunque en ocasiones dicha operación provoca que un mismo marco se duplique en el destino. Dado el caso es obligación detectar tal anomalía y corregirla. También en esta capa se decide cómo acceder al medio físico.

Capa Física. Esta capa tiene que ver con el envío de bits en un medio físico de transmisión y asegura que si de un extremo del medio se envía un 1 del otro lado se reciba ese 1. Brinda los medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace físico entre los sistemas.

Gráficamente el modelo conceptual se puede representar como se muestra en la figura 1.9.

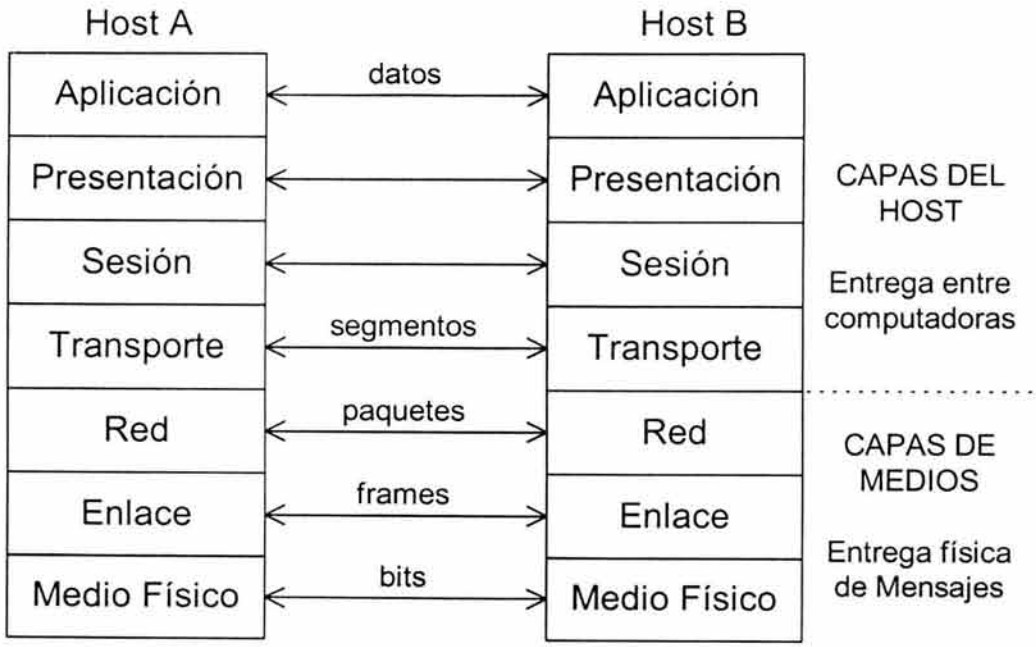

Figura 1.9. Modelo OSI.

1.5.1. Transmisión de datos en el modelo OSI

Un envío de datos típico bajo el modelo de referencia OSI comienza con una aplicación en un nodo cualquiera de la red. Esta aplicación genera los datos que quiere enviar a su contraparte en otro nodo.

1. La Capa de Aplicación toma los datos y los encapsula añadiendo un encabezado que puede contener información de control o estar vacío. Envía el paquete resultante a la Capa de Presentación.

2. La Capa de Presentación recibe el paquete y no intenta decodificarlo o separar sus componentes, sino que lo toma como datos y le añade un encabezado con información de control de esta capa.

3. Las Capas de Sesión y de Transporte reciben el paquete, que también son sólo datos para ellas y le añaden un encabezado de control. El resultado es enviado a la capa inferior.

4. La Capa de Red se encarga de enrutar el paquete a su destino.

5. La Capa de Enlace y Física toman, respectivamente, el paquete que les envía la capa superior y añaden a éste un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultado a la capa inferior.

6. La Capa Física, por último, traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.

7. En el nodo destino comienza el camino inverso; es decir que cada capa quita su encabezado de control y envía el paquete a la capa superior hasta llegar a la de Aplicación en el nodo destino.

Como puede apreciarse, todas las capas, excepto la de Aplicación, procesan los paquetes realizando operaciones que sirven para verificar que el paquete de datos real esté íntegro, o para que éste llegue a su destino sin que los datos sufran alguna alteración.

Las funciones descritas por el modelo OSI se llevan a cabo a través de la utilización de diversos protocolos de red.

1.6. PROTOCOLOS DE RED

En las redes, las computadoras deben comunicarse entre sí e intercambiar datos con sistemas operativos y *hardware* muy distintos.

En el nivel físico, esto se realiza a través de tarjetas de red, y una conexión entre las mismas. Lógicamente se debe establecer una comunicación "del mismo lenguaje" entre distintos sistemas operativos y tarjetas de red. Este lenguaje es lo que se llama protocolo.

Algunos protocolos se encargan de transportar datos, mientras que otros se encargan de la comunicación entre computadoras, y otros de convertir correctamente los datos. Así, protocolo es el conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Actualmente existen protocolos para cualquier tipo de comunicación; muchos de ellos han caído en desuso y otros se encuentran en su plenitud de utilización. Esto es producto de una sociedad cada vez más intercomunicada y relacionada, en donde lo importante es que la información llegue a su destino sí, pero también lo es que llegue en las mismas condiciones en que ha sido enviada y en el tiempo previsto.

Algunos de los protocolos más conocidos y ampliamente difundidos son NetBIOS y TCP/IP.

1.6.1. NetBIOS

El protocolo NetBIOS (Network Basic Input Output System, Sistema Básico de Entrada - Salida para Red) es el más sencillo. Está compuesto por menos de 20 comandos que se ocupan del intercambio de datos. Se ha perfeccionado y ampliado recibiendo el nuevo nombre NetBEUI (NetBIOS Extended User Interface) pero continúa utilizando el juego de comandos del NetBIOS. Posteriormente, para hacerlo compatible con otros protocolos como IPX–SPX (Internetwork Packet Exchange–Sequenced Packet Exchange), se amplió nuevamente recibiendo el nombre de NWLink (NetWare Link).

NetBIOS toma el puerto 137 a 139 en computadoras que utilizan el sistema operativo Windows. Está considerado el protocolo más fácilmente vulnerable de los existentes, a punto tal que cualquier especialista de seguridad recomienda no utilizarlo.

1.6.2. TCP/IP

En los años 80s una gran cantidad de instituciones estaban interesadas en conectarse a una gran red que se expandía por todo EE.UU. (ahora Internet). Para esto definieron un conjunto de reglas que establecen cómo conectar computadoras entre sí para lograr el intercambio de información.

Actualmente TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Internet) se utiliza ampliamente en la versión 4 (IPv4) que no incluye la seguridad como parte de su construcción. Sin embargo se encuentra en aumento el uso de IPv6 (o IPSec) que dentro de sus estándares soporta autentificación, integridad y confidencialidad.

El TCP/IP es actualmente el protocolo más ampliamente utilizado por su independencia del Sistema Operativo y *hardware* utilizado. Es un protocolo eficaz orientado por paquetes; es particularmente adecuado como plataforma para protocolos de los más distintos servicios y aplicaciones que se pueden conseguir a través de la red.

Funcionamiento de TCP/IP

Las aplicaciones de red presentan los datos a TCP. Este divide los datos en trozos (paquetes), y le otorga a cada uno un número. El conjunto de paquetes ordenados pueden

representar imágenes, documentos, videos, o cualquier otra información que el usuario desee enviar.

Luego, TCP presenta los datos a IP, quien agrega su información de control (como la dirección de origen y destino). Si por algún motivo IP no puede entregar algún paquete, TCP pedirá el reenvío de los faltantes. Por último TCP se encarga de reensamblar los paquetes en el orden correcto, basándose en los números asignados previamente.

Las capas del modelo TCP/IP

Basado en las capas del modelo OSI, se definió un conjunto de protocolos de TCP/IP, que consta de 4 capas principales y que se han convertido en un estándar a nivel mundial. TCP/IP no es un único protocolo, sino que en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP y el IP, que son los que dan nombre al conjunto. Se diferencian cuatro capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI, como se muestra en la figura 1.10.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de Enlace respecto al modelo OSI. Por este motivo los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio físico, de forma que sea posible intercambiar información entre medios diferentes y tecnologías que inicialmente son incompatibles.

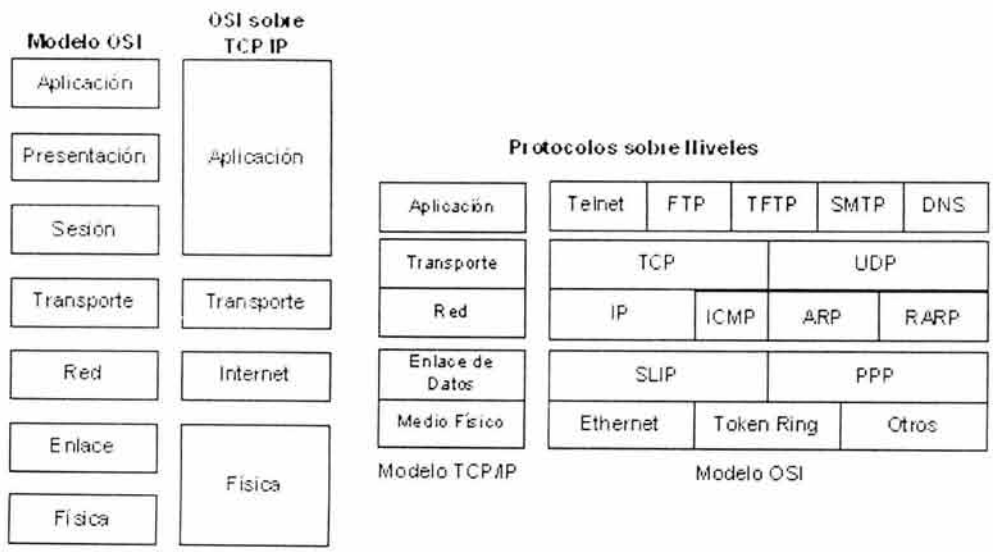

Figura 1.10. Comparación modelo OSI – TCP.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren. En TCP/IP cada una de estas unidades de información recibe el nombre de "Datagrama" (datagram), y son conjuntos de datos que se envían como mensajes

1.6.3. Nivel físico del modelo TCP/IP

Es la interfaz de red y corresponde al nivel de Enlace y Físico del modelo OSI. La capa inferior, que podemos nombrar como Física respecto al modelo OSI, contiene varios estándares (conocidos con el nombre del IEEE 802.X) que establecen las reglas para enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10BaseT), fibra óptica (10BaseF) y su propio método de acceso.

Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada *host*, como puede ser una línea punto a punto o una red Ethernet.

ARP

El ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones) no se dedica al transporte de datos sino a convertir las direcciones IP en direcciones de la red física. El protocolo consigue la dirección mediante la difusión de un paquete de petición ARP que contiene la dirección IP del sistema destinatario. Todas las computadoras de la red detectan estas difusiones y aquel que contenga la dirección IP solicitada, la transmitirá al sistema solicitante mediante una respuesta de paquete ARP. Luego el solicitante almacena estas direcciones en una tabla para su uso posterior; y esta tabla además servirá de referencia a otros equipos para evitar la búsqueda de las mimas direcciones.

RARP

El RARP (Reverse Address Resolution Protocol, Protocolo de Resolución de Direcciones Inverso) realiza el trabajo inverso de ARP. Es decir que obtiene la dirección IP a partir de una dirección física.

ICMP

El ICMP (Internet Control Message Protocol, Protocolo de Control de Mensajes de Internet) es de características similares al UDP, pero con un formato aún más simple. Su utilidad no está en el transporte de datos "de usuario", sino en los mensajes de error y de control necesarios para los sistemas de la red.

1.6.4. Nivel de datos del modelo TCP/IP

El nivel de Datos también es conocido como nivel de Internet y es equivalente al nivel de Red del modelo OSI. Incluye los protocolos SLIP, PPP y, parcialmente al

protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

SLIP

El SLIP (Serial Link Internet Protocol, Protocolo de Internet de Enlace Serial) brinda una conexión de velocidad aceptable, con la posibilidad de admitir varias conexiones simultáneas con un mismo modem. Es usado todavía en los accesos a Internet por medio de la línea telefónica. El mecanismo es sencillo: se llama al proveedor, quien funciona de puente entre la computadora y el resto de la red, y una vez establecida la comunicación se tiene acceso total a los servicios. Es un protocolo pequeño para la baja velocidad de los enlaces telefónicos, por lo que ha caído en desuso.

Este protocolo apoya solamente a IP, no provee detección de errores ni de autentificación y tiene la desventaja de que existen muchas implementaciones incompatibles entre ellas.

PPP

El PPP (Point to Point Protocol, Protocolo Punto a Punto) fue desarrollado por el IETF (Internet Engineering Task Force) en 1993 para mejorar algunas deficiencias de SLIP, y crear un estándar internacional.

PPP es un protocolo mucho más amplio, más potente y adaptable. Proporciona un método de enlace bidireccional *full dúplex* para transportar datagramas multiprotocolo sobre enlaces simples (conexión directa) de un equipo a otro (punto a punto), en cualquier situación sin importar el tipo de conexión, el *hardware* ni el sistema operativo.

Sus principales características son:

- Es transparente a las capas superiores.
- Transmite protocolos IP, IPX, Apple Talk, etc.
- Es ampliable ya que no fue pensando para solucionar un problema en concreto.

PPP esta dividido en dos subprotocolos:

- **LCP** (Link Control Protocol, Protocolo de Control de Enlace): es el encargado de comenzar una conexión (fase abierta), definir como se producirá el intercambio de datos (tamaño de los paquetes, identificación, tiempos de espera, etc.) y de finalizar la conexión (enlace muerto).

- **NCP** (Network Control Protocol, Protocolo de Control de Red): se encarga de negociar y configurar las opciones de los diferentes protocolos de red (IP, IPX, etc.) abriéndolos uno a la vez. Cuando un NCP ha alcanzado el estado abierto, PPP transportará los correspondientes paquetes. Cualquier paquete recibido mientras su NCP no esté en el estado abierto es descartado.

1.6.5. Nivel de red del modelo TCP/IP

El nivel de Red contiene uno de los protocolos más relevantes del conjunto TCP/IP: el protocolo IP.

IP

El IP define la base de todas las comunicaciones en Internet. Es utilizado por los protocolos del nivel de transporte (como TCP) para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando.

La cabecera IP tiene un tamaño de 160 bits y está formada por varios campos de distinto significado entre los que se destaca el tipo de protocolo de transporte del datagrama, el número de paquete (para su posterior ensamble), la dirección de origen y la de destino, etc.

Cabe destacar que este protocolo no garantiza la llegada de los paquetes al destino (conexión sin garantía), ni su orden; sólo garantiza la integridad del encabezado IP. La fiabilidad de los datos deben garantizarla los niveles superiores. También se trata de una transmisión sin conexión, porque cuando se envía el paquete no se avisa al receptor para que esté preparado (no existe una conexión directa emisor–receptor). De hecho, muchas veces se mandan paquetes a un destino inexistente o que no se encuentra disponible.

El protocolo IP identifica a cada equipo que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe ser único para cada *host*, y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos (por ejemplo: 205.025.076.223).

En el nivel IP se definen los siguientes aspectos de intercambio de información:

- Un mecanismo de direcciones que permite identificar de manera unívoca al emisor y al receptor, sin considerar las ubicaciones ni las arquitecturas de las redes a las cuales pertenece cada uno. Este mecanismo permite la universalidad de la red.

- Un concepto relativo al transporte de los paquetes de datos, para que el mismo llegue al receptor a través de los nodos de las redes involucradas. Dentro de cada red tendrá que haber al menos un receptor (ruteador) que esté conectado con otra computadora en otra red en el exterior. Los ruteadores reconocen un paquete y comprueban que no sea para alguna máquina conectada a su red y entonces lo manda a otra, más cercana al destino. Esto se hace sucesivamente hasta que el paquete llega al ruteador de la red donde se encuentra la computadora destinataria del mensaje.

- Un formato para los paquetes (cabecera). Con ésta, el ruteador podrá identificar al destinatario del mensaje, ya que como se explicó, uno de los datos de la cabecera es el nombre de destino del mensaje.

La dirección IP se utiliza para identificar tanto a la computadora en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron cuatro clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

Clase A: son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de las computadoras (*Hosts*) que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de Hosts en cada una de las 126 redes de esta clase. Este tipo de direcciones es usado por redes muy extensas.

Clase B: estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, debiendo ser un valor entre 128.001 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador de la computadora permitiendo, por consiguiente, un número máximo de 64,516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes.

Clase C: en este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.001.001 hasta 223.254.254. De esta manera queda libre un byte para el *host*, lo que permite que se conecten un máximo de 254 computadoras en cada red.

Clase D: esta clase se usa con fines de multidifusión a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Actualmente se planea la utilización de redes Clase E que comprenderían el rango desde 240.0.0.0 hasta 247.255.255.255.

Nombres de Dominio

Ya que para el ser humano se hace difícil recordar direcciones IP como 209.89.67.156 se creó lo que dió en llamar DNS (Domain Name Server, Servidor de Nombres de Dominio), el cual es el encargado de convertir la dirección IP en un nombre de dominio generalmente fácil de recordar y viceversa. Así www.clarin.com será entendida, de acuerdo al servicio de DNS como 110.56.12.106 o \\Carlos se convertirá en 10.0.0.33.

Puertos

Para acceder desde el nivel de Red al nivel de Aplicación no sirve simplemente indicar la dirección IP, se necesitarán más especificaciones para que el *host* de destino pueda escoger la aplicación correcta. Estas especificaciones harán necesario la definición de Puerto. Un puerto se representa por un valor de 16 bits y hace la diferencia entre los posibles receptores de un mensaje.

La combinación Dirección IP + Puerto identifican una región de memoria única denominada *Socket*. Al indicar este *Socket*, se puede trasladar el paquete a la aplicación correcta (FTP, Telnet, WWW, etc.) y, si además recibe el puerto desde donde fue enviado el mensaje, se podrá suministrar una respuesta.

En la tabla 1.1, se muestran los puertos y las aplicaciones más usados.

Puerto	**Aplicación**	**Protocolo**	**Descripción**
20	FTP–Data	TCP/UDP	Transferencia archivos
21	FTP	TCP	Control Transferencia Archivos
23	TELNET	TCP/UDP	Servicio Remoto
25	SMTP	TCP/UDP	Envío de mails
43	Whois	TCP/UDP	
53	DNS	TCP/UDP	Servicio de Nombre de Dominios
70	Gopher	TCP/UDP	
79	Finger	TCP/UDP	
80	WWW–HTTP	TCP/UDP	World Wide Web
110	POP3 (PostOffice)	TCP/UDP	Recepción de mail
119	UseNet	TCP	Newsgropus de usuarios
137	NetBIOS	UDP	
194	IRC	TCP/UDP	Chat
443	HTTPS	TCP	http Seguro vía SSL
750	Kerberos	TCP/UDP	
6667	IRC	TCP	Chat

Tabla 1.1. Puertos de aplicación.

Actualmente existen miles de puertos ocupados de los $2^{16} = 65535$ posibles, de los cuales apenas unos cuantos son los más utilizados y se encuentran divididos en tres rangos:

- Desde el puerto 0 hasta el 1023: son los puertos conocidos y usados por aplicaciones de servidor.
- Desde el 1024 hasta el 49151: son los registrados y asignados dinámicamente.
- Desde el 49152 hasta 65535: son los puertos privados.

Alternativamente al protocolo IP, son utilizados otros protocolos como son Apple Talk e IPX-SPX.

AppleTalk

Este protocolo (de nivel de red) está incluido en el Sistema Operativo de Apple Macintosh desde su aparición, permite interconectar computadoras y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte.

IPX-SPX

El IPX-SPX es el protocolo de nivel de red propietario de NetWare (para su sistema operativo Novell) siendo utilizado en las redes tipo LAN.

1.6.6. Nivel de transporte del modelo TCP/IP

Coincide con el nivel de Transporte del modelo OSI. Esta capa está implementada por dos protocolos: el TCP y el UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario). El primero es un protocolo confiable y orientado a conexiones, lo cual significa que ofrece un medio libre de errores para enviar paquetes. El segundo es un protocolo no orientado a conexiones y no es confiable. El TCP se prefiere para la transmisión de datos a nivel red de área amplia y el UDP para redes de área local.

TCP

El TCP nació principalmente por la necesidad de una comunicación "segura" entre el emisor y el destinatario del mensaje. Así, las aplicaciones pueden encargarse de su tarea sin preocuparse de la seguridad en la comunicación.

TCP divide el mensaje original en datagramas de menor tamaño (segmentos de 32 bits), y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga, además, de añadir cierta información necesaria al inicio de cada uno de los datagramas (cabecera). Luego, se ocupa de que los datos sean entregados y que los paquetes sean reensamblados correctamente, asegurando así que lo que se recibe sea efectivamente lo enviado.

Si ocurriera algún error en la transmisión, TCP se encargará de reenviar los paquetes. TCP sabrá que hubo errores o que el paquete fue entregado correctamente gracias a un paquete de respuesta (acuse de recibo) que envía el destinatario al emisor (para que vuelva a realizar el envío) en donde indica si faltan paquetes, tamaños o datos erróneos, etc.

Las principales características de este protocolo son:

- Servicio orientado a conexión: el destino recibe exactamente la misma secuencia de bytes que envía el origen.
- Conexión de circuito virtual: durante la transferencia, el protocolo en las dos máquinas continúan comunicándose para verificar que los datos se reciban correctamente.
- Transferencia con memoria intermedia: la aplicación utiliza paquetes del tamaño que crea adecuado, pero el *software* de protocolo puede dividir el flujo en subpaquetes o armar uno con un grupo de ellos, independientemente de la aplicación. Esto se realiza para hacer eficiente el tráfico en la red. Así, si la aplicación genera piezas de un byte, el protocolo puede armar datagramas razonablemente más largos antes de hacer el envío, o bien, forzar la transferencia dividiendo el paquete de la aplicación en datagramas más pequeños.
- Flujo no estructurado: se refiere a la posibilidad de envío de información de control de estado junto a los datos propiamente dichos.
- Conexión *full duplex*: permite la transferencia concurrente en ambas direcciones, sin ninguna interacción. La ventaja es que puede enviar datagramas desde el origen al receptor e información de control en sentido opuesto, reduciendo el tráfico en la red.

En la figura 1.11 se detalla la constitución de cada datagrama del protocolo TCP (con un tamaño de 20 a 24 bytes). Comprender este diagrama es de especial interés para cualquiera que desee manipular datos en una comunicación actual.

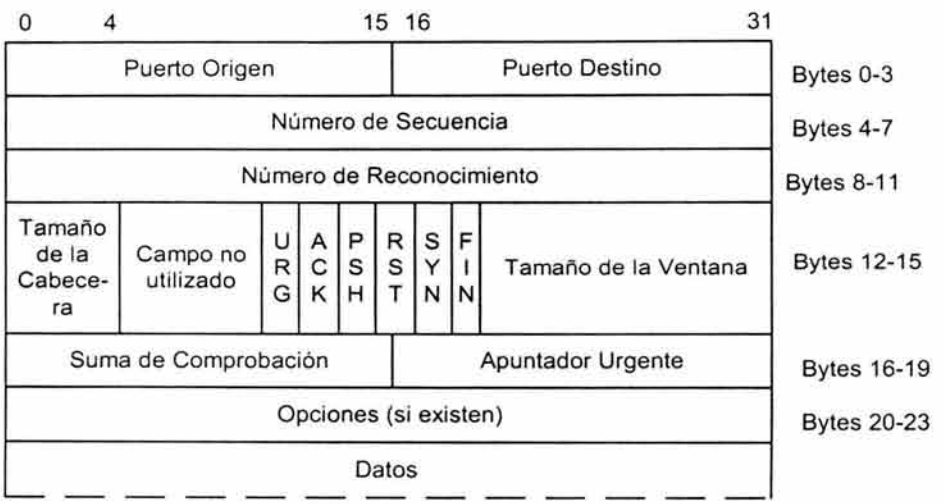

Figura 1.11. Constitución de un datagrama TCP.

Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo sistema puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos.

El Puerto de Origen y Destino. Se asigna un campo de 16 bits para cada puerto. Cada campo contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa cliente utiliza números aleatorios, el servidor deber tener asignado un número estándar para que pueda ser utilizado por el cliente (ver Tabla 1.1). Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

Número de Secuencia. Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración, mediante números de secuencia (de 32 bits), de los mismos para que puedan ser ensamblados en el orden correcto.

Número de Reconocimiento. En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor señales de confirmación, de 32 bits, una vez que se ha recibido y comprobado la información satisfactoriamente. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar.

Tamaño de la Cabecera. (4 bits) Indica la cantidad de palabras de 32 bits contenidas en la cabecera TCP. Esta información es necesaria porque el campo de Opciones es de longitud variable, por lo que la cabecera también. Esto permite determinar el lugar donde comienzan los Datos.

Cada datagrama tendrá un estado que le indicará al servidor el contenido, motivo y la forma en que deberá ser atendido ese paquete. Este campo contiene los siguientes estados (Si estado = 1, se considera verdadero):

- **URG**ent: Identifica datos urgentes.
- **ACK**nowledge: Indica que el campo de confirmación es válido.
- **PuSH**: Aunque el *buffer* de datos no esté lleno, se obliga el envío.
- **ReSeT**: Abortar la conexión. Todos los *buffers* asociados se vacían.
- **SY**nchronize sequence **N**umber: Sincronizar los números de secuencia.
- **FIN**ish: Se solicita el cierre de la conexión.

Tamaño de la Ventana. Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada computadora puede procesar los datos que le son enviados. Si esto no se tuviera en cuenta, el equipo de mayor potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla. Este inconveniente se soluciona mediante un campo de 16 bits, en el cual

se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar en un momento dado.

Suma de Comprobación. También puede ocurrir que la información del datagrama llegue con errores a su destino. Para poder detectarlos, cuando sucede esto, se incluye un campo de 16 bits, el cual contiene un valor calculado a partir de la información del datagrama completo. En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera. Si el valor es distinto significará que el datagrama es incorrecto.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo suma de comprobación de la cabecera del datagrama siguiente. De esta manera el primero empezará en cero; el segundo contendrá el tamaño de la parte de datos; el tercero contendrá la suma de ese número más el tamaño de los datos del segundo datagrama; y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Opciones. Campo de 32 bits que permite que una aplicación negocie durante la configuración de la conexión, características como el tamaño máximo del segmento TCP. Si este campo tiene el primer octeto a cero, indica que no hay opciones.

Todas estas características se traducen en un complejo por el envío de señales de confirmación y la velocidad se ve sacrificada en pos de la fiabilidad de los datos.

UDP

El UDP puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. Puesto que UDP no admite numeración de los datagramas, este protocolo se utiliza principalmente cuando el orden en que se reciben los mismos no es un factor fundamental, cuando se quiere enviar información de poco tamaño que cabe en un único datagrama o si la fiabilidad de los datos no es un factor de relieve.

Cuando se utiliza UDP la garantía de que un paquete llegue a su destino es mucho menor que con TCP, debido a que no se utilizan las señales de confirmación. Por todas estas características la cabecera del UDP es bastante menor en tamaño que la de TCP. Esta simplificación resulta en una mayor eficiencia en determinadas ocasiones. Es utilizado en redes con muy buen cableado.

1.6.7. Nivel de aplicación del modelo TCP/IP

Dentro de los diferentes servicios que proporciona el protocolo TCP/IP encontramos:

FTP

El FTP se incluye como parte del TCP/IP, estando destinado a proporcionar el servicio de transferencia de archivos. Depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con Telnet (protocolo para la conexión remota).

FTP utiliza dos canales de conexión separados: uno es el canal de comandos que permanece abierto durante toda la sesión y el otro es el canal de transmisión de archivos (ver figura 1.12).

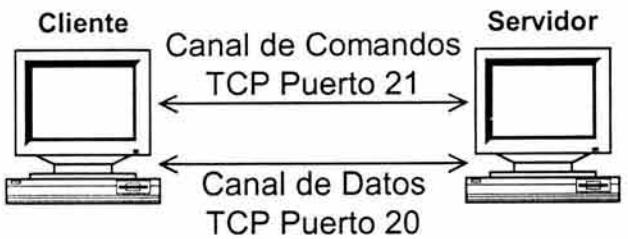

Figura 1.12. Conexión FTP.

El FTP permite acceder a algún servidor que disponga de este servicio y realizar tareas tales como moverse a través de su estructura de directorios, ver y descargar archivos al ordenador local, enviar o copiar archivos directamente de un servidor a otro de la red. Lógicamente y por motivos de seguridad se hace necesario contar con el permiso previo para poder realizar todas estas operaciones. El servidor FTP pedirá el nombre de usuario y clave de acceso al iniciar la sesión (*login*). Este debe ser suministrado correctamente para poder utilizar el servicio.

La manera de utilizar FTP es por medio de una serie de comandos, los cuales suelen variar dependiendo del sistema en que se esté ejecutando el programa, pero básicamente con la misma funcionalidad. Existen aplicaciones de FTP para prácticamente todos los sistemas operativos.

Existe una forma muy utilizada para acceder a fuentes de archivos de carácter público por medio de FTP y es el acceso FTP Anónimo, mediante el cual se pueden copiar archivos de uso público. Generalmente el acceso anónimo tendrá algunas limitaciones en los permisos, siendo normal en estos casos que no se permita realizar acciones tales como añadir archivos o modificar los existentes.

El FTP proporciona dos modos de transferencia de archivos: ASCII y binario. El modo de transferencia ASCII se utiliza cuando se quiere transmitir archivos de texto puro. El binario se debe utilizar en cualquier otro caso (datos que no son texto plano).

HTTP

Este protocolo es la base de toda comunicación desarrollada en la Web. Utilizado desde principios de lo 90s es un protocolo ASCII que se ocupa de establecer una comunicación TCP segura entre el cliente y el servidor a través del puerto 80. HTTP es un protocolo de aplicación genérico, sin estado, orientado a objetos, que se puede utilizar para muchas tareas, como servidores de nombres y sistemas de gestión de objetos distribuidos, por medio de la ampliación de sus métodos de petición o comandos.

Sus principales características son:

- Protocolo de Aplicación: aunque generalmente se implementa sobre el TCP/IP, también es capaz de hacerlo sobre otros protocolos de capas más bajas. HTTP presupone únicamente un transporte fiable, así que puede utilizar cualquier protocolo que garantice este requisito mínimo.

- Sistemas de información distribuidos: HTTP soporta sistemas de información distribuidos, es decir, sistemas esparcidos por múltiples servidores.

- Genérico: HTTP no dicta el contenido de los datos que transfiere; simplemente actúa como un conducto para mover datos de aplicación, por lo que se puede transferir cualquier tipo de información por medio de HTTP.

- Sin estado: HTTP no mantiene un estado. Cuando se solicita una transferencia a través de HTTP, se crea la conexión, se produce la transferencia y se termina la conexión. Esta es una de las debilidades de HTTP; sin información de estado, es difícil desarrollar una aplicación basada en la Web que permita que un usuario se conecte en una página y que mantenga la información de conexión durante todo el tiempo que el usuario esté accediendo activamente al destino. Cualquier documento transferido a través de HTTP no tiene ningún contexto y es completamente independiente de todos los documentos transferidos antes de él.

- Orientado a objetos, escritura y negociación de la representación de los datos: HTTP no está orientado a objetos en el mismo sentido que un lenguaje de programación. Esta descripción significa simplemente que HTTP tiene etiquetas que indican el tipo de datos que se van a transferir por medio de la red, así como métodos, que son comandos que indican qué debe transferirse.

- Sistema creado independientemente de los datos que se transfieren: Debido a que HTTP sólo mueve datos, no necesita tener información sobre cada uno de los tipos a transferir. Por ejemplo, un servidor Web no necesita un conocimiento específico sobre el funcionamiento interno del formato de un archivo de video para hacer el envío.

La comunicación que se establece en una conexión HTTP es de muy corta duración. El cliente establece la conexión con el servidor HTTP y le solicita un documento

determinado. El servidor recibe la consulta, la evalúa y envía el documento solicitado (si existe) o un mensaje de error en caso contrario. Luego el servidor finaliza la conexión sin que existan otros estados intermedios (ver figura 1.13).

El protocolo HTTP en su estructura, divide el mensaje en encabezado (*Header*) y en cuerpo (*Entity*), separados entre sí por una línea en blanco.

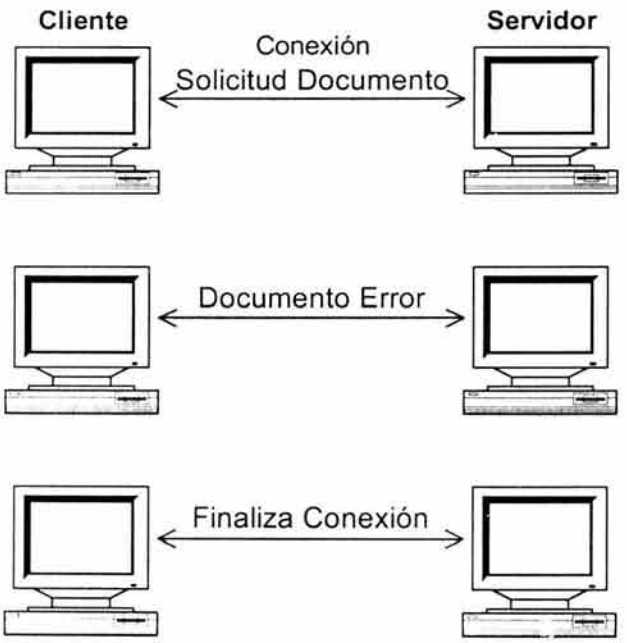

Figura 1.13. Conexión HTTP.

SMTP

El servicio de correo electrónico se proporciona a través del protocolo SMTP, (empleando redes TCP/IP) y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no sólo se puede intercambiar texto, sino también archivos binarios de cualquier tipo.

Generalmente los mensajes de correo electrónico no se envían directamente a las computadoras personales de cada usuario, sino a un servidor de correo, que actúa como almacén de los mensajes recibidos. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio equipo para leerlos de forma local vía POP (Post Office Protocol, Protocolo de Oficina de Correo).

El cliente de correo envía una solicitud a su servidor de correo (al puerto 25) para enviar un mensaje (y almacenarlo en dicho servidor). El servidor establece una conexión

SMTP donde emisor y receptor intercambian mensajes de identificación, errores y el cuerpo del mensaje. Luego de esto el emisor envía los comandos necesarios para la liberación de la conexión (ver figura 1.14).

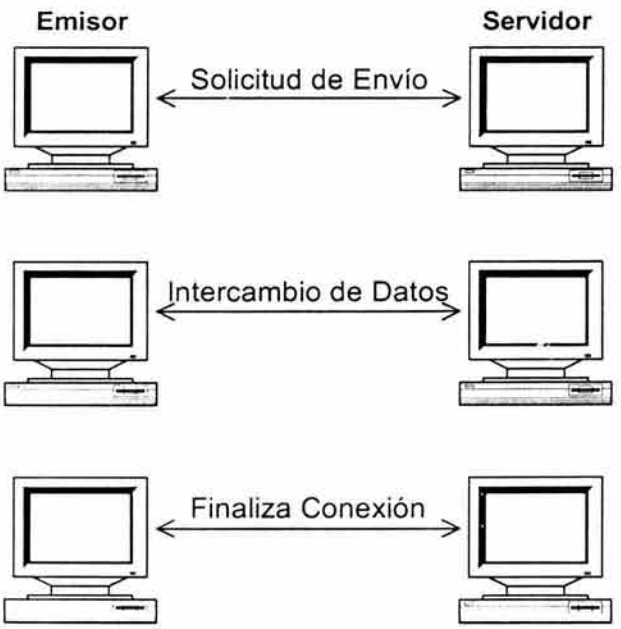

Figura 1.14. Conexión SMTP.

POP

El servidor POP fue diseñado para la recuperación de correo desde el servidor de correo hacia la computadora destinataria del mensaje.

Al igual que sucede con SMTP, inicialmente el proceso escucha el puerto del protocolo POP (el 110) y cuando el emisor solicita el mensaje se establece una conexión full duplex donde se intercambian los mensajes Emisor–Servidor para luego finalizar la conexión cuando se hallan enviado cada uno de los correos que se almacenaban en el servidor.

Actualmente el protocolo POP se encuentra en su tercera implementación por lo que generalmente se conoce como POP3 (ver figura 1.15).

MIME

El protocolo MIME (Multipurpose Internet Mail Extensions, Extensiones Multipropósito de Correo de Internet) es una extensión del protocolo SMTP y se creó con el fin de soportar algunos juegos de caracteres extendidos (no US–ASCII) no soportados por este último.

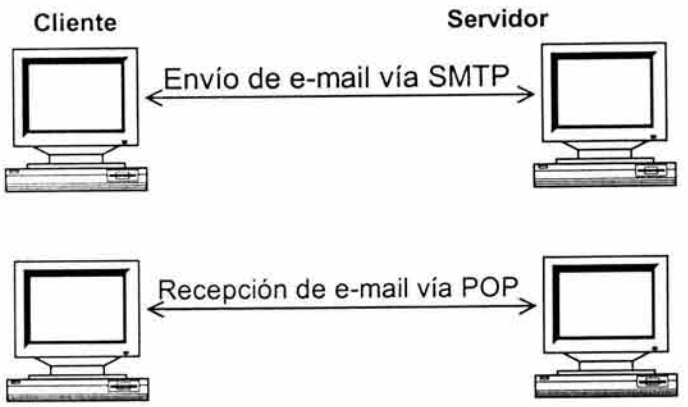

Figura 1.15. Relación SMTP-POP.

MIME especifica tres campos que se incluyen en la cabecera del mensaje, para hacer la conversión adecuada al juego de caracteres no US–ASCII utilizado:

- MIME–Versión: especifica la versión de MIME utilizado para codificar el mensaje.
- Content–Type: especifica el tipo y subtipo de los datos no ASCII.
- Content–Tranfer–Encoding: especifica el tipo de codificación usado para traducir los datos en ASCII.

NNTP

El NNTP (Network News Transfer Protocol, Protocolo de Transferencias de Noticias en Red) fue diseñado para permitir la distribución, solicitud, recuperación y envío de noticias. NNTP está basado en las especificaciones de UseNet pero con algunas modificaciones en su estructura que le permiten ser adaptable a otros grupos de noticias.

SNMP

El SNMP (Simple Network Management Protocol, Protocolo para la Administración Simple de una Red) se utiliza para monitorizar, controlar y administrar múltiples redes físicas de diferentes fabricantes, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace y, aunque es parte de la familia TCP/IP, no depende del IP, ya que fue diseñado para ser independiente y puede funcionar igual sobre, por ejemplo, IPX de Novell.

Una vez que hemos presentado los conceptos relacionados con el presente tema de tesis, procederemos a explicar las generalidades de seguridad en redes.

CAPÍTULO 2

GENERALIDADES DE SEGURIDAD EN REDES

En este capítulo hablaremos sobre aspectos de seguridad, además de presentar un panorama general de los servicios vulnerables en la interconexión de redes.

2.1. INTRODUCCIÓN A LA SEGURIDAD

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecta, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. "*Hackers*", "*crakers*", entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

Es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

Por esto, y por cualquier otro tipo de consideración que se tenga en mente, es realmente válido pensar que cualquier organización que trabaje con computadoras, y hoy en día más específicamente con redes de computadoras, debe tener normativas que mantengan el buen uso de los recursos y de los contenidos, es decir, el buen uso de la información.

Se puede considerar que la seguridad en redes "es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de los mismos".

La seguridad indicará el índice en el que un sistema informático esté libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir en un 100% por lo que sólo se habla de fiabilidad y se le define como "la probabilidad de que un sistema se comporte tal y como se espera de él", y se habla de sistema fiable en vez de sistema seguro.

Comprender y conocer de seguridad ayudará a llevar a cabo el análisis sobre los riesgos, las vulnerabilidades, amenazas y contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, con base en las necesidades de seguridad.

El objetivo que se pretende alcanzar en el presente trabajo es el de mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales), control y autenticidad de la información manejada a través de políticas de seguridad.

2.2. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del sistema de seguridad que la organización posee para salvaguardar sus activos. Las políticas de seguridad informática constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategias que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización. Ellas deben responder a intereses y necesidades organizacionales, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización.

Las políticas de seguridad informática involucran los siguientes aspectos:

- La seguridad física, como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego y el agua, y otras similares.

- Medidas técnico-administrativas, la existencia de procedimientos para la correcta administración de la seguridad o auditoría de sistemas de información interna.

- La llamada seguridad lógica, como el control de accesos a la información, exige la identificación y autentificación del usuario, o el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, o de información transmitida por línea.

En lo que respecta al presente trabajo, nos enfocaremos al aspecto de la seguridad lógica, dado que el objetivo que perseguimos es fortalecer este tópico dentro de nuestra red corporativa.

2.2.1. Seguridad lógica

Antes de comenzar el análisis de la seguridad lógica se deberá conocer las características de lo que se pretende proteger: la información.

La información "es una agregación de datos que tiene un significado específico más allá de cada uno de éstos", y tendrá un sentido particular según cómo y quién la procese. Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es información.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Los distintos aspectos que la seguridad lógica debe proteger de la información son: confidencialidad, integridad, autenticidad, no repudio, disponibilidad de los recursos y de la información, consistencia, control de acceso y auditoría.

Confidencialidad

Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

Integridad

Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de *hardware* y/o *software*.
- Causadas de forma intencional.
- Causadas de forma accidental.

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

Autenticidad

En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

No repudio

Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

Disponibilidad de los recursos y de la información

De nada sirve la información si se encuentra intacta en el sistema, pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La

disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

Consistencia

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

Control de acceso a los recursos

Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Auditoría

Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre "espiar" y "monitorear" a los mismos. La ética es algo que todo buen administrador debe conocer y poseer.

Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible definir de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo, antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

Las políticas de seguridad informática deben orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere considerar entre otros, los siguientes elementos.

2.2.2. Elementos de una política de seguridad informática

Con las políticas de seguridad se orientan las decisiones que se toman y deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

- Objetivos de la política y descripción de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para la configuración de la seguridad de los sistemas involucrados en el alcance de la política.

- Definición de violaciones y de las consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que tienen acceso.

Las políticas de seguridad informática establecen las expectativas de la organización en relación con la seguridad y deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, las políticas deben especificar a la autoridad qué debe hacerse para que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Finalmente, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, entre otros.

Si bien las características descritas hasta el momento nos muestran una perspectiva de las implicaciones en la creación de estas directrices, cabe destacar algunos aspectos generales recomendados para la formulación de las mismas:

- Efectuar un ejercicio de análisis de riesgos informáticos, a través del cual valore sus activos y permita afinar sus políticas.

- Involucrar a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer las políticas.

- Comunicar a todo el personal los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Desarrollar un proceso de monitoreo periódico de las directrices, que permita una actualización oportuna de las mismas.

A manera de ejemplo, se propone una forma de realizar las políticas de seguridad informática para llevar a cabo un sistema de seguridad. Tomando para ello como base el diagrama presentado en la figura 2.1.

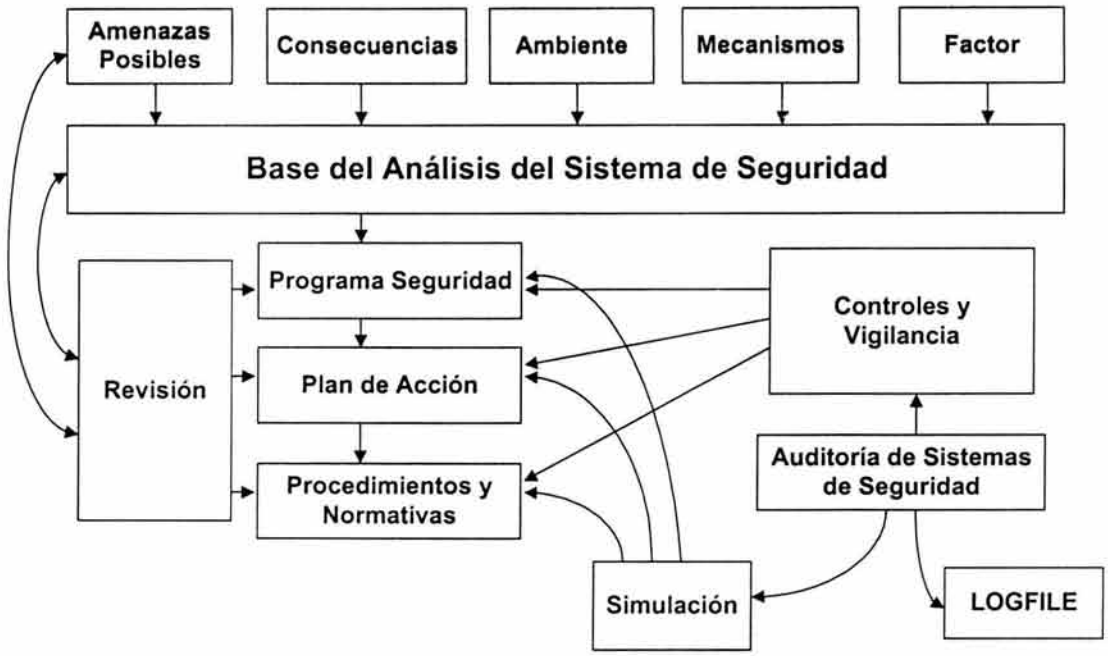

Figura 2.1. Diagrama para el análisis de un sistema de seguridad.

Se comienza realizando una evaluación del factor humano involucrado, teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad, así como de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos); luego, el medio ambiente en que se desempeña el sistema, las consecuencias que pueden generar defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las amenazas posibles.

Una vez evaluado todo lo anterior, se origina un programa de seguridad, que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.

Con el propósito de asegurar el cumplimiento de todo lo anterior, se realizan los controles y la vigilancia que aseguran el fiel cumplimiento de los puntos anteriores.

Para asegurar un marco efectivo, se realizan auditorías a los controles y a los archivos logísticos que se generen en los procesos implementados.

Para confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad del sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción, y a los procedimientos y normas. Estas revisiones, tendrán efecto sobre los puntos tratados y, de esta manera, el proceso se vuelve a repetir.

Es claro que el establecimiento de políticas de seguridad informática es un proceso dinámico sobre el que hay que estar actuando permanentemente, de tal manera que no quede desactualizado; y que cuando se descubran debilidades, éstas sean subsanadas y, finalmente, que su práctica por los integrantes de la organización no caiga en desuso.

Dentro de las políticas de seguridad informáticas se encuentran aspectos que forman parte de la seguridad a nivel de sistema y a nivel de red.

La seguridad a nivel de sistema incluye aspectos de configuración de los equipos, centrándose sobre todo en aquellos equipos multiusuario (equipos de correo, servidores de archivos, etc).

La seguridad a nivel de red trata sobre las medidas para evitar los ataques desde el exterior de una organización, y el desarrollo de filtros que se deberían instalar en los ruteadores externos de las mismas para evitar diversos ataques típicos que se producen.

En el desarrollo del presente trabajo, debido a necesidades de la compañía, nos dedicaremos a elaborar una solución en el nivel de red.

2.3. SEGURIDAD A NIVEL DE RED

Los ataques a nivel de red siguen siendo muy frecuentes. Aunque las capas TCP/IP de los distintos sistemas operativos son cada vez más robustas, todavía son frecuentes los ataques de denegación de servicio en servidores NT y Unix, debidos al empleo de generadores de datagramas IP erróneos o complicados de procesar. Al mismo tiempo, las tecnologías de seguridad adquieren una importancia vital, para prevenir la corrupción de datos y la intrusión y para eliminar las vulnerabilidades de los sistemas.

Es también frecuente el empleo de herramientas automatizadas de barrido y comprobación de vulnerabilidades en redes, así como la utilización de programas específicos que explotan una determinada vulnerabilidad de un servidor o servicio concreto para atacarlo.

En esta sección vamos a tratar sobre todo las medidas que creemos que se deben establecer en las organizaciones mediante el filtrado de diversos protocolos en los ruteadores de acceso, para así evitar el acceso desde fuera a estos servicios. Estas medidas no serán efectivas contra ataques internos, salvo que se apliquen medidas internas concretas en aquellas organizaciones que tienen un direccionamiento plano de red, el cual se refiere a un esquema de direccionamiento que no utiliza una jerarquía lógica para determinar una ubicación, permitiendo como mínimo reducir ciertos problemas como el SPAM (correo electrónico basura) o los ataques contra servicios bien conocidos como NFS (Network File System, Sistema de Archivos de Red), NetBios, etc. Además permitirán que incluso si los usuarios finales activan esos servicios en sus máquinas, estos no serán accesibles desde el exterior, evitando así múltiples problemas.

2.3.1. Filtrado de paquetes

Aunque la seguridad a nivel de sistema sigue teniendo una importancia vital, los fallos en varios servicios TCP/IP y la existencia de protocolos defectuosos hace imprescindible el uso de filtros a nivel de red, que permitan a una organización restringir el acceso externo a estos servicios. De esta forma, sólo aquellos servicios que deban estar accesibles desde fuera del área local serán permitidos a través de filtros en los ruteadores. Además es importante que estos filtros determinen las condiciones de acceso a los servicios permitidos. En particular, se recomienda que se filtren los servicios mostrados en la tabla 2.1, si no es necesario su acceso desde fuera de una organización. Estos consejos ayudarán a las organizaciones a implementar sus propios filtros en función a sus necesidades y topología de red concreta.

Nombre	Puerto	Tipo de conexión	Servicio
Echo	7	TCP/UDP	Eco: Devuelve los datos que se reciben
Systat	11	TCP	Información del sistema
Netstat	15	TCP	Información sobre la red
Chargen	19	TCP/UDP	Prueba la máquina
SMTP	25	TCP	Puerto de correo
Domain	53	TCP/UDP	Servidor de Nombres (DNS)
Bootp	67	UDP	Arranque de estaciones remotas sin disco
TFTP	69	UDP	Arranque de equipos remotos, carga de configuraciones
Link	87	UDP	Implementa servicio de datagrama
News	119	TCP	Servidores de News
Netbios	137-139	UDP/TCP	Servicios NetBios sobre TCP/IP (Windows)
SNMP	161	UDP	Gestión remota de equipos mediante SNMP
Xdmpc	177	UDP	Llegada de correo
Exec	512	TCP	Ejecución remota de comandos (rexec)
Login	513	TCP	Acceso remoto a un sistema (rlogin)
SHELL	514	TCP	Ejecución remota de ordenes a una máquina
Biff	512	UDP	Servicio de notificación de nuevo correo electrónico
Who	513	UDP	Información sobre los usuarios que hay conectados en un equipo remoto
Syslog	514	UDP	Almacenamiento de las bitácoras de los sistemas remotos
UUCP	540	TCP	Envío de archivos y mensajes mediante UUCP (Unix to Unix Copy Protocol), actualmente en desuso
Route	520	UDP	Información sobre enrutamientos
NFS	2049	TCP/UDP	Sistema de archivos remotos de Sun y Unix en general
x-windows	6000 + n	TCP	Servidor X-Windows

Tabla 2.1. Descripción de servicios y tipo de conexión.

De los servicios a proteger que se mencionan anteriormente, se describen los servicios más comunes: echo, charger, SMTP, domain, TFTP, sunrpc, NFS, netbios, SNMPs, biff, who y syslog.

- **Echo y chargen: Puertos 7 y 19 (TCP/UDP).** Es muy importante para evitar ataques de denegación de servicio por puertos UDP, filtrar a nivel de ruteador o *firewall* los servicios *chargen* y *echo* y en general todos los servicios UDP que operen por debajo del puerto 900, con excepción de aquellos que se necesiten explícitamente.

- **SMTP: Puerto 25 (TCP).** Es importante configurar el ruteador de manera que todas las conexiones SMTP procedentes de fuera de una organización pasen a una zona central desde donde se distribuya el correo internamente. Este tipo de filtros permitirá que no existan puertos 25 descontrolados dentro de una organización, ya que suelen ser foco de importantes problemas de seguridad, además de un registro centralizado de información, que podrá ayudar a la hora de detectar el origen de intentos de ataque. El administrador del sistema o el responsable de seguridad sólo se tendrá que preocupar de tener actualizado este servidor para evitar ataques aprovechando vulnerabilidades o fallos bien conocidos en los mismos.

- **Domian (DNS): Puerto 53 (TCP/UDP).** Es necesario filtrar el acceso desde el exterior a todos los equipos. Un servidor DNS se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando éste está bien configurado.

- **TFTP: Puerto 69 (UDP).** En general cualquier servicio UDP que responde a un paquete de entrada puede ser víctima de un ataque de denegación de servicio (DoS). Un acceso no restringido al servicio TFTP permite a sitios remotos recuperar una copia de cualquier archivo, entre los que se pueden incluir archivos críticos como archivos de configuración de ruteadores y archivos de claves. Es por ello que aquellas organizaciones que no necesiten usar este servicio deberían filtrarlo, y aquellas que necesiten usarlo lo configuren adecuadamente, teniendo en cuenta las medidas de seguridad a nivel de aplicación.

- **Sunrpc y NFS: Puertos 111 y 2049 (TCP/UDP).** Filtrar el trafico NFS evitará que sitios ajenos a la organización accedan a sistemas de archivos exportados por máquinas de la red corporativa, pero como ocurría en el caso anterior, no se evitará que se realicen ataques desde dentro del área local. La mayoría de las implementaciones NFS emplean el protocolo UDP, por lo que es posible, en algunos casos, el envío de peticiones NFS falsificando la dirección origen de los paquetes (*IP-spoofing*). Es por tanto muy aconsejable la instalación de las versiones actualizadas de los servidores y clientes NFS que tienen estas características.

- **NetBios: Puertos 137, 138 y 139 (TCP/UDP).** Estos puertos son los empleados en las redes Microsoft (Windows para Trabajo en Grupo, dominios NT y LAN

Manager), tanto para la autenticación de usuarios como para el uso compartido de recursos (impresoras y discos). Es frecuente el permitir el acceso global a uno de estos dispositivos, ignorando que es posible el acceso a estos recursos desde cualquier dirección de Internet.

- **SNMP: Puerto 161 (UDP/TCP).** Muchos equipos disponen en la actualidad de gestión SNMP incorporada. Dado que estas facilidades de gestión no suelen necesitar accesos externos, se deben establecer filtros a nivel de ruteador que eviten que se pueda obtener información sobre los dispositivos (ruteadores, concentradores, *switches*) desde el exterior o incluso se gestionen los equipos en remoto.

- **Biff, who, syslog: Puertos 512, 513 y 514 (UDP).** Estos comandos incrementan el peligro de que sean interceptados contraseñas en texto plano cuando se presenta un ataque utilizando rastreadores o *sniffers* de red, pero lo más importante es que son una fuente bastante frecuente de ataques y vulnerabilidades. Filtrando los puertos 512, 513 y 514 (TCP) en el *hardware* de red se evitará que personas ajenas a la organización puedan explotar estos comandos, pero no lo evitará a personas de la propia organización.

Para prevenir ataques basados en "bombas" ICMP (que consiste en mandar mensajes ICMP muy rápidamente a la víctima, causándole retrasos del módem, causará tanto retraso que el servidor de IRC (Intenet Relay Chat, Charla o Conferencia en Internet) desconectará al usuario por pensar que ya no está en el IRC), se deben filtrar los paquetes de redirección ICMP y los paquetes de destino ICMP inalcanzables. Además, y dado que actualmente el campo de opciones de los paquetes IP apenas se utiliza, se pueden filtrar en la totalidad de las redes los paquetes de origen enrutado (*source routed packets*). Estos paquetes indican el camino de vuelta que ha de seguir el paquete, lo cual es algo inseguro, ya que alguno de los puntos intermedios por los que pase el paquete pueden estar comprometidos.

Con el protocolo IP que actualmente está mayoritariamente en uso, es casi imposible eliminar el problema del *IP-spoofing* (falsificación de la IP). Sin embargo, se pueden tomar algunas medidas que reducirán el número de paquetes de este tipo que entran y existen en una red local. Actualmente, el mejor modo de realizar esto es restringir la entrada en la interfaz externa (filtro de entrada), no permitiendo que un paquete entre a nuestra red si tiene la dirección origen de la red interna. De la misma forma, se deberán filtrar los paquetes salientes que tengan una dirección origen distinta a la correspondiente a la red interna. La combinación de estos dos filtros prevendrá que un atacante de fuera de nuestra red envíe paquetes simulando hacerlo desde dentro de nuestra red, así como que paquetes generados dentro de nuestra red parezcan haber sido generados fuera de la misma.

En la entrada a la interfaz interna de una red se deben filtrar los bloques de paquetes con las siguientes direcciones:

- Pertenecientes a la red interna.

- Números de red privada reservados: No se debe recibir tráfico desde o hacia las siguientes direcciones, a través de los ruteadores, puesto que se trata de redes privadas reservadas:

  * 10.0.0.0 - 10.255.255.255 10/8 (reservada).
  * 127.0.0.0 - 127.255.255.255 127/8 (*loopback* o bucle).
  * 172.16.0.0 - 172.31.255.255 172.16/12 (reservada).
  * 192.168.0.0 - 192.168.255.255 192.168/16 (reservada).

Otras medidas convenientes que se pueden realizar son: configuración de capas TCP/IP, monitoreo de ruteadores y equipos de acceso y separación de las redes.

2.3.2. Configuración de las capas TCP/IP en equipos finales

Gran parte de los ataques de denegación de servicio (DoS) se producen debido a fallos en las implantaciones de las capas TCP/IP en los sistemas operativos. Así, son famosos los ataques de denegación de servicio mediante el envío de datagramas IP con información ICMP errónea, que provocan el reinicio del equipo o impidiendo el normal funcionamiento de los servidores. En la medida de lo posible, se debe revisar la configuración de estos sistemas, en especial la configuración de "reenvío de datagramas IP" (*IP-forwarding*), que permite que un sistema funcione como un ruteador.

2.3.3. Monitoreo de ruteadores y equipos de acceso

Los ruteadores de interconexión y cualquier dispositivo (*switch*, concentrador ATM, etc.), deben estar monitoreados. Las bitácoras deben configurarse para ir enviando los mensajes de la consola a un equipo central, donde se deben almacenar durante un periodo razonable de tiempo, de forma que se puedan comprobar los intentos de conexión no autorizados y las caídas que se producen en estos equipos.

En instalaciones con mucho equipamiento de red puede ser recomendable el empleo de alguna herramienta de monitoreo SNMP de los equipos, de forma que las incidencias que vayan ocurriendo sean notificadas en tiempo real a los administradores de la red.

2.3.4. Separación de las redes

Los equipos de acceso general (bibliotecas, salas de prácticas comunes, aulas de estudiantes, etc.) deben estar separados mediante puentes o *switches* del resto de la red, para evitar que se puedan obtener, mediante *sniffers*, claves de acceso de otros grupos de usuarios. En general, los equipos que necesiten el empleo de sistemas inseguros de transmisión de claves deberían estar aislados de la red, de forma que estas claves no se transmitan por toda la red.

Debemos considerar, además, las posibilidades de gestión y consola remota que disponen muchos concentradores y *switches*: hay que cambiar las claves por defecto que suelen tener estos equipos y deshabilitar la gestión remota de estos si no se va a hacer uso de ella (SNMP, consolas remotas, servidor de HTTP, etc.).

Además de realizar el filtrado de paquetes en una red, es necesario conocer las amenazas existentes para mejorar la eficacia de un sistema de seguridad.

2.4. AMENAZAS EXISTENTES EN UNA RED TCP/IP

Cabe definir amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático: la prevención, la detección y la recuperación.

- *Prevención.* Mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo, el cifrado de información para su posterior transmisión.

- *Detección.* Mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

- *Recuperación.* Mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo, recuperación desde las copias de seguridad (respaldo) realizadas.

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa.

Cada riesgo, ya sea que se trate de actos naturales, errores u omisiones humanas y actos intencionales, debería ser atacado de las siguientes maneras:

- Minimizando la posibilidad de su ocurrencia.
- Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
- Diseño de métodos para la más rápida recuperación de los daños experimentados.
- Corrección de las medidas de seguridad en función de la experiencia recogida.

Una de las amenazas que los sistemas de seguridad deben evitar son los intrusos o atacantes: personas que acceden (o intentan acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

Los tipos de intrusos podríamos clasificarlos desde el punto de vista del nivel de conocimiento, como: Clase A, Clase B, Clase C y Clase D.

- *Clase A.* El 80% de los nuevos intrusos son los que bajan programas de Internet y hacen pruebas.

- *Clase B.* El 12% son más peligrosos, ya que saben compilar programas aunque no saben programar. Prueban programas, conocen cómo detectar qué sistema operativo está usando la víctima, prueban las vulnerabilidades del mismo e ingresan por ellas.

- *Clase C.* El 5% de gente que sabe, conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

- *Clase D.* El 3% restante, cuando entran a determinados sistemas buscan la información que necesitan.

La identificación de amenazas requiere conocer los tipos de ataques. Existen diferentes tipos de ataques perpetrados, principalmente por *hackers*. Estos ataques pueden ser realizados sobre cualquier tipo de red o sistema operativo, usando diferentes protocolos y herramientas.

2.4.1. Tipos de ataques

Desde 1990 hasta nuestros días, el CERT (Computer Emergency Response Team, Equipo de Emergencia del Internet) ha venido desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

Anteriormente, los ataques involucraban poca técnica. Los operadores o programadores utilizaban sus permisos para alterar archivos o registros. Éstos ingresaban a la red simplemente averiguando una contraseña válida. A través de los años se han desarrollado formas cada vez más avanzadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Existen multitud de ataques, pero pueden ser clasificados en dos grandes grupos: ataques pasivos y ataques activos.

Ataques pasivos

El atacante no altera la comunicación, sino que únicamente la "escucha" o monitorea, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:

- Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitoreados.

- Control del volumen de tráfico intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por *hackers*, piratas informáticos o intrusos remunerados y se les puede subdividir en cuatro categorías:

- *Interrupción:* si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- *Intercepción:* si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- *Modificación:* si además de conseguir el acceso consigue modificar el objeto.
- *Fabricación:* se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
- *Destrucción:* es una modificación que inutiliza el objeto.

Debemos recordar que el concepto de seguridad es relativo, sin embargo existen niveles de seguridad mínimos exigibles. Este nivel dependerá de un análisis de los riesgos que estamos dispuestos a aceptar, sus costos y de las medidas a tomar en cada caso.

Para ejemplificar, veamos los datos obtenidos en marzo de 2001 por la consultora Ernst & Young sobre 273 empresas de distintos sectores de actividad y países.

- El 40% de las empresas estudiadas consideran como un problema grave la seguridad informática.
- El "gasto" en Seguridad Informática oscila entre el 4% y el 10% del gasto total informático.
- El 83% de las empresas reconoce no haber emprendido nunca acciones legales después de un ataque.
- El 72% se muestra reacia a admitir que sus sistemas han sido saboteados.
- El 79% cree que existen mayores probabilidades de sufrir un ataque informático procedente del exterior.
- El 66% consideran a la seguridad y privacidad de la información el impedimento principal para el crecimiento del comercio electrónico.
- El 80% manifestó no haber experimentado un ataque por intrusión durante el año anterior; pero sólo el 33% indicó su capacidad para la detección de dichos ataques.
- Sólo el 39% hace uso de *software* estándar de seguridad y el 20% de este total hace uso avanzado de estas herramientas.

En la figura 2.2 se detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

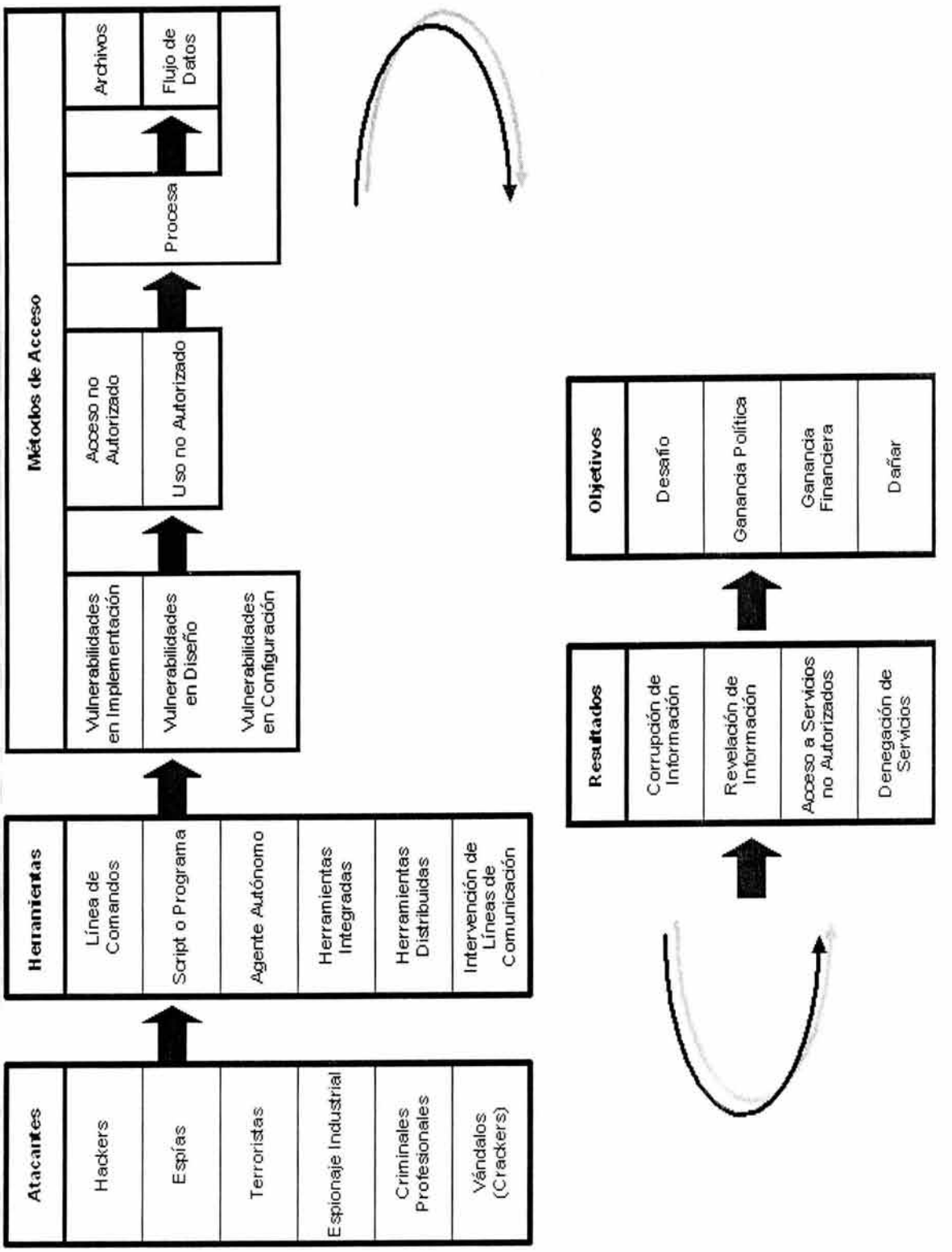

Figura 2.2.Detalle de ataques.

Los tipos de ataques mencionados anteriormente se pueden clasificar a su vez en: ataques de monitoreo, de autentificación y denegación de servicio.

Ataques de monitoreo

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

Ataque de señuelo

Los señuelos son programas diseñados con la misma interfaz que otro original. En ellos se imita la solicitud de un acceso y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas".

Una técnica semejante es aquella en la cual, mediante un programa, se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

Ataques de búsqueda

El barrido (*scanning*), como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular.

Explorar puertos implica usar las técnicas de fuerza bruta, la cual consiste en una técnica usada en *hacking* y *cracking,* que necesita mucho esfuerzo y mucho tiempo de proceso o de intentos. Por lo que, puede tratarse de probar infinidad de contraseñas hasta encontrar la correcta, para lo cual se utilizan programas que prueban automáticamente todas las combinaciones o con las almacenadas en un diccionario de contraseñas. Para ello envía una serie de paquetes para varios protocolos y se deduce que servicios están "escuchando" por las respuestas recibidas o no recibidas.

Ataque de husmeo de paquetes

Un husmeador, también conocido como *sniffer,* consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el *sniffer*).

Inicialmente este tipo de *software*, de husmeo de paquetes, era únicamente utilizado por los administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Normalmente los buenos husmeadores no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, sí pueden ser detectados con algunos trucos.

Ataques de curiosos

Los ataques de esta categoría (*snooping*) tienen el mismo objetivo que el husmeador, obtener la información sin modificarla. Sin embargo, los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos una copia de documentos de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

Ataques de autentificación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña.

Ataque por falsificación

Con estos ataques, conocidos también como *spoofing*, se puede conseguir el nombre y contraseña de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él. En este caso también es posible la eliminación de la identificación y la ubicación del atacante. Para conocer su ubicación, el investigador debe contar con la colaboración del administrador de cada red utilizada en la ruta.

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo *spoofing* más conocidos son la falsificación de IP, DNS y de Web.

- *Falsificación de IP.* El atacante genera paquetes de Internet con una dirección de red falsa en el campo *From*, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso.
- *Falsificación de DNS.* Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el DNS.
- *Falsificación de Web.* El atacante crea un sitio Web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las contraseñas, números de tarjeta de créditos, etc. El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

Ataque de IP hijacking

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

Ataque de puertas traseras

Es también conocido como *backdoor*. A pesar de que no se consideran propiamente como virus, representan un riesgo de seguridad importante, y usualmente son desconocidos los problemas que éstas puedan llegar a causar. Al hablar de este tipo de ataque nos referimos genéricamente a una forma "no oficial" de acceso a un sistema o a un programa.

Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo, en otras ocasiones existen debido a fallos o errores.

Estos programas usualmente son enviados con el fin de tener acceso a nuestros equipos a través del correo electrónico, por lo que no son fáciles de detectar y por si solos no siempre causan daños ni efectos inmediatos, por lo que pueden llegar a permanecer activos mucho tiempo sin que nos percatemos de ello. Generalmente estos programas se hacen pasar por otros, es decir, se ocultan en otro programa que les sirve de caballo de troya para que el usuario los instale por error. Son utilerías de administración remota de una red y permiten controlar las computadoras conectadas a ésta. El hecho que se les clasifique como *software* malévolo en algunos casos, es que cuando corren, se instalan en el sistema sin necesidad de la intervención del usuario y una vez instalados, en la mayoría de los casos, no se pueden visualizar estas aplicaciones en la lista de tareas. Consecuentemente las puertas traseras pueden supervisar casi todo proceso en las computadoras afectadas, desinstalar programas, descargar virus en la PC remota, borrar información, entre otras muchas cosas más.

Ataque de utilización de exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte de la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de *exploits* y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (*hardware* o *software*) para ingresar al mismo.

Ataque de obtención de contraseñas

Este método comprende la obtención por "fuerza bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados.

Muchas contraseñas de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, ésta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la contraseña correcta.

Ataque de denegación de servicio

Los ataques de denegación de servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP. El sistema responde al mensaje, pero como no recibe respuesta, acumula *buffers* con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones disponibles que pueden manejar en un momento determinado. Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando.

A parte de los ataques clasificados anteriormente, existen otro tipo de amenazas catalogados como virus.

2.4.2. Virus

Los virus informáticos o electrónicos o computacionales son segmentos de código ejecutable escrito en lenguaje ensamblador o lenguaje de macro, capaz de tomar el control de la máquina o aplicación en algún momento y auto replicarse, alojándose en un soporte diferente al que se encontraba originalmente y provocar anomalías en las computadoras al desarrollar su función destructora. Ningún programa de virus puede funcionar por si sólo, requiere de otros programas para poderlos corromper. Se les ha dado el nombre de virus por la analogía que tiene su comportamiento con el de los virus biológicos.

Ciclo de vida

Los virus informáticos tienen un ciclo de vida, que empieza cuando son creados y termina cuando son erradicados completamente. Las etapas de este ciclo son: creación, gestación, reproducción, activación, descubrimiento, asimilación y eliminación.

- *Creación.* En el pasado, crear un virus requería del conocimiento del lenguaje de programación ensamblador. Hoy en día, cualquiera con un poco de conocimiento en programación puede crear un virus. Generalmente, los creadores de los virus, son personas maliciosas que desean causar daño a las computadoras.

- *Gestación.* Luego de que el virus es creado, el programador hace copias asegurándose de que se diseminen. Generalmente esto se logra infectando un programa popular y luego enviándolo a algún BBS (Bulletin Board System, Sistema de Mensajería Electrónica) o distribuyendo copias en oficinas, escuelas u otras organizaciones.

- *Reproducción.* Los virus se reproducen naturalmente, es decir, un virus bien diseñado se reproducirá por un largo tiempo antes de activarse, lo cual permite que se disemine por todos lados.

- *Activación.* Los virus que contienen rutinas dañinas, se activarán bajo ciertas condiciones, por ejemplo, en determinada fecha o cuando el usuario haga algo determinado. Los virus sin rutina dañina no se activan, pero causan daño al robar espacio en el disco.

- *Descubrimiento.* Cuando se detecta y se aísla un virus, se envía a la Asociación Internacional de Seguridad en Washington D.C, para ser documentado y distribuido a los encargados de desarrollar los productos antivirus.

- *Asimilación.* En este punto, quienes desarrollan los productos antivirus, modifican su programa para que éste pueda detectar los nuevos virus. Esto puede tomar de un día a seis meses, dependiendo de quien lo desarrolle y el tipo de virus.

- *Eliminación.* Si suficiente cantidad de usuarios instalan una protección antivirus actualizada, se puede eliminar cualquier virus. Hasta ahora, ningún virus ha desaparecido completamente, pero algunos han dejado de ser una amenaza.

Para evitar la intervención del usuario, los creadores de virus debieron inventar técnicas, por lo tanto, surgieron varios tipos de virus.

Tipos de virus

Existen múltiples clasificaciones dada la cantidad de virus existentes, algunos de los criterios bajo los cuales se pueden clasificar son: respecto al medio y las técnicas de infección.

Respecto al medio, se dividen en cuatro clases: de archivo, de *boot*, virus macro y virus de enlace o de directorio.

Medios de infección

- *Virus de archivo.* Este virus se encarga de infectar programas ejecutables (archivos con extensiones *.exe, *.com,*.dvr, *.dll, *.bin, *.gvl, *.sys) y mediante la ejecución de manera directa o indirecta, el virus se activa produciendo los efectos dañinos que le caractericen en cada caso. Se pueden reproducir por diferentes técnicas infectando el archivo al principio o al final. La mayoría de los virus

existentes son de este tipo, y los podemos clasificar de acuerdo a su modo de actuación; pueden permanecer residentes en memoria durante mucho tiempo después de haber sido activados (virus residentes), o actuar contra el sistema sólo al ser ejecutado el programa infectado (virus de acción directa), algunos no respetan la información del archivo sobre el que se encuentran y la destruyen totalmente dejándolos inservibles (virus de sobrescritura).

- *Virus de boot.* Usualmente atacan sólo disquetes, CD-ROMs, unidades Zip, etc. Estos se instalan en el sector de arranque del disco duro o disquete, y se cargan en memoria RAM aún antes que los archivos de sistemas, así toman el control total de las IRQs (Interruption Request, Petición de Interrupción), para ocultarse, diseminarse y provocar daños. Por lo general reemplazan el contenido del sector de arranque con su propio contenido y desplazan el sector original a otra área del disco.

- *Virus de macro.* Es una familia de virus de reciente aparición y gran expansión. Estos están programados usando el lenguaje de macros WordBasic, gracias al cual pueden infectar y replicarse a través de archivos Ms-Word. En la actualidad esta técnica se ha extendido a otras aplicaciones como Excel y a otros lenguajes de macros. Se ha de destacar, de este tipo de virus, que son multiplataformas en cuanto a sistemas operativos, ya que dependen únicamente de la aplicación. De acuerdo con la Asociación Internacional de Seguridad, los virus macro forman el 80% de todos los virus y son los que más rápidamente han crecido en toda la historia de las computadoras. A diferencia de otros tipos de virus, los virus macro no son exclusivos de ningún sistema operativo y se diseminan fácilmente a través de archivos adjuntos de *e-mail*, disquettes, descargas de Internet, transferencia de archivos y aplicaciones compartidas.

- *Virus de enlace o de directorio.* Se encargan de alterar las direcciones, nombre y lugar en el que se encuentran guardados los archivos. En el momento en que se quieren utilizar guarda en otro lugar la dirección correcta y apunta hacia a él la dirección modificada. Este tipo de virus tiene una alta probabilidad de infectar todo el sistema.

Técnicas de infección

Cada uno de los miles de virus existentes utiliza diferentes mecanismos, tanto para realizar la infección como para ocultarse y pasar desapercibido. Estas técnicas evolucionan con el tiempo, al igual que las técnicas utilizadas por los programas antivirus para detectarlos. Los mecanismos utilizados por los virus son: ocultamiento, evasión, autoencriptación, polimorfismo, protección antivirus, etc.

- *Ocultamiento (Stealth).* Los virus que utilizan esta técnica intentan pasar desapercibidos ante los ojos del usuario, no levantan ninguna sospecha sobre la infección que ya han efectuado; los virus residentes son los que más la utilizan, aunque no es exclusiva de este tipo de virus. Cuando un virus infecta un determinado archivo, normalmente deja signos evidentes de su presencia como: aumento de tamaño en el archivo infectado, modificación de la fecha y hora de

creación en el archivo infectado, secciones marcadas como defectuosas, disminución de la capacidad en la memoria, etc. En este caso el virus se encargará de que cada una de estas pistas no puedan ser visualizadas.

- *Evasión (Tunneling).* Se trata de una técnica especialmente diseñada para imposibilitar la protección antivirus en cualquier momento. Mientras el análisis permanente, o residente, del programa antivirus que se encuentre instalado intenta realizar detecciones, el virus actúa en su contra. Todas las operaciones que se realizan sobre cualquiera de los archivos son inspeccionadas por el antivirus mediante la interceptación de las acciones que el sistema operativo lleva a cabo para hacerlas posible; al mismo tiempo, el virus interceptará estas peticiones o servicios del sistema operativo, obteniendo las direcciones de memoria en las que se encuentran. Así el antivirus no detectará la presencia del virus. Sin embargo, existen técnicas antivirus alternativas que permiten la detección de virus que realicen este tipo de operaciones.

- *Autoencriptación.* Los programas antivirus se encargan de buscar determinadas cadenas de caracteres (lo que se denomina la firma del virus) propias de cada uno de los posibles virus; estos, por su parte y mediante la técnica de autoencriptación, infectarán de forma diferente en cada ocasión. Esto significa que el virus utilizará una cadena concreta para realizar una infección, mientras que en la siguiente infección utilizará otra distinta. Por otro lado, el virus codifica o cifra sus cadenas para que al antivirus le sea difícil encontrarlo. Sin embargo, los virus que utilizan este tipo de técnicas, emplean siempre la misma rutina o algoritmo de encriptación, con lo que es posible su detección.

- *Polimorfismo.* Basándose en la técnica de autoencriptación, el virus se codifica o cifra de manera diferente en cada infección que realiza (su firma variará de una infección a otra) y adicionalmente el virus cifrará también el modo (rutina o algoritmo) mediante el cual realiza el cifrado de su firma. Todo esto hace posible que el virus cree ejemplares de sí mismo diferentes de una infección a la siguiente, cambiando de "forma" en cada una de ellas.

- *Protección antivirus (Armouring).* Mediante esta técnica el virus impide que se examinen los archivos que él mismo ha infectado. Para conocer más datos sobre cada uno de ellos, éstos deben ser abiertos (para su estudio) como archivos que son, utilizando programas especiales (*Debuger*) que permiten descubrir cada una de las líneas del código (lenguaje de programación en el que están escritos). En un virus que utilice la técnica de *Armouring* no se podrá leer el código.

Otro tipo de clasificación

- *Virus puro.* Tiene la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor cuidado posible y de forma transparente al usuario; a este proceso de autoréplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la

medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea archivo, sector de arranque, partición, etc. Un virus puro también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma transparente al usuario.

- *Caballo de troya.* Es un virus muy común el cual llega a la PC en forma de programa utilitario, o sea un supuesto programa para solucionar algún inconveniente y que en realidad es un virus que se activa al ejecutar el programa en cuestión. Otro tipo de Troyanos de gran evolución y técnica refinada son el *Netbus* y el *Subseven* que permiten que el virus tome total control de la PC y monitoree paso a paso lo que el usuario haga en la misma. Incluso tomar todas y cada una de sus claves y contactos para enviarlas vía Internet al creador del virus o a quien lo ha remitido. Este tipo de virus bien pueden ser llamado programa, ya que utilizan un modulo de ejecución refinado. Al contrario que el virus puro, un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este último. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

- *Bomba lógica.* Se trata de un programa maligno que permanece oculto en memoria y que sólo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto, cuando se ejecuta cierto programa o cierta combinación de teclas.

- *Gusano o Worm.* Es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la memoria RAM.

La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas.

Daños causados

Se define daño como una acción indeseada, y se clasifican según la cantidad de tiempo necesaria para reparar dichos daños. Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad: triviales, menores, moderados, mayores, severos e ilimitados.

- *Daños triviales.* La forma de trabajo del virus *Form*, por ejemplo en el día 18 de cada mes, cualquier tecla que presionemos hace sonar un *beep*. Deshacerse del virus implica, generalmente, segundos o minutos.

- *Daños menores.* Este virus borra todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente.

- *Daños moderados.* Cuando un virus formatea el disco duro, mezcla los componentes de la FAT (File Allocation Table, Tabla de Ubicación de Archivos), o sobrescribe el disco duro.

- *Daños mayores.* Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un respaldo se vuelva al último estado de los datos.

- *Daños severos.* Es cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado.

- *Daños ilimitados.* Crea un nuevo usuario con los privilegios máximos, fijando el nombre y la clave. El daño es entonces realizado por una tercera persona, quien ingresa al sistema y hace lo que quiere.

Una vez expuestos los elementos descritos en este capítulo, procedemos al análisis de la red corporativa.

CAPÍTULO 3

ANÁLISIS DE LA RED CORPORATIVA

En este capítulo describiremos la metodología empleada para conocer el estado actual de la red corporativa, dando un panorama general de las vulnerabilidades existentes dentro de esta red, además de mencionar su problemática y proporcionar recomendaciones de solución.

3.1. DEFINICIÓN DEL PROBLEMA

La extensión de las redes en el ámbito mundial, que interconectan recursos informáticos de todo tipo, ha hecho que los peligros que sufre la información almacenada en los diversos sistemas crezcan considerablemente y se diversifiquen, y que las medidas adoptadas internamente en las empresas resulten insuficientes.

En los últimos años no sólo la prensa especializada en informática, sino todos los medios de difusión, han hecho eco del futuro de las autopistas de la información, cuya principal representante es la red Internet. A raíz de la interconexión del mundo empresarial a esta red, viaja por ella y se almacena información de todo tipo, que abarca desde noticias, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren medidas de seguridad que garanticen la confidencialidad, la integridad y el origen de los datos.

La obtención y posible manipulación de información privada, y los sabotajes realizados tanto por atacantes externos como internos, están causando últimamente la pérdida de grandes cantidades de dinero.

Internet nace como una serie de redes que promueven el intercambio de información entre investigadores que colaboran en proyectos conjuntos o comparten resultados usando los recursos de la red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Era totalmente inapropiado usarla para el envío de documentos sensibles o clasificados que pudieran manejar los usuarios. Situación muy común, pues hay que recordar que Internet nace de un proyecto del Departamento de Defensa Americano en el año de 1968, para conectar entre sí tanto las Universidades como los Centros de Investigación que colaboran de una manera u otra con las Fuerzas Armadas Norteamericanas.

Los protocolos de Internet fueron diseñados de una forma deliberada para que fueran simples y sencillos. Llego un momento en que fue necesaria su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser necesarios.

En la actualidad se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, la cooperación altruista, la práctica política o, simplemente el juego. En medio de esta variedad de usos han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas.

También existen varias herramientas que un usuario de Internet puede utilizar para perpetrar en algún sistema o darse cuenta de qué vulnerabilidades existen en algún equipo dentro de nuestra red, incluso tiene la posibilidad de lanzar un ataque a los servicios o robar una contraseña, con algún programa que le permita adivinarlo.

La red corporativa de datos y servicios permite el uso de correo electrónico, servidor de páginas Web, servidor de archivos, servidor de dominios y servidores de FTP, por mencionar los más importantes. Al encontrarse esos servicios disponibles dentro de la red pública, nos exponemos a ataques o intrusiones a nuestros servidores que pueden llegar a perjudicar la disponibilidad de los servicios.

El número creciente y la gravedad de estas amenazas requieren de revalorar la importancia de la vigilancia y de un plan de seguridad de la red para bloquear tales ataques con inteligencia. Además, es importante recalcar que una componente significativa para la protección de los sistemas es el administrador de la red corporativa, porque es considerado responsable de su seguridad, por tanto, debe contar con una serie de procedimientos para poder realizar un seguimiento de las actividades de quienes emplean la red, el equipo de cómputo y la información existente en ella.

El valor de la información que se genera en la red corporativa es considerado crucial. Si los sistemas no se encuentran disponibles entonces su costo se convierte en pérdidas financieras, como pueden ser:

- Costos económicos (perder oportunidades de negocio).
- Costos de recuperación.
- Costos de reparación.
- Costos de tiempo.
- Costos legales y judiciales.
- Costos de imagen.
- Costos de confianza de clientes.

Por tales motivos, se busca que la red corporativa cuente con un sistema de seguridad, implementado de tal manera que nos aporte, con mayor eficiencia, los siguientes aspectos:

- Alta disponibilidad en los servicios.
- Menor riesgo de pérdida de información.
- Disminución del riesgo de intrusión.
- Mejor control de los servicios en red.

Dentro de los puntos mencionados, el aspecto de una alta disponibilidad en los servicios es considerado por el corporativo como un elemento crucial, a tomar en cuenta durante el proceso de una propuesta de solución a sus problemas de seguridad.

Para lograr cumplir con los puntos anteriores, es preciso considerar el uso de una metodología para la elaboración de un sistema de seguridad.

3.2. METODOLOGÍA PROPUESTA PARA EL ANÁLISIS

Para nuestra red en particular, y para tener una mejor atención y vigilancia continua, es necesario contar con un conocimiento detallado del estado actual y funcionamiento de la red corporativa; con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad. Para tal efecto se considera adecuada la realización de una auditoría de seguridad.

Una vez conocido el estado actual de la red corporativa, se podrá efectuar un análisis de la información a fin de detallar las debilidades encontradas, para finalmente emitir recomendaciones que contribuyan a mejorar su nivel de seguridad, proceso que obliga al corporativo a redactar sus propios procedimientos de seguridad, los cuales deben estar basados en políticas fundamentadas en dichas recomendaciones.

Como resultado de las recomendaciones se conseguirá proporcionar los lineamientos para promover el mejoramiento y la implementación de un esquema de seguridad en el corporativo, además de satisfacer su necesidad trascendental de protección a sus servicios.

Para el desarrollo de los puntos considerados se tiene previsto la ejecución de una metodología.

3.2.1. Aspectos de la metodología

La metodología a utilizar para la realización del sistema de seguridad en alta disponibilidad para la red, se basa en el desarrollo de las siguientes actividades:

Fase 1: Auditoría

- Definición de objetivos y alcance de la auditoría.
- Revisión y recopilación de fuentes de información.
- Generación del plan de trabajo, asignación de recursos y establecimiento de plazos de tiempo.
- Generación de cuestionarios.
- Realización de la auditoría:

  * Entrevistas a:

    - Miembros del Directorio: Gerente General y Gerente Contable.
    - Responsable del Departamento de Sistemas: administradores.
    - Personal del Departamento de Sistemas: administrador de Web, responsables del mantenimiento.
    - Usuarios del sistema: personal del área administrativa y vendedores.

  * Recolección de documentos organizacionales.

* Reconocimiento del entorno y del ámbito de trabajo.

Fase 2: Análisis de la información

- Análisis de los datos recabados.

Fase 3: Recomendaciones

- Hallazgo de debilidades y generación de recomendaciones.
- Presentación del informe a los directivos del corporativo.

De acuerdo a lo anterior y para alcanzar el propósito descrito, se procedió a desarrollar la auditoría de seguridad informática.

3.3. AUDITORÍA

Con el fin de estar al tanto de la consistencia de los sistemas de información y de control, y de la eficiencia y efectividad de los programas y operaciones que se realizan en la red corporativa, es necesaria la realización de una auditoría informática.

En gran medida, el éxito o fracaso de un sistema de seguridad depende del esfuerzo realizado en implementar los controles de seguridad que se diseñan para la organización. Por eso se deben conocer cuáles son los criterios o estándares más importantes que se aplican actualmente en el mundo de la seguridad para tal efecto.

Por lo tanto requerimos de fuentes de información para establecer el nivel de seguridad en el que se encuentra actualmente la red corporativa.

3.3.1. Fuentes de información

Para efectuar la auditoría, se deben considerar previamente las fuentes de información en los que estará fundamentada. Para el caso en cuestión se tiene prevista la utilización de criterios y estándares para desarrollar los conceptos de seguridad para la red corporativa. Así, entre los estándares internacionales más usados en el ámbito de la seguridad se encuentran: TCSEC, ITSEC, CC, ISO 17799, ISACA-COBIT, NIST, CERT, etc.

TCSEC

El criterio TCSEC (Trusted Computer System Evaluation Criteria, Criterio de Evaluación de Sistemas de Cómputo Confiables) fue desarrollado por el gobierno de Estados Unidos en 1980, para proveer un estándar en la fabricación de sistemas gubernamentales y como un criterio de evaluación para determinar el grado de confianza que posee un sistema de información. Lo conforman la serie de documentos del DoD

(Department of Defense of the United States, Departamento de Defensa de los E.U.) llamados "arcoiris", por el color de las portadas de los libros, donde el más reconocido es el libro Naranja para la evaluación de seguridad.

El Libro Naranja es consecuencia de la creciente conciencia de la seguridad por parte el gobierno de los Estados Unidos y de la industria para estandarizar el propósito y el uso de las computadoras por el gobierno federal. El Libro Naranja define cuatro extensas divisiones jerárquicas de seguridad para la protección de la información, las cuales son consideradas por orden creciente de confiabilidad, según:

- D Protección Mínima.
- C Protección Discrecional.
- B Protección Obligatoria.
- A Protección Controlada.

Cada clase consiste en una o más clases numeradas, entre más grande sea el número se indica un mayor grado de seguridad. De tal manera que la división C contiene dos distintas clases C1 y C2 (de acuerdo a la nomenclatura adoptada: C2 ofrece una mayor seguridad que C1). La división B contiene 3 clases B1, B2 y B3 (B3 ofrece mayor seguridad que B2 y B2 ofrece más seguridad que B1). La división A cuenta sólo con la clase A1. Cada clase se define con un grupo específico de criterios que un sistema debe cubrir, para ser certificado con la evaluación en alguna clase. Este criterio cae en 4 categorías generales: políticas de seguridad, responsabilidad, confianza y documentación.

Un criterio, basado en TCSEC para máquinas y sistemas de comunicaciones en red, es el TNI (Trusted Network Interpretation, Interpretación de Redes Confiables) que surge debido a la necesidad de intercambiar información por medio de la red. Debido a la evolución de las redes de computadoras se crea la necesidad de este criterio de evaluación, el cual en 1987 es desarrollado por el gobierno de Estados Unidos.

ITSEC

El ITSEC (International Technology Security Evaluation Criteria, Criterio de Evaluación Internacional de Tecnologías de Seguridad) fue desarrollado por países europeos y nace de la combinación del criterio del Libro Naranja y las mejores prácticas europeas, adicionalmente cubre la integridad y disponibilidad, que no se tenían contempladas en el TCSEC.

CC

El CC (Common Criteria, Criterio Común) representa los esfuerzos de la comunidad internacional en alinear y desarrollar un criterio de evaluación en seguridad, como resultado de los estándares europeos y norteamericanos. El Criterio Común combina los mejores elementos del ITSEC, la CTCPEC (de Canadá) y el Criterio Federal Norteamericano (FC). El propósito del Criterio Común es identificar y evaluar características en productos y sistemas.

ISO 17799

El estándar de ISO está basado en el estándar Británico BS7799 de 1995 y fue desarrollado para proveer una coherencia en los controles de las mejores prácticas en información de seguridad. De otros sistemas de gestión de seguridad, ISO 17799 sigue siendo el de mayor cobertura y efectividad al gestionar seguridad, esquemas de medición y mejoría de procesos.

ISACA-COBIT

La ISACA (Information Systems Audit and Control Association, Asociación de Auditoría y Control de Sistemas de Información) propone la metodología COBIT (Control Objectives for Information and Related Technology, Objetivos de Control de Información y Tecnologías Relacionadas). Es un documento realizado en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones, así como la confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos.

NIST

El NIST (National Institute of Standards and Technology, Instituto Nacional de Normas y Tecnología) fue creado por el Ministerio de Comercio del Gobierno de E.U. para apoyar a la industria en el desarrollo de la tecnología necesaria para mejorar la calidad y modernizar los procesos de fabricación, para asegurar la confiabilidad en los productos basados en los recientes descubrimientos de las ciencias y facilitar su rápida comercialización.

El programa del NIST en materia de tecnologías de la información comprende numerosos proyectos en las siguientes áreas: tecnologías de redes avanzadas, seguridad de las computadoras, acceso a la información e interfaces para usuarios, procesamiento y servicios de información distribuidos, sistemas y servicios de alto nivel de ejecución, diagnósticos del "*software*" y pruebas de conformidad.

CERT

El CERT (Computer Emergency Response Team, Equipo de Respuesta de Emergencias de seguridad en Cómputo) fue formado por DARPA (Defense Advanced Research Projects Agency, Agencia de Proyectos de Investigación de Defensa Avanzada) en el año 1988, en respuesta a las necesidades requeridas durante el incidente del gusano *Morris*, que llevó al 10 por ciento de los sistemas en Internet a una parálisis en noviembre de ese año. El CERT trabaja con la comunidad Internet para facilitar las respuestas a incidentes de seguridad que afectan a sus máquinas, con el objetivo de utilizar las medidas oportunas de prevención, investigar y mejorar la seguridad de los sistemas que existen.

A partir de entonces, se han ido constituyendo CERTs en diferentes países, para proporcionar información sobre como tratar un problema conocido de seguridad. El CERT trabaja con los fabricantes para emitir un informe o un añadido para un problema determinado, y no lo hace público hasta que el informe o el añadido están disponibles. Un aviso del CERT también puede alertar sobre la continuidad de algunos ataques.

Con base en la información presentada, para la realización de la auditoría de seguridad informática planteado, se utilizaron los siguientes estándares y guías:

Estándares:

- COBIT
  - * "Audit Guidelines" 3ra. Edición. COBIT, Julio de 2000.
  - * "Control Objectives" 3ra. Edición. COBIT, Julio de 2000.
- ISO
  - * "Estándar de Seguridad ISO 17799" (British Standard 7799).
- DoD
  - * "Trusted Network Interpretation of the TCSEC" (TNI), 1987 (Red Book).
  - * "Password Management Guideline", 1985 (Green Book).

Guías de referencia y soporte:

- NIST
  - * "Guide for Developing Security Plans for Information Technology Systems" Marianne Swanson, 1998.
  - * "Security Self-Assessment Guide for Information Technology Systems" Marianne Swanson, 2001.
- CERT
  - * "Tutorial de seguridad" CERT.

Con base en los puntos considerados más importantes de los estándares de seguridad antes mencionados, se ha podido determinar el objetivo y el alcance de la implementación de la auditoría de seguridad.

3.3.2. Objetivo general

El objetivo general consiste en averiguar las vulnerabilidades de seguridad existentes, como medio para el desarrollo de recomendaciones, que definirán los lineamientos para promover la implementación de un esquema de seguridad en la red corporativa.

3.3.3. Alcance

La auditoría informática propuesta comprende fundamentalmente la planificación y ejecución de los siguientes aspectos:

Evaluación de la seguridad lógica

- Identificación de usuarios.
- Autentificación.
- Contraseñas.

Evaluación de la seguridad en las comunicaciones de red

- Topología de red.
- Comunicaciones externas.
- Tráfico de red.
- Interoperatividad.
- Correo electrónico.
- Antivirus.
- Pruebas de red.
- Ataques de red.

Evaluación de la seguridad de las aplicaciones

- *Software.*
- Seguridad de bases de datos.
- Control de aplicaciones en PCs.
- Control de datos en las aplicaciones.
- Ciclo de vida del desarrollo de *software.*

Evaluación de la seguridad física

- Equipamiento.
- Control de acceso físico al centro de cómputo.
- Control de acceso a equipos.
- Dispositivos de soporte.
- Estructura del edificio.
- Cableado estructurado.

Evaluación de la administración del área de sistemas

- Administración del centro de operaciones de red.
- Capacitación de usuarios.
- Copias de seguridad.
- Documentación.

Evaluación de las auditorías y revisiones

- Verificaciones del sistema.
- Responsabilidades de los encargados de seguridad.

- Auditorías de control de acceso.
- Auditorías de las comunicaciones de red.

Evaluación del plan de contingencias

- Plan de administración de incidentes.
- Respaldo de equipamiento.
- Estrategias de recuperación de desastres.

Para llevar a cabo la auditoría se requirió de la elaboración de un plan de trabajo para asignar los recursos necesarios y el establecimiento de plazos de tiempo, además de la generación de los cuestionarios para su aplicación. Los formatos de dichos cuestionarios se incluyen en el apéndice del presente trabajo para su consulta.

La realización de la auditoría, como se menciono antes, se basó en entrevistas. Conjuntamente se hizo la revisión de documentos organizacionales y el reconocimiento del entorno y del ámbito de trabajo.

Después de haber efectuado la auditoría de seguridad informática, se obtuvieron una serie de datos sobre la red corporativa, mismos que fueron empleados para realizar un análisis de información.

3.4. ANÁLISIS DE INFORMACIÓN

A continuación se describen los datos y la información recogida durante la auditoría realizada a la red corporativa, detallando cada uno de los controles que se implementan en la actualidad. Se empezará por la evaluación de la seguridad lógica.

3.4.1. Evaluación de la seguridad lógica

En esta sección de la auditoría se evaluaron los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

Identificación de usuarios

Altas

Cuando un usuario nuevo ingresa a la empresa, el área de Recursos Humanos toma sus datos, dando de alta su registro, sin embargo, no existe un procedimiento formal a seguir para realizar estas tareas. Si este usuario necesita del sistema informático, Recursos Humanos hace el pedido al Departamento de Sistemas, donde se genera el alta del usuario al sistema. Los datos que se ingresan en la cuenta son los siguientes:

- ID de usuario, inicialmente será el número de registro, aunque se comprobó que no corresponde realmente con este número.
- Contraseña, inicialmente será el número de registro, y se instruye al usuario para que lo modifique.
- Nombre y apellido completo, obtenidos del archivo de Recursos Humanos.
- Sección del corporativo donde trabajará.
- Grupo al que pertenece, según el área de la empresa que le fue asignada por el Departamento de Recursos Humanos. Se pudo comprobar que en algunos casos este campo permanece vacío, permitiendo que el usuario acceda a todos los menús del sistema.
- Fecha de expiración de la contraseña, el cual es de un año, aunque para algunos usuarios este campo no se completa, permitiendo que nunca se actualice la contraseña.
- Fecha de anulación de la cuenta, para dar de baja la cuenta.
- Contador de intentos fallidos, el cual bloquea el *login* si es igual a dos (si el usuario ha ingresado mal la contraseña dos veces seguidas), en este caso el usuario debe solicitar al administrador la reactivación de la cuenta.
- Autorización de impresión, ya que no todos los usuarios pueden imprimir los datos del sistema.

Bajas

Las cuentas de los usuarios no se eliminan del sistema, se deshabilitan, actualizándoles la fecha de anulación de dicha cuenta. De esta forma los datos de las cuentas dadas de baja quedan almacenados en el disco y no es posible repetir los IDs de usuarios anteriores para nuevos empleados.

No hay ningún procedimiento formal para dar de baja un usuario del sistema. El departamento de Recursos Humanos informa al sector de cómputo, y allí se procede a dar de baja el empleado una vez que se ha desvinculado de la empresa.

Mantenimiento

No se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

Permisos

El control de acceso en la empresa no se basa en los perfiles de los usuarios y la asignación o denegación de permisos a los mismos, sino más bien en perfiles de grupos. Estos grupos se generan en concordancia con las áreas de la empresa y es el Departamento de Recursos Humanos el que asigna cada usuario a un grupo determinado. Luego, los usuarios son dados de alta en el sistema, y los administradores del sistema son los encargados de la asignación de permisos.

El sistema informático está desglosado en una gran cantidad de módulos diferentes, donde cada uno de ellos es un programa en sí mismo. De esta manera cada usuario del sistema, según el grupo al que pertenece en la organización, dispone de los accesos directos a los programas que corresponden a su área. Así, los usuarios sólo pueden interactuar con los datos a los que dichos módulos les permiten acceder. Los accesos directos a los que el usuario tiene acceso los genera el administrador del sistema a mano, una vez que el usuario fue dado de alta.

A medida que la responsabilidad del usuario en la empresa es mayor, son necesarios más datos, y por ende más módulos, o accesos a programas. A modo de ejemplo, esto quiere decir que en un cargo gerencial puede haber 15 módulos disponibles, mientras que los vendedores sólo tienen un módulo de consulta de datos. Se comprobó que en ciertos casos sobran funcionalidades. Al tratar de acceder a datos críticos el sistema requerirá nuevamente el número de registro y la contraseña. Este control sirve para comprobar que el usuario ingresado es el mismo que está intentando acceder a estos datos sensibles, de manera que si este segundo *login* no coincide con el primero, los datos no serán mostrados.

No existe en el sistema informático una lista de control de acceso que se utilice para identificar los tipos de permiso que tiene cada usuario con respecto a los datos. Sólo existe una relación entre los sectores de la empresa, los menús y los usuarios correspondientes a cada sector. En las carpetas de documentación del desarrollo, relativas a cada módulo de programa, se explica la relación que existe entre cada módulo de programa y los datos.

No se tiene en cuenta ninguna restricción horaria para el uso de los recursos. Tampoco se considera una restricción física sobre la máquina desde donde ingresa cada usuario.

Inactividad

Si el usuario ingresado permanece un período de tiempo sin actividad, el sistema no ejecuta ninguna acción; los administradores sólo advierten a los usuarios sobre la necesidad de no dejar las máquinas con sesión abierta e inactivas.

Si cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones, no pasan a un estado de suspensión.

El super-usuario accede a los servidores durante las 24 horas del día, debido a que estos equipos no se apagan en ningún momento.

Cuentas de usuario

Los usuarios del departamento de ventas no son identificados en forma personal, sino que todos usan el mismo nombre y contraseña para ingresar al sistema informático. Este módulo del sistema sólo permite hacer consultas a las bases de datos (listas de precios, planes de ventas, etc.), pero no les está permitido hacer ninguna modificación a los datos.

Los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y varias sesiones del mismo menú. No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar simultáneamente.

No se eliminan los usuarios que vienen predeterminados en el sistema operativo como son las cuentas "invitado". Estas cuentas permanecen activas en el sistema sin que ningún usuario las utilice.

En la empresa hay tres personas con perfil de administrador. Cada una de ellas tiene su cuenta con una contraseña personal, pero para fines prácticos, los tres conocen las contraseñas de las tres cuentas, ya que no hay una clara definición de tareas. Además, el administrador puede acceder desde cualquier terminal de la empresa.

Existe, además, un servicio de mantenimiento externo que utiliza la misma cuenta del administrador para hacer modificaciones en los sistemas operativos de los servidores vía Internet, ya que el administrador del centro de cómputo se lo proporcionó. Una vez finalizado el mantenimiento, el administrador del sistema no cambia la contraseña, de manera que ésta continúa siendo conocida por el personal externo.

Autentificación

En la pantalla de ingreso de los sistemas se muestran los siguientes datos:

- Nombre de usuario (a completar por el usuario).
- Contraseña (a completar por el usuario).
- Opción para cambiar la contraseña.

Cuando un usuario ingresa su contraseña al sistema, aparecen asteriscos en lugar de mostrar el dato que está siendo ingresado. Una vez que algún usuario ha logrado ingresar en el sistema, aparece en pantalla el nombre del usuario.

Existe una aplicación de importante y significativa sensibilidad con la cual es posible gestionar los datos de los usuarios, incluidos sus permisos y contraseñas. Esta aplicación sólo puede ser ejecutada por el administrador a través de la línea de comandos de Windows, escribiendo toda la ruta hasta ella, ya que no hay íconos de acceso directo desde ninguna terminal.

Los datos de autentificación de los usuarios del sistema de la empresa se almacenan en el servidor de aplicaciones Windows, sin ningún control de acceso. Además, estos datos son transferidos, desde la terminal que se está utilizando hasta el servidor, en formato de texto plano.

Dentro de la empresa no se usa ningún tipo de firma digital, ni para mensajes internos ni para los externos, ya que las directivas de importancia no son enviadas vía *mail*.

En cuanto a la configuración de las estaciones de trabajo, no hay ningún control de acceso a sus sistemas BIOS, de manera que al momento del encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

Contraseñas

Generación

Las contraseñas que existen en la empresa son generadas en forma manual, sin procedimientos automáticos de generación. Como restricción, deben tener una longitud máxima de 10 caracteres, numéricos o alfanuméricos. Cuando se da de alta un empleado en el sistema, su contraseña se inicializa con el mismo nombre de la cuenta (que es igual al número de registro del usuario), advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.

Durante la auditoría pudimos comprobar que las contraseñas de acceso a los super-usuarios de los servidores eran iguales.

Cambios

Los cambios en las contraseñas los hacen los usuarios a través de la pantalla de ingreso, allí hay un botón que muestra la opción para su modificación. Aunque generalmente las contraseñas no son actualizadas por los usuarios, permaneciendo iguales por largos períodos de tiempo, ya que tienen un plazo de expiración de 1 año. No se controla si el usuario utiliza siempre la misma contraseña simulando cambiarla pero ingresando nuevamente la clave que ha estado usando hasta ahora.

Si un usuario olvida su contraseña, debe advertirle al administrador del sistema, el cual se fijará (con el sistema de administración de perfiles de usuario) cuál es la clave del usuario. Al decírsela, no se requiere que el usuario la modifique, por lo que no se controla esta situación. Ocurre lo mismo cuando un usuario ingresa mal su contraseña dos veces seguidas, ya que el sistema lo bloqueará y el usuario no podrá ingresar, por lo que deberá recurrir al administrador.

3.4.2. Evaluación de la seguridad de las comunicaciones de red

Durante la auditoría informática se deberá evaluar la topología de la red, la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

Topología de red

La red se encuentra operando bajo el estándar de IEEE 802.3, con una topología tipo estrella, usando el método de acceso CSMA/CD. El medio está basado en cableado

estructurado bajo la norma ANSI/TIA/EIA 568. El tipo de cable empleado es par trenzado con la categoría 5. Esta categoría es una de las más populares para redes nuevas, ya que permite alcanzar velocidades de transmisión hasta de 100 Mbps y maneja una longitud máxima por segmento de 100 metros. La técnica empleada para la señalización es banda base.

Descripción de la red

Actualmente la red corporativa está basada en la tecnología Gigabit Ethernet, esta tecnología permite manejar grandes tráficos TCP. La red dispone de 10 centros de servicio, ver figura 3.1, los cuales están conectados al edificio corporativo a través de enlaces privados, formando en conjunto la red de datos corporativa. Los centros de servicio y el edificio corporativo se han englobado en una red troncal. Dentro del edificio corporativo se encuentra el *backbone* (o columna) y las sedes remotas forman nubes que se conectan a éste mediante enlaces DS0 (Digital Signal, Señal Digital X). Este edificio tiene una arquitectura de LAN *Switches,* los cuales sostienen comunicación entre los servidores y el ruteador principal, la finalidad de esto es de compartir a los usuarios internos y a los centros de servicio las aplicaciones que se requieran y el Internet.

Los servicios de acceso hacia la red corporativa se centralizan en el edificio principal o corporativo para evitar puertas traseras o agujeros de seguridad. Desde este punto en la red, se da acceso a Internet y a los centros de servicio utilizando para ello un ruteador con posibilidad de disponer diferentes interfaces WAN, dependiendo de las necesidades de conectividad con redes externas.

Los *switches* han sido programados para direccionar los paquetes transmitidos por sector, según la dirección IP que traen, distinguiendo a qué sector de la empresa van. De esta manera, al no repetir los paquetes de datos a toda la red, se disminuye el uso de ancho de banda y se evita la divulgación de los mensajes, mejorando la seguridad de la topología de red.

Es importante mencionar que la red trabaja con el protocolo de comunicación basado en TCP/IP, por lo que es necesario hacer referencia al direccionamiento, ya que es el método por el que todos los host pueden establecer una comunicación entre ellos.

Direccionamiento TCP/IP

La red posee un direccionamiento privado, con un número determinado de direcciones públicas para elementos como los nodos de conmutación, los ruteadores y los servidores. Para la traducción de las direcciones públicas y privadas se emplea la herramienta NAT (Network Address Translation, Traducción de Direcciones de Red).

Para su instalación, se determinó una red clase B privada y por medio de crear subredes adecuadas se realiza la gestión de la red corporativa. Una de las ventajas principales del uso de crear subredes consiste en segmentar una red muy extensa en pequeñas subredes más fáciles de administrar. Los ruteadores tienen la facilidad de separar subredes, de manera que disminuyen los dominios de colisión entre segmentos.

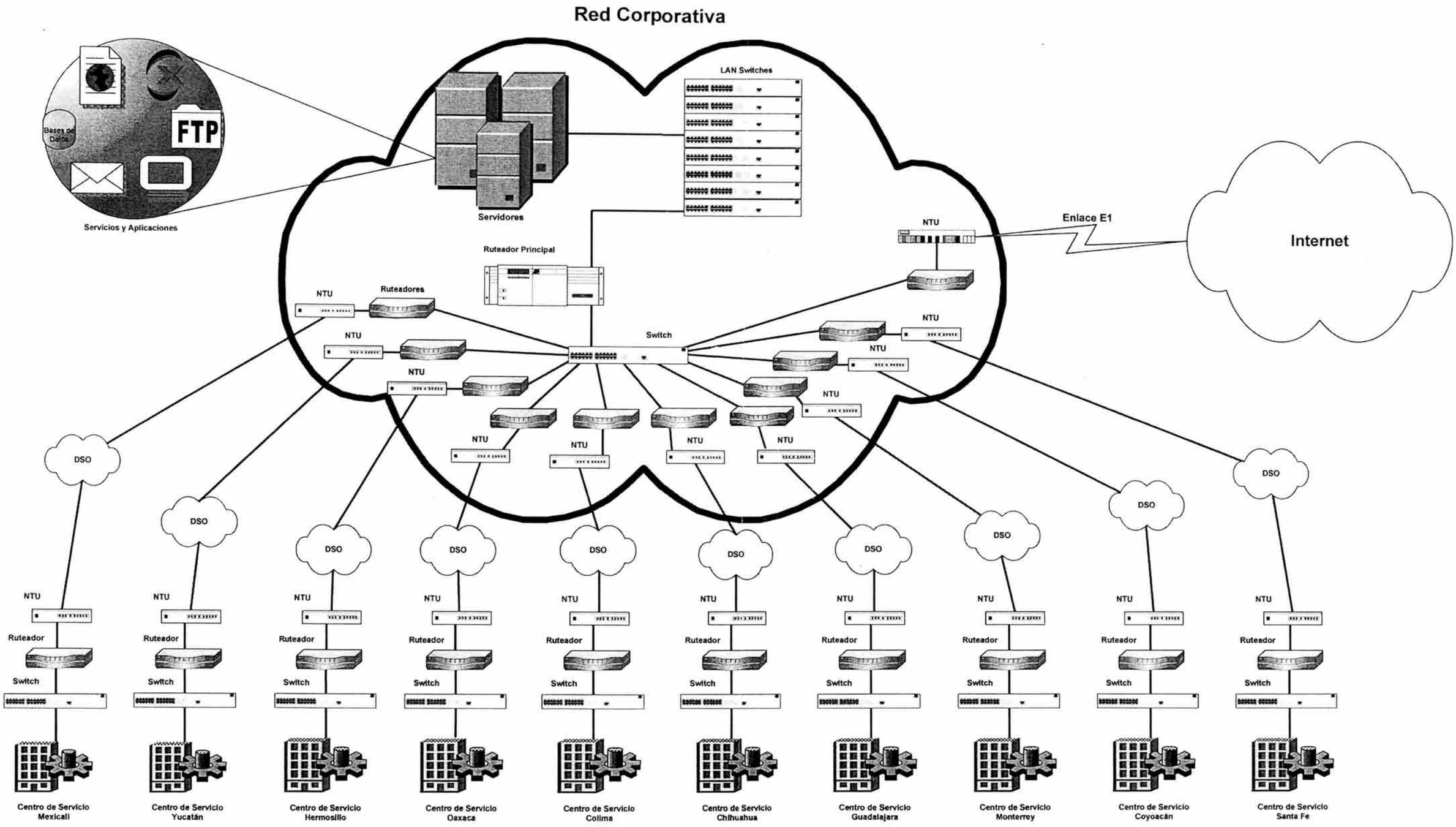

Figura 3.1. Esquema general de la red de datos.

Dentro de la red corporativa de la empresa, cada equipo respeta el protocolo de red TCP/IP y por consiguiente tiene asignada una dirección IP. La dirección IP tiene que ser única, para evitar conflictos de comunicación entre *hosts*. La red corporativa está configurada con un direccionamiento 172.30.X.Y, donde la X hace referencia a un segmento de red y Y al *host* perteneciente a dicha red, cada segmento de red tiene de 1 a 254 *host* disponibles por asignar. La red del edificio corporativo tiene 5 segmentos de red, cada segmento tiene asignada una ubicación física dependiendo del piso en que se encuentre.

Direccionamiento IP	Ubicación del Equipo
172.30.0.xx	Planta Baja
172.30.10.xx	1er Piso
172.30.20.xx	2° Piso
172.30.30.xx	3er Piso
172.30.40.xx	4° Piso

Para cada red se tienen definidas direcciones con un rango de 1 a 255, dejando la dirección 254 para cada *switch*, la dirección 255 es la dirección de *broadcast*, además se usa como máscara de subred la dirección 255.255.255.0 con el fin de ocupar todo el rango de direcciones para *hosts*.

Una vez que se ha mencionado el direccionamiento empleado dentro de la red corporativa, describiremos los componentes que forman la red informática.

Componentes de red

La red informática del corporativo se compone del siguiente equipamiento:

- 50 PCs distribuidas entre los 10 centros de servicio, adicionalmente otras 300 de ellas en el edificio del corporativo.
- 4 Servidores Sun 3500, uno como servidor de archivos FTP, otro para el sitio Web de la página de la empresa, otro para aplicaciones y renta de sitos Web y uno más para correo electrónico. Se usa un servidor Servidor Compaq Proliant DL760 con Windows 2000 para las PCs.
- 10 enlaces DS0 (64 kbps).
- Cableado UTP categoría 5.
- Conexión E1 (2 Mps) como salida a Internet.
- 15 *switches* Cisco Catalyst 5500 en la red matriz.
- Un ruteador Cisco en la red matriz.
- 20 ruteadores Cisco 2600, dos para cada enlace hacia los centros de servicio.
- 10 switches Cisco 1900 de 12 entradas, uno en cada en cada centro de servicio.
- 20 NTUs Tellabs, dos para cada centro de servicio.
- 1 NTU Tellabs, que conecta la red corporativa con Internet.

Además de la descripción de la red corporativa es importante detallar la forma en como las oficinas remotas se adjuntan a la red de datos e Internet a través de las conexiones externas.

Conexiones externas

Conexión de los centros de servicio

Como se había mencionado en párrafos anteriores, la empresa cuenta con 10 centros de servicio repartidos en toda la república mexicana. Estos centros se comunican hacia la red corporativa a través de enlaces DS0 (64 kbps), estos últimos proporcionados por TELMEX y pagando una renta mensual por el uso de las líneas. A su vez, estos centros de servicio cuentan con 5 PCs en promedio, de 12 posibles, en cada uno. Un ejemplo de esta conexión se detalla en la figura 3.2.

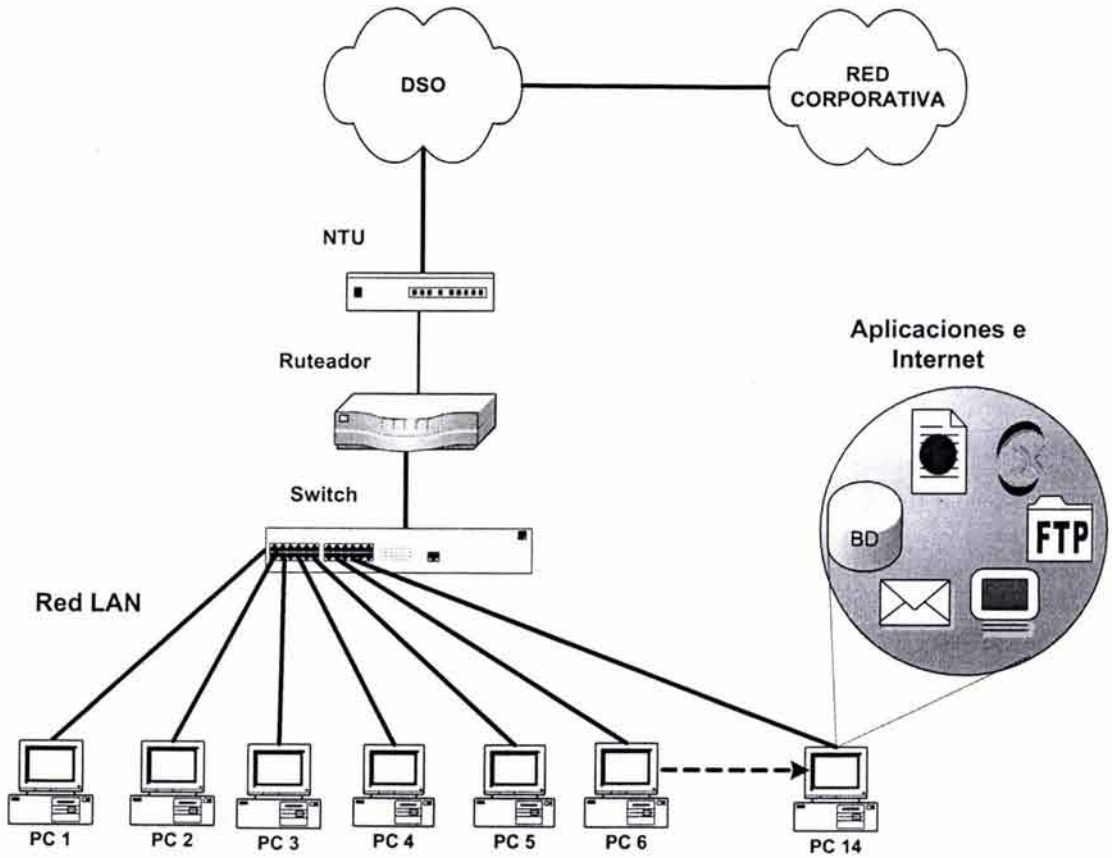

Figura 3.2. Esquema general de la conexión del centro de servicio al corporativo.

El direccionamiento para cada centro de servicio también es del tipo clase B, 172.35.X.Y, cabe destacar que Y sólo puede tomar 14 valores según sea el caso.

Los centros de servicio tienen 10 segmentos de red, cada segmento tiene asignada una ubicación física, dependiendo del centro de servicio en que se encuentre. Las direcciones correspondientes a los centros de servicio son:

Direccionamiento IP	Ubicación del Equipo
172.35.0.1-172.35.0.14	C.S. Santa Fe
172.35.1.1-172.35.1.14	C.S. Coyoacán
172.35.2.1-172.35.2.14	C.S. Guadalajara
172.35.3.1-172.35.3.14	C.S. Monterrey
172.35.4.1-172.35.4.14	C.S. Chihuahua
172.35.5.1-172.35.5.14	C.S. Hermosillo
172.35.6.1-172.35.6.14	C.S. Mexicali
172.35.7.1-172.35.7.14	C.S. Colima
172.35.8.1-172.35.8.14	C.S. Oaxaca
172.35.9.1-172.35.9.14	C.S. Yucatán

Para cada segmento de red se tienen definidas direcciones con un rango del 1 al 14, dejando la dirección 172.35.X.1 para cada *switch*, donde X está definido del 0-9, la dirección 172.35.X.14 es la dirección de *broadcast*, además se usa como máscara de subred la dirección 255.255.255.240 con el fin de ocupar todo el rango de direcciones para *hosts*.

Los centros de servicios y el corporativo tienen acceso a Internet, por el método NAT, esta conexión a Internet se hace a través de un enlace con características propias.

Conexión a Internet

El acceso hacia Internet es para la empresa un punto importante, ya que por este medio los empleados, clientes y distribuidores realizan conexiones hacia los servicios como bases de datos, consulta de estados de cuenta, activación de líneas para teléfonos celulares, correo electrónico, renta de espacio para páginas Web, venta de tiempo aire para teléfonos celulares, consultas de catálogos de equipos de telecomunicaciones, consultas del estado de las ordenes de garantía de equipos, entre otros servicios adicionales.

Para lograr el acceso desde la red corporativa hacia Internet, se requiere de equipos apropiados como ruteadores y NTUs (Network Teminal Unit, Unidad Terminal de Red). Éstos últimos son instalados y configurados por la compañía que presta el servicio de Internet. Este acceso se realiza por medio de un enlace dedicado de alta capacidad E1 (2 Mbps) hacia el ruteador de la empresa que proporciona el acceso a Internet, tal y como lo muestra la figura 3.3.

Tráfico de la red

Con el fin de obtener las características del tráfico de información existente en la red corporativa, se realizó un análisis. Se tomó una muestra a lo largo de una semana de la actividad y del comportamiento de las comunicaciones dentro de la red.

Con la información obtenida se realizaron estadísticas generales sobre el tráfico de la red.

Estadísticas generales

En esta sección se hace una revisión general de la actividad de comunicación con los protocolos más comunes en la red, esto nos ayudará a validar cuál es el requerimiento de ancho de banda que necesita nuestra solución para el diseño del sistema de seguridad.

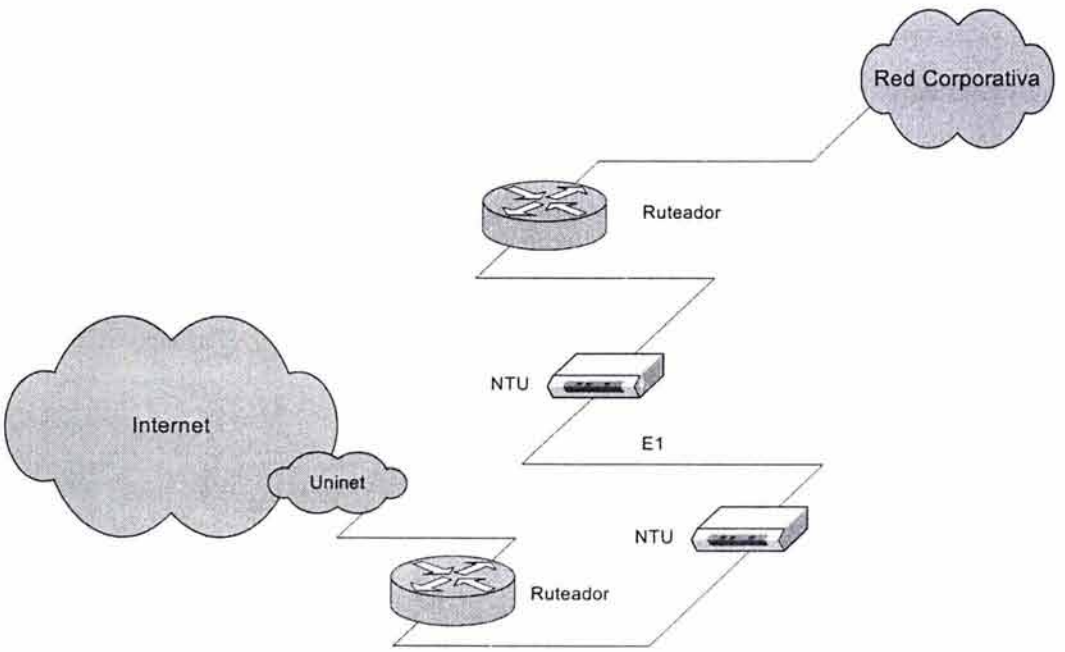

Figura 3.3. Conexión a Internet.

El volumen de tráfico lo mostramos en kb transferidos. El volumen de transferencia fue realizado desde la red corporativa hacia la red pública y viceversa (ver tabla 3.1 y figura 3.4).

Podemos ver en la gráfica que la gran concentración de uso de ancho de banda lo hacen los protocolos que operan dentro de las aplicaciones de la empresa; también se observa que los protocolos más usados son el servicio de correo electrónico y servicio de consultas a páginas electrónicas (HTTP).

Debemos considerar también que los protocolos de FTP y TELNET están presentes y figuran dentro de la utilización del ancho de banda pero en menor escala.

Estadísticas Generales	
Fecha del Reporte Generado	**Jueves 9 Octubre, 2003 - 09:28:41**
Total de número de eventos	9,689,887
Total de eventos criticos	120,762
Total de errores	3,791,078
Total de bytes de conexiones a la red pública	3,418,993k
Total de bytes de conexiones a la red corporativa	1,435,826k
Total de eventos por día	1,076,654
Total de bytes por día, en conexiones hacia fuera de la red	379,888k
Total de bytes por día, en conexiones hacia adentro de la red	159,536k
Porcentaje de ancho de banda dedicado a la actividad web	36.27%
Porcentaje de ancho de banda dedicado a la actividad de correo electrónico	37.51%
Porcentaje de ancho de banda dedicado a la actividad FTP	0.96%
Porcentaje de ancho de banda dedicado a la actividad TELNET	0.00%
Porcentje de ancho de banda dedicado a otras actividades	21.69%

Tabla 3.1. Estadísticas generales.

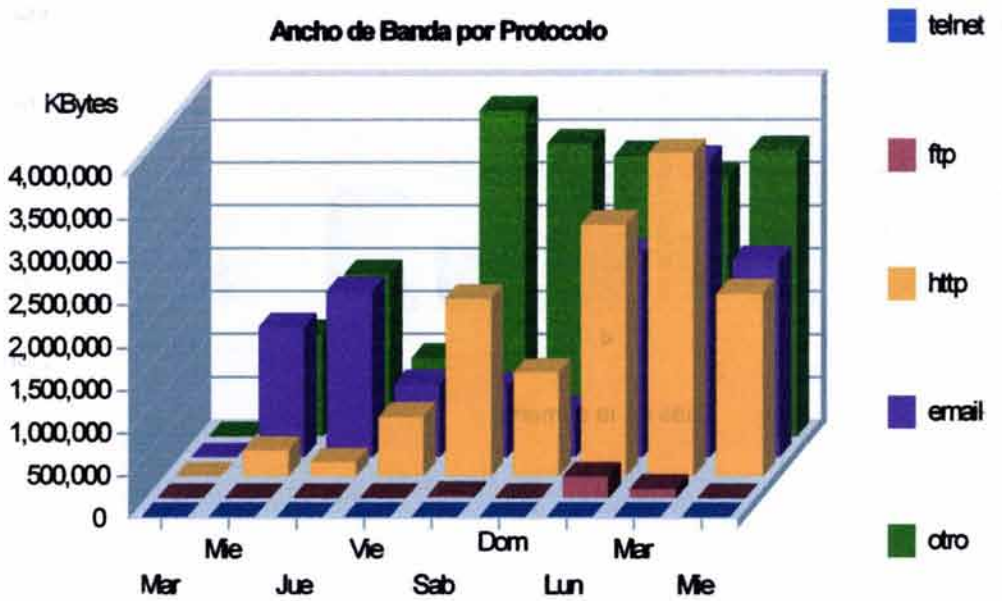

Figura 3.4. Uso del ancho de banda por protocolo.

Volumen de tráfico

En esta sección se muestra el volumen de tráfico que se genera desde la red pública hacia la red corporativa por día de la semana (ver tabla 3.2 y figura 3.5).

Tráfico de entrada por día de la semana				
	Día	**# de Eventos**	**% del Total de Eventos**	**kbytes**
1	Lun	686784	31.77%	4,679,939
2	Mar	200526	9.27%	2,777,398
3	Mie	303925	14.06%	2,822,428
4	Jue	125115	5.78%	1,495,620
5	Vie	417756	19.32%	654,804
6	Sap	293181	13.56%	1,343,332
7	Dom	134163	6.2%	584,734
	Total de días	**1734106**	**80.22%**	**9,093,585**
	Total de fin de semana	**427344**	**19.77%**	**5,264,674**

Tabla 3.2. Tráfico de entrada a la red corporativa por semana.

Figura 3.5. Tráfico de entrada a la red corporativa por día.

Observamos que el mayor número de eventos se presentan todos los días lunes. Los fines de semana observamos poco tráfico debido a que son días de descanso para la mayoría de los usuarios de la red corporativa. Por otro lado, dentro de la red corporativa se cuenta con una seguridad física y técnico administrativa, que es aplicada a todo el personal que labora dentro de ella.

Interoperatividad

Interoperatividad windows – unix

Los recursos de Unix se comparten en la red de Windows usando aplicaciones basadas en Java. Con esta aplicación, una porción del disco del servidor de aplicaciones se encuentra compartida con la red de Windows. Esto hace posible el entendimiento entre Windows y Unix, permitiendo a los usuarios de Windows acceder a datos que se encuentren en el sector compartido del servidor Unix, a través del Explorador de Internet.

Recursos compartidos

El entorno de red de cada uno de los usuarios está configurado para que el usuario no vea toda la red, sino sólo una parte de la misma.

Ninguno de los equipos comparte sus archivos, a excepción de los siguientes:

- En el servidor de Windows se comparten dos carpetas. Una es la utilizada para almacenar las actualizaciones del antivirus y los programas de instalación más utilizados, y la otra es la que emplea la aplicación que sincroniza la fecha y hora de las PCs de la red.
- En el servidor de aplicaciones se comparte una carpeta donde los usuarios guardan los datos que necesiten grabar en un CD, ya que la grabadora se encuentra en éste.

Para las aplicaciones del sistema informático de la empresa (ejecutables) y los sistemas en desarrollo, los usuarios acceden desde Windows.

Correo electrónico

No todos los empleados tienen una cuenta de correo electrónico, sólo hay 150 cuentas de correo, ya que hay muchos empleados que no necesitan este servicio. Todos los Jefes de área disponen de una. Este medio se utiliza para enviar todo tipo de información.

Herramientas

La empresa cuenta con un sistema de correo electrónico que se aloja en un servidor dedicado. El correo tiene como dominio @ledaxis.com.

El correo se lee con Outlook Express en las PCs de la empresa. En el servidor se usa el i-Planet, un administrador de correo, configurado por los técnicos encargados del mantenimiento, y gestionado por el administrador del centro de cómputo.

El *software* Outlook Express se instala con su configuración predeterminada y puede ser modificado por el usuario, sólo en las siguientes características:

- Vista previa.

- Confirmación de lectura.
- Bloqueo de remitente.
- Controles ActiveX y Scripts.

Alta de usuarios de correo

Si un empleado necesita una dirección de correo, porque su puesto de trabajo lo amerita, el Gerente del área al que pertenece le avisa al administrador del centro de cómputo, y éste le asigna una.

Cuando se genera una nueva cuenta de correo, el administrador del sistema debe definir al usuario y darlo de alta en el sistema operativo del servidor de correo de la empresa, después debe configurar el i-Planet, y por último el Outlook Express de la máquina del empleado.

En el momento de generar la nueva cuenta, el administrador le asigna un nombre y una contraseña a la nueva cuenta. Esto impide que un empleado utilice la cuenta de otro, ya que la única persona que conoce las contraseñas es el administrador del centro de cómputo.

Las cuentas de los usuarios no están publicadas en Internet. Lo que se publica en la página son cuentas generales con alias, que apuntan a las cuentas de los Jefes de área, por ejemplo existe una cuenta de ventas (ventas@ledaxis.com) que está dirigida a la cuenta del Gerente de Ventas.

Recepción y envío de correos

Cada diez minutos el i-Planet checa las casillas de correos del servidor. En el caso que exista algún mensaje nuevo, éste los baja al servidor de Internet. El *software* Outlook Express de las máquinas de los usuarios verifica el servidor de correo cada cinco minutos. Cuando actualizan sus bandejas de entrada, el *mail* es borrado del servidor y enviado a la máquina del usuario, sin quedar ninguna copia del mismo en el servidor.

Los empleados no usan el *mail* solamente para funciones laborales, sino también con fines personales. Es posible ver los *mail* que se envían, pero actualmente no se realizan controles, de manera que pueden usarlo para cualquier fin. No se hace ningún control para comprobar si los usuarios se suscriben a listas de correo, no hay prohibiciones en este sentido.

Cuotas de disco

En el momento en que se crea un usuario de *mail* en el i-Planet, se le asigna una cuota de disco del servidor de Internet para los mensajes de entrada, con un tamaño de 4 Mb para cada usuario. No existe límite de tamaño para los mensajes de salida, ya que no quedan almacenados en el servidor.

Si alguna de las cuentas llega a los 4 Mb, entonces el i-Planet manda un *mail* al usuario, avisando que se está quedando sin espacio de disco, éste deja de recibir el correo y se bloquea la cuenta.

Opciones seguras de configuración

Copia Oculta (CCO). Los empleados de Gerencia usan el campo de copia oculta, generalmente para comunicarse con las fábricas, y cuando se envían mensajes a diferentes áreas, se les adjunta una copia oculta al Jefe del Sector.

Correo basura. No hay ninguna configuración especial para evitar el correo basura o *mail bombing*. Pero como las direcciones son locales, manejadas con servidores propios, no han ocurrido problemas en este sentido.

Antivirus. El antivirus que está en el servidor de Internet verifica el correo, inspeccionando todos los mensajes entrantes y salientes, y sus archivos adjuntos. En el caso de encontrar un *mail* infectado, se encarga de borrarlo, y se envía un *mail* al destinatario del mensaje avisando que el mismo se eliminó.

Chat y file sharing. No están prohibidos los programas de *chat* (generalmente se usa el MSN). Tampoco están prohibidos los programas de archivos compartidos o *file sharing*. Esto se da porque los servicios que utilizan estos programas no están deshabilitados.

Prioridades. No se implementa un sistema de prioridades de los mensajes.

Copia de seguridad. No se generan copias de seguridad de los mensajes, ni en el i-Planet ni en el Outlook Express de los usuarios.

Privacidad, firma digital y encriptación de correo. No se utilizan firmas digitales ni encriptación en el correo electrónico. Algunos usuarios utilizan firmas de Outlook para enviar sus mensajes. No hay prohibiciones de envíos de archivos confidenciales vía *mail*.

Antivirus

En la empresa no ha habido grandes problemas con virus, a excepción de una gran cantidad de PCs con Windows infectadas con el virus K-Lez, pero este virus no afectó a los servidores. Esta infección generó gran tráfico de red y congestionó las líneas, pero pudieron erradicarse con el uso del antivirus.

Herramientas

En la empresa disponen de una versión corporativa del Norton Antivirus, de manera que en el servidor de aplicaciones hay una versión para el servidor y en el resto de las PCs hay una versión cliente de este antivirus. En el servidor de Internet está instalado el PC Cillin de Trend Micro para el control de virus. Ambos antivirus están ejecutándose continuamente y controlan la recepción y el envío de *mail*, tanto en el servidor como en las

PCs. Hay discos de rescate o de emergencia del antivirus, con los que se *lanzan* (*"bootea"*) desde DOS, en caso de la restauración de máquinas infectadas.

Actualización

De Internet se actualizan las listas de virus del Norton Antivirus a través de un *script*, y el archivo ejecutable se almacena en una carpeta del servidor. Los usuarios son los responsables de actualizar sus propios antivirus.

Este *script*, al ejecutarse y bajar las actualizaciones, envía un *mail* a los usuarios advirtiendo que actualicen el programa. Al respecto no se hacen chequeos.

Escaneos de virus

No se hacen escaneos periódicos buscando virus en los servidores ni en las PCs. No hay ninguna frecuencia para realizar este procedimiento, ni hay algún responsable. En algunas máquinas (en las que han tenido problemas frecuentes con virus), cuando el equipo se inicia, entonces comienza un escaneo del Norton antes del inicio de Windows.

Pruebas de red

El encargado de mantenimiento controla que los servicios permitidos sean los correctos, pero esta tarea la realiza sin ninguna frecuencia. Debido a que estas pruebas que se realizan no son formales, no se genera documentación alguna.

Nunca se hicieron pruebas de auto-*hackeo*, ni *escaneos*, ni intentos de intrusión o de escucha. Tampoco se hacen pruebas periódicas de puertos o de los servicios que están habilitados. Sólo se revisan las instalaciones cuando hay quejas de los usuarios.

No se disponen de medios para monitorear ciertos parámetros de la red, como el tráfico, parámetro que se evaluó en el presente trabajo por cuenta propia. Estos parámetros no son considerados fuente de alarmas ante problemas por parte del corporativo.

Falla en servidores

En el caso que haya algún problema con el servidor de Internet, no se usaría el servidor de aplicaciones como reemplazo. Aunque no es deseable, para la empresa es preferible prescindir de los servicios de Internet hasta que el servidor sea reparado, a arriesgar los datos del servidor de aplicaciones exponiéndolos en Internet.

Parches de seguridad

Las versiones del sistema operativo instaladas en los servidores son antiguas, por lo que casi no se consiguen actualizaciones. Esto puede repercutir en la seguridad de los servicios usados, como el SSH, generando nuevas vulnerabilidades.

Ataques de red

La empresa no dispone de herramientas destinadas exclusivamente para prevenir los ataques de red, debido a que no se han presentado problemas en este sentido.

Tampoco hay zonas desmilitarizadas y el corporativo explica que se debe a que sólo se dispone de un servidor, aunque haya datos publicados *on line* desde el interior de la empresa.

Intrusiones

No hay herramientas para detección de intrusos, sólo se cuenta con antivirus.

Denegación de servicio

No hay controles con respecto a la ocurrencia de DoS. No existen herramientas que lo detecten, ni líneas de base con datos sobre la actividad normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

Se dispone de una herramienta de monitoreo que se ejecuta en una página HTML con datos sobre el tráfico de red, la cantidad de archivos abiertos, de usuarios conectados a la red, uso de la memoria del servidor y del *swap*.

Sniffing y spoofing

En la empresa la red se encuentra segmentada a través de *switches*, que efectivamente reducen la posibilidad de *sniffing*, ya que direccionan los paquetes de red de acuerdo al destino que tienen (sector de la empresa al que están dirigidos). Así se evita que el paquete viaje a través de toda la red o por destinos innecesarios. Además, con este direccionamiento de paquetes, también se reduce el riesgo de que se presente un ataque *spoofing,* poniendo en peligro nombres y contraseñas de usuarios. De cualquier modo no existe ninguna herramienta anti-*spoofing*.

Ataque a las contraseñas

El archivo de las contraseñas del sistema no se almacena en el directorio por defecto de Windows, ahí sólo se almacena un archivo con los nombres y demás datos de usuarios. Este archivo está en texto plano y puede ser accesible ya que no está encriptado. Este archivo se encuentra en otro directorio, al cual sólo el super-usuario tiene permisos para accederlo, éste es un archivo encriptado. Se usa encriptación *one way* (en un sólo sentido), de manera que no es posible desencriptarlo.

3.4.3. Evaluación de la seguridad en las aplicaciones

Se evaluó la seguridad de las aplicaciones utilizadas en el corporativo, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de

las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

Se inició con la evaluación del *software*.

Software

En el corporativo hay cinco servidores, un servidor funciona como servidor de archivos FTP, otro se usa para el sitio Web de la página de la empresa, otro para aplicaciones y renta de sitos Web y uno más para correo electrónico. El servidor de aplicaciones Unix, el servidor de páginas Web y el correo electrónico tienen plataforma Solaris 8 instalada. Para los usuarios internos se tiene un servidor con Windows 2000. La seguridad en estos sistemas es la configurada por el administrador.

El 80% de las PCs usan el sistema operativo Windows 98, en el resto de ellas hay Windows 2000. No usan *software* comprado, a excepción de los sistemas: Microsoft Office, StarOffice, Norton Antivirus y demás utilitarios, conjuntamente con sistemas de facturación. La seguridad en estos sistemas es la predeterminada por su instalación.

Las aplicaciones específicas del corporativo están desarrolladas en Java de entorno gráfico, y se encuentran funcionando desde hace aproximadamente tres años.

Seguridad de bases de datos

En la empresa se utiliza el Oracle para el desarrollo y la administración de los datos, los cuales están almacenados en un sistema de archivos. Existe un control que restringe el acceso a ciertos datos críticos en las aplicaciones propias de la empresa, pero no hay una clasificación formal de estos datos.

Las únicas personas que pueden tener acceso a los archivos de la base de datos son los administradores y todo aquel que opere el servidor de aplicaciones (es decir las personas que tengan acceso físico al equipo).

Los aplicativos que administran la base de datos disponen de recursos suficientes para su funcionamiento, ya que aproximadamente sólo el 30% de los recursos del servidor están en uso, el resto está ocioso.

Cuando algún usuario elimina registros de una base de datos, éstos no se borran físicamente sino que son marcados como borrados. De esta forma siempre permanecen los registros de las transacciones realizadas.

Control de aplicaciones en PCs

No hay estándares definidos ni procedimientos a seguir, tampoco documentación respecto a la instalación y actualización de la configuración de las PCs. Sólo hay una instalación básica de alguna versión de Windows, Internet Explorer, Norton Antivirus y aplicaciones desarrolladas.

En el caso de que una PC presente errores en su configuración, se utilizan herramientas de reparación de errores, como el Norton Disk Doctor, con el fin de evitar la reinstalación total del sistema y así causar una pérdida innecesaria de tiempo.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer y el Microsoft Office. No se buscan Service Packs ni nuevas versiones. La política de actualización de programas que se lleva a cabo permite actualizar los programas sólo si es necesario debido a algún mal funcionamiento o nuevo requerimiento, lo que facilita la continuidad de los programas. Las únicas versiones que se actualizan y quedan documentadas son las de los programas desarrollados por la empresa, a pedido de algún departamento. Estas versiones se actualizan directamente en el servidor, lo que evita hacer el control en cada una de las máquinas.

Solamente los administradores del centro de cómputo son los encargados de las instalaciones en las PCs, aunque para los usuarios no existen restricciones con respecto a la instalación de programas. Pueden bajar de la Web cualquier aplicación e instalarla en su PC sin ningún control sobre las licencias ni autorización previa. Esto se debe a que, para controlar problemas de licencias, virus o programas no permitidos, no hay ninguna herramienta en uso ni se realizan auditorías internas periódicas. En una sola oportunidad fue necesario el registro *on line* de un aplicativo de emisión de correos que solicitó la gerencia.

Cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de las modificaciones.

Después de la evaluar el punto anterior, se procedió de igual forma con el control de datos en las aplicaciones.

Control de datos en las aplicaciones

En las aplicaciones desarrolladas en la empresa se implementan controles en los datos de entrada y de salida, que aseguran su integridad, exactitud y validez.

Con respecto a los datos de salida se deshabilitan los portapapeles, se restringen las impresiones en ciertos sectores de la empresa (ventas) y de cierta información confidencial, se deshabilita la barra de herramientas de manera que no se puedan grabar ni imprimir los datos, se deshabilita el menú contextual (surgido del botón derecho del *mouse*), lo que sólo permite que la información sea leída.

Se utiliza un programa gratuito, cuya función es sincronizar la fecha y hora de cada una de las PCs de la red cada un minuto, de acuerdo al horario del servidor. De esta forma los *logs* y los datos siempre se generan con la fecha del servidor.

Ciclo de vida del desarrollo de *software*

El corporativo cuenta con aplicaciones propias desarrolladas para cada uno de los sectores que la componen, por su grupo de programadores internos. Este desarrollo no sigue una metodología estándar, pero se usa la misma nomenclatura para denominar variables, tablas, parámetros, etc. Durante el ciclo de vida no se priorizaron los requisitos de seguridad del sistema, debido a la urgencia que requería el proceso de reingeniería de sistemas.

Análisis: debido a que se trata de una reingeniería de sistemas, no se realizó un levantamiento de datos formal para el desarrollo. Los programadores tenían noción de los requerimientos y necesidades de los usuarios por el conocimiento del sistema anterior, y a éste se le mejoró implementando nuevas funciones que demandaban los jefes de cada sector.

Desarrollo: la implementación del sistema se está desarrollando en Java. Al comienzo del desarrollo se evaluaron las incidencias que podían representar los cambios en el sistema con respecto al sistema anterior, completándose así un análisis de riesgo preliminar. No se utilizaron métricas para la estimación ni durante el desarrollo.

Prueba: para verificación del sistema se generan casos de pruebas, donde se definen tablas con valores de entrada al sistema. Cuando se hacen modificaciones en los programas, los casos de pruebas que se usan sobre el *software* modificado son los mismos que se usaron antes, de manera de comprobar que los valores obtenidos en las últimas pruebas sean los mismos que los que surgieron de las primeras. Las pruebas se realizan por módulos, y al integrar los módulos se realizan pruebas de integración. Los resultados obtenidos en las pruebas son documentados en las carpetas relativas a cada uno de los módulos.

Instalación y modificaciones: una vez hecha la instalación, las únicas modificaciones que se realizan son a pedido del gerente del área correspondiente, pero sin la implementación de un formulario de solicitud de cambio. Antes de hacer las modificaciones solicitadas, se confecciona un análisis de riesgos, considerando el impacto que puede provocar el cambio, con el fin de decidir la implementación del mismo. No se lleva a cabo ningún control de versiones ni gestión de configuración de las modificaciones.

Documentación: cada módulo desarrollado posee una carpeta con diagramas y documentación sobre él mismo. Se han desarrollado manuales para el área de Gestoría y para el sector de Ventas de la empresa, aunque todavía no están confeccionados los manuales para la totalidad de los módulos. Una meta del equipo de desarrollo es documentar el sistema en su totalidad, e incluso modificar los manuales existentes para generar un manual de usuario completo que englobe todo el sistema de la empresa.

Terceros: con respecto a la participación de terceros en el desarrollo, existió un único caso, que consistió en el desarrollo de una página Web dinámica, implementada por un programador externo. Ésta fue entregada al corporativo, con su código fuente desarrollado en PHP, junto con los manuales de uso.

La página Web fue diseñada para que todo el mantenimiento pueda desarrollarse desde el interior de la empresa, a excepción de las modificaciones que se llevan a cabo en la estructura de la página. La página se modifica desde el servidor de Internet, con un administrador desarrollado en HTML para este fin. Esta página se encuentra *on line* en un *host* interno, lo que aumenta gran cantidad de riesgos a la empresa, debido a que permite que se reciba requerimientos del exterior vía Web, lo que podría atentar contra la integridad de los datos.

3.4.4. Evaluación de la seguridad física

Se evaluó el centro de cómputo, los equipos, los dispositivos, los medios de almacenamientos y se verificó que las personas que conforman el sistema informático del corporativo cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

La primera evaluación fue la parte del equipamiento.

Equipamiento

Características de los servidores

En el edificio corporativo existen:

- Servidores Sun 3500, comprados en el 2000. Un servidor funciona como servidor de archivos FTP, otro se usa para el sitio Web de la página de la empresa, otro para aplicaciones y renta de sitos Web y uno más para correo electrónico. Para la red de PCs se cuenta con un Servidor Compaq Proliant DL760.

Adicionalmente, los servidores cuentan con sistemas de suministro alternativo de energía UPS (Uninterruptible Power Supply, Fuente de Alimentación Ininterrumpida).

Características de las PCs

La empresa en su totalidad posee alrededor de 350 PCs, de las cuales 300 están en el edificio del corporativo. El 100% de estas PCs es de marca Dell GX1. La empresa ha tomado la decisión de asegurar su red, debido al gran costo que implicaba contratar un mantenimiento permanentemente por parte de terceros.

Control de acceso físico al centro de cómputo

En el momento de la instalación del centro de cómputo, en este caso un NOC (Network Operation Center, Centro de Operación de Red), no se efectuó un análisis de costo-beneficio para determinar que controles de acceso físico sería necesario implementar. Existe un circuito cerrado de cámaras de video. Este sistema no es exclusivo del NOC, ya que las cámaras están en toda el área administrativa del corporativo, ubicadas en puntos

estratégicos, como en la puerta de ingreso, pero ninguna de éstas cámaras apunta al centro de cómputo o a su puerta de ingreso.

La empresa cuenta con guardias de seguridad; en horarios laborales se ubican en el interior y exterior de la misma, y cuando se cierra el edificio corporativo sólo quedan en el exterior, porque queda activado el sistema de alarma. No hay tarjetas magnéticas de entrada ni llaves cifradas en ningún sector del edificio.

El personal de cómputo, administración y gerencia tienen el acceso permitido a la red corporativa y están en el mismo ambiente, separados del resto de la empresa por una doble puerta. Las demás áreas no tienen permiso de acceso. Esta doble puerta tiene la función de evitar el acceso físico de cualquier persona no autorizada, sin identificación previa. De manera que las personas que pretenden entrar deben permanecer entre dos puertas, ya que no se puede abrir la segunda si no se cierra la primera, a partir de ahí un encargado debe autorizar el acceso mirando por un circuito cerrado de televisión.

Por más que siempre hay personal de sistemas en el interior del NOC, cualquier persona ajena a la empresa que necesite realizar una tarea de mantenimiento relativa al NOC deberá anunciarse en la puerta de entrada. El personal del NOC es el encargado de escoltarlo hasta el edificio, acompañándolo durante el tiempo que permanezca ahí.

El siguiente punto evaluado es el control de acceso a equipos.

Control de acceso a equipos

Todas las máquinas de la empresa disponen de unidad para *floopy* y manejadores de CDs, aunque el 90% de los usuarios no las necesita. Sólo algunas máquinas de administración que reciben disquetes deben utilizarlas como medios de entrada de datos, a pesar de que se está empezando a utilizar Internet para el intercambio de información.

Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe inicializar desde estos dispositivos. Nunca hubo robo de datos usando medios externos, sólo fue necesario hacer bloqueos de las impresoras para restringir los datos de salida del sistema, previniendo posibles fraudes. En el centro de cómputo hay unidades *zip* no utilizadas, guardadas sin llave ni control de acceso adicional. Esto implica que podrían ser fácilmente robados, o cualquier persona que disponga de los programas de instalación necesarios, podrá instalar dichas unidades en cualquier PC de la empresa.

Los *racks* donde se ubican los *switches* de cada una de las sucursales están cerrados con llave, para evitar que el personal de limpieza o cualquier persona desconecten las entradas, y como medida de precaución, debido a que hay contactos libres en estos dispositivos. Las llaves de todos los *racks* están en el centro de cómputo del edificio corporativo, en poder del administrador del sistema. Todos ellos están ubicados fuera del alcance del personal

No se realizan controles periódicos sobre los dispositivos de *hardware* instalados en las PCs, de manera que alguien podría sacar o poner alguno. Una vez que se ha completado la instalación de algún equipo, el administrador del sistema sólo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

Los servidores del centro de cómputo no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realizan trabajos, permanecen ociosos, debido a que no existen procedimientos en lote (todos los programas se ejecutan *on line*).

Dispositivos de soporte

En el corporativo se disponen de los siguientes dispositivos para soporte del equipamiento informático:

- Aire acondicionado y calefacción: la temperatura se mantiene entre 19°C y 20°C. Cuentan con un equipo de refrigeración central, y en el centro de cómputo hay un equipo adicional de aire acondicionado, sólo para esta área, con el fin de mantener ésta temperatura en verano. Estas especificaciones las sugirió el personal que provee los equipamientos.

- Extintores: son equipos químicos manuales y están instalados y mantenidos por una empresa externa, quienes deciden el lugar en que van a estar ubicados. El centro de cómputo cuenta con uno propio, ubicado en la habitación de los servidores.

- Alarmas contra intrusos: existe una alarma en la empresa que se activa en los horarios no laborables, generalmente de noche cuando se cierra la empresa.

- Generador de energía: en la empresa cuentan con un generador de energía debido a los frecuentes cortes de luz. Necesita de un breve tiempo de puesta en marcha, pero debido a que los cortes también son breves (5 minutos) pocas veces se utiliza.

- UPS: en el centro de cómputo hay dos UPS en serie, que pueden mantener los servidores y las máquinas de desarrollo funcionando por 2 horas.

- Regulador de tensión: la corriente eléctrica proviene de un tablero independiente que va a tres reguladores de tensión de donde salen tres líneas. Se dividió la carga eléctrica en tres sectores para un mejor funcionamiento: un sector abarca el centro de cómputo, y los demás usuarios de la empresa se reparten entre las otras dos líneas libres.

- Descarga a tierra: hay dos pararrayos, una para el edificio y otra para el centro de cómputo.

- Luz de emergencia: en el centro de cómputo hay una luz de emergencia que permanece en carga las 24 horas del día y en el caso de un corte de luz se activa automáticamente.

- Humidificador: este dispositivo existe para la biblioteca de cintas del NOC, pero no hay archivos en cintas por lo que no son necesarios.

- Piso aislante: el personal que suministró el equipamiento sugirió poner un piso aislante de goma, que se usaba para los centros de cómputo cuando las máquinas generaban mucha inducción, pero debido a que los dispositivos actuales no generan ese nivel de inducción, no fue necesaria esta protección.

Estructura del edificio

Cuando se construyó el edificio del corporativo, se tuvo en cuenta el diseño del NOC y sus condiciones de seguridad. Por este motivo se ubicó en el sector posterior del edificio, para restringir el acceso.

Las paredes externas del NOC son elevadas (aproximadamente 6 m.) y las ventanas tienen rejas soldadas y vidrios espejados que impiden la visibilidad desde el exterior del mismo.

En toda la empresa hay vidrios esmerilados, que dividen los sectores del área administrativa, por lo que sólo se ven los monitores desde el interior de cada área.

El equipamiento informático fue provisto por una empresa que se encargó del asesoramiento técnico. A estos proveedores les consultaron cuáles eran los requisitos mínimos necesarios para que las garantías cubriesen los equipamientos (la instalación eléctrica necesaria, la refrigeración correcta del área, los métodos de aislamiento magnético, etc.) Para determinar qué medidas tomar en la instalación se realizó un análisis costo – beneficio donde se decidió, por ejemplo, no implementar un piso falso en el centro de cómputo para el aislamiento, debido a que no representaba riesgo, y el costo era alto.

El centro de cómputo se diseñó pensando en su futuro crecimiento y actualmente sus instalaciones se encuentran convenientemente ubicadas, con la posibilidad de expandirse sin inconvenientes.

Cableado estructurado

La instalación del cableado fue realizada por terceros, con una garantía escrita. Para diagramar los canales de red se tuvieron en cuenta los posibles desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos.

Se implementó un techo falso, por donde tendieron el cableado, de fácil accesibilidad. Desde allí los cables pasan por las columnas del edificio, desde las cuales bajan hasta los perfiles de aluminio de los paneles y por éstos llegan hasta el suelo. Estos

paneles no son prácticos a la hora de hacer modificaciones en el cableado, debido a la cantidad de cables que pasan por ellos y al poco espacio con el que cuentan, pero resultaron económicos y son seguros porque no es fácil desarmarlos. Por este motivo, y para facilitar la tarea de agregar cables en el interior de los paneles, hay tendido de cableado redundante. Estos cables no tienen conectores instalados, pero sí están conectados al *switch*.

En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP, en cuyo caso se utiliza fibra óptica.

En los *switches* hay un contacto dedicado a cada máquina, y sobran varios para una posible ampliación de la red.

Para que no haya interferencias se utilizó cableado UTP categoría 5, fibra óptica para el *backbone* y enlaces DS0 para enlazar los centros de servicio.

Los cables en el panel de parcheo están numerados de manera que se les puede identificar fácilmente.

Cerca de cada máquina hay un contacto triple que tiene conectores para UTP, energía eléctrica y línea telefónica.

Todas estas líneas no producen interferencias debido a la calidad de los cables de red, y a que la línea eléctrica está regulada. Además, la empresa encargada de la instalación de la red midió la interferencia que hay en los contactos de red de las PCs encontrando que eran muy bajas y no representaban riesgos.

Falla en la red

Por norma, cuando hay un corte de luz se graban los datos y se deja de trabajar *on line*. Si el corte supera la media hora de duración, entonces apagan los servidores como una medida de prevención y si es necesario, se enciende el generador de energía. Mientras tanto, las tareas continúan realizándose en forma manual.

En el caso de un corte en el servicio de red por falta de energía o en el *switch*, el área más crítica sería la del sector que hace facturación en tiempo real.

3.4.5. Evaluación de la administración del área de sistemas

En esta parte se evaluó la correcta organización y administración del área de sistemas, así como la asignación de tareas y responsabilidades del personal que la conforma; a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo a las normas existentes que regulan esta actividad.

Dado que esta área involucra funciones como son la instauración de las soluciones de cómputo, necesarias para cubrir las necesidades de la empresa y de sus usuarios; la implementación y desarrollo de proyectos informáticos, y el desarrollo de planes de capacitación y documentación de las aplicaciones utilizadas, su evaluación se considera apropiada dentro de la auditoría.

Administración del NOC

Responsabilidad del equipo de sistemas

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general del área de sistemas, que es el administrador del centro de cómputo. Él es el que planifica y delega responsabilidades y tareas a los empleados del centro de cómputo, generalmente una vez por semana. Además del administrador, hay una persona dedicada al mantenimiento de la página y cuatro desarrolladores de aplicaciones específicas para el corporativo.

El administrador es el encargado de reportar a los gerentes sobre las actividades en el centro de cómputo. Estos reportes generalmente se realizan para cotejar que se cumplan con los objetivos encargados por éstos últimos.

Planes de sistemas

No se han desarrollado planes formales del departamento de sistemas, sólo se hace una distribución de tareas semanalmente entre el personal de esta área.

El perfeccionamiento de las aplicaciones específicas es el proyecto prioritario, luego tienen proyectos a futuro, como es la migración del sistema de archivos a una base de datos. Se van asignando prioridades a las tareas a medida que surgen. No hay normas, estándares o procedimientos en las que se basen para la planificación, el control y la evaluación de las actividades del área de sistemas de información.

Permisos de los encargados del centro de cómputo

Cuando entra un nuevo empleado al centro de cómputo, no se le asignan los mismos permisos que al resto de los empleados. A medida que le son asignadas más responsabilidades y sean necesarios más permisos, se va modificando su cuenta de usuario. Estos permisos son asignados por el administrador del centro de cómputo.

Importancia de la seguridad

Los empleados de la gerencia y de los cargos más altos tienen plena conciencia de la importancia de la seguridad en la empresa, porque fueron ellos quienes propusieron los requerimientos que tiene actualmente el sistema, aunque pudimos comprobar que no siempre cumplen las disposiciones de seguridad impuestas. Los demás empleados de la empresa tienen conocimientos de las normas pero no siempre son conscientes de su importancia.

Un aspecto importante a considerar son las ventanas de mantenimiento.

Mantenimiento e inventario

Mantenimiento preventivo: en este momento en el centro de cómputo no se desarrolla ningún mantenimiento preventivo, debido al costo de contratar personal que se dedique a esto, ya que los empleados del centro de cómputo están encargados de actividades de mayor prioridad para el corporativo.

Clasificación de datos y *hardware*: los equipos de la empresa no han sido clasificados formalmente según su prioridad, aunque se puede identificar que las máquinas que están en el sector de facturación tienen mayor prioridad. Le siguen las de la administración, y por último el resto de las PCs.

Rótulos: no hay procesos para rotular, registrar y dar de baja un equipo, sus periféricos o los medios de almacenamiento, sólo las licencias de *software* están registradas. Las máquinas y dispositivos no se identifican entre ellas aunque hay un inventario de la cantidad de máquinas que existen pero no tiene detalles suficientes.

Comunicación con el usuario

Publicidad de normas: normalmente los avisos cotidianos o de rutina se hacen a través de correo electrónico. Para el anuncio de una nueva norma o la modificación de un procedimiento existente se emplearía la misma metodología que en la capacitación de los usuarios, con correos informativos y reuniones.

Boletín informativo: en la empresa utilizan un boletín informativo que se emite sin frecuencia fija, que es utilizado cada vez que es necesario informar al usuario de las tareas de mantenimiento que se deben realizar en sus equipos, por ejemplo, actualizar el antivirus, hacer copias de respaldo de sus datos, desfragmentar el disco, modificar y proteger sus contraseñas, borrar archivos temporales, entre otras.

Solicitud de asistencia: cada vez que los usuarios necesitan asesoramiento o servicios del centro de cómputo, se comunican con el administrador explicando su situación. No queda ninguna constancia de las tareas desarrolladas por los empleados del centro de cómputo, ni de las solicitudes de los usuarios.

Buzón de sugerencias: no han implementado un buzón de sugerencias donde los usuarios puedan expresar sus inquietudes.

Programas de instalación

Los programas de instalación de las aplicaciones utilizadas en la empresa se encuentran en sus CDs originales, almacenados en un armario del centro de cómputo, y no se disponen de disquetes de instalación. Los de uso más frecuente, como los del Norton Antivirus o del Acrobat Reader, están *on line* en el servidor y se instalan desde carpetas

compartidas. Otros igualmente utilizados, como las distintas versiones de Windows, se ejecutan desde copias, para evitar posibles daños en los discos originales.

Licencias

Como ya se describió en la parte de mantenimiento e inventario, en el centro de cómputo se mantiene un registro de los números de licencia de las aplicaciones instaladas en las PCs y los servidores de la empresa. Los programas de los que se disponen licencias son los siguientes: Windows 98 y 2000, Microsoft Office y StarOffice, Norton Antivirus Corporativo e IncrediMail. El resto de las aplicaciones son propietarias, por lo que no necesitan de licencias, o son gratuitas como el Acrobat Reader.

Capacitación

Cuando ingresa un empleado nuevo a la empresa se le capacita en el uso del sistema, de la misma forma en que han sido capacitados los empleados anteriores. El encargado del departamento de sistemas enseña al empleado nuevo el funcionamiento del sistema. Se le instruye sobre consideraciones de seguridad, como es el no usar contraseñas fáciles de descifrar, no divulgarlas, escribirlas o guardarlas; entender que la administración de contraseñas es el principal método de seguridad del sistema; no modificar la configuración de las PCs (configuración de red o del sistema) o no abrir correos con asuntos ni de destinos desconocidos.

Esta explicación la da el administrador del sistema junto con dos personas del equipo. Una vez que ha sido instruido con una capacitación teórica, un empleado del departamento de sistemas se sitúa junto con el usuario en el puesto de trabajo, para asistirlo hasta que adquiera práctica, comprobando que el manejo del sistema sea el adecuado.

A los usuarios en ningún momento se les explica que el corporativo no solicita autorización para auditar sus actividades en el sistema, ni declaraciones que indiquen su conocimiento de las normas de "buen uso" del sistema, en caso de incurrir en violaciones a las mismas.

Copias de seguridad

Copias de seguridad en el servidor

Cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de estas modificaciones. No hay ningún procedimiento formal para la realización ni la recuperación de las copias de seguridad. Además no se realizan chequeos para comprobar que el funcionamiento sea el correcto.

Los respaldos se hacen diariamente. Es un proceso que no está automatizado, por lo que todos los días, antes de finalizar sus labores, cada desarrollador copia los archivos de las aplicaciones en desarrollo que ha modificado durante el día a una carpeta del servidor de aplicaciones. Luego se agregan los archivos de la empresa modificados por los usuarios.

Una vez generada esta carpeta, el administrador del sistema la comprime y copia este archivo a una cinta, proceso que demora 1 hora aproximadamente.

Los respaldos mencionados son incrementales, es decir que se agregan a la carpeta los archivos modificados y se copia todo lo que ésta contiene. Debido a que se realizan estos tipos de respaldos incrementales, es imposible recuperar versiones antiguas de aplicaciones desarrolladas y luego modificadas, ya que se sobrescriben con las versiones nuevas.

Para realizar el respaldo se utilizan cinco cintas, uno para cada día hábil de la semana, y se regraba la cinta que corresponde a ese día. Las cintas usadas en la empresa no han sido reemplazadas por otras nuevas. No hay políticas de reemplazo de estos medios de almacenamiento, ni se les realizan controles para comprobar que están en buen estado y que su funcionamiento sea el correcto. Aunque generalmente el responsable del área o administrador del NOC realiza los respaldos, es una actividad ajena a sus funciones. Tampoco hay alguna política en cuanto a asignar un responsable para la restauración de los datos de los respaldos, esta tarea también la realiza el administrador.

Respaldo de datos en las PCs

Es responsabilidad de los usuarios realizar sus propios respaldos de los datos almacenados en sus máquinas. Debido a que los archivos que almacenan son de soporte o de poca importancia para la empresa, generalmente no lo hacen.

Los usuarios han sido instruidos a almacenar en la carpeta "Mis Documentos" todos los datos que ellos generen. Si hacen un respaldo deberían hacerlo en sus propias máquinas o en disquetes, aunque hay un usuario que tiene asignado un espacio del servidor para guardar allí sus copias de respaldo, debido a que sus datos son más sensibles. Este respaldo se realiza a través de un archivo .bat que copia sus datos al servidor.

Respaldo de la página Web

El administrador del sistema realiza un respaldo de la página Web completa pero sin una frecuencia preestablecida.

Respaldo de logs

No se hace ningún respaldo de los *logs* generados por las diferentes aplicaciones del servidor, sólo los almacena y se depuran mensualmente.

Protección de los respaldos

Los archivos respaldados no están protegidos con ningún control de acceso ni encriptación. Esta situación puede resultar peligrosa ya que estos archivos contienen las bases de datos de la empresa y, ante cualquier incidente o extravío de los mismos, es fácil recuperar los datos en su formato original.

Documentación del respaldo

No hay documentación escrita sobre los datos que se respaldan, dónde se hace esta copia, ni datos históricos referidos a la restauración de los mismos.

Documentación

Documentación del NOC

En el NOC existe documentación sobre licencias del *software* y en qué máquinas está instalado, números IP de las máquinas y de los *switches*, planos de la ubicación de los canales de red desarrollados por la empresa que instaló la red, gráficos de la ubicación física de los equipos de los distintos centros, inventario de insumos y documentación del desarrollo del sistema.

No hay respaldos de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

Manuales de procedimientos

No hay ningún plan de contingencia a seguir, ni un plan de continuidad. No hay desarrollado algún plan de seguridad ni procedimientos formales. Se comenzó a desarrollar un manual de usuario para las aplicaciones específicas del corporativo pero se completó sólo el 30% del mismo, y ahora ha quedado obsoleto. Está en los planes del administrador del centro de cómputo retomar esta actividad.

Documentación sobre actualizaciones

Existe una carpeta con diagramas y documentación referente a cada módulo del sistema utilizado, y allí se registran los cambios que se producen durante el uso del mismo. Estos registros se generan durante las etapas de desarrollo y mantenimiento, pero no se actualizan los demás documentos o manuales cuando se hace una modificación del sistema, de manera que el cambio sólo queda registrado en papel.

3.4.6. Auditorías y revisiones

En esta sección se evaluaron las metodologías de control, auditorías internas y revisiones que se llevan a cabo en forma periódica, con el fin de encontrar debilidades y proponer mejoras, con base en las normativas que regulan el buen desempeño de la auditoría interna en una Organización.

Verificaciones del sistema

Herramientas de generación y administración de logs

Las siguientes aplicaciones o sistemas generan *logs* de auditoría:

- El *kernel* del sistema operativo de los servidores.
- El antivirus y el *proxy* del servidor de Internet.

Para graficar los *logs* de auditoría, se utiliza una aplicación llamada WebTrends. Ésta lee los *logs* generados por las distintas aplicaciones cada cinco minutos, calcula las estadísticas y, cuando se llama al programa, grafica estos valores. Este programa no consume gran cantidad de recursos.

Todos los registros (del sistema operativo, del *proxy* y del antivirus) se almacenan durante tres meses, y la aplicación WebTrends se encarga de hacer la rotación mensual y eliminar los *logs* del mes saliente. Los chequeos de *logs* se hacen manualmente, ya que no hay una aplicación de administración de *logs* que genere reportes, ni hay alarmas en el sistema que avisen al administrador de la ocurrencia de un evento en particular.

Todos los logs contienen los siguientes campos:

- Fecha y hora.
- Fuente (el componente que disparó el evento).
- ID del evento (número único que identifica el evento).
- Computadora (máquina donde se produjo el evento).
- Descripción (datos asociados con el evento o mensajes de error).

Logs de los servidores

El *kernel* de Unix monitorea los servidores, generando, entre otros, *logs* sobre los servicios de *mail*, de red, configuración, utilización del CPU y reinicio de servidores. No se han buscado nuevas herramientas de generación ni gráfico de *logs*, por falta de tiempo.

Línea de base

Existen estadísticas de red generadas por el WebTrends en forma diaria, semanal, mensual y anual, con datos sobre tráfico de red, cantidad de archivos abiertos, uso de memoria, uso del disco y uso del *swap*. Todos estos datos no generan una línea de base ya que no están almacenados como tal, sino que son datos estadísticos no persistentes calculados por el WebTrends para realizar los gráficos.

Al hacer alguna modificación en la configuración del sistema, se genera una nueva compilación de datos (nueva línea de base), que no queda documentada. Esto se presta a confusiones, ya que no se identifica si ha habido algún incidente o si la variación se debe a cambios realizados en el sistema.

Auditorías internas

En la empresa no se realizan auditorías programadas, ni rutinas de chequeos de *logs*, debido a que la política actual de la empresa es realizar controles sólo cuando se presentan problemas o ante necesidades puntuales.

Responsabilidades de los encargados de seguridad

El encargado del centro de cómputo realiza las siguientes actividades:

- Administra, desarrolla e implementa los procedimientos de auditoría y revisión.
- Monitorea y reacciona a los avisos y reportes.
- Realiza chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
- Revisa los reportes de auditorías o *logs* cuando es advertido de anomalías.

El encargado del mantenimiento de los servidores determina qué *logs* se generan, qué eventos de seguridad se auditan y qué datos se recogen. Además se encarga de buscar nuevas herramientas que faciliten la auditoría.

Un punto necesario en la evaluación es el procedimiento con el que se lleva a cabo el control de acceso a los diferentes elementos que involucran la red corporativa.

Auditorías de control de acceso

Control de acceso a logs

Los *logs* se almacenan en el servidor de aplicaciones y en el de Web, por lo que cuentan con el control de acceso físico al servidor, pero no hay ningún control de acceso lógico a las carpetas donde están almacenados. Éstos pueden ser accedidos desde cualquier máquina conectada a la red, conociendo la clave de administrador, a través del WebTrends.

Control de acceso a Internet

Con respecto a las conexiones a Internet, existen registros con información sobre el número IP de la máquina conectada y la dirección de las páginas visitadas.

Modificación de datos

El sistema operativo genera *logs* indicando qué datos se han modificado y en que momento, pero estos no son analizados por los administradores, sólo se almacenan y se borran periódicamente. Existen *logs* sobre la mayoría de los movimientos de los usuarios en el sistema de la empresa, generados por Windows, en lo que se refiere a acceso a archivos abiertos y modificados. Esta aplicación genera reportes sobre qué máquina es ingresada, la hora a la que ingresa, a qué archivos accede y la hora a la que se desconecta, pero no contiene datos sobre el usuario que se está conectando.

Cambio de contraseña

No se generan *logs* cuando un usuario modifica su contraseña, no se guardan las contraseñas anteriores (para evitar la repetición), no se determina que aplicación se ha usado para realizar el cambio ni, en caso que el cambio resulte fallido, el motivo del fallo.

Logs del administrador

No se examinan periódicamente para verificar que no hayan sido alterados por intrusiones, o que registren algún tipo de problema.

Login fallido

Tanto el *login* exitoso como el fallido generan un *log* en Windows. El *log* no especifica el motivo del fallo, sólo se identifica que hubo un error de conexión.

Bloqueo de un usuario

La única manera de bloquear un usuario es porque ingresó mal la contraseña dos veces consecutivas, pero no se genera un registro de este evento, sino que el usuario debe avisar al administrador del sistema.

Perfil de usuario

Con los *logs* que existen en la empresa sería posible generar perfiles de los requerimientos de cada usuario, pero no se hacen estas tareas y los datos se encuentran en bruto sin analizar.

Logs de impresión

En la empresa hay impresoras en red, por lo que las impresiones no se ejecutan en impresoras locales. No hay generación de *logs* cuando se requiere una impresión de algún dato suministrado por el sistema de la empresa.

Auditorías de las comunicaciones de red

Reportes de correo

De los *logs* del correo no se calculan estadísticas, no se sacan líneas de base ni se grafican. El administrador sólo los lee cuando supone que puede haber algún problema, a solicitud de los usuarios, por una supuesta falla en el servicio de correo. En el caso que se llene el espacio en disco de alguna cuenta, se envía un correo indicando el problema, pero no se emiten alarmas ni se generan *logs*.

i-Planet genera *logs* del tráfico de correo, aunque estos no se leen ni auditan. Estos *logs* se guardan durante 30 días y se eliminan mediante la rotación de *logs*. En la ocasión en que no se realizó la rotación correctamente, los *logs* del i-Planet superaron los 2 Gb de datos, por lo que fue necesario que el administrador los borrara manualmente.

En estos *logs* se almacena el cuerpo del correo completo, pero no se guardan los archivos adjuntos, sólo es posible consultar si contenía o no archivos, y los nombres de los mismos. No se generan estadísticas sobre qué departamento o usuario de la empresa utiliza más el servicio de *mail*, o si a algún usuario le llega más correo que la cantidad promedio,

aun cuando en los *logs* figuran los datos del usuario necesarios para realizar dichos cálculos.

El antivirus (PC Cillin) genera *logs* con datos sobre el correo entrante y saliente, la hora de envío, el contenido y asunto del correo, archivos adjuntos, reporte de virus de cada parte del mensaje, máquina destino y fuente y direcciones IP de estas máquinas. Estos reportes se almacenan durante 15 días.

Estadísticas de red

Existen, como citamos anteriormente, gráficos sobre el tráfico en la red, proporcionados por el programa de administración de red denominado WebTrends. Pero no existen datos detallados sobre el consumo de ancho de banda por terminal ni por sector de la empresa, de manera que se tenga la posibilidad de individualizar cuál de las terminales usa más tráfico de red o en qué parte de la línea el tráfico es más intenso. Sólo existen datos indicando la cantidad de bytes entrantes y salientes, pero no se detalla desde dónde se generan, ni con qué aplicación (*mail*, datos, aplicaciones, mensajes, Internet, etc.).

El Proxy utilizado genera *logs* muy detallados, con datos sobre las páginas visitadas, el usuario, los horarios de entrada y salida, aunque no se generan reportes con datos relativos a los archivos descargados desde Internet. Esta aplicación tiene la capacidad de generar gráficos con los *logs*, aunque no se utiliza.

Tampoco existen reportes sobre las aplicaciones utilizadas por cada usuario, ni las prioridades de estas aplicaciones con el fin de discriminar qué cantidad de tráfico generan. Sería útil para ver qué aplicación usa más recursos, y restringir en el caso que sea necesario.

No hay datos estadísticos de los intentos de ataques. Cada vez que ocurre uno desde el exterior de la empresa el sistema operativo envía un *mail* al administrador advirtiendo de esta situación. Tampoco se hace ningún seguimiento de los *logs* en busca de cambios en las estadísticas, como puede ser el incremento en el uso de Internet, en los ataques o en la modificación de los permisos.

3.4.7. Evaluación del plan de contingencias

En este apartado se trató de determinar cuáles son los activos con mayor nivel de impacto y más vulnerables de la empresa, con el fin de asesorar en el futuro un posible desarrollo de un plan de contingencia y de continuidad de servicios críticos, teniendo en cuenta los riesgos más probables y considerando las distintas soluciones posibles.

Plan de administración de incidentes

En la empresa no hay planes formales para la administración de incidentes, como planes de contingencia, de recuperación de desastres o de reducción de riesgos. Pero se dispone de respaldos de *hardware* y de servicios que prestan terceros para garantizar la

continuidad de los servicios ante alguna contingencia. Estos terceros son una aseguradora y personal técnico especializado de mantenimiento.

Actualmente las emergencias son administradas por el encargado del centro del NOC, aunque no hay responsabilidades formales asignadas a los empleados. Existen tres personas que generalmente se distribuyen las tareas a medida que se presentan, y esto se realiza sin ninguna planificación.

Respaldo de equipamiento

Equipamiento de los servidores

En cada servidor existen 3 discos duros con tecnología SCSI (Small Computer System Interface, Interfaz Pequeña para Sistemas de Computadoras), donde cada uno de ellos tiene una capacidad de 18 Gb. Uno de ellos trabaja como disco raíz o de sistema, un segundo disco funciona como disco espejo del primero, y el tercer disco es de respaldo (este disco no contiene datos). Para los sistemas que requieren mayor almacenamiento de datos, se tiene un arreglo de disco externo SCSI adjunto a estos sistemas.

Los discos internos son del tipo "*hot swap*", es decir que pueden reemplazarse mutuamente sin la necesidad de reiniciar el equipo. Con esta metodología pueden caerse hasta dos discos simultáneamente, sin inconvenientes para el funcionamiento del sistema, y al reponer el disco que falta el servidor actualiza los datos automáticamente.

El servidor de Web, ante una contingencia, puede funcionar como servidor de aplicaciones, ya que sus estructuras físicas son idénticas. De esta manera es posible cambiar los discos duros y el servidor de Web se convierte en el servidor de aplicaciones. Además el servidor de Web posee un respaldo de los datos del servidor de aplicaciones. Esta copia se actualiza con un proceso del sistema operativo cada hora. Este proceso no funciona en sentido inverso, es decir que el servidor de Web no está respaldado en el servidor de aplicaciones.

En el caso de una falla de disco, sólo es necesario sacar el disco dañado del servidor y cambiarlo por el disco espejo correspondiente, ya que existen 2 discos iguales de sistema operativo.

Se realizaron pruebas de esta configuración cuando se instaló el sistema operativo por primera vez. Estas pruebas demoraron 4 minutos y sus resultados fueron satisfactorios; después de éstas no se realizaron pruebas posteriores.

Equipamiento de red

No hay respaldo de *hardware* debido a que ésta red se encuentra asegurada, de manera tal que ante una contingencia física en algún equipo, la aseguradora garantiza la reparación o el reemplazo del dispositivo. Se optó por esta alternativa basándose en un análisis costo / beneficio que abarcó la totalidad de la infraestructura de la empresa,

teniendo en cuenta los costos de implementación, mantenimiento, entrenamiento técnico del personal, y de restauración en caso de una emergencia.

NOC alternativo

Los datos de la empresa y los servidores se encuentran en la misma habitación física, ya que no hay ningún centro de procesamiento de datos alternativo, porque no se justifica esta inversión.

Estrategias de recuperación de desastres

Es muy importante para cualquier empresa de servicios de datos contar con las medias necesarias para la recuperación de su información o incluso de todo el equipo de cómputo como tal, es por eso que se enuncian las siguientes estrategias de recuperación en caso de ocurrir algún desastre.

Estrategia preactiva

En el caso en que se genere un plan de emergencia, el responsable del desarrollo e implementación del plan debería ser el administrador del NOC. En cada área de la empresa existe un líder que sería el jefe o encargado del área, debido a la responsabilidad que tiene en el grupo. Éste debería sugerir al Administrador las medidas de seguridad a implementar en el plan que requiera su sector.

Sistemas de información

No hay ningún responsable por la información de cada departamento, cada usuario es responsable de sus datos. Tampoco están identificados todos los sistemas de información, a modo de inventario, contemplando sus características principales, de manera que no es posible asignarles prioridades y así determinar qué sistema es más importante a la hora de recuperar la operatividad luego de un desastre.

Equipo de cómputo

No hay inventarios de los equipos de *hardware* ni de *software*, ni documentación con respecto a los equipos de la red física, de manera que no se les asigna un orden de importancia. Pero en el caso de necesitar restaurar las PCs, primero se deben asegurar las del sector de Ventas de las sucursales, las de la Gerencia, las del área de Sistemas, y las de Contaduría.

Establecimiento del plan de acción

En caso de una emergencia sería necesario desarrollar un plan de acción, en el cual el servidor de aplicaciones Unix sería el activo con mayor importancia al momento de continuar con las tareas, debido a que en él se encuentran los sistemas propios de la empresa y sus datos. Todos estos sistemas tienen la misma prioridad en el caso de una

contingencia, aunque existe una alternativa manual para el desarrollo de todas las actividades. En el caso de los datos, los activos más críticos a proteger serían:

- Base de datos, datos compartidos, documentación del NOC y de los sistemas.
- Programas fuentes y ejecutables del sistema de la empresa.

En el caso del *hardware*:

- Servidores, *switch* central y *switches* de las sucursales, equipamiento del NOC y canales de fibra óptica.
- Soporte físico de respaldos.

Definición de niveles críticos de servicio

Los servicios definidos como críticos por la empresa son: la atención personalizada a sus clientes en los diferentes centros de servicio en el país, los sistemas de facturación y los sistemas que poseen las aplicaciones de valor agregado (Correo Electrónico, FTP, Alojamiento de sitios Web entre otros). Por posibles contingencias con la red, en el caso que se demore o no haya continuidad el servicio, se disponen de consultas con las listas de precios físicamente ubicadas en las máquinas de atención al público; y para el área financiera y demás sectores existen procedimientos manuales para todas las actividades de la empresa. En el caso de la facturación no existe una contingencia viable hasta el momento.

No se hacen simulaciones de siniestros para el entrenamiento del personal. Sólo en el momento de instalar los servidores se hizo un simulacro de sustitución de discos, de manera de comprobar su funcionamiento.

Estrategia de acción

No hay funciones claras que debe realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas. Las situaciones se resuelven a medida que transcurren, sin la implementación de una norma a seguir formalmente documentada.

Estrategia reactiva

Una vez que ha ocurrido una contingencia, los encargados de evaluar los daños son los responsables de cada una de las áreas de la empresa, reportando a un miembro de la Gerencia que actúa como coordinador, el cual evalúa los resultados obtenidos al aplicar la solución.

Ejecución de actividades

Una vez ocurrido el siniestro, el administrador del sistema trata de llevar el sistema informático de la empresa a su funcionamiento normal, realizando las actividades de recuperación sin respaldarse en un plan o manual formal de procedimientos.

Retroalimentación del plan de acción

No hay un plan de acción a seguir, pero se toman acciones correctivas una vez que ha ocurrido una emergencia, de manera de evitar la misma contingencia en el futuro y mejorar la eficacia de las directivas. Una vez que han ocurrido los desastres no se genera documentación con respecto a las modificaciones implementadas ni a las acciones correctivas que se llevaron a cabo.

Realizado el análisis de la información, se generó una serie de recomendaciones, en donde se muestran cuales fueron las debilidades halladas y cuales son las sugerencias que pueden implementarse ante la ausencia o falla en los controles para el tratamiento de la seguridad de la información.

3.5. RECOMENDACIONES

En el presente trabajo se muestran las debilidades que fueron encontradas durante la etapa de análisis, así como las sugerencias que pueden implementarse ante la ausencia o falla en los controles para el tratamiento de la seguridad de la información. Se sugiere tomar medidas correctivas, preventivas o simplemente efectuar las recomendaciones para el mejoramiento de la seguridad de la red corporativa.

3.5.1. Seguridad lógica

Mencionaremos las debilidades encontradas en la identificación, autentificación y contraseñas.

Identificación de usuarios

Debilidad: durante el proceso de auditoría pudimos comprobar que la identificación de los usuarios (IDs) en el sistema, que debería corresponder a sus propios números de contrato, no existían como tales, sino que eran generados al azar por el administrador del sistema.
Efectos: esto genera un inconveniente en el usuario al momento de memorizar su ID de acceso al sistema, provoca errores de inconsistencia con la base de datos de recursos humanos y dificulta la manipulación de datos de usuarios en el sistema.
Recomendación: se podría comprobar con la tabla de personal que el número de contrato existe, o bien se recomienda implementar otro sistema de identificación de usuarios, donde se manejen usuarios universales con caracteres alfanuméricos.

Debilidad: durante la inspección de auditoria verificamos que algunos usuarios no tenían asignado un grupo de trabajo o un perfil bien definido dentro de la empresa, dejando este campo vacío en la base de datos.
Efectos: esta situación genera problemas en la identificación del sector de la empresa al que pertenecen los usuarios, ya que en el caso de que el campo esté vacío, el sistema considera que el usuario no tiene restricciones y le da acceso completo a los datos. Esto genera una falla en la confidencialidad y posible divulgación de datos.

Recomendación: deberá tenerse en cuenta que no puede existir el valor NULL en el campo "grupo" de los datos de usuario, ya que de él dependen los futuros permisos que se le asignen.

Debilidad: existen usuarios en el sistema para los cuales no estaba asignada una fecha de expiración de su contraseña.
Efectos: el principal problema de esta situación consiste en que el usuario no es obligado, en ningún momento, a modificar su clave de acceso, de manera que se facilita su revelación o robo.
Recomendación: el sistema no debe permitir que el campo donde se ingresa la fecha de expiración de la contraseña sea nulo, ya que de él depende el requerimiento de cambio de contraseña.

Debilidad: cuando un usuario ingresa dos veces mal la contraseña de ingreso, éste usuario es bloqueado por el sistema y el administrador debe desbloquearlo.
Efectos: es posible que el usuario olvide o confunda sus contraseñas, de manera que puede ingresar erróneamente la clave varias veces y bloquearse su cuenta en repetidas oportunidades, lo que genera molestias en el administrador y en el propio usuario.
Recomendación: suponemos que el sistema puede resultar más eficiente si el número de intentos fallidos se incrementa a cinco, así se generarían menos bloqueos de usuarios y menores interrupciones a las tareas del administrador.

Debilidad: no hay en la empresa un procedimiento formal para efectuar las bajas de los empleados del sistema.
Efectos: es posible que los empleados próximos a desvincularse de la empresa (cualquiera sea el motivo de esta situación) emprendan acciones de vandalismo o sabotaje, por rechazo o insatisfacción con esta decisión, o bien para beneficios personales.
Recomendación: sería conveniente que el área de Recursos Humanos de aviso al administrador del sistema, con un período de tiempo previo al despido, de esta manera es posible llevar a cabo una política de desvinculación del personal, a través de la cuál se quitan permisos al usuario en forma periódica. Con esto se disminuye el riesgo de vandalismo por insatisfacción con la decisión de la empresa.

Debilidad: no se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.
Efectos: es posible que, por error, negligencia, fraude o algún otro motivo, la cuenta o los permisos de algún usuario sean modificados, permitiendo que usuarios no habilitados accedan a datos que no le están permitidos.
Recomendación: periódicamente sería conveniente controlar las cuentas de usuarios, verificando que:

- Estén activas sólo las cuentas necesarias.
- No se hayan creado ni borrado cuentas.
- Los datos del usuario sean consistentes.
- Los permisos que le corresponden son los que tiene asignados.
- Las contraseñas no estén expiradas y hayan sido cambiadas periódicamente.

Debilidad: no existe en el sistema una lista de control de acceso, esto imposibilita relacionar los usuarios con los datos que les es posible acceder, y qué permisos tienen sobre estos datos (lectura, escritura, modificación, borrado).
Efectos: la ausencia de esta relación dificulta la verificación de las acciones, de manera que resulta complicado identificar los permisos de los usuarios con respecto a los datos, archivos y carpetas del sistema, en el caso que sea necesaria una auditoría o revisión de la actividad particular de un usuario.
Recomendación: recomendamos la generación de una lista de control de acceso donde se identifiquen a todos los usuarios habilitados en el sistema, los datos a los que pueden acceder y los tipos de permisos que los usuarios poseen sobre los mismos. Con esta herramienta sería posible personalizar perfiles de usuarios, que no dependan exclusivamente del grupo al que pertenecen. Esta lista de control de acceso debería almacenarse en el servidor de aplicaciones cifrada, de manera que los permisos de los usuarios no sean revelados a personas no autorizadas, y así evitar la posibilidad de una modificación no autorizada. Con esta configuración puede utilizarse una herramienta que genere automáticamente los accesos directos a los programas de acuerdo a cada usuario en particular al momento del ingreso.

Debilidad: los accesos directos a los que el usuario tiene acceso los genera el administrador del sistema a mano, una vez que el usuario fue dado de alta.
Efectos: esta acción puede resultar poco práctica e ineficiente, debido a que una posible equivocación del administrador del sistema implicaría que usuarios no autorizados accedan a menús y datos que no le están permitidos. Además podría ocurrir que otra persona genere estos accesos directos (de la misma manera que lo hace el administrador), con la misma consecuencia descripta anteriormente.
Recomendación: es recomendable que, una vez que el usuario se ha registrado en el sistema, éste cree (o haga visibles) los accesos directos que son necesarios de forma automática, de acuerdo al perfil que le corresponde a cada usuario.

Debilidad: no se tiene ninguna restricción horaria en el momento de permitir a un usuario la entrada al sistema.
Efectos: esta debilidad puede permitir que un usuario no autorizado intente ingresar al sistema en horario no laboral (por ejemplo, desde el exterior de la empresa), condición que se ve agravada por el hecho que los servidores no se apagan sino que permanecen prendidos las 24 horas del día.
Recomendación: debería discriminarse el horario en que puede ser utilizado el sistema informático de la empresa, de manera que las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan (debido a que diferentes grupos pueden tener diferentes horarios). Por ejemplo, durante las vacaciones, días feriados o ausencias temporales, las cuentas de usuarios deben desactivarse.

Debilidad: no se tiene en cuenta ninguna restricción con respecto al equipo desde donde accesa cada usuario al sistema.
Efectos: al no controlar el dispositivo físico desde donde los usuarios acceden a la red, puede ocurrir que alguna persona no autorizada tenga acceso a un equipo que no le corresponde, permitiéndosele ver información para la que no tiene autorización.

Recomendación: se deberá tener en cuenta la localización de la PC que intenta accesar, para así poder relacionar cada usuario con su propia PC, o con su propio grupo de trabajo, de manera que un usuario de ventas sólo podrá accesar desde alguna de las PCs del departamento de ventas y un gerente sólo desde su propia PC.

Debilidad: aunque el usuario permanezca un largo período de tiempo sin actividad, el sistema no ejecuta ninguna acción; los administradores sólo advierten a los usuarios sobre la necesidad de no dejar las máquinas con sesiones productivas abiertas. Esta situación pudo comprobarse también en los servidores.
Efectos: el peligro en el que se incurre con esta debilidad radica en la posibilidad de que un usuario autorizado entre al sistema y abandone su puesto de trabajo. Si otro usuario no autorizado tiene acceso físico a esta PC, éste último también tendrá acceso a datos que le están prohibidos. Esta situación se ve agravada si los equipos a los que se hace referencia son los servidores de la empresa, debido a que no sólo se tiene acceso a datos críticos sino también a opciones de configuración de los sistemas.
Recomendación: si el sistema permanece ocioso durante cinco minutos, el programa debería encargarse de cerrar la sesión. Cuando el usuario regrese, se debería solicitar nombre de usuario y contraseña nuevamente. Además, sería conveniente que las PCs utilicen algún protector de pantalla con contraseña. Estas recomendaciones se deben tener presentes en la administración de los servidores.

Debilidad: la sesión del usuario *root* permanece activa en los servidores durante las 24 horas. De esta manera la seguridad de los datos de la empresa que residen en el servidor sólo dependerá del acceso físico al equipo.
Efectos: cualquier persona que consiga ingresar al centro de cómputo podría acceder a los datos y a la configuración de los servidores.
Recomendación: el administrador sólo debería utilizar este usuario del sistema en caso que fuera necesario realizar alguna tarea que así lo requiera. Para las demás actividades debería contar con otro usuario, con menos privilegios y por lo tanto menos riesgoso.

Debilidad: los usuarios del departamento de ventas no son identificados en forma personal, sino que todos usan el mismo nombre y contraseña de ingreso al sistema informático.
Efectos: ante un posible error, fraude o robo de algún dato de este sistema, sería imposible identificar qué persona accedió a la información, en qué momento lo hizo, etc., es decir, que no pueden rastrearse las acciones de los usuarios en el sistema.
Recomendación: todos los usuarios deben poder identificarse en el sistema de manera única para así poder seguir los rastros a través de las bitácoras de auditoría que se generen.

Debilidad: no se eliminan los usuarios que vienen predefinidos en el sistema operativo, como las cuentas de invitado, estas cuentas permanecen en el sistema sin que ningún usuario las utilice.
Efectos: en el caso que una persona no autorizada conozca la existencia de estas cuentas puede llegar a utilizarlas para tener acceso al sistema operativo del servidor.
Recomendación: sería conveniente eliminar estos tipos de usuarios. No deben existir en el sistema más usuarios que los necesarios para la empresa.

Debilidad: en la empresa hay tres personas con el mismo perfil de administrador, cada una de ellas tiene una cuenta diferente con una contraseña determinada, pero a fines prácticos, los tres conocen todas las contraseñas de las demás cuentas.
Efectos: con este esquema de acceso se imposibilita rastrear las acciones de cada uno de los administradores, así no pueden asignarse responsabilidades ante un posible error.
Recomendación: no es conveniente que varias personas accedan a la misma cuenta de usuario. Por este motivo sugerimos que no se revelen las contraseñas personales, de manera que se puedan diferenciar a los tres administradores del sistema. Debería existir un administrador total del sistema (*root*); y sugerimos que la contraseña de super-usuario sólo sea conocida por el administrador del sistema. El segundo en responsabilidad (un super-usuario) tiene permisos iguales al anterior, con una restricción que lo imposibilita de borrar el usuario *root*. Además existiría una tercera cuenta de administrador, que tenga a su cargo un grupo de tareas de menor importancia y cotidianas del administrador. En caso de que falte el administrador (el super-usuario) por algún motivo, y el segundo requiera alguna tarea de mayor responsabilidad, este deberá recurrir a la cuenta de *root*. Una vez que esta cuenta ha sido usada, y el administrador retorna a sus tareas, deberá cambiar la contraseña de esta cuenta y guardarla de forma secreta.

Debilidad: el administrador puede ingresar al sistema desde cualquier terminal de la empresa, además de tener la posibilidad de abrir varias sesiones al mismo tiempo.
Efectos: esta situación resulta riesgosa ya que el administrador podría dejar por error una terminal con esta cuenta, lo que permitiría a cualquier usuario que acceda a esta terminal realizar cambios en los perfiles de usuarios y sus permisos, entre otras actividades.
Recomendación: Para evitar esta contingencia, el administrador debe poder ingresar solamente desde ciertas terminales, las que se encuentren en el centro de cómputo, y en una terminal específica y habilitada por cada sucursal. Para poder realizar el mantenimiento del resto de las PCs sugerimos que se cree una cuenta de mantenimiento donde el administrador tenga permisos que le permitan realizar sus tareas habituales.

Debilidad: el mantenimiento técnico especializado externo utiliza la misma cuenta del administrador para hacer modificaciones en los sistemas operativos de los servidores vía Internet, y una vez finalizado el mantenimiento el administrador del sistema no cambia la contraseña.
Efectos: esta situación resulta inadmisible, debido a que existe otra persona, ajena a la organización, que conoce la contraseña del administrador del sistema, de manera que se aumenta el riesgo de intrusión a los sistemas y divulgación o robo de datos. Si esta contraseña es utilizada a través de Internet, el riesgo se hace todavía más grande debido a la posibilidad de escuchas o intercepciones en la comunicación, que podrían resultar en el robo de la contraseña.
Recomendación: sugerimos que, para resolver esta situación, se cree una nueva cuenta de usuario para realizar el mantenimiento externo, con los permisos necesarios para dicha tarea. Una vez finalizado el mantenimiento, el administrador del sistema podría modificar la contraseña, de manera de evitar entradas no autorizadas. De esta manera, cada vez que sea necesario realizar un mantenimiento, el administrador del sistema debería proporcionar la nueva contraseña al personal externo. Esta cuenta, por la peligrosidad que enviste, debería ser verificada periódicamente por el administrador, comprobando las tareas que desde allí se realizan.

Autentificación

Debilidad: una vez que algún usuario ha logrado ingresar en el sistema se muestra solamente el nombre de usuario en la pantalla.
Efectos: si en una cuenta de usuario hubo un intento de intrusión, o se logró la intrusión, el usuario nunca se percatará de este ataque, como tampoco lo hará el administrador del sistema.
Recomendación: en una pantalla intermedia se podría indicar, para un control personal del usuario, la siguiente información:

- Nombre de usuario.
- Fecha y hora de la última conexión.
- Localización de la última conexión (Ej. número de terminal).
- Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

De esta manera el usuario puede llevar un control sobre sus conexiones. Esto es posible ya que toda esta información está guardada en la bitácora del sistema.

Debilidad: los datos de autentificación son almacenados y transmitidos sin ningún cifrado.
Efectos: al no existir encriptación en los datos de autentificación, puede ocurrir que alguien acceda al archivo de contraseñas del sistema de la empresa, y disponga de acceso a todas las cuentas de usuarios existentes y de esta forma no tendría ninguna restricción en el acceso a los menús del sistema. Al no cifrar durante la transmisión de datos, puede ocurrir que alguien intercepte el canal de comunicaciones, consiguiendo las contraseñas y nombres de usuarios en texto plano.
Recomendación: el archivo con los datos de usuarios del sistema debería almacenarse en un formato no legible, es decir encriptado, y almacenado en el servidor de aplicaciones en una carpeta protegida por una contraseña gestionada por el administrador. Además, sería conveniente que los datos de autentificación viajen encriptados a través de la red, durante toda la transmisión. El archivo que almacena las contraseñas de los usuarios no debería poder modificarse, solamente a través de la aplicación de gestión de cuentas. Otra opción que puede adoptarse es no desencriptar las contraseñas para su comparación cuando se realiza un ingreso, sino directamente comparar las contraseñas encriptadas en el archivo contra lo ingresado por el usuario.

Debilidad: en cuanto a los mensajes externos de la gerencia hacia los centros de servicio, que pueden revestir mayor importancia, podría utilizarse un sistema de firma digital.
Efectos: se reduciría la posibilidad de un ataque de Ingeniería Social, así como también contar con el beneficio del no repudio.
Recomendación: podría tenerse en cuenta la posibilidad de implementar un sistema de firmas digitales para así identificar fehacientemente al emisor; aunque esta recomendación sólo sería conveniente en ciertos mensajes, aquellos que la gerencia considere de mayor importancia.

Contraseñas

Debilidad: las contraseñas no tienen una longitud mínima requerida por el sistema, sólo tienen que respetar un largo máximo de 10 caracteres alfanuméricos.
Efectos: al no haber una longitud mínima, los usuarios pueden poner una contraseña de un sólo carácter (por ejemplo un espacio, o un sólo número) lo que las hace fácilmente descifrables, generando vulnerabilidades importantes en los datos que éstas protegen.
Recomendación: es necesario que exista un número mínimo de caracteres (6) que conforman las contraseñas. Además puede requerirse que dicha contraseña esté compuesta de datos alfanuméricos, numéricos y caracteres especiales.

Debilidad: no se realiza ningún control sobre las cuentas de los usuarios, para comprobar que cambian la contraseña asignada por primera vez.
Efectos: de ser así, el usuario permanecerá con una contraseña fácilmente descifrable, facilitando la divulgación de esta contraseña y el robo de datos.
Recomendación: es necesario que, cuando el usuario se ingresa por primera vez al sistema, éste lo obligue a modificar su contraseña, impidiéndole el acceso hasta que éste procedimiento no haya terminado con éxito. Esto se logra ingresando la fecha de expiración de la contraseña como vencida en el momento de realizar el alta de un nuevo usuario.

Debilidad: pudimos ver que la contraseña de un usuario era un número fácilmente imaginable.
Efectos: al ingresar al sistema con una contraseña fácilmente descifrable, es posible que los demás usuarios lo obtengan y accedan a datos que les están prohibidos.
Recomendación: Deberán considerarse herramientas para controlar que la contraseña no sea fácil de descifrar, como puede ser realizar comparaciones contra una lista de palabras reservadas, por ejemplo el nombre de la empresa, el nombre de cuenta del usuario, números o letras repetitivas, entre otras.

Debilidad: durante la auditoría pudimos comprobar que las contraseñas de acceso con el super-usuario *root* de los servidores son iguales.
Efectos: en una situación como ésta se incrementa el riesgo de divulgación y robo de datos, debido a que, si alguien tiene acceso a la contraseña en un servidor, también podrá accesar a otro con los permisos de administrador.
Recomendación: sugerimos que las contraseñas sean diferentes en los servidores, y que sean modificados con mayor frecuencia que las contraseñas de los usuarios.

Debilidad: no se controla si el usuario cambia su contraseña ingresando siempre la misma contraseña, simulando cambiarlo, pero éste ingresa nuevamente la clave que ha estado usando siempre.
Efectos: las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas, debido a que seguramente habrá más oportunidades de descifrarlas.
Recomendación: deberá controlarse que el usuario ingrese una clave nueva cada vez que la modifique, así como que las últimas 5 letras no se repitan. Esto puede hacerse utilizando una base de datos donde se acumulen las últimas cinco palabras que ha empleado cada usuario.

Debilidad: generalmente, las contraseñas no son actualizadas por los usuarios, permaneciendo iguales por largos períodos de tiempo, ya que tienen un plazo de expiración de 1 año.
Efectos: las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas por más usuarios, debido a que seguramente habrá más oportunidades de descifrarlas.
Recomendación: consideramos que el período de vigencia de las contraseñas no debería ser tan largo, suponemos que sería conveniente utilizar una de 4 meses.

Debilidad: cuando un usuario olvida su contraseña o es bloqueado por el sistema, recurre al administrador, el cual lee la contraseña del usuario (en el sistema de gestión de cuentas de usuario), recordándoselo. Pero en ningún momento se le invita a modificar la contraseña revelada.
Efectos: en esta situación el administrador del sistema conoce la contraseña del usuario, lo que genera divulgación de información innecesaria. Esto se agrava cuando ocurre el mismo suceso varias veces, de manera que el administrador conocerá el patrón de contraseñas utilizado por el usuario.
Recomendación: para resolver esto el administrador modificará la fecha de expiración de la contraseña, obligando así al usuario a cambiarla en el momento del ingreso. La aplicación, en ningún momento, revelará la contraseña del usuario al administrador.

3.5.2. Seguridad de las comunicaciones de red

En este punto mencionaremos los problemas que se presentan en la topología de red, en conexiones externas, configuración lógica de red, correo electrónico, antivirus y ataques de red.

Topología de red

No se hallaron debilidades significativas con respecto a este tema.

Conexiones externas

Debilidad: la comunicación de toda la red hacia Internet se realiza por medio de un ruteador. Esta comunicación se realiza sin la supervisión de algún tipo de *firewall*, siendo pocos los controles existentes para la seguridad de la red.
Efectos: una conexión a Internet sin resguardo es peligrosa, ya que aumenta los riesgos de intrusiones, virus, entre otros sucesos no deseables.
Recomendación: es conveniente que se utilice un *firewall* en la conexión hacia Internet.

Interoperatividad

Debilidad: no hay ninguna medida tomada para que un usuario pueda proteger sus datos.
Efectos: algún usuario puede acceder a datos de otro usuario que no deberían ser divulgados.

Recomendación: podría utilizarse alguna aplicación para el control de perfiles. Con esta se podría gestionar la protección de las distintas carpetas, incluyendo las de *backup* de la página Web y de los usuarios.

Debilidad: existen carpetas compartidas en los servidores.
Efectos: al haber carpetas compartidas en el servidor pueden generarse intrusiones, robos de información o infecciones de virus.
Recomendación: no deberían existir carpetas compartidas en los servidores. Si es necesario grabar un CD aconsejamos que el usuario tenga una carpeta compartida en su PC con una contraseña que conocerá el administrador del sistema. En el momento de grabar el CD el usuario avisará al administrador, y éste copiará los datos al CD. En cuanto a la carpeta compartida en el servidor de Internet, para actualizar el antivirus sugerimos que una vez que la actualización sea descargada de Internet se copie a otra máquina y desde allí se ejecute, o bien que desde Internet se baje directamente a otra máquina que no sea servidor.

Correo electrónico

Debilidad: al instalar los Outlook Express en las PCs no se modifican las opciones de configuración por default, es decir que la vista previa y los controles ActiveX y Scripts están habilitados.
Efectos: la vista previa de los *mails* y la ejecución de controles ActiveX y Scripts son riesgosas, ya que facilitan la infección con virus que se ejecutan automáticamente.
Recomendación: es conveniente exigir normas respecto a la habilitación y deshabilitación de dichas características y la configuración mínima que debe poseer el Outlook Express en las PCs. Debe deshabilitarse la vista previa de los mensajes y prohibirse la ejecución de controles ActiveX y Scripts.

Debilidad: no se asocia una cuenta de correo a un equipo específico.
Efectos: un usuario, conociendo el nombre de cuenta y la contraseña de correo de otro usuario, puede configurarla en su máquina y así enviar y leer mensajes ajenos.
Recomendación: que el servidor asocie una cuenta de correo a una PC determinada, de manera que sólo pueda usarse ese equipo en particular para leer o enviar correos desde esa cuenta.

Debilidad: los empleados no usan el *mail* solamente para funciones laborales, sino también con fines personales. Actualmente no se controla el envío de correos a cuentas externas y pueden usarlo para cualquier fin. No se hace ningún control de que los usuarios se suscriban a listas de correo, no hay prohibiciones en este sentido.
Efectos: al utilizarse el servicio de *mail* indiscriminadamente se baja el desempeño de la red y se incrementa el riesgo de infección con virus.
Recomendación: debería controlarse que el servicio de correo se use sólo para fines laborales, notificando a los usuarios de esta norma. Además sería conveniente hacerles advertencias con respecto a la suscripción a listas de correo. Se podría calcular una estadística del nivel medio de tráfico de red generado por el correo electrónico, de manera que aquel usuario que sobrepase la media será evaluado para controlar si el uso que le da a este servicio es el correcto. De no ser así deberían tomarse las acciones correctivas respectivas.

Debilidad: la cuenta de correo asignada por el administrador a un miembro de la gerencia se satura ocasionalmente.
Efectos: al no hacerse la descarga de mensajes, la cuenta se bloquea impidiendo la comunicación.
Recomendación: sería conveniente verificar la cuenta frecuentemente para evitar este problema.

Debilidad: no están prohibidos los programas de chateo ni los de *file sharing* (transferencia de archivos por Internet).
Efectos: estas aplicaciones incrementan el riesgo de ingreso de virus, troyanos e intrusos al sistema.
Recomendación: deberían restringirse este tipo de aplicaciones, deshabilitando los servicios que utilizan (como el SOCKS en el caso del MSN).

Debilidad: no se implementa un sistema de prioridades de correo.
Efectos: podría mejorarse el envío de los correos a destinos como fábricas, bancos, y otros que merezcan mayor consideración.
Recomendación: el servidor de correo podría configurarse para que aquellos mensajes enviados por la gerencia o los que tienen ciertos destinatarios, como fábricas o bancos, se envíen con prioridad alta.

Debilidad: no se generan copias de seguridad de los mensajes.
Efectos: en el caso de una contingencia con el servidor de Internet, los usuarios perderían los correos que no hayan leído hasta el momento del incidente.
Recomendación: podrían realizarse respaldos de sólo los mensajes con prioridad alta que se almacenan en el servidor de Internet.

Debilidad: no se utilizan firmas digitales ni encriptación en el correo electrónico a nivel gerencial.
Efectos: sin la utilización de firma digital se puede correr el riesgo de ataques de ingeniería social.
Recomendación: podría utilizarse la firma digital o encriptación para los mensajes con prioridad alta de las cuentas de correo de la gerencia, y así poder realizar un envío seguro al transmitir documentos confidenciales. Por ejemplo, podría comprimirse la información de los mensajes para que no viaje en texto plano y protegerla con una contraseña para mayor seguridad.

Antivirus

Debilidad: los usuarios son los responsables de actualizar sus propios antivirus.
Efectos: al no tener implantada una conciencia de seguridad, los usuarios no actualizan la aplicación antivirus.
Recomendación: la actualización de la aplicación antivirus debería ser responsabilidad del administrador o de un empleado del área de sistemas designado por él. Éste debería, además, realizar chequeos aleatorios verificando que las actualizaciones estén al día y que se realicen periódicamente búsquedas de virus. Estas tareas deben realizarse tanto en las PCs como en los servidores.

Debilidad: no hay procedimientos formales a seguir en caso de infección de virus.
Efectos: al no utilizar un procedimiento como guía, puede ocurrir que el virus no sea eliminado completamente del equipo y se contagie a través de la red interna, además de la posibilidad de pérdida de datos en los equipos infectados.
Recomendación: debería haber un procedimiento documentado a seguir para el caso que se encuentre un virus en el sistema. Sugerimos las siguientes actividades:

- Verificar el disco con el antivirus para determinar si hay alguna infección, y qué virus es, así como eliminarlo.
- Cerrar los programas, apagar la máquina y encenderla desde el disco de rescate del antivirus.
- Hacer un nuevo chequeo de virus en el disco duro.
- Verificar el resto de los dispositivos de datos (unidad floppy, disco removibles, etc.), para saber de dónde vino el virus.
- Tratar de determinar la fuente del virus. La persona que hizo llegar el virus debe ser informada.
- Avisar a todos los usuarios del sistema que hayan intercambiado datos con la computadora infectada.
- Si el virus borró o modificó algún dato, tratar de restaurarlo desde los respaldos y restaurar los programas involucrados.
- Hacer una nueva búsqueda en los datos restaurados.

Ataques de red

Debilidad: en la empresa no se disponen de herramientas destinadas exclusivamente para la detección de intrusos.
Efectos: al no haber un sistema de detección de intrusos instalado en los servidores, los atacantes tienen una barrera menos en el momento de ingresar a los datos de la empresa.
Recomendación: se debería usar algún sistema de detección de intrusos, estos deberían ser tolerantes al fallo, y ejecutarse con los mínimos recursos posibles. Ejemplos: OmniGuard, RealSecure, Cisco Secure IDS.

Debilidad: el archivo que contiene los datos de los empleados de la empresa se encuentra almacenado en el servidor, en texto plano, sin ningún control de acceso.
Efectos: ante el acceso indebido a datos del servidor, se divulgarían los datos de los empleados de la empresa.
Recomendación: este archivo debería estar encriptado, y la carpeta donde se almacena debería tener una clave de acceso.

Debilidad: no se encuentran restringidos los servicios y protocolos que no son necesarios para el funcionamiento del sistema.
Efectos: esta situación genera una exposición innecesaria aumentando la probabilidad de ataques o intrusiones.
Recomendación: sería conveniente restringir más los accesos en el interior de la red. Los siguientes servicios no son necesarios y pueden desactivarse:

- Los RSHELL, RLOGIN y REXECUTE pueden remplazarse con los servicios del SSH, por lo que no deben habilitarse.
- No deberían habilitarse el TALK y el FINGER, ya que brindan gran cantidad de información a cualquier persona que la solicite.
- Los APPLETS y los SCRIPTS no deberían poder ejecutarse en el servidor, aunque sí en las PCs, ya que se dificultaría mucho la navegación si éstos no estuvieran.
- El SYSTAT no es necesario salvo cuando se requiere hacer un mantenimiento. Sugerimos que se habilite *on demand* para esta práctica.
- El puerto 22 (de SSH) puede restringirse más, habilitándolo *on demand*, y desde alguna PC determinada, la que se usará para el mantenimiento de la red. Se puede hacer lo mismo con el FTP, permitiendo su uso sólo desde una PC en particular y en un horario determinado.
- Además sería conveniente deshabilitar definitivamente todos los servicios de puertos bajos no necesarios, que están habilitados desde el interior de la red, ya que no deberían utilizarse.

Es conveniente la utilización de herramientas de monitoreo de red. Puede ser conveniente la utilización de una aplicación (TCP WRAPPER) que habilita el uso de servicios como el FTP y el TELNET pero restringe el acceso de acuerdo a ciertas reglas de restricción, en función de la dirección (o el usuario) de origen. Así es posible permitir solamente que se utilice, por ejemplo el FTP, desde una determinada PC.

Debilidad: la dirección IP del servidor de Internet se publica en una página Web de manera que el encargado de mantenimiento tenga acceso a él cuando lo necesite, para realizar el mantenimiento a través de acceso remoto.
Efectos: es muy probable que la dirección IP sea hallada en Internet por intrusos, ya que sólo está protegido por una contraseña. Esto puede provocar el acceso externo de posibles atacantes.
Recomendación: esto puede resultar cómodo para el encargado de mantenimiento externo pero resulta peligroso. Sería conveniente que el personal de mantenimiento solicite la dirección IP actual al administrador del sistema, junto con la contraseña de la cuenta de mantenimiento externo. Con esta metodología, el administrador posee pleno conocimiento de todas las tareas que se llevan a cabo en los servidores.

3.5.3. Seguridad de las aplicaciones

Las aplicaciones que se evaluaron son: *software*, bases de datos, aplicaciones en PCs, control de datos y ciclo de vida.

Software

No se hallaron debilidades significativas con respecto a este tema.

Seguridad de bases de datos

Debilidad: las aplicaciones utilizan un sistema de archivos indexados para almacenar los datos de la empresa.
Efectos: al usar archivos indexados no se aprovechan las ventajas de un sistema de base de datos relacionales, una de las más importantes es que no es necesario trabajar con los índices, los que no son del todo confiables al momento de trabajar con grandes volúmenes de datos. Otra desventaja es no asegurar la inexistencia de redundancia, cuando en las bases de datos relacionales ésta es una de los principales beneficios. La principal desventaja del archivo secuencial indexado es que el rendimiento baja al crecer el archivo; aunque esto se puede evitar reorganizándolo, no es conveniente realizar esta operación frecuentemente.
Recomendación: consideramos necesario que este sistema de archivos sea reemplazado por uno de bases de datos relacionales. Recomendamos que esta migración se realice una vez que el sistema de seguridad en alta disponibilidad para la red esté desarrollado, probado e instalado en su totalidad. Para desempeñar este cambio es conveniente generar un plan de migración, evaluando las posibles contingencias y los planes de prueba necesarios para comprobar el buen funcionamiento de la operación.

Debilidad: los datos de la empresa no se clasifican formalmente según su importancia.
Efectos: la clasificación de la información de acuerdo a su importancia permite asignar distintos niveles de controles de seguridad según la confidencialidad que sea necesaria, la falta de clasificación en los datos puede provocar la mala asignación de controles de acceso, y así posibilitar la divulgación de información.
Recomendación: sería conveniente que se clasifique la información en la empresa, de acuerdo a la importancia de la misma, es decir teniendo en cuenta la confidencialidad y la disponibilidad que debe tener. Se podrían definir tres niveles de información: crítica (el no disponer de esta información ocasionaría daños monetarios en la empresa), confidencial (en poder de personas no autorizadas compromete los intereses de la empresa) y pública (información de libre circulación). Esta clasificación deberá ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.

Debilidad: a la información de la empresa no se le asigna un responsable.
Efectos: al no haber un responsable encargado de la información, puede ocurrir que no se asignen los controles de acceso correctos, o alguien que responda ante los directivos en el caso de una contingencia (como puede ser pérdida o divulgación de información).
Recomendación: se recomienda asignar a la información un responsable, que asegure la confidencialidad, disponibilidad e integridad de dicha información. Con base en la clasificación enunciada anteriormente, el administrador y el responsable de la información deberían definir los controles de acceso a los datos.

Debilidad: no se realizan controles de acceso lógico al sistema de archivos indexados que conforman la base de datos de la empresa, así como al aplicativo que edita dichos archivos.
Efectos: debido a que la seguridad del sistema de archivos indexados se centra solamente en el acceso físico a los servidores, cualquier persona que tenga acceso al NOC podría acceder a los datos utilizando el editor.
Recomendación: sugerimos algún tipo de control de acceso lógico a la carpeta donde se almacenan los archivos indexados y al editor. Consideramos que puede agregarse una

contraseña de ingreso a la carpeta con los archivos indexados, así como también implementar una contraseña de ejecución a la aplicación de edición.

Control de aplicaciones en PCs

Debilidad: no hay estándares definidos ni procedimientos a seguir, ni tampoco documentación respecto a la instalación y actualización de la configuración de las PCs.
Efectos: al no haber estándares en cuanto a la instalación de un puesto de trabajo, puede realizarse una configuración equivocada, incurriendo en una pérdida de tiempo y productividad. Además puede ocurrir que cada empleado instale puestos de trabajo con una configuración diferente, lo que dificultaría el mantenimiento de los mismos.
Recomendación: sugerimos desarrollar un procedimiento formal a seguir cada vez que sea necesario instalar un nuevo puesto de trabajo en la empresa, o reparar alguna PC con errores de configuración, con el fin de establecer un estándar. Podría utilizarse, como complemento, alguna herramienta de restablecimiento y copia de configuración (como el Norton Ghost). Sería recomendable documentar, no sólo el procedimiento de instalación y reparación de puestos de trabajo, sino además cada uno de los mantenimientos que se les realizan, a modo de historial de cada PC. Con esto se logra una documentación de la configuración actual de cada una de las máquinas.

Debilidad: para los usuarios no existen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo, ya que están habilitados los dispositivos externos y algunos disponen de conexión a Internet sin restricciones.
Efectos: la instalación indiscriminada de aplicaciones puede traer problemas en relación a las licencias de los programas y virus. Otro punto a tener presente es la pérdida de productividad del empleado y de recursos, ya que pueden instalarse juegos y demás programas que no aportan al funcionamiento de la empresa, arriesgando la integridad y la confidencialidad de los datos.
Recomendación: para evitar esta situación, es recomendable que, en el momento que el usuario ingresa a la empresa, se le notifique y éste acepte que está prohibida la instalación de cualquier producto de *software* en los equipos. Con este requerimiento es posible tomar medidas a posteriori de la infracción, además de ayudar a generar una "cultura de la seguridad". Sugerimos que algún encargado del NOC designado por el administrador, realice chequeos periódicos de las PCs, identificando así los nuevos productos que han sido instalados. Además sería conveniente instalar una herramienta que audite en forma automática y verifique las PCs en busca de modificaciones y genere reportes cada vez que suponga un problema, de esta manera no se necesitará realizar los chequeos con tanta frecuencia.

Debilidad: la ventana de comandos del DOS está disponible para todos los usuarios de Windows.
Efectos: esta aplicación posee una gran cantidad de herramientas peligrosas para la estabilidad del sistema, tales como el *format* o el *deltree*, que pueden ser ejecutados por usuarios inexpertos o maliciosos.
Recomendación: este comando (command.com) debería eliminarse de los sistemas Windows y en el caso que el administrador necesite de esta aplicación, podría utilizarla a través de la red o de un dispositivo externo.

Control de datos en las aplicaciones

No se hallaron debilidades significativas con respecto a este tema.

Ciclo de vida del desarrollo de *software*

Debilidad: no existe un plan de desarrollo de sistemas formal, ni se utilizan métricas durante el ciclo de vida del *software*.
Efectos: al no tener un plan de desarrollo, puede ocurrir que se administren mal las prioridades, lo que implica un atraso en el desarrollo del sistema. Además, genera un despilfarro de recursos y una administración de tiempos generalmente deficiente. Al no utilizarse métricas con el objetivo de cuantificar los pasos del desarrollo, la estimación de los recursos a utilizar puede desviarse mucho de la realidad, generando más problemas en el desarrollo.
Recomendación: sería conveniente que el equipo de desarrolladores siguiera un plan detallado, generado por el administrador de sistemas, donde se definan las asignaciones de recursos, el establecimiento de prioridades, la administración de tiempos y la utilización de métricas de *software*, con el objeto de garantizar en forma eficiente el cumplimiento de las tareas propuestas.

Debilidad: no se aplica una gestión de configuración o un control de versiones durante el desarrollo.
Efectos: la gestión de la configuración se encarga de la administración de las modificaciones del sistema, si esta tarea del desarrollo no se aplica, entonces existirán inconsistencias en las modificaciones realizadas y en cada oportunidad se hará más difícil agregar nuevas modificaciones al sistema, además de no tener bien documentados los cambios realizados.
Recomendación: es imprescindible implementar una gestión de configuración o un control de versiones, para así documentar los cambios y poder analizarlos. Suponemos que una mejor administración de los cambios puede implementarse utilizando un documento formal de solicitud de cambio, donde quede reflejado el motivo del cambio y la solicitud requerida. Así quedará registrado dentro de la gestión de configuración y este mismo documento será utilizado para actualizar la documentación, tanto de las carpetas de los módulos como de los manuales de usuario. Además sería conveniente tener en cuenta, durante el análisis de requisitos, evaluar los requerimientos de seguridad necesarios.

Debilidad: no hay políticas formales definidas para la contratación de terceros en el desarrollo.
Efectos: el tercero, al no tener conocimiento de las normas de seguridad implementadas en la empresa, puede no cumplirlas poniendo en riesgo la seguridad de los activos.
Recomendación: se debe informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El administrador del centro de cómputo, junto con los directivos, deberían ser quienes especifican los requerimientos de seguridad, los pasos a seguir en caso que no se respete lo establecido en el contrato y piden al tercero en cuestión que informe posibles brechas de seguridad existentes. Adicionalmente, los contratos con terceros deberían contener una cláusula que

indique "Derecho de auditar" para asegurar que el personal de la empresa o las autoridades representativas puedan evaluar su desempeño.

3.5.4. Seguridad física

En este punto se hizo una evaluación del equipamiento, control de acceso físico al NOC, a equipos, dispositivos de soporte, estructura del edificio y cableado estructurado.

Equipamiento

No se hallaron debilidades significativas con respecto a este tema.

Control de acceso físico al centro de cómputo

Debilidad: no hay control de acceso físico al NOC, ya que ninguna de las cámaras del circuito cerrado de video lo apunta a él o a su puerta de ingreso.
Efectos: al no haber un control de acceso especial, cualquier persona que tenga acceso al área de administración y ante una distracción del personal, puede ingresar en él, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos.
Recomendación: sería conveniente que el área del NOC tenga una medida de seguridad extra, a través de la cuál sólo se permita el acceso a los administradores. Esto podría implementarse con una llave, ya que no implica mucho gasto y pueden darse copias sólo al personal necesario. O, en reemplazo de esta medida, puede agregarse una cámara extra de video que grabe el interior del centro de cómputo.

Debilidad: pudimos comprobar, durante la auditoría, que algún personal de mantenimiento técnico externo a la empresa ingresó al centro de cómputo y realizó sus actividades sin supervisión del personal de la empresa.
Efectos: esta situación puede resultar peligrosa, ya que, como mencionamos anteriormente, en esta habitación se almacenan gran cantidad de equipo, corriendo el riesgo de robo de equipamiento o datos. El incumplimiento de esta norma no ayuda a generar en los empleados una "cultura de la seguridad" sino que produce el efecto inverso, debilitándola.
Recomendación: cualquier persona ajena a la empresa que necesite realizar una tarea de mantenimiento relativa al NOC, debería anunciarse en la puerta de entrada. El personal del NOC debería escoltar a los visitantes desde la puerta hacia el interior del edificio, acompañándolos durante el transcurso de sus tareas, hasta que éstas sean concluidas.

Control de acceso a equipos

Debilidad: las máquinas de la empresa disponen de unidad floppy y lectoras de CD, aunque sólo el 10% de los usuarios las necesitan. Estos dispositivos están habilitados y no hay ningún control sobre ellos.
Efectos: debido a que cualquier usuario puede introducir un disquete o un CD con virus o intentar arrancar desde estos dispositivos, esto implica un gran riesgo a la integridad del equipo y sus datos.

Recomendación: sería conveniente que las unidades floppy y lectoras de discos se deshabilitaran desde el BIOS de cada máquina. Si llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de sistemas puede ingresar al BIOS del equipo (utilizando la contraseña que él suministró), habilitar el dispositivo necesario y, una vez utilizado, deshabilitarlo nuevamente.

Debilidad: no hay control de acceso a la configuración del BIOS de las PCs y de los servidores.
Efectos: de esta forma al momento del encendido de la máquina cualquiera podría modificar las opciones de configuración de los equipos.
Recomendación: sería conveniente que las máquinas tuvieran configurado una contraseña de administrador en el acceso al *setup* (BIOS), para evitar que se modifiquen las configuraciones base de los equipos, esto podría aplicarse tanto a las PCs como a los servidores. Estas contraseñas debería gestionarlas el administrador del sistema, en todos los equipos de la red.

Debilidad: no existe un control de acceso físico en el momento del encendido de los servidores.
Efectos: los servidores podrían ser encendidos por cualquier persona, sin que tenga que ingresar ninguna contraseña de ingreso.
Recomendación: sería conveniente que los servidores tengan implementado un sistema de llave de *hardware*, de manera que solamente el administrador del sistema, o la persona designada por él, pueda encenderlos.

Debilidad: en el NOC hay unidades de zip no utilizadas, guardadas sin llave ni control de acceso adicional.
Efectos: estos dispositivos podrían ser fácilmente robados, o cualquier persona que disponga de los programas de instalación necesarios, podrá instalar dichas unidades en cualquier PC de la empresa.
Recomendación: consideramos que sería conveniente agregar otro control a esta clase de dispositivos, guardándolos en algún armario con llave.

Debilidad: no se realizan controles sobre los dispositivos de *hardware* instalados en las PCs, una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos.
Efectos: cualquier usuario podría sacar, poner o reemplazar algún dispositivo sin que se advierta la modificación.
Recomendación: sería conveniente que el administrador, o algún encargado de cómputos designado por él, realice chequeos periódicos para comprobar la correcta instalación de los dispositivos de los equipos, su buen funcionamiento y que sus números de series correspondan con los datos registrados por el administrador al momento de la instalación.

Debilidad: los servidores del centro de cómputo no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realicen trabajos, permanecen ociosos.

Efectos: al permanecer prendidos sin justificación, se acorta el tiempo de vida útil del *hardware* y se predispone a que se produzcan posibles intrusiones en el momento en que no hay nadie en el NOC para mitigar el ataque.
Recomendación: debido a que no es necesario que los servidores permanezcan prendidos las 24 horas, podrían apagarse automáticamente a las 20:30, horario en que han cerrado todas las sucursales de la empresa.

Dispositivos de soporte

No se hallaron debilidades significativas con respecto a este tema.

Estructura del edificio

No se hallaron debilidades significativas con respecto a este tema.

Cableado estructurado

Debilidad: en el caso de ocurrir una contingencia con los enlaces DS0, los centros de servicio quedan imposibilitados de realizar transacciones *on line*.
Efectos: no existe alguna forma de comunicación adicional hacia el edificio corporativo.
Recomendación: en el caso de ocurrir esta contingencia recomendaríamos utilizar un sistema *off line*. Es decir, contar con un sistema isla de entrada de datos que, una vez reestablecido el servicio de red haga una actualización de los datos al sistema central.

3.5.5. Administración del área de sistemas

Para esta administración se realizaron evaluaciones en cuanto a la administración del NOC, capacitación y respaldos.

Administración del NOC

Debilidad: no se asignan responsabilidades puntuales a cada empleado en cada tarea, ni hay un empleado del NOC designado como responsable de la seguridad de la organización.
Efectos: al no haber responsabilidades puntuales asignadas a cada empleado, pueden generarse malas interpretaciones con respecto a las tareas a desarrollar, lo que genera una pérdida de productividad.
Recomendación: deberían designarse responsabilidades claras y documentadas para cada empleado del NOC, las que deberán constar los procedimientos formales que se desarrollen para cada actividad. De acuerdo a las funciones que desempeñen deberán distribuirse los permisos particulares de cada uno de los usuarios en sus respectivas cuentas del sistema. Además debería haber un empleado a cargo de la seguridad del sistema, que coordine las tareas relativas a este tema, haciendo cumplir las políticas de seguridad en toda la empresa.

Debilidad: no se han desarrollado planes formales del NOC.
Efectos: sin planes de sistema se genera una deficiencia en la administración de tiempo, recursos humanos, costos, etc., lo que dificulta la productividad y eficiencia del área.

Recomendación: una medida de control útil sería desarrollar un plan de sistemas a corto plazo, que permita una supervisión continua y directa de las tareas que realiza el personal del NOC, y que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo de un año, debido a las cambiantes exigencias del sector. Además podría considerarse el desarrollo de un plan estratégico a largo plazo, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.

Debilidad: no hay, en los empleados de la empresa, plena conciencia con respecto a la importancia de la seguridad informática.
Efectos: al no existir una cultura de la seguridad implementada en la empresa, no se asegura el cumplimiento de normas y procedimientos.
Recomendación: a pesar de que existe una cierta conciencia sobre la seguridad de la información en el sector gerencial de la empresa, el equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, haciéndolos más responsables y partícipes de las medidas de seguridad, ya que son los principales involucrados, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debería ser renovado y transmitido a los usuarios en forma mensual para asegurar que todos los usuarios que están afectados tengan acceso a las novedades sobre aspectos de seguridad.

Debilidad: cada vez que los usuarios necesitan asesoramiento o servicios del NOC se comunican telefónicamente con alguno de los miembros del área.
Efectos: no queda ninguna constancia de las tareas desarrolladas por los empleados del NOC, ni de las solicitudes de los usuarios.
Recomendación: sería conveniente que los usuarios envíen correos al NOC, solicitando asesoramiento o servicios, o para reportar incidentes o problemas con sus equipos, de manera que quede constancia de la misma. Además debería llevarse un registro de los trabajos efectuados por los empleados del centro de cómputo, es decir tener algún tipo de mecanismo o historial de reportes. Podría ser útil y eficiente la implementación de un buzón de sugerencias (por ejemplo una dirección de correo), donde los usuarios puedan recomendar mejoras o realizar cualquier tipo de comentarios, expresando sus inquietudes.

Debilidad: en el NOC no se desarrolla ningún mantenimiento preventivo.
Efectos: al no tener implementado un mantenimiento preventivo de los equipos y sistemas de la empresa, será necesario esperar a que ocurran los desastres para arreglarlos, lo que ocasiona pérdida de eficiencia de los empleados.
Recomendación: cuando finalice el desarrollo, alguno de los empleados podría asumir la responsabilidad de llevar a cabo un mantenimiento preventivo, monitoreando, verificando y auditando las PCs y demás dispositivos que conforman la red.

Debilidad: no existe un inventario donde se documenten todos los sistemas de información y sus características principales.
Efectos: al generar un inventario detallado es posible discriminar los responsables de la información que administra cada sistema, las áreas en la que interviene y el nivel de prioridad con que cuenta en caso de una emergencia.

Recomendación: es conveniente la generación de un inventario donde se detallen los sistemas de información utilizados en la organización, documentando las siguientes características:

- Nombre.
- Departamento de la empresa que genera la información (dueño del sistema).
- Departamentos de la empresa que usan la información.
- Volumen de archivos con los que trabaja.
- Volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- Equipamiento necesario para un manejo óptimo del sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este sistema para la empresa (medido en horas o días en que la institución puede funcionar adecuadamente, sin disponer de la información del sistema).
- Relación de equipamiento mínimo necesario para que el sistema pueda seguir funcionando. Será necesario mantener esta relación siempre actualizada.
- Actividades a realizar para volver a contar con el sistema de información (actividades de restauración).

Puede ser útil disponer de un responsable a cargo de la actualización del mismo, que controle periódicamente estos dispositivos y la información almacenada.

Debilidad: no hay inventarios de los equipos de *hardware*, ni documentación con respecto a los equipos de la red física.
Efectos: esta documentación facilitaría las actividades de los administradores del NOC, en el momento de realizar tareas de mantenimiento y para el desarrollo del plan de contingencias.
Recomendación: se debe implementar un inventario detallado de los equipos de cómputo, donde se incluya:

- *Hardware*: dispositivos instalados en cada máquina, con su número de serie, y demás datos sobre procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, ruteadores, *bridges*, etc.
- *Software* en los equipos: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones, números de licencias, etc.
- Datos o principales archivos que contienen los equipos: durante la ejecución, almacenados en línea, archivados fuera de línea, *backup*, bases de datos, dueño designado de la información, etc.
- Configuración de los equipos (y sus archivos de configuración).
- Ubicación de los equipos.
- Nivel de uso institucional de los equipos.

Puede ser útil disponer de un responsable a cargo de la actualización del mismo, que controle periódicamente estos dispositivos y la información almacenada. Sugerimos,

además desarrollar procesos para rotular, manipular y dar de baja una computadora, sus periféricos y medios de almacenamiento removibles y no removibles.

Debilidad: los usuarios deben realizar tareas de mantenimiento, como actualizar el antivirus, hacer copias de respaldo de sus datos, desfragmentar el disco, modificar y proteger sus contraseña, borrar archivos temporales, entre otras.
Efectos: estas son tareas de gran importancia en el funcionamiento de los equipos, y una falla en su realización puede generar el mal funcionamiento de los mismos.
Recomendación: estas tareas de mantenimiento de las PCs de los puestos de trabajo deberían ser llevadas a cabo por el administrador del NOC, o por alguien designado por él.

Debilidad: los programas de instalación de *software* de uso más frecuente están en el servidor y se instalan desde carpetas compartidas por éste.
Efectos: compartir carpetas en el servidor significa un gran riesgo para la administración de red ya que facilita la intrusión.
Recomendación: seria conveniente almacenar estos programas de instalación fuera del servidor, en particular recomendamos que se guarden en el mismo equipo que se utiliza para los demás *backups* de la empresa (detallado más adelante), en una carpeta protegida con contraseña, o podrían generarse CDs con estos programas.

Capacitación

Debilidad: en ningún momento hay consentimiento por parte de los usuarios a que auditen sus actividades, ni declaraciones de que conocen las normas de "buen uso" en el sistema.
Efectos: no hay un aval de que el usuario ha comprendido las normas de buen uso del sistema, y que está dispuesto a cumplirlas.
Recomendación: una vez que el usuario ha sido capacitado en la realización de sus tareas cotidianas, y tenga una clara visión del manejo del sistema, se le podría comunicar la política de seguridad de la información y los procedimientos establecidos por la empresa, además de un resumen por escrito de las medidas básicas, junto con una copia que debería ser firmada por él y resguardada en el expediente del empleado. Esto implica que está de acuerdo con las normas impuestas, y es conciente de las consecuencias que acarrea el incumplimiento de estas normas.

Copias de seguridad

Debilidad: no se documentan los cambios que se realizan en la configuración de los servidores, ni la fecha de estas modificaciones.
Efectos: al no tener documentación actualizada de los cambios realizados, se dificulta conocer la configuración exacta y actual de cada servidor, y de esta forma se obstaculiza la tarea del mantenimiento.
Recomendación: sugerimos que se documente cada uno de estos cambios, para tener un control y una identificación de los mismos, así se podrá generar un historial de modificaciones y calcular estadísticas de los mismos, y con éstas será posible hacer más eficiente la configuración de los servidores.

Debilidad: no hay ningún procedimiento formal para la realización ni la recuperación de los *backups* de los datos almacenados en los servidores de la empresa.
Efectos: las copias de respaldo son el principal método de recuperación de datos del que dispone la organización y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente.
Recomendación: consideramos necesario que exista un procedimiento escrito y formal de política de *backup*, que contenga las recomendaciones que se describen a continuación:

- Sería conveniente que el administrador del NOC designe a un responsable para la realización de las copias de seguridad y de su restauración, así como un suplente.
- El procedimiento de generación de *backup* debería estar automatizado con alguna herramienta de generación de copias de respaldo de datos.
- Las copias de respaldo deben realizarse en el momento en que se encuentre la menor cantidad posible de usuarios en el sistema.
- Debería realizarse un *backup* incremental diario, todos los días de la semana, mientras que una vez por semana sería conveniente realizar un *backup* completo de los datos más significativos.
- Deberían realizarse chequeos para comprobar que los procedimientos de restauración son eficientes.
- Los archivos de *backup* deberían tener una contraseña que los proteja o bien encriptarse, ya que contienen información confidencial.
- Las cintas deberían permanecer en el interior de la empresa resguardadas en un lugar ajeno al NOC.
- Deberían realizarse chequeos para comprobar el funcionamiento correcto de los medios externos donde se realizan las copias de respaldo.
- Debería existir una política de reemplazo de cintas, donde conste que deberían reemplazarse cada 6 meses, para evitar posibles fallas en el momento de la recuperación, debido al tiempo de vida útil del medio.
- Debería existir un procedimiento de recuperación de copias de respaldo, donde se incluya la metodología a seguir, quién tiene el permiso para realizarlo y en qué casos será permitido.
- Debería existir documentación de los respaldos generados, incluyendo:

    * Qué datos contienen estas copias.
    * Fechas de realización.
    * Fechas de restauración.
    * Errores obtenidos.
    * Tiempo empleado en el proceso.
    * Además de datos que se consideren necesarios en la administración de este procedimiento.

Debilidad: los usuarios hacen respaldos de sus datos en sus propias máquinas o en disquetes.
Efectos: hacer un respaldo en la misma máquina donde están los archivos originales no es garantía, y hacerlos en disquetes tampoco sirve por la mala calidad del medio.

Recomendación: debido a que los usuarios no deberían tener habilitados dispositivos de almacenamiento externo (como unidades de discos flexibles) lo más conveniente sería que el administrador del sistema disponga de una máquina para la realización de respaldos. Allí debería generar todas las copias de respaldo de los datos de los usuarios. La carpeta donde se guarden estos respaldos deberá estar protegida con una contraseña gestionada por el administrador para restringir el acceso de otros usuarios.

Debilidad: no hay ningún procedimiento formal para la realización ni la recuperación de los respaldos de la página Web de la empresa.
Efectos: las copias de respaldo son el principal método de recuperación de datos del que dispone la organización y la ausencia de procedimientos, para su implementación, puede generar errores en el momento de un incidente.
Recomendación: debería existir un procedimiento formal de respaldo de la página Web, éste debe contener toda la página completa, y debe hacerse cada vez que se modifique la estructura de la misma. Éste debería almacenarse en el mismo equipo que los respaldos de los usuarios, en otra carpeta protegida con contraseña.

Debilidad: no hay un buen soporte de documentación en el NOC.
Efectos: al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre y dificulta la administración de incidentes.
Recomendación: sugerimos que la documentación posea más detalles respecto a los siguientes datos:

- Diagrama de la distribución física de las instalaciones, identificación de PCs y equipos, y puestos de trabajo.
- Número de serie de *hardware*.
- Número de licencia del *software*.
- Inventario de *hardware* y *software*.
- Fallas en equipos y trabajos de mantenimiento.
- Entrada del personal externo.
- Configuración de equipos y servidores.
- Cambios en la topología de red.
- Modificaciones de emergencia realizadas a sistemas y *hardware*.
- Procesos estándares del sistema operativo.
- Métodos para compartir datos entre sistemas (por ejemplo entre los centros de servicio).

Toda esta documentación debería generarse teniendo en cuenta tanto el edificio corporativo como los centros de servicio.

Debilidad: no hay planes de seguridad desarrollados, procedimientos formales, ni manuales o documentos de soporte para la gestión de la seguridad en la red informática.
Efectos: al no poseer un buen soporte, se dificulta la administración general.
Recomendación: sugerimos que la documentación posea más detalles respecto a los siguientes datos:

- Plan de contingencia.
- Política de seguridad.
- Manual de procedimientos.
- Manual de usuario (del *software* y del *hardware*).
- Manual de seguridad para el sistema: en donde se detallan las funciones y privilegios de la seguridad. Que contenga: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.
- Manual de seguridad para el usuario: que asista a los usuarios del sistema, describa como usar las protecciones, y las responsabilidades de la seguridad del sistema.

Debilidad: durante el desarrollo de sistemas, la documentación no es completa y las actualizaciones se realizan informalmente.
Efectos: por fallas en la gestión de la documentación pueden producirse errores en el desarrollo del sistema, así como una mala administración de recursos y equivocaciones en la estimación de tiempos.
Recomendación: sugerimos la realización de los siguientes documentos para mejorar la documentación existente y así lograr una organización eficiente:

- Objetivos.
- Alcances.
- Diagramas general y de funciones o de procesos.
- Diagrama de flujo.
- Archivos de entrada-salida.
- Responsable del módulo (analista que lo desarrolló).
- Registro de modificaciones.
- Lenguaje de programación.
- Problemas o limitaciones conocidas.
- Sectores de la organización a los que afecta.
- Descripción del *hardware* y *software* utilizados.
- Características de seguridad.

Consideramos necesario que cada vez que se produzca una modificación en algún módulo del sistema, se modifique toda la documentación correspondiente. Las modificaciones deben hacerse de acuerdo a un procedimiento formal definido en la gestión de configuración.

3.5.6. Auditorías y revisiones

Las auditorías y revisiones se llevaron a cabo fundamentando chequeos del sistema, control de acceso y auditoría de redes.

Verificaciones del sistema

Debilidad: no cuentan con una aplicación que genere alarmas o avisos cuando ocurre un evento que revista un determinado grado de riesgo.
Efectos: para que el administrador tome conocimiento de la ocurrencia de algún incidente problemático, debe leer los registros generados por las aplicaciones, analizarlos y tratar de encontrar problemas en un archivo de texto. Esta situación no resulta práctica, y puede ocurrir que la notificación del problema llegue tarde, cuando el error ya está avanzado.
Recomendación: contar con una aplicación para generar reportes y alarmas, ya que la lectura de los *logs* es tediosa y poco práctica, sería conveniente generar alarmas o algún otro mecanismo de alerta cuando ocurra algún evento en particular. Usar una aplicación que administre los *logs*, teniendo en cuenta la severidad de los eventos, e identificando el usuario asociado al evento.

Debilidad: no se buscan nuevas herramientas de generación ni gráfico de *logs*.
Efectos: puede perderse efectividad y eficiencia con el uso de herramientas poco prácticas y desactualizadas, que no poseen generación de reportes ni alarmas, para que el administrador esté siempre al tanto de las situaciones riesgosas.
Recomendación: sería conveniente actualizar continuamente las herramientas que se usan para graficar la información generada en los *logs*. Debería asignarse la responsabilidad de esta tarea a una persona específica.

Debilidad: no existe una línea de base definida, sólo disponen de los datos almacenados en los *logs*.
Efectos: no es posible comparar medias o promedios generados en la empresa en situaciones normales con los valores actuales obtenidos de los *logs*, e identificar actividades inusuales.
Recomendación: sería conveniente generar líneas de base, en vez de un conjunto de datos históricos, para poder tener información sobre las PCs, los servidores y el sistema en general con detalles sobre, por ejemplo:

- Qué usuario, sector o tarea utiliza más recursos de CPU.
- Qué datos son los que consumen más tráfico de red, memoria o CPU.
- Qué datos se utilizan o se modifican con más frecuencia.
- Qué archivos tienen mayor índice de crecimiento.
- Qué aplicaciones son más utilizadas.
- Qué aplicaciones consumen más recursos.
- Quién utiliza más memoria del servidor.
- En qué momento surgen cuellos de botella y en qué recursos.
- En qué momento o por cuánto tiempo la memoria o el CPU permanecen usados en un 100% de su capacidad.

Debilidad: al hacer alguna modificación en la configuración del sistema, se genera una nueva compilación de datos (nueva línea de base), que no se documenta.

Efectos: esta situación genera confusiones, ya que no se identifica si se han modificado los valores debido a algún incidente o si la variación se debe a cambios realizados en el sistema.
Recomendación: sería conveniente documentar las nuevas líneas de base cuando se hace alguna modificación en el sistema, generando así un historial de líneas de base y sus variaciones por incidentes. Esto se debe a que pequeños cambios en las configuraciones pueden producir grandes impactos en el desempeño.

Debilidad: los *logs* se eliminan sin generar un respaldo de sus datos.
Efectos: al no hacer respaldo de los datos de los *logs* no es posible obtener datos estadísticos para la generación de las líneas de base.
Recomendación: sería recomendable, antes de eliminar los *logs*, generar un resumen de líneas de base y estos resultados guardarlos en cintas.

Debilidad: en la empresa no se realizan auditorías programadas. ni rutinas de chequeos de *logs*.
Efectos: al no realizar controles aleatorios resulta difícil verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
Recomendación: sería conveniente que se programen auditorías y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la empresa, documentando la ejecución y los resultados de dichas pruebas. Debe tenerse en cuenta la recomendación sobre separación de tareas, ya que la persona que realice dichas revisiones no debería estar comprometida con la tarea de auditar. Además, si el tamaño de la auditoría lo justifica, sería conveniente que la lleve a cabo un grupo de dos o más personas, para disminuir las tentativas de corrupción.

Auditorías de control de acceso

Debilidad: los *logs* se guardan en el servidor de aplicaciones y en el de Internet, sin controles de acceso lógico a las carpetas donde están almacenados. Además pueden ser accedidos desde cualquier máquina conectada a la red, por usuarios o administradores, conociendo la clave del administrador.
Efectos: la modificación del contenido de los *logs* es considerada como muy crítica, debido a que usuarios, administradores o intrusos mal intencionados pueden borrar las pistas de auditoría correspondientes a violaciones del sistema.
Recomendación: sería conveniente reforzar con una contraseña las carpetas donde se almacenan los *logs* para que los usuarios o administradores no puedan borrar o modificar los *logs*. Debe tenerse presente que, incluso para el administrador del sistema, esta contraseña debe ser desconocida, por lo que sugerimos que lo conserve algún miembro de la gerencia.

Debilidad: la información que se almacena en los *logs* con respecto a las conexiones a Internet no es suficiente, ya que sólo se almacena el número IP de la máquina conectada y la dirección de las páginas visitadas.
Efectos: al no disponer de la información necesaria, no será posible conocer las actividades de los usuarios en la red, como por ejemplo identificar la procedencia de posibles virus.
Recomendación: sería útil poseer información más detallada sobre:

- *Cookies* guardadas.
- Archivos descargados.
- Servicios utilizados.
- Aplicaciones utilizadas.

Debilidad: no se identifican los usuarios que acceden a datos.
Efectos: no puede identificar qué usuario accede a los datos, debido a que hay información sobre la máquina que ingresa al sistema pero no del usuario que accede a los datos y cualquier usuario podría utilizar cualquier máquina.
Recomendación: es conveniente que se identifique al usuario, y no a la máquina que accede a los datos y así será posible rastrear las acciones de cada usuario.

Debilidad: no se generan reportes relativos a las actividades de los usuarios sobre los datos.
Efectos: para el administrador del sistema resulta muy complicada la revisión de las actividades de los usuarios basándose en un estudio de los *logs*, debido a la cantidad de tiempo que implica esta tarea.
Recomendación: podría utilizarse una herramienta de generación de reportes de manera automática con datos sobre:

- Cantidad de usuarios que acceden simultáneamente a la base de datos (cantidad de conexiones activas).
- Estadísticas de entrada-salida para cada usuario.
- Tiempo y duración de los usuarios en el sistema.
- Usuarios que no han ingresado al sistema por un largo período de tiempo.
- Generación de nuevos objetos de bases de datos.
- Modificación de datos.
- Número de intentos fallidos de conexiones a bases de datos.

Se deberán generar estadísticas o líneas de base de estos datos, a fin de utilizarse para el control de la información de la base de datos.

Debilidad: no se realizan chequeos periódicos a los *logs* generados por el usuario administrador del sistema.
Efectos: al no generarse reportes sobre las actividades del usuario administrador, se corre el riesgo de que algunas acciones de intrusos o no permitidas pasen inadvertidas.
Recomendación: deberían realizarse controles sobre estos *logs*, comprobando que las acciones realizadas por el administrador correspondan con los datos que en ellos figuran, de manera de identificar posibles intrusiones o anomalías. El estudio de estos reportes no debería ser realizado por el administrador, sino por su superior. Para que esta recomendación tenga validez, deberá cumplirse la sugerencia que imposibilita a los usuarios y administradores la modificación de los *logs*.

Debilidad: no se generan *logs* cuando un usuario modifica su contraseña.
Efectos: deben poder rastrearse todas las actividades del usuario en el sistema.

Recomendación: sugerimos que se generen *logs* cuando un usuario modifica su contraseña, agregando datos como la aplicación desde la que se realizó el cambio y en caso que el cambio resulte fallido, el motivo del fallo.

Debilidad: los *logs* generados por un acceso fallido no especifica el motivo del fallo.
Efectos: al no incluir el motivo del fallo en los *logs*, no será posible determinar si hubo un error en el sistema, intento de intrusión o el usuario confundió su contraseña, entre otras.
Recomendación: detallar el motivo del acceso fallido en el contenido del *log*.

Debilidad: no se genera un registro cuando la cuenta de un usuario ha sido bloqueada, ni tampoco un sistema de alerta ante este bloqueo.
Efectos: el no poseer registros de los bloqueos de los usuarios imposibilita la generación de estadísticas al respecto. Al no tener un sistema de alerta que avise al administrador de esta situación, no le será posible identificar los intentos de intrusión en el momento en que ocurren.
Recomendación: sería conveniente que se generen *logs* cuando ocurra un evento de este tipo, y que se avise al administrador por medio de un sistema de alerta. Con este sistema podrían detectarse anticipadamente intentos de intrusión.

Debilidad: no se generan perfiles de los usuarios con respecto a sus actividades.
Efectos: sin estos perfiles no se pueden identificar anomalías por grupos de usuarios.
Recomendación: sería conveniente generar estos perfiles con el objeto de saber qué uso le dan a Internet, el tráfico de *mails*, el tráfico de red que genera cada usuario o sector de la empresa, qué terminales utilizan, las horas de acceso, etc., para así determinar qué acciones son inusuales y deban ser investigadas.

Debilidad: no se generan *logs* cuando se requiere una impresión de algún dato suministrado por el sistema de la empresa.
Efectos: al no generar *logs* no se tiene un control sobre los datos de la empresa que son impresos, ni de los usuarios que solicitan esta tarea.
Recomendación: cuando un usuario solicita una impresión de algún dato del sistema de la empresa, debería generarse un *log* de dicho evento.

Auditorías de las comunicaciones de red

Debilidad: no poseen un plan de monitoreo general de la red.
Efectos: al no tener un plan organizado de monitoreo, puede ocurrir que baje el rendimiento del sistema debido a cuellos de botella en los recursos.
Recomendación: generar un plan de monitoreo, teniendo en cuenta que éste tiene un impacto directo en el rendimiento del sistema. Se podría utilizar, por ejemplo, alguna herramienta para monitorear el tráfico y el rendimiento de red.

Debilidad: no se auditan regularmente ni se generan estadísticas sobre los *logs* referentes al correo electrónico.
Efectos: al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al administrador sobre anomalías o posibles errores.

Recomendación: el administrador o un encargado del NOC debería ser responsable del monitoreo de estos *logs*, generando reportes diarios o mensuales, con los siguientes datos:

- Poco espacio libre de cuotas asignadas al correo.
- Disminución en el desempeño del correo.
- Demasiados mensajes entrantes o salientes fuera de lo normal.
- Departamento o usuario de la empresa que utiliza más el servicio de correo.
- Avisos o advertencias ante la aparición de un virus.
- Estadísticas sobre *mails* infectados con virus, períodos de mayor infección, máquinas más afectadas, direcciones fuentes qué mas correos infectados envían, cantidad de archivos infectados por extensión (como los archivos de Word se infectan más que los de Excel).

Debilidad: no se auditan regularmente ni se generan estadísticas sobre los *logs* referentes a la administración de red. Además no se hace ningún seguimiento de los *logs* en busca de cambios en las estadísticas o en las líneas de base.
Efectos: al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al administrador sobre anomalías o posibles errores, en lo respectivo al tráfico de red o utilización de recursos del servidor. Además pueden generarse nuevos cuellos de botella en algún recurso del sistema, y el administrador puede no notarlo hasta que algún usuario se lo advierta.
Recomendación: el administrador o un encargado del NOC debería ser responsable del monitoreo de estos *logs*. Podrían generarse gráficos y estadísticas diarios o mensuales compuestos por datos suministrados por las distintas aplicaciones que se utilizan en la empresa y que generen *logs*. Así podría obtenerse un reporte más detallado con datos y estadísticas como:

- Consumo de ancho de banda por terminal o por sector de la empresa o cuellos de botella en el tráfico de red.
- Cantidad de tráfico que genera cada aplicación utilizada por cada usuario.
- Cantidad de recursos que utilizan las aplicaciones.
- El estado de cada aplicación (en cola, ejecutándose, esperando una respuesta, etc.).
- Intentos de intrusión.
- Estadísticas del uso de los protocolos.
- Páginas de Internet más visitadas, con información sobre los archivos descargados, los usuarios conectados, el horario, etc.

El seguimiento de estadísticas puede ser automatizado por medio de herramientas que realicen las tareas y sólo informen de las desviaciones con respecto a las líneas de base, a través de un *mail* o alerta. Podrían generarse avisos cuando exista:

- Incremento en el uso de Internet o del servicio de correo.
- Tráfico excesivo de red, sectores o PCs que superan el promedio de ancho de banda.
- Incremento en los ataques o sospecha de intrusión.
- Poco espacio en disco de servidores o de PCs.

- Poca disponibilidad de CPU, memoria o algún recurso en los servidores.
- Violaciones a las reglas de servicios de red, modificación en los permisos de los servicios o mala utilización de los mismos.

Debilidad: no se hicieron pruebas de auto-*hackeo*, escaneos o intentos de intrusión o de escucha en la red informática. Tampoco se hacen pruebas periódicas de puertos o de los servicios que están habilitados.
Efectos: al no hacer pruebas o chequeos pueden pasar inadvertidas situaciones que sólo serán reveladas utilizando casos prácticos.
Recomendación: sería conveniente programar chequeos periódicos de la red, incluyendo los siguientes controles, los servicios, su configuración y su buen funcionamiento:

- Tratar de escuchar o hacer un ataque de intrusión periódicamente, para comprobar que la red sigue siendo inaccesible desde el exterior.
- Realizar pruebas de auto-*hackeo*:

  * A los servidores, desde dentro del mismo.
  * A los servidores, desde la red interna.
  * A Intranet desde dentro de ella.
  * Accesos desde el exterior y/o Internet.

Podrían utilizarse herramientas que permiten hacer estas inspecciones en la red en forma automática, para comprobar en qué estado está y determinar si existen vulnerabilidades en algunos sectores de acuerdo a líneas de base ingresadas por el administrador (como COPS, NOCOL, SATAN, SNORK o TRIPWIRE). Además sería posible hacer auto-escaneos para verificar los recursos compartidos, y auto-*hackeos* para prevenir ataques de intrusión. Sugerimos documentar las pruebas y sus resultados cada vez que se realicen.

3.5.7. Plan de contingencias

Respecto al plan de contingencias que se propone, éste se consideró para la administración de incidentes, *backup* de equipamiento y recuperación en desastres.

Plan de administración de incidentes

No se hallaron debilidades significativas con respecto a este tema.

Respaldo de equipamiento

Debilidad: no se realizan pruebas periódicas de los mecanismos de respaldo de los servidores.
Efectos: ante una emergencia, puede ocurrir que estos mecanismos no funcionen correctamente o que los responsables del NOC no desempeñen sus funciones correctamente por falta de práctica.

Recomendación: deberían realizarse planes de prueba periódicas, comprobando todos los mecanismos de respaldo con los que cuentan los servidores de la empresa.

Estrategias de recuperación de desastres

Debilidad: no se asignan prioridades a los sistemas de información ni a los equipos de *hardware* de la red física.
Efectos: al no asignar niveles de prioridad a los sistemas o equipamientos no es posible determinar cuáles son los que deberían recuperarse de inmediato en caso de una emergencia.
Recomendación: se debería asignar un orden de importancia a cada uno de los sistemas de información y de los equipos de la red, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia. La prioridad mayor la tendrá aquel sistema que es más importante a la hora de recuperar la operatividad luego de un desastre. Los equipos podrían estar señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

Debilidad: no se han identificado las funciones más críticas para las actividades de la empresa.
Efectos: al no identificar las funciones que interrumpen la productividad de la empresa debido a su aspecto crítico, se corre el riesgo de no tenerlas en cuenta en el momento de la restauración del sistema.
Recomendación: sería conveniente definir las funciones o servicios de la empresa que sean más críticos. Cada jefe o encargado de área debe interactuar con el administrador y definir estos servicios junto con los recursos mínimos necesarios para su funcionamiento, y asignarles una prioridad en el plan de restauración. Además, sería conveniente identificar las contingencias que podrían ocurrir para cada nivel de servicio determinando, considerando:

- Cuáles serían los peores problemas a los que se puede ver sometida la empresa.
- Cuáles serían las peores contingencias.
- Cuáles serían las más probables.
- Cuáles son las que ocurren más a menudo.
- Cuáles son las que no ocurren nunca.

Debilidad: no se hacen simulaciones de siniestros.
Efectos: sin estas simulaciones no será posible comprobar que los empleados hayan comprendido las tareas a su cargo y será imposible predecir su comportamiento ante una emergencia.
Recomendación: para el entrenamiento del personal deberían generarse simulacros de siniestros y así evaluar la efectividad del plan.

Debilidad: en la empresa no hay planes formales para la administración de incidentes ni funciones claras que deba realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas.

Efectos: al no haberse designado claramente las responsabilidades de los empleados frente a una emergencia, las acciones que se tomen en caso de contingencia resultarán caóticas, comprometiendo la integridad de los datos y equipos.
Recomendación: debería conformarse un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada. Estas tareas deberían estar claramente definidas y documentadas, y tener asignado un responsable para su ejecución, considerando los distintos escenarios posibles (por ejemplo durante el día o la noche). Algunos ejemplos de tareas que se pueden desarrollar son:

- En caso de incendio:
  * Identificar las vías de salida.
  * Generar un plan de evacuación del personal.
  * Desarrollar un plan de puesta a buen recaudo de los activos.
  * Ubicación y señalización de los elementos contra el siniestro.
- En caso de intrusión interna o externa:
  * Desconectar los servidores.
  * Cerrar todos los accesos a los datos.
  * Rastrear al intruso.

Deberían contemplarse las siguientes características:

- Debería estar documentado y probado antes de su puesta en práctica.
- Debería basarse en un análisis de riesgo, determinando que acciones merecen estar incluidas.
- Debería abarcar toda la empresa, no sólo el área de cómputo.
- Debería entrenarse a los responsables y a los usuarios.
- Debería mantenerse actualizado de acuerdo a nuevos puestos de trabajos y funciones.
- Debería ser retroalimentado después de cada incidente.
- Debería ser probado frecuentemente.
- Debería contener la siguiente información:
  * Objetivo del plan.
  * Modo de ejecución.
  * Tiempo de duración.
  * Costos estimados.
  * Recursos necesarios.
  * Evento a partir del cual se pondrá en marcha el plan.

Debilidad: no se documentan los acontecimientos ocurridos durante las emergencias, ni se hacen evaluaciones formales de los daños sufridos.
Efectos: al no documentarse los acontecimientos ni daños, se corre el riesgo de no hacer las correcciones necesarias para que no ocurran las mismas contingencias. Puede ocurrir

también que durante el incidente se realicen modificaciones de urgencia en alguna parte del sistema y éstas no queden documentadas.
Recomendación: sugerimos que se documente la realización de las siguientes actividades después de que ha ocurrido algún desastre:

- Determinar la causa del daño.
- Evaluar la magnitud del daño que se ha producido.
- Qué sistemas se han afectado.
- Qué modificaciones de emergencia se han realizado.
- Qué equipos han quedado en estado no operativo.
- Cuáles se pueden recuperar y en cuánto tiempo.

Se debería actualizar la documentación del centro de cómputo con las modificaciones implementadas y las acciones correctivas que se llevaron a cabo como consecuencia del incidente.

Debilidad: una vez ocurrido el siniestro, el administrador del sistema realiza las actividades de recuperación sin respaldarse en un plan o manual formal de procedimientos.
Efectos: al no tener una guía es muy probable que se cometan errores u omisiones en las acciones de restablecimiento.
Recomendación: se debería asignar el papel de coordinador a un empleado, que se encargará de las operaciones necesarias para que el sistema funcione correctamente después de la emergencia. Esta persona debería determinar las acciones a seguir de acuerdo al tipo de emergencia que ha ocurrido, basándose en el plan de emergencias. Un ejemplo de acciones principales a seguir en el caso de la caída del sistema serían:

- *Setup* e instalación de los componentes de *hardware* necesarios.
- Carga del *software* del sistema.
- Instalación del *software* de aplicación.
- Provisión de los datos necesarios (*backup*), incluyendo archivos de configuración.
- Re-arrancar el equipo.
- Se debe asegurar que se empiece a auditar una vez que se reinicia.

Debilidad: debido a que no hay implementado un plan de acción en caso de desastres, no se realiza una retroalimentación con los datos obtenidos luego de una emergencia.
Efectos: si no se aprende del resultado de estas acciones, no será posible evitar la misma contingencia en el futuro ni mejorar la eficacia de las directivas.
Recomendación: se debería tener en cuenta la experiencia que se obtiene luego de una contingencia para retroalimentar el plan, y así obtener uno de mayor eficiencia. Esto se logra generando una lista de recomendaciones para minimizar los riesgos de futuros incidentes similares. Con base en la experiencia obtenida, evaluar:

- El desempeño del personal inmerso en la emergencia, y reordenar la lista.
- Si algún elemento o tarea tenía asignada una prioridad que no le correspondía, se deberían modificar estas prioridades.
- La introducción de actividades que no se contemplaron en el plan de emergencia.

- La generación de sugerencias y posibles mejoras.

Del análisis que se realizó a la empresa, presentamos los resultados principales y damos alternativas de solución viables, además de las que permitirán tener una seguridad óptima en la misma. Dicho análisis fue presentado a los directivos del corporativo, quienes procedieron a evaluarlo y determinar la prioridad de las recomendaciones que se plantearon, así como su asignación a las diferentes áreas para su ejecución posterior. En nuestro caso, debido al sector de la empresa en que nos ubicamos, trataremos el aspecto asignado de las comunicaciones de red.

Una vez realizado el análisis de las debilidades que presenta la empresa, procedemos al desarrollo e implementación de la solución de seguridad en el área de comunicaciones.

CAPÍTULO 4

DISEÑO E IMPLEMENTACIÓN

En este capítulo describiremos los aspectos de diseño, así como las consideraciones que se deben de tomar para la implementación de un sistema de seguridad en alta disponibilidad para una red de datos.

4.1. TECNOLOGÍAS DE SEGURIDAD

Hoy en día existen tecnologías de seguridad que son muy empleadas en todo el ámbito de la seguridad informática, y que además se encuentran integradas en la mayor parte de las empresas que consideran a sus datos como críticos, además que éstas se utilizan para proteger la información de servicios prestados a través de la red de datos.

Actualmente, los elementos más utilizados para mejorar la seguridad de una red de datos son: el uso de sistemas de detección de intrusos, el uso de *firewalls*, antivirus y filtros de correo como *spam* y *spyware*.

4.1.1. Sistema de detección de intrusos

Cuando una intrusión alcanza a penetrar la red interna, sólo queda detectar las acciones que pueden comprometer la integridad, confidencialidad o disponibilidad de la información o un recurso informático, es decir, detectar el ataque o intrusión lo antes posible para que cause el menor daño en el sistema.

Esta tarea es realizada por productos conocidos como IDS (Intrusion Detection System, Sistemas de Detección de Intrusos). Estos sistemas basan su funcionamiento en la recolección y análisis de información de diferentes fuentes, que luego utilizan para determinar cuándo la actividad de un usuario se aleja de lo que se considera un comportamiento normal y se vuelve un ataque o intrusión.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un subconjunto de las actividades anómalas. En ocasiones una actividad intrusiva es consecuencia de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Por tanto, las actividades se clasifican en:

- *Intrusivas pero no anómalas.* Se les denomina falsos negativos y en este caso la actividad es intrusiva pero como no es anómala no se consigue detectarla. Se denominan falsos negativos porque el sistema erróneamente indica ausencia de intrusión.

- *No intrusivas pero anómalas.* Se denominan falsos positivos y en este caso la actividad es no intrusiva, pero como es anómala el sistema decide que es intrusiva. Se denominan falsos positivos, porque el sistema erróneamente indica la existencia de intrusión.

- *Ni intrusiva ni anómala.* Son negativos verdaderos, la actividad es no intrusiva y se indica como tal.

- *Intrusiva y anómala.* Se denominan positivos verdaderos, la actividad es intrusiva y es detectada.

Un sistema IDS debe ser capaz de evitar los falsos negativos porque el intruso puede operar libremente en el sistema, y minimizar los falsos positivos para evitar ignorar los avisos del sistema de seguridad, incluso cuando sean acertados.

En caso de que exista la suficiente certeza de la detección de un incidente, el IDS tiene como función principal alertar al administrador o personal de seguridad. En caso de implementaciones más complejas pueden ejecutar acciones automáticas que impidan el desarrollo de éste.

Después del proceso de recopilación de información, se lleva a cabo el proceso de análisis. La detección de intrusiones también se puede clasificar según los objetivos del motor de análisis. Los dos tipos principales de análisis son:

- *Detección de usos indebidos (misuse).* Para encontrar usos indebidos se comparan firmas con la información recogida en busca de coincidencias.

- *Detección de anomalías.* Para la detección de anomalías se manejan técnicas estadísticas que definen de forma aproximada lo que es el comportamiento usual o normal.

Aparte del análisis basado en firmas y estadísticas, también existe el análisis de integridad. Este es el método utilizado por las herramientas de verificación de integridad de archivos, que complementan a los IDSs. Estas herramientas detectan cambios en archivos u objetos, utilizando mecanismos robustos de encriptación.

El mecanismo de respuesta es otro de los factores que ayudan a definir el tipo de sistema de detección de intrusiones:

- *Respuestas pasivas.* En este caso, el detector no toma acciones que puedan cambiar el curso de un ataque. En vez de esto, se limita a enviar o registrar la alarma correspondiente al responsable calificado.

- *Respuestas activas.* Pertenecen a esta categoría aquellos sistemas que, además de generar la alarma correspondiente, reaccionan modificando el entorno. Un ejemplo de este tipo de respuesta activa consiste en el bloqueo de las acciones del intruso, o el cierre de la sesión del usuario sospechoso.

Lo visto hasta ahora nos permite realizar una clasificación de los sistemas IDS según diversos criterios. Aunque hay más formas de clasificar estos sistemas.

4.1.2. Firewall

Una de las estrategias más efectivas y ampliamente usadas para preservar la seguridad de las redes corporativas es un *firewall*. La idea básica es que los *hosts* y las redes dentro del *firewall* son confiables, y los de afuera son generalmente no confiables.

Todas las comunicaciones entre *hosts* dentro y fuera de la red pasan a través del *firewall*. El trabajo de éste es monitorear y filtrar todo el tráfico pasando por él y sólo permitir la comunicación correspondiente a ciertos servicios predefinidos o sistemas externos confiables. Por lo tanto, el tráfico entrante puede ser configurado para permitir el acceso solamente a los privilegiados y el tráfico de salida puede ser limitado si hay ciertos lugares indeseables.

Los *hosts* dentro del *firewall* tienen un grado razonable de confianza y por lo tanto tienen que aplicar menor control entre ellos. Usualmente secciones de una red interna emplearán por sí mismas *firewalls* para restringir el dominio de *hosts* confiables. Este arreglo es usualmente aplicado dentro de las redes de alto desempeño para dar capas de protección a la información. Con el crecimiento de las Extranets, un esquema similar es utilizado para crear zonas DMZ (Demilitarized Zones, Zonas Desmilitarizadas), donde la información compartida entre organizaciones está protegida del mundo pero continúa disponible para cualquier Intranet o VPN.

Los primeros *firewalls* para redes TCP/IP aparecieron en la mitad de la década de los 80s. Desde esos primeros *firewalls,* que implementaban simples y rudimentarios filtros de paquetes, hasta los actuales equipos capaces de analizar simultáneamente la actividad en múltiples capas de la red, la tecnología ha evolucionado mucho creando herramientas más sofisticadas y más seguras. La popularización de Internet ha originado múltiples problemas de seguridad hasta el punto en que, hoy por hoy, esta inseguridad inherente a la red, es según todos los expertos, el principal obstáculo para el éxito de las actividades de Comercio Electrónico. Los *firewalls* se han convertido, de esta forma, en equipo indispensable dentro de la arquitectura de cualquier red de computadoras que tenga acceso a Internet.

A pesar de que la familia de protocolos TCP/IP fue desarrollada inicialmente para el Departamento de Defensa de los Estados Unidos, existe en ella un número considerable de problemas de seguridad graves, inherentes al protocolo e independientes del nivel de corrección de cualquier implementación. El hecho de que un *host* confíe en algo tan vulnerable como la dirección IP que viene escrita en un paquete como única autentificación de la procedencia de dichos datos, los casi inexistentes mecanismos de validación asociados a los protocolos de ruteo o la falta de mecanismos que garanticen la confidencialidad y la integridad de los datos que viajan a través de una red son claros ejemplos de ello. Algunos de estos problemas pueden ser solventados mediante el uso de un *firewall*.

Los *firewalls*, junto con los antivirus, constituyen hoy en día la herramienta de seguridad más efectiva y ampliamente extendida en un nivel corporativo (y crece poco a poco a nivel casa, oficina o escuela gracias a la proliferación de *firewalls* personales) y se revela como el único mecanismo de seguridad verdaderamente efectivo para protegernos de estas vulnerabilidades intrínsecas al protocolo TCP/IP.

Los principales riesgos de una red con salida a Internet son los mismos que debemos tener en cuenta a la hora de proteger un sistema cualquiera: confidencialidad, integridad, autenticidad y disponibilidad.

Generalmente, los *firewalls* se configuran para protegernos contra cualquier intento de acceso no autorizado o no correctamente autentificado desde el exterior hacia el interior de nuestra red, o viceversa.

Adicionalmente, uno de los puntos más importantes a tener en cuenta es que un *firewall* nos proporciona un punto único e ineludible de acceso a nuestra red, donde podemos centralizar las medidas de seguridad y auditoría sobre la misma.

Un *firewall* no puede protegernos contra amenazas que no pasan a través de él. Como se indicó anteriormente, el *firewall* debe de ser el punto de acceso a nuestra red. Si esto no es así su efectividad es sólo parcial. Ejemplo de esto son las amenazas que proceden del interior de nuestra red. Un empleado malicioso, un troyano o algunos tipos de virus pueden usar mecanismos válidos 'desde dentro' para realizar acciones dañinas.

Los *firewalls* tampoco pueden protegernos contra clientes o servicios que admitimos como válidos pero que son vulnerables, como son mecanismos de *tunneling* sobre HTTP, SMTP u otros protocolos. Por último, los *firewalls* no son muy efectivos contra los virus, a pesar de que algunos fabricantes así lo anuncian. Los *firewalls* no pueden ni deben sustituir otros mecanismos de seguridad que reconozcan la naturaleza y efectos de los datos y aplicaciones que se estén manejando.

Para seleccionar un *firewall* adecuado a las necesidades de la organización es recomendable tener un análisis previo de los requerimientos, en lo que se refiere al uso de la infraestructura de red, así como un documento con las características y restricciones de la red actual; esto permitirá definir con mayor facilidad la ubicación, cantidad, características y tipo de *firewall* requerido, y reducirá problemas de compatibilidad con otros elementos de la red.

Descripción de tecnologías de *firewall*

Los *firewalls* son sistemas que controlan el flujo de tráfico entre dos o más redes empleando ciertas políticas de seguridad. Básicamente son equipos cuya funcionalidad se limita a permitir o bloquear el tráfico entre dos redes con base a una serie de reglas. Su complejidad reside en las reglas que admiten y en como realizan la toma de decisiones con base a dichas reglas.

La tecnología empleada en el *firewall* ha ido madurando con el avance de la industria especializada y ahora tenemos una amplia variedad de dispositivos que realizan la misma función de distintas formas. Una forma práctica y sencilla de comparar las bondades de cada plataforma es examinando las capas del modelo OSI, donde el *firewall* interactúa.

Como regla general, podemos afirmar que cuanto más bajas sean las capas en las que el *firewall* trabaja, su evaluación será más rápida y transparente pero su capacidad de acción ante ataques complejos es menor.

Básicamente existen 4 tipos de *firewall* con características y funciones claramente definidas: filtrado de paquetes, nivel de circuito, nivel de aplicación (*proxy*) y filtrado de paquetes dinámico.

Filtrado de paquetes

El filtrado de paquetes es una tecnología de primera generación que analiza el tráfico de la red en la capa de transporte. En una red de computadoras el paquete se examina para ver si cumple con las reglas definidas en el *firewall*, estas reglas identifican si la comunicación se permite, basadas en información propia del paquete, títulos de la capa de transporte y la dirección IP del paquete.

El filtrado de paquete se basa en los siguientes puntos, para decidir si el paquete puede comunicarse con nuestra red:

- La interfaz de la red física en que el paquete llega.
- La dirección IP de origen.
- La dirección IP de destino.
- El tipo de capa de transporte (TCP, UDP, ICMP).
- La capa de transporte del puerto de origen.
- La capa de transporte del puerto de destino.

El filtrado de paquetes generalmente no entiende a los protocolos de la capa de aplicación, usados en los paquetes de comunicación. En cambio, ellos trabajan aplicando un conjunto de reglas que se mantiene en el centro de TCP/IP.

Con ayuda de algunos ruteadores, se decide si se bloquea o se permite el tránsito de paquetes, mediante listas de control de acceso en función de ciertas características. Generalmente estas características para determinar el filtrado son: las direcciones origen y destino, el protocolo, los puertos origen y destino (en el caso de TCP y UDP), el tipo de mensaje (en el caso de ICMP) y la interfaz de entrada y salida en el ruteador.

Dicho filtrado se lleva acabo en la capa de red, ya que generalmente no procesan la información en los protocolos de alto nivel, como FTP. Los filtros de paquetes más empleados pueden descubrir IP, TCP, UDP, e ICMP. Usando un filtro de paquete que incluya el TCP/UDP, se pueden hacer o rechazar conexiones a computadoras, ese es el objetivo del filtro (ver figura 4.1).

Este tipo de tecnología no inspecciona los datos de la capa de aplicaciones del paquete de red, tampoco rastrea el estado de las conexiones, por lo que esta tecnología no es la solución más segura. Sin embargo, el filtrado de paquetes es la tecnología más rápida disponible, ya que su instalación y su administración son fáciles, y tiene más exactitud en el filtrado.

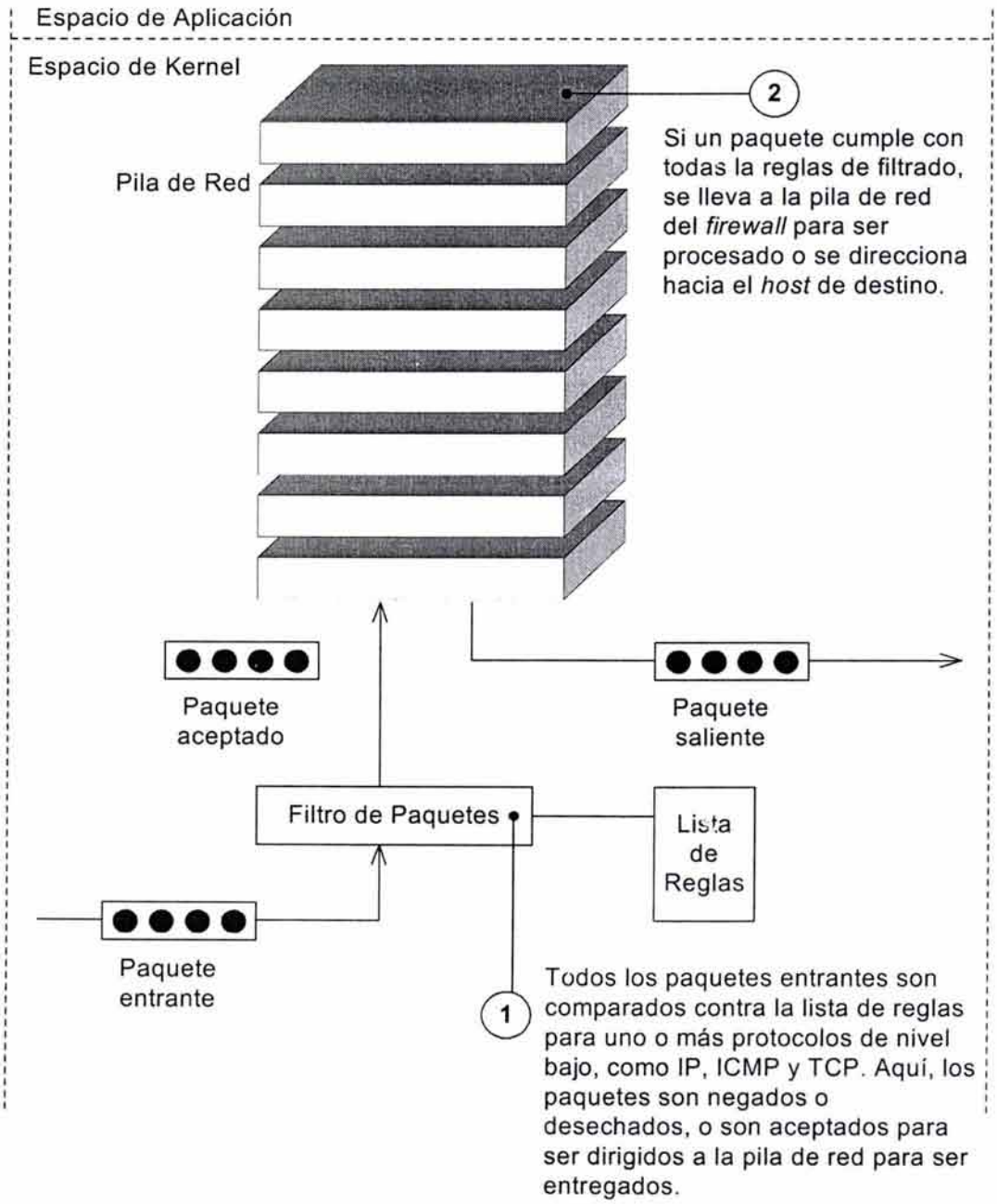

Figura 4.1. Arquitectura de firewall por filtrado de paquetes.

Los *firewalls* con la tecnología de filtrado de paquetes cambian la dirección IP de los paquetes de la red para que el tráfico que sale aparezca como si se hubiera originado en un transmisor diferente en lugar de un transmisor interior. El proceso de cambiar la

dirección IP de los paquetes de la red es llamado traducción de dirección de red. Ésta esconde la topología y se dirige a redes de la zona no confiable.

Esta tecnología tiene las siguientes ventajas:

- Es generalmente más rápido que otras tecnologías de *firewall*, porque estos hacen menos evaluaciones.
- Una sola regla puede ayudar a proteger la red completa, prohibiendo conexiones entre Internet y las computadoras internas.
- No es necesario configurar las computadoras cliente, el filtrado de paquete hace el trabajo.
- Junto con la traducción de dirección de red, se pueden usar los *firewalls* de filtrado de paquete para enmascarar la dirección IP interna.

Algunas de las desventajas del filtrado de paquete son:

- No entienden los protocolos de la capa de aplicación. Estos no pueden restringir el acceso a los subconjuntos protocolares para incluso los servicios más básicos, como los PUT o GET comandos en FTP.
- No guardan información sobre una sesión o aplicación.
- Tienen habilidades limitadas al manipular información dentro de paquetes.
- No ofrecen valor agregado, como HTTP o URL (Uniform Resource Locator, Localizador Uniforme de Recursos), ni autentificación, ya que no entienden los protocolos.
- No pueden restringir la información interna. Sólo restringen la información que puede ir hacia el *firewall*. Así, los intrusos pueden acceder a servicios en el servidor del mismo.
- No genera una auditoría.

Filtrado a nivel de circuito

Esta tecnología también es conocida como de inspección de estado. Esta pertenece a la tecnología de segunda generación de los *firewalls*. Trabajan para validar el hecho de que un paquete sea una petición de conexión o un paquete que pertenece a una conexión, o circuito virtual, entre dos capas de transporte.

Para validar una sesión, un *firewall* con tecnología a nivel circuito examina cada conexión para asegurarse de que sea auténtica para el protocolo de transporte que se está utilizando. Además, los paquetes no son enviados a su destino hasta que se complete la petición de conexión. El *firewall* mantiene una tabla de conexiones válidas (la cual incluye el estado de las conexiones) y permite que los paquetes de datos pasen a través de él cuando la información de estos paquetes concuerda con algún registro en la tabla de circuitos virtuales existentes. Una vez que la conexión finaliza, su registro en la tabla se elimina y el circuito virtual entre esas dos capas de transporte se cierra. La figura 4.2 muestra el proceso de evaluación utilizado por un *firewall* con tecnología a nivel circuito.

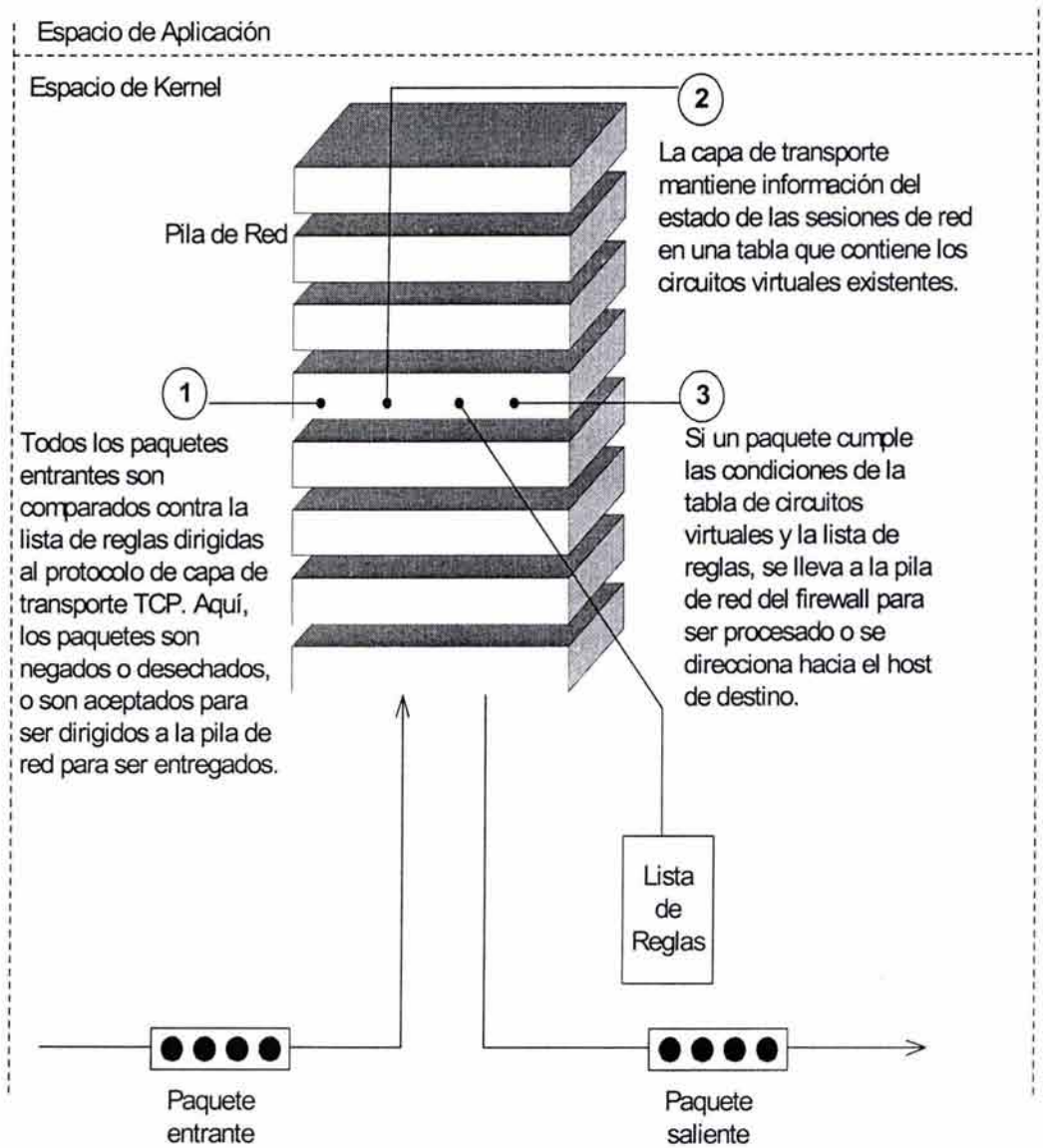

Figura 4.2. Arquitectura de firewall por filtrado a nivel circuito.

Cuando una conexión se completa, el *firewall* con esta tecnología registra información como:

- Un identificador de sesión único, que se utiliza para monitoreo de la conexión.
- El estado de la conexión: petición, establecimiento o cierre.
- La información de secuencia.
- La dirección IP de origen y destino.
- La interfaz física de red por la que entra el paquete.
- La interfaz física de red por la que sale el paquete.

Utilizando esta información, el *firewall* con tecnología a nivel circuito verifica la información de cabecera contenida en cada paquete de red para determinar si el equipo transmisor tiene permiso de enviar información al equipo receptor, y si el equipo receptor tiene permiso de recibir esa información.

Estos tienen un entendimiento limitado de los protocolos utilizados en los paquetes de red. Sólo pueden detectar un protocolo de capa de transporte, TCP. Trabajan aplicando un conjunto de políticas al igual que los *firewall* con tecnología de filtrado de paquetes.

Sólo aquellos paquetes de red que están asociados con una conexión existente son aceptados por el *firewall*. Cuando se recibe un paquete de establecimiento de conexión, el *firewall* con tecnología a nivel circuito verifica sus políticas y decide si la conexión debe ser aceptada o no.

Si la conexión es permitida, todos lo paquetes de red asociados con esa conexión son enrutados o encaminados por el *firewall,* como está definido en la tabla de enrutamiento sin ningún otro chequeo de seguridad. Este método es muy rápido y provee una cantidad limitada de chequeos.

Con está tecnología se puede realizar verificaciones adicionales para asegurar que un paquete de red no ha sido falsificado y que los datos de la cabecera del protocolo de transporte cumplen con la definición adecuada para ese protocolo, lo cual permite al *firewall* detectar formas limitadas de paquetes de datos modificados.

También usualmente modifica paquetes de red con el fin que las peticiones de *hosts* internos parezcan haber sido originadas desde éste, y gracias a esta característica son capaces de direccionar las respuestas de peticiones hacia los *hosts* internos.

En resumen los *firewalls* con tecnología a nivel circuito cuentan con estas ventajas:

- Son generalmente más rápidos que los de capa de aplicación, ya que realizan menos evaluaciones.
- Pueden ayudar a proteger una red entera prohibiendo conexiones entre fuentes específicas en Internet y *hosts* internos.
- En conjunto con NAT, se pueden asegurar IPs internas de la red pública.

Sus desventajas:

- No pueden restringir accesos a otros protocolos que no sean TCP.
- No pueden verificar la seguridad en una capa de más alto nivel, en caso que así se requiera.
- Tienen habilidades limitadas de generación de eventos de auditoría.
- No ofrecen características de valor agregado, como filtrado de páginas Web, almacenamiento de objetos HTTP, y autentificación porque no soportan los protocolos que se utilizan y no pueden diferenciar entre ellos.
- Puede ser difícil probar reglas de acceso y negación.

Filtrado a nivel de aplicación

El *firewall* con tecnología de capa de aplicación pertenece a la tecnología de tercera generación usada en *firewalls*, la cual funciona evaluando paquetes de red con la finalidad de validar los datos a nivel de capa de aplicación, antes de establecer una conexión. Este tipo de tecnología examina todos los paquetes de red a nivel de capa de aplicación, de acuerdo con el modelo de referencia OSI y mantiene un estado de conexión completa, además mantiene la secuencia de la información. Adicionalmente, este elemento de seguridad puede validar también otros datos que sólo aparecen en la capa de aplicación, tales como contraseñas de usuarios y otras peticiones de servicios.

Muchos de los *firewalls* con tecnología de capa de aplicación incluyen *software* de aplicaciones especializadas y servicios de *proxy*. Los servicios de *proxy* son programas de propósito especial que manejan el tráfico a través de un *firewall* para un servicio en específico, tal como HTTP o FTP. Los servicios de *proxy* son específicos para el protocolo que han sido diseñados, y pueden proporcionar un incremento en el control de accesos, cuidando de forma detallada la validación de los datos, generando también registros de auditoría acerca del tráfico que estos están transfiriendo.

Este tipo de arquitectura analiza el conjunto de comandos para un sólo protocolo en un espacio de la aplicación. Los servicios de *proxy* pueden analizar los datos de un paquete para proveer una seguridad adicional, incluso para los servicios de valor agregado como son los filtros de URL y autentificación de usuarios.

Cada *proxy* de aplicación requiere de dos componentes que son típicamente implementados como un ejecutable: un servidor *proxy* y un cliente del *proxy*. Un servidor *proxy* actúa como un servidor terminal para todas las peticiones de conexión originadas desde una red confiable por un cliente real. La comunicación de los usuarios internos hacia Internet pasa a través del servidor *proxy,* en lugar de permitir a los usuarios comunicarse directamente con otros servidores en Internet. Un usuario interno o cliente envía una petición al servidor *proxy* para conectarse con un servicio externo, tal como FTP o TELNET. El servidor *proxy* recibe la petición y éste, basado en ciertas reglas, definidas por el administrador de seguridad, permitirá o negará dicha petición. Los servidores *proxy* entienden el protocolo del servicio que se les está solicitando y por lo tanto sólo permiten el flujo de esos paquetes. A parte poseen beneficios adicionales, como es el registro de las sesiones de información y la autentificación de los usuarios importantes.

Por otro lado, un cliente del *proxy* es parte de la aplicación de un usuario que se comunica con el servidor *proxy* desde una red externa de parte de un cliente real. Cuando un cliente real hace peticiones de algún servicio en particular, el servidor *proxy* evalúa esas peticiones contra ese *proxy* y de acuerdo a ciertas reglas definidas en éste, se determina si se aprueba la petición. Si la petición es aprobada, el servidor envía la autorización al cliente del *proxy*, lo que origina una comunicación real con el servidor (ver figura 4.3).

Los servicios del *proxy* no permiten direcciones de una forma directa, además que los paquetes de red son forzados a pasar a través de éste para ser examinados y filtrados.

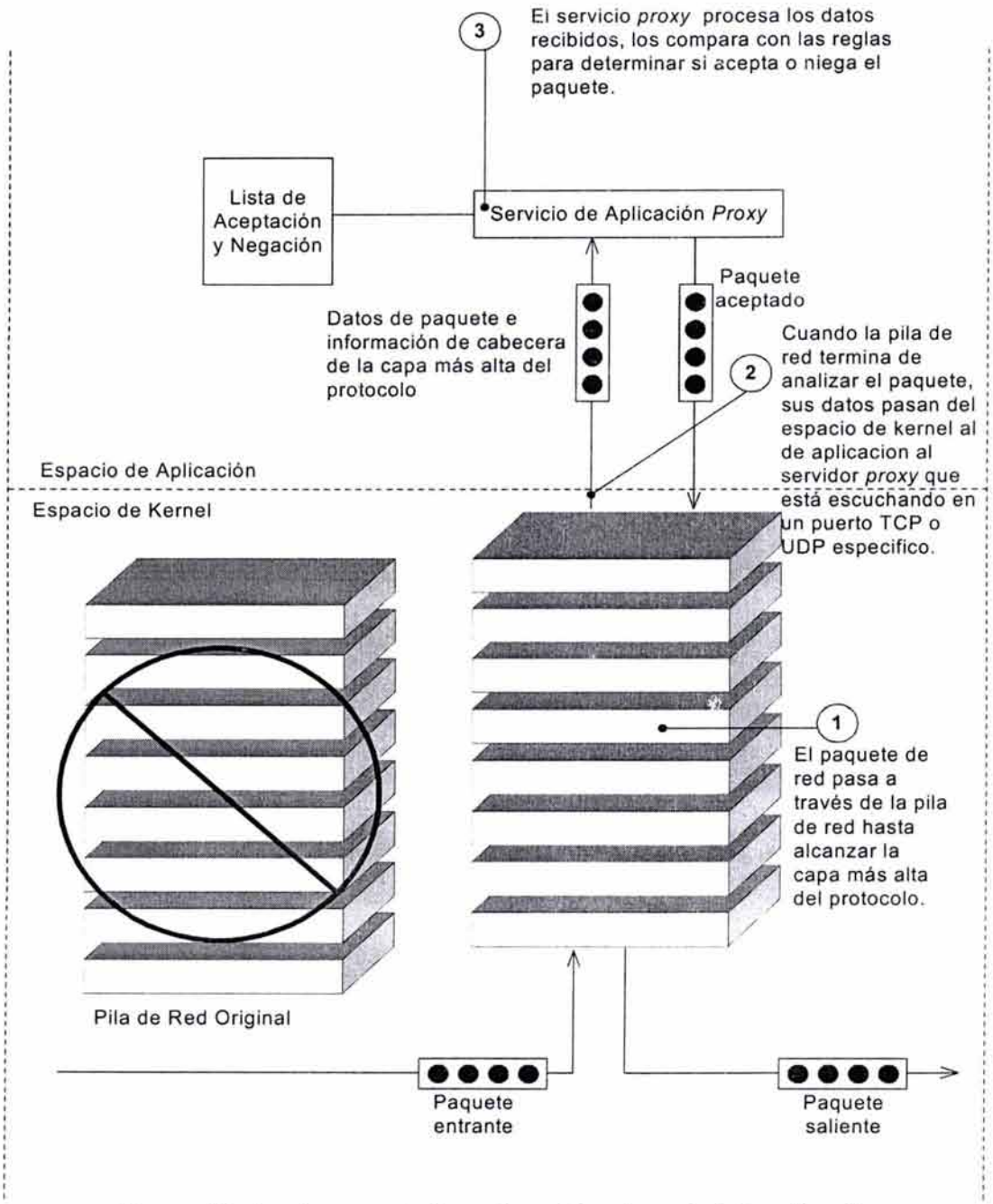

Figura 4.3. Arquitectura de firewall por filtrado a nivel de aplicación.

En vez de que la comunicación sea directamente con el servicio real, el usuario se tiene que comunicar primero con el *proxy* (ya que el *gateway* por omisión es un punto del servidor *proxy* sobre el *firewall*) para que éste preste el servicio solicitado y viceversa. Los *proxy* manejan todas las comunicaciones entre el usuario y el servicio real.

Un servicio de *proxy* se coloca en una forma transparente entre un usuario de una red interna y el servicio solicitado desde una red externa. El usuario hace una solicitud directa al servicio, mientras que el servicio hace la conexión directamente con el servidor *proxy*, en vez de la computadora terminal del usuario.

Los servicios de *proxy* están implementados en la parte más alta del *firewall* y operan en la sección de aplicación en el sistema operativo. Los paquetes deben pasar a través de los protocolos de bajo nivel del *kernel* antes de pasar al espacio de la aplicación. Este proceso provoca una notoria lentitud ya que para cada petición se hace una inspección de cada uno de los paquetes.

Como los *firewalls* con tecnología nivel de circuito, los *proxy* pueden ejecutar revisiones adicionales para asegurarse que los paquetes no han sido alterados o malformados y además hacen la traducción de direcciones de red.

Las ventajas principales que poseen los *proxy* son:

- Tienen la capacidad de entender protocolos de alto nivel, tal como los protocolos HTTP y FTP.
- Tienen la facultad de negar o permitir ciertos servicios de red.
- Son capaces de manipular y procesar paquetes de datos.
- No permiten una comunicación directa con el usuario final, así que externamente no se puede conocer a las terminales de cómputo confiables, es decir el *proxy* aísla la red interna del mundo exterior.
- Dan la apariencia de que el usuario está conectado al mundo exterior sin pasar por una barrera de protección.
- Tienen la capacidad de encaminar servicios hacia el interior de la red.
- Pueden generar registros de conexión, para cada sesión de los usuarios.
- También son capaces de realizar un filtrado de URL y pueden autentificar usuarios.

Pero también presentan ciertas desventajas, como son:

- Con ciertos servicios el *proxy* sufre retrasos, lo cual lo hace lento en su operación.
- No brindan protección para los protocolos UDP y RPC (Remote Process Call, Llamada de Procedimiento Remoto), entre otros servicios de la misma familia de protocolos.
- Son vulnerables a ciertos sistemas operativos y errores en el nivel de aplicación de ciertos servicios.
- Requieren de contraseñas o algunos otros procedimientos de validación, lo que provoca retrasos para el usuario.

Filtrado de paquetes dinámico

El *firewall* con tecnología de filtrado de paquetes dinámico es de segunda generación. Permite la modificación al vuelo de las reglas de seguridad en que se basa. Es

el más útil para proveer soporte al protocolo de transporte UDP, que es típicamente usado en el intercambio de peticiones y consultas (limitadas) del protocolo de nivel de aplicación.

Este *firewall* con tecnología de filtrado de paquetes dinámico complementa su funcionamiento asociando una conexión virtual a los paquetes UDP que cruzan el perímetro de seguridad. Si un paquete de respuesta es generado y enviado de vuelta al solicitante, entonces una conexión virtual se establece y al paquete le es permitido atravesar el servidor del *firewall*. La información asociada con una conexión virtual es recordada típicamente por un periodo corto de tiempo, y si no se recibe un paquete de respuesta dentro de ese lapso, la conexión virtual es invalidada.

Los *firewall* con tecnología de filtrado de paquetes dinámico tienen las mismas ventajas y desventajas que la tecnología de filtrado de paquetes de primera generación, con la notable excepción de no permitir paquetes UDP no solicitados en la red interna. Tan pronto como un paquete de petición UDP es originado en la red interna y entregado al *host* no confiable, el servidor del *firewall* permite que parezca como un paquete de respuesta por ser entregado al *host* no confiable que lo originó. El paquete de respuesta permitido debe contener una dirección destino que coincida con la dirección origen inicial, un puerto de destino que coincida con el puerto origen inicial y el mismo tipo de protocolo de nivel de transporte (ver figura 4.4).

Esta característica es muy útil para permitir que los protocolos de nivel de aplicación, como DNS, operen a través del perímetro de seguridad. Un servidor DNS interno debe originar peticiones a otros servidores DNS en Internet para recibir información de dirección de *hosts* desconocidos. Los servidores DNS pueden tomar estas peticiones usando una conexión TCP o una conexión virtual de UDP.

Los *firewalls* con tecnología de filtrado de paquetes dinámico también pueden ser usados para proveer soporte a un subconjunto limitado del protocolo de transporte ICMP.

Con frecuencia el ICMP es usado para probar la conectividad de la red al enviar un par de paquetes de red entre dos *hosts* en operación. Debido a que el servidor del *firewall* puede permitir que una respuesta cruce el muro como petición de un *host* interno, el *host* interno es capaz de deducir que existe un *host* en una red no confiable. Esta arquitectura provee gran desempeño para un subconjunto de paquetes de red.

Consideraciones para la elección de un *firewall*

La elección del tipo de *firewall* adecuado depende de las necesidades de seguridad de la organización pero típicamente se puede clasificar su uso de la siguiente manera:

- Filtrado perimetral entre redes con diferentes niveles de confianza y separación de redes: *firewall* por filtrado de paquetes y de nivel de circuito.

- Filtrado general a nivel de ruteo: *firewall* por filtrado de paquetes (los ruteadores son dispositivos que pueden considerarse en esta categoría).

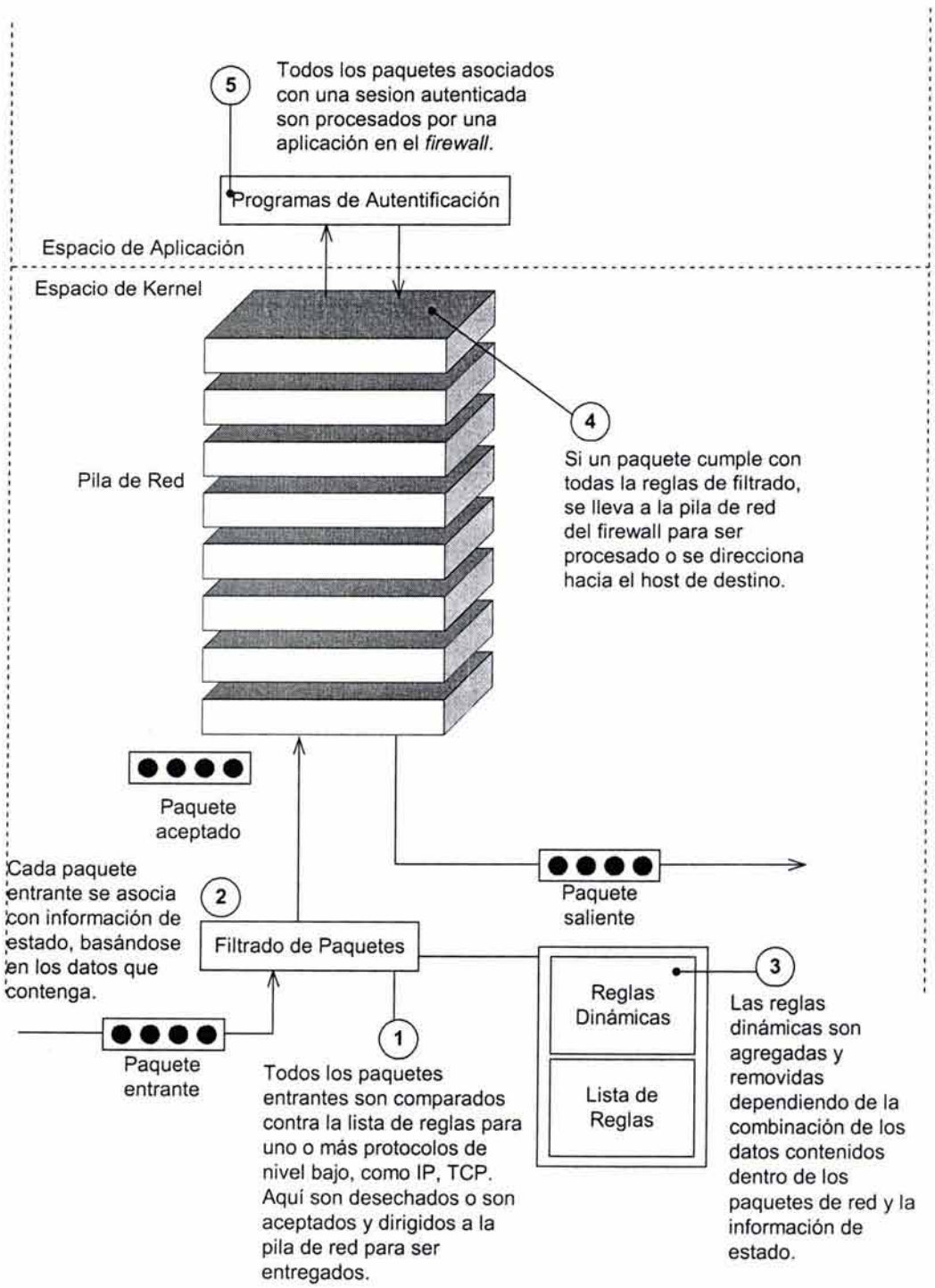

Figura 4.4. Arquitectura de firewall por filtrado de paquetes dinámico.

- Filtrado específico para acceso a servicios públicos (servicios proporcionados por servidores en zonas desmilitarizadas como son HTTP, SMTP, FTP, etc.) y control de acceso a servicios críticos en zonas de seguridad internas (por ejemplo acceso a bases de datos corporativas en la red local): *firewall* a nivel de aplicación.

No se puede considerar que un tipo de *firewall* sea mejor que otro, ya que cada uno posee funciones específicas. La combinación de los tipos de *firewall* en una arquitectura de seguridad ofrece el mayor nivel de seguridad posible y es recomendable.

Es importante recordar que los *firewalls* existentes hoy en día suelen combinar 2 o más tipos en un solo producto. El utilizar un solo producto que combina diferentes tipos de *firewall* tiene el inconveniente de generar un punto único de fallo pero es aceptable para la mayoría de las configuraciones.

Además de lo anterior, se debe considerar que los *firewall* pueden ser basados en *hardware* o *software*. La elección de uno u otro dependerá del caso específico y del análisis que haya realizado cada organización. A continuación, en la tabla 4.1, se comparan algunas características de ambos tipos de *firewalls* que pueden ser útiles en la selección de alguno de ellos:

	Firewall* basado en *hardware	***Firewall* basado en *software***
Escalabilidad	Las opciones de crecimiento de *hardware* son limitadas y suele ser necesario cambiar todo el dispositivo.	La integración a nivel aplicación permite seleccionar y modificar la base de *hardware* con mayor flexibilidad. Esto permite cambiar el *hardware* fácilmente cuando sea necesario.
Estabilidad	Estos dispositivos incluyen *hardware* y un sistema operativo extensivamente probado y adecuado por el fabricante para garantizar un correcto desempeño y compatibilidad.	Es necesario configurar manualmente dispositivos y sistema operativo para garantizar un desempeño adecuado. Se requiere efectuar también de un reforzamiento de la seguridad a nivel sistema operativo.
Flexibilidad en configuración de *hardware* y sistema operativo	Las opciones de configuración en *hardware* y sistema operativo subyacente están limitadas por el fabricante para garantizar estabilidad.	Existe mayor libertad para modificar la configuración de *hardware* y sistema operativo en caso necesario.

Tabla 4.1. Comparación de firewall.

Típicamente, los *firewalls* basados en *software* suelen ser más útiles a aquellas organizaciones que:

- Tienen cambios constantes en su infraestructura tecnológica y de red.

- Poseen personal dedicado para la administración y operación de los dispositivos y están altamente capacitados en el manejo de *hardware* y en la administración y configuración de sistemas operativos de la organización.

Asimismo, los *firewalls* de tipo *hardware* suelen traer más beneficios a organizaciones que:

- Carecen de personal dedicado (y especializado) para la administración, instalación y configuración del *firewall*.
- Carecen de personal especialista en sistemas operativos.
- Tienen pocos cambios (o cambios graduales) en su infraestructura tecnológica y de red.

Servicios adicionales

Un valor añadido sobre los *firewalls* actuales son los servicios adicionales de que disponen y que facilitan las labores de protección y administración de la red. Se trata de servicios específicos desarrollados a parir de los mismos y otros adquiridos de nuevas tecnologías pero que, en cualquier caso, representan un punto importante a la hora de decidirnos por una u otra implementación. En este apartado veremos brevemente algunos de ellos, como son: traducción de direcciones de red, protocolo de configuración dinámica de *hosts*, redes privadas virtuales, modeladores del ancho de banda o reguladores, autentificación de usuarios, balanceo de carga, integración de sistemas de detección de intrusos, PPTP (Point to Point Tunneling Protocol, Protocolo de *Tunneling* Punto a Punto) e IPsec.

Traducción de direcciones de red

Los servicios de NAT resuelven dos de los principales problemas de seguridad e infraestructura de las redes actuales. En primer lugar, constituyen una herramienta muy efectiva para esconder las direcciones de red reales de nuestra red interna. En segundo lugar, y debido a la reducción del espacio de direcciones IP disponibles, muchas organizaciones usan NAT para permitir la salida a Internet de sus equipos de la red interna con un mínimo de direcciones legalmente válidas.

Existen tres estrategias diferentes para implementar NAT: traducción de direcciones de red estática, de red oculta y de puertos.

Traducción de direcciones de red estática

En este esquema de NAT cada sistema interno de la red privada tiene su propia dirección IP exterior. Con este sistema se logra esconder el esquema interno de nuestra red, pero no la reducción de direcciones IP válidas de acceso al exterior. Los *firewalls* que incluyen esta característica usan para ello una simple tabla de correspondencia entre unas direcciones y otras.

Traducción de direcciones de red oculta

Con este esquema todos los sistemas de la red interna comparten la misma dirección IP externa. Reviste dos importantes inconvenientes: es imposible poner a disposición de los usuarios externos ningún recurso de la red interna, y obliga al *firewall* a usar su propia dirección externa como sustituta de la dirección de todos los equipos que protege, con lo cual implícitamente estamos revelando la dirección del mismo y lo hacemos susceptible de ser atacado directamente, además de restarle flexibilidad al sistema.

Traducción de puertos

El sistema PAT (Port Address Traslation, Traducción de Direcciones de Puerto) resuelve los dos problemas vistos en el esquema anterior, convirtiéndolo en la mejor forma de implementar NAT. En primer lugar no es necesario usar la dirección externa del *firewall*, sino que podemos crear otra dirección virtual para este propósito. En segundo lugar, es posible hacer accesibles recursos internos a los usuarios del exterior.

El *firewall* usa el puerto del cliente para identificar cada conexión entrante y construye a tal efecto una tabla de traducciones como la mostrada a continuación en la tabla 4.2.

Dirección IP interna	Puerto Cliente Interno	PAT
192.168.1.108	1028	3313
192.168.1.112	1039	3314
192.168.1.102	1400	3315
192.168.1.101	1515	3316
192.168.1.115	1027	3317
192.168.1.120	1026	3318

Tabla 4.2. Ejemplo de traducción de puertos.

La traducción de puertos se realiza de manera sucesiva y secuencial, dentro de un rango de puertos válidos. La tabla 4.2 es un ejemplo de este tipo de traducción, lo cual verificamos en la columna correspondiente a PAT de la misma tabla.

Por lo anterior, la traducción de puertos es la estrategia más conveniente, flexible, segura y por tanto la más ampliamente usada en la actualidad.

Protocolo de configuración dinámica de hosts

El servicio que proporciona el DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Hosts) es un servicio de asignación automática de direcciones IP con ventajas administrativas, importantes y evidentes, a la hora de mantener redes de tamaño medio o amplio, que muchos *firewalls* (sobre todo los que trabajan en las capas 2, 3 y/o 4) incluyen como valor añadido.

Redes privadas virtuales

Uno de los servicios adicionales más valorados de los *firewalls* actuales es la posibilidad de construcción de VPNs (Virtual Private Networks, Redes Privadas Virtuales), que permiten extender a las comunicaciones externas la seguridad del interior de nuestra red.

Una VPN se construye en la cúspide de la pila de protocolos ya existentes en la red usando protocolos adicionales y fuertes cifrados, así como mecanismos de control de integridad, sustitución o repetición de la información transmitida.

Existen diferentes formas de construir una VPN. Quizás la forma más lógica y comúnmente usada es utilizar para ello el estándar IPSec (IP Security, IP Seguro), consistente en una porción de las características de seguridad de IPv6, separadas y portadas para ser usadas en IPv4. Otras opciones son el estándar propuesto por Microsoft llamado PPTP o L2TP (Layer 2 *Tunneling* Protocol, Protocolo de Capa a *Tunneling*), propuesto por la IETF.

El motivo por el que se coloca el servidor de VPN en el *firewall* es evidente: colocarlo detrás de él haría que el tráfico cifrado entrante y saliente generado por el servidor VPN no pudiese ser inspeccionado totalmente y hubiera que obviar funciones como las de autenticación, *logging*, escaneo de virus etc. sobre todo este tráfico. Colocando el servidor VPN delante del *firewall* lo hacemos vulnerable a ataques directos.

El principal problema de las VPN es el elevado coste de recursos que supone el cifrado completo de las comunicaciones lo cual reduce considerablemente el ancho de banda efectivo. Una solución para mitigar este problema es usar una tarjeta de cifrado por *hardware*, las cuales suelen reducir en aproximadamente un 50% el tiempo necesario en realizar la encriptación.

Modeladores del ancho de banda o reguladores

Estos dispositivos, denominados *Bandwidth Shapers* o *Throttlers* en la literatura anglosajona, están adquiriendo un auge asombroso en los últimos tiempos y son ya muchas las formas en las que nos los encontramos: programas o elementos específicos o servicios de valor añadido en ruteadores o *firewalls*.

Un modelador del ancho de banda se emplaza entre la red interna y la salida a Internet (el mismo lugar del *firewall*, de ahí su inclusión en los mismos) y puede ser comparado con un 'guardia de tráfico'. Mediante reglas, se definen distintas colas, cada una de las cuales alberga un tipo distinto de tráfico: *e-mails*, transferencias de archivos, tráfico HTTP, archivos musicales o de video, etc. Cada una de las colas de tráfico posee una prioridad distinta, de forma que podemos poner en primer lugar aquellas que correspondan al tráfico más crítico para nuestra organización. El modelador realiza la distinción entre los distintos tipos de tráfico de formas muy diferentes, por ejemplo, inspeccionando directamente las cabeceras en busca de identificar un determinado protocolo, en función de

los puertos a los que son dirigidos los paquetes, etc. En algunos casos los *shapers* usan métodos similares a los antivirus y buscan patrones que identifican estos tráficos.

Aunque pueda parecer que estos métodos introducen más retardo que desahogo en el tráfico de la red, no es así en absoluto: los *shapers* analizan, al igual que los *firewall* con inspección de estado, sólo los primeros paquetes de una conexión y una vez que ésta es identificada la asignan a una cola de tráfico en particular hasta que ésta finaliza.

Autentificación de usuarios

Otro servicio básico en los *firewalls* a nivel de aplicación es la autenticación de usuarios, que en los dispositivos a nivel de red debe limitarse a la dirección IP de procedencia de la petición, con el consiguiente riesgo de suplantación, mientras que en estos pueden habilitarse servicios clásicos de combinación *login* y contraseña.

Balanceo de carga

Como hemos visto en las descripciones anteriores, uno de los principales inconvenientes de los *firewalls* es la disminución del rendimiento que provocan, efecto que se ve agravado en algunos esquemas más que en otros. Los *firewalls* empresariales de gama alta suelen ofrecer una solución para atenuar este problema al mismo tiempo que ofrecen redundancia mediante el balanceo de carga entre dos o más dispositivos *firewall*. Logramos, de esta forma, mejorar el problema del rendimiento y ofrecer alta disponibilidad y tolerancia a fallos en nuestra política de seguridad.

Integración con sistemas de detección de intrusos

Los IDS son herramientas o dispositivos que nos permiten inspeccionar nuestro sistema y generar alertas que nos ayudan a conocer cuando alguien ha tratado de penetrar en nuestro sistema o lo ha conseguido. Se trata de una tecnología relativamente nueva y en un grado aún bajo de madurez, pero que va ganando cada vez más importancia y mejores resultados. Existen dos tipos de sistemas IDS, los de *hosts* y los de redes. Los de redes se subdividen, a su vez, en distribuidos o no. Los IDS de *hosts* se basan en el análisis de las estadísticas de uso de ciertos recursos del sistema. Los IDS de red buscan patrones sospechosos en los paquetes TCP, malformaciones en la estructura de los mismos, etc. Se comportan como *sniffers* que poseen tablas (actualizables) con los patrones característicos usados en los intentos de entrar en un sistema.

PPTP

El protocolo PPTP, antecesor de L2TP, es una extensión del protocolo PPP. Fue diseñado por Microsoft para proporcionar comunicaciones autenticadas y cifradas entre un cliente y un *gateway* o entre dos *gateways* (sin necesitar una infraestructura de clave pública) utilizando un ID de usuario y una contraseña. PPPT proporciona un forma de enrutar paquetes de protocolos de punto a punto como IP, IPX o NetBEUI sobre un red TCP/IP. Apareció por primera vez en 1996, dos años antes de la disponibilidad de IPSec y

L2TP, y su objetivo era la simplicidad en su diseño, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP.

IPSec

A principios de 1995 el IETF desarrolló un conjunto de estándares para la seguridad del protocolo IP, conocida como IPSec. Este estándar es válido para IPv4 e IPv6, y provee un marco que permite a dos o más partes el uso de distintos algoritmos de encriptación y métodos de autentificación en una misma sesión de comunicación. Esta flexibilidad permite incorporar esta tecnología para integrar distintos participantes a bajo costo, sin necesidad de dispositivos adicionales.

IPSec modifica el protocolo IP (capa de red y superiores) y proporciona autenticación de origen, comprobación de integridad y, opcionalmente, confidencialidad de contenido basado en claves criptográficas.

IPSec implementa la seguridad al nivel de red. Esto permite a las aplicaciones permanecer independientes de la infraestructura de seguridad subyacente. Los datagramas IP se protegen sin tener en cuenta la aplicación que inicialmente generó el tráfico. IPSec es transparente para las aplicaciones.

Beneficios de un *firewall*

Los *firewall*s manejan el acceso entre dos redes; y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red dependería de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El *firewall* es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, cediendo al administrador la responsabilidad de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de *firewall*s se halla convertido en casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el *firewall*.

Los *firewall*s también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los *firewall*s también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

4.1.3. Antivirus

Los antivirus son programas que tratan de detectar si una aplicación ejecutable es infectada por un programa virus.

La mayoría de los antivirus pueden restaurar el archivo infectado a su estado original, aunque no siempre es posible, dado que los virus pueden haber hecho cambios no reversibles. Los antivirus pueden también borrar los archivos infectados o hacer el virus inofensivo.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener su operación y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.

Los antivirus se clasifican dependiendo de los servicios que nos proporcionan.

Tipos de antivirus

- Clasificación A, por acción:
  * Sólo detección.
  * Detección y desinfección.
  * Detección y aborto de la acción.
  * Detección y eliminación del archivo/objeto.

- Clasificación B, por método de detección:
  * Comparación directa.
  * Comparación por firmas.
  * Comparación de firmas de archivo (detección por comparación con atributos guardados).
  * Por métodos heurísticos.

- Clasificación C, por instante de activación:
  * Invocado por el usuario.
  * Invocado por actividad del sistema (abrir, ejecutar, copiar, guardar archivo).

- Clasificación D, por objeto infectado:
  * Sector de arranque.
  * Archivo ejecutable.
  * Macrovirus (Excel, Word).
  * Java.

Por otro lado, la estructura de un programa antivirus se compone de módulos.

Módulos antivirus

Un antivirus está compuesto por dos módulos principales: el primero denominado de control y el segundo denominado de respuesta.

- Módulo de control. Es una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera. Permite la identificación de virus, la identificación de código dañino, también posee una administración de recursos para efectuar un monitoreo de las rutinas a través de las cuales se accede al *hardware* de la computadora.

- Módulo de respuesta: La función alarma se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

La pauta en el desarrollo de antivirus la marca la asociación AVPD (Antivirus Product Developers, Desarrolladores de Productos Antivirus), una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

- Cheyenne Software.
- B. M.
- Intel.
- McAfee Associates.
- ON Tecnology.
- Stiller Research Inc.
- S&S International.
- Symantec Corp.
- ThunderByte.

4.1.4. Filtros

Los filtros son elementos adicionales de seguridad nivel de aplicación. Los más comunes son: filtros para correo *spam* y filtros para *spyware*.

Filtros para correo *spam*

Como se mencionó en capítulos anteriores, el *spam* es denominado como correo basura, el cual se encarga de inundar Internet con varias copias (incluso millones) del mismo mensaje.

El *spam* ocasiona problemas que nos cuestan tiempo y dinero. Para aquellos que acceden a su correo por un servicio tarificado en base en el tiempo de conexión, los costos siguen corriendo mientras se lee o recibe el correo, lo cual, al recibir montones de basura, les cuesta dinero adicional. A un nivel superior, a los proveedores de Internet y a los servicios en línea les cuesta dinero el transmitir el correo basura, costo que se añade posteriormente a la cuota de sus suscriptores.

La inmensa mayoría de los correos basura, que son indiscriminadamente enviados por la red, casi sin excepción anuncian géneros sin el más mínimo valor, engañosos y en ocasiones fraudulentos.

Una forma de evitar que se reciba correo indeseado consiste en filtrar todo el correo entrante. Existen soluciones de correo electrónico que permiten tener un mayor control del tráfico de correo electrónico. Estos productos ofrecen protección contra *spam* y virus, y permiten establecer políticas de seguridad mediante diversas herramientas de administración.

No existe ninguna duda de que el *spam* y los virus suponen un serio problema para empresas conectadas a Internet, provocando períodos de inactividad, pérdida de productividad y confidencialidad de datos.

Las opciones de configuración de estos filtros permiten que las organizaciones definan la identificación de sp*am* y aseguren el cumplimiento de políticas internas. También permiten la verificación de cada mensaje que pasa por el servidor de correo electrónico, ofreciendo un nivel extra de protección contra gusanos de correo electrónico y virus. Así, se protegerá la red contra la entrada de código malicioso.

Filtros de *spyware*

Los *spyware* o archivos espías son pequeñas aplicaciones cuyo objetivo es el envío de datos del sistema donde están instalados, mediante la utilización de la conexión a la red, a un lugar exterior, el cual por lo general resulta ser una empresa de publicidad de Internet. Estas acciones son llevadas a cabo sin el conocimiento del usuario.

Hay que aclarar que, aunque evidentemente tienen cierta similitud con los programas troyanos, los *spyware* no representan un peligro de manipulación ajena del sistema, ni de daños a nuestro ordenador por parte de terceros. Sus efectos son, simple y llanamente, la violación de nuestros derechos de confidencialidad de nuestros datos, así como una navegación por Internet más lenta.

Normalmente estos archivos vienen acompañando a programas de tipo "*shareware*" (gratuitos por cierto tiempo).

Terminada la breve descripción de las soluciones, que hoy en día podemos obtener para proveer seguridad a las redes, se hace la propuesta de integración.

4.2. PROPUESTA DE SOLUCIÓN INTEGRAL

Después de haber descrito las principales tecnologías hasta hoy existentes para el aseguramiento de una red, y de hacer un análisis de las debilidades que la red posee, nos hemos inclinado por la integración de un sistema de seguridad que contenga las soluciones más robustas del mercado, con el fin de disminuir en la medida de lo posible las vulnerabilidades que la red corporativa presenta.

Nuestra propuesta comprende la integración de varios sistemas de seguridad como son: *firewall*, un sistema de detección de intrusos, antivirus y filtros.

El equipo *firewall* se colocaría en la frontera de la red corporativa e Internet; con esta solución detendríamos tráfico no deseado, como servicios no explícitamente autorizados a través de políticas o reglas determinadas. Asimismo, este equipo deberá permitirnos la posibilidad de desarrollar un esquema de alta disponibilidad en los servicios proporcionados por el corporativo.

Los *firewalls* son cada vez más capaces de proveer encripción y esto es usado para crear, a partir de este equipo, túneles VPN seguros sobre redes públicas como Internet. Los encriptores están incrementando sus capacidades para decidir que información pasar y/o rechazar o encriptar utilizando ciertas reglas. Estas reglas pueden abarcar las direcciones fuente, direcciones destino, tipo de protocolo e información de la capa de transporte. Por lo tanto hay una tendencia para que los *firewalls* incluyan finalmente todas las propiedades de los encriptores.

Adicionalmente, se propone la instalación de un sistema de seguridad IDS que incluye métodos de detección de tráfico malicioso, con la capacidad de abortar ataques y prevenir los daños que éstos puedan generar a la red. Dicho equipo está basado en firmas de seguridad que reconocen casi todos los patrones de ataque. Esta solución de seguridad puede ser colocada delante de un ruteador o *firewall* y tiene como objetivo proteger, asegurar, controlar, monitorear y analizar todo el tráfico de la red. Además, posee la capacidad de determinar que tráfico es válido y que tráfico es malicioso, ya sea de la red pública hacia la red corporativa o viceversa.

Otro sistema importante que debe estar presente en la seguridad de la red es el antivirus, en este caso no se integra a la solución de seguridad propuesta, ya que actualmente se tiene un sistema de antivirus corporativo ya implementado. Sin embargo, se propone en la propuesta económica que se mencionará en párrafos siguientes.

De manera suplementaria se tiene previsto el uso de aplicaciones de filtrado de correo *spam* y *software spyware*, con la intención de preservar la eficacia de los servicios de Internet proporcionados a los empleados autorizados del corporativo, ya que aunque son considerados sucesos eventuales, hoy en día se ha incrementado la frecuencia con que terceras personas emplean estas técnicas en Internet, creando una amenaza para el desarrollo de las actividades de los usuarios de la red corporativa.

Con los elementos contemplados en la propuesta anterior se obtiene un sistema de seguridad que integra algunas de las tecnologías de seguridad mencionadas, y mejora las estrategias de seguridad previamente existentes en la red corporativa, cubriendo el aspecto crucial de la empresa de mantener sus servicios en alta disponibilidad.

Para la implementación de la propuesta se realizó una evaluación de equipos que contemplamos en la misma.

4.2.1. Comparación de equipos IDS

Recientemente, a finales del año 202, la revista CRN (Computer Reseller News, Noticias De Distribuidores de Computadoras) publicó una evaluación de productos IDS disponibles en el mercado, comparando equipos de los fabricantes Cisco, NetScreen y Sleuth9.

En la tabla 4.3 se muestran las calificaciones que obtuvieron los productos.

CRITERIOS TECNICOS	CISCO	NetScreen	Sleuth9
Confiabilidad del producto	98.7	93.7	85.0
Precisión	94.7	91.0	83.5
Precio/desempeño	69.3	85.6	70.0
Facilidad de administración	71.9	80.0	70.4
Escalabilidad	78.2	70.6	67.6
Promedio técnico compuesto	82.6	84.0	75.3
CRITERIOS DEL PROVEEDOR			
Soporte Técnico	87.7	82.7	79.2
Rentabilidad	71.3	71.9	71.2
Retorno de la inversión	69.9	72.2	70.3
Capacitación y certificación	59.9	54.4	54.7
Soporte de Mercadotecnia	54.3	53.3	53.0
Soporte de Ventas	53.3	48.3	53.7
Promedio combinado del proveedor	66.2	63.9	63.7
PROMEDIO GENERAL	**73.6**	**72.9**	**69.0**

Tabla 4.3. Calificaciones de comparación de productos IDS.

Calificaciones: 100 = muy satisfecho, 1 = insatisfecho.
Familias de productos: Cisco Intrusion Detection System, Netscreen y Sleuth9.
Proveedores de soluciones entrevistados: 331.

En esta evaluación Cisco IDS recibió la calificación general más alta, superando a NetScreen por sólo 0.7 puntos; NetScreen recibió la mayor calificación técnica contra Cisco, superando también a Sleuth9. En revisiones similares de la revista CRN, NetScreen

también ocupó un lugar alto por los mejores productos *firewall*, haciendo claramente a NetScreen el mejor proveedor de soluciones de seguridad de la industria.

Algunos puntos importantes que llevaron a NetScreen a su actual posicionamiento son:

- La calificación técnica general más alta contra Cisco y Sleuth9, citando el mejor precio/desempeño y la mejor facilidad de administración como fortalezas particulares.
- En el criterio combinado del proveedor, NetScreen ganó las marcas más altas por el potencial de rentabilidad, así como su robusto retorno de la inversión.
- NetScreen fue declarado ganador entre los grandes proveedores de soluciones mientras que Cisco fue declarado una mejor opción para los pequeños proveedores de soluciones.
- NetScreen tiene una mejor capacidad de administración, un ámbito que Cisco ahora pretende mejorar.
- Cisco tiene deficiencias en precio/desempeño debido a que el costo de propiedad del producto es mucho mayor que el de NetScreen y Sleuth9.

4.2.2. Comparación de equipos *firewall*

Los principales fabricantes de *firewalls* del mercado que ofrecen equipos de alto rendimiento, prestaciones y con las principales funcionalidades en cuanto a gestión, filtros, reglas, mecanismos de autentificación, generación de bitácoras e integración con herramientas de terceros fabricantes para filtrado de contenidos son: NetScreen, Cisco y Nokia/CheckPoint.

NetScreen 204

La tecnología NetScreen produce dispositivos de propósito específico para la seguridad de redes (medianas, grandes, sitios de comercio electrónico, centros de datos, etc.) que combinan *firewall*, VPN (Virtual Private Network, Red Virtual Privada) y funciones de administración de tráfico. Se caracteriza por contar con encripción IPsec, permitiendo su integración a cualquier red de datos. Su administración es sencilla ya que se realiza por medio de cualquier explorador de Internet.

Cuenta con cuatro puertos ethernet 10/100 Base-T que auto-detectan la velocidad y polaridad de equipo al otro lado del cable. Al utilizar múltiples interfaces las redes pueden ser segmentadas, aumentando así la separación de las amenazas de los recursos críticos.

El *firewall* de NetScreen utiliza tecnología basada en la inspección de estado, protegiendo así las redes contra intrusos y ataques de negación de servicio, SYN, inundación ICMP, escaneo de puertos y otros, sin importar el número de sesiones abiertas. Cada interfaz soporta la configuración de hasta 28 prevenciones de ataques.

Una característica importante es que las políticas de acceso y los algoritmos de encripción se procesan en *hardware*, el cual es un método significativamente más rápido que el proceso por *software*, ya que libera el CPU para que éste controle el flujo de datos. El proceso por *hardware* está ligado firmemente al sistema operativo propietario ScreenOS, para eliminar agujeros de seguridad que se encuentran en otros productos construidos sobre sistemas operativos de propósito general.

Es posible utilizar el servicio NAT y PAT, para proteger IPs internas e IPs que no son direccionables.

Todos los equipos NetScreen soportan la conexión VPN entre ellos o la conexión con un cliente remoto aún cuando existan dispositivos que utilizan NAT. Combina junto con ésta la encripción DES (Data Encryption Standard, Estándar de Encripción de Datos), 3DES (Triple Data Encryption Standard, Estándar de Encripción de Datos Triple) y AES (Advanced Encryption Standard, Avance del Estándar de Encripción) utilizando certificados digitales a una velocidad de 200 Mbps. Es posible crear varias VPNs de los sitios remotos hacia el centro de cómputo central para que este último se encargue de direccionar el tráfico y lograr VPNs de sitios remotos a sitios remotos, evitando así la configuración de cada uno de ellos hacia los restantes.

La administración de tráfico permite el monitoreo, análisis y asignación de ancho de banda utilizado por varios tipos de tráfico de red en tiempo real, esto contribuye a que el tráfico crítico de la red no se vea afectado por aplicaciones que podrían pasar a segundo término. Esta administración se realiza con base en las direcciones IP, usuario, aplicaciones u hora del día. También es posible asignar un ancho de banda garantizado para algunas aplicaciones y fijar a otras un máximo. El *firewall* realiza sus funciones a una velocidad de 400 Mbps.

Soporta la configuración en alta disponibilidad, manteniendo sincronización completa de sesiones incluyendo asociaciones con IPsec. Debido a que todas las sesiones e IPsec son mantenidas por ambos dispositivos, la interrupción de los servicios es cercana a cero en el momento de la activación del *firewall* de respaldo.

Puede ser configurado como servidor DHCP para asignar direcciones IP a la red interna. Esto aleja la pesada administración asociada con el manejo de las direcciones IP. También elimina la necesidad de instalar y configurar un servidor que proporcione esta función.

Los *firewalls* NetScreen pueden opcionalmente se integrados con Websense, para bloquear contenido inapropiado y eliminar la navegación en Internet que reduce las horas de trabajo efectivo. Websense puede ser instalado en el mismo sitio junto con el dispositivo NetScreen, así los sitios remotos podrán filtrar tráfico por medio del servidor Websense sin tener que contar con su propio servidor de filtrado.

Todos los *firewalls* NetScreen soportan la configuración en modo transparente, donde las interfaces no cuentan con una dirección IP. Esto permite que el dispositivo de seguridad se implemente de forma más fácil en redes complejas, debido a que los otros

dispositivos no necesitan de un cambio significativo en su configuración. En este modo de operación se soportan las características de protección contra ataques, túneles VPN y administración de tráfico.

Cisco PIX 525

Este *firewall* proporciona seguridad para redes de empresas medianas y grandes en un dispositivo de propósito específico. Está integrado en un diseño de montaje en *rack*. En el núcleo del sistema se encuentra un esquema de protección basado en ASA (Adaptive Security Algorithm, Algoritmo de Seguridad Adaptable) que ofrece funciones de *firewall* orientadas a la conexión. La seguridad es menos compleja y más robusta que el filtrado de paquetes. También ofrece un mayor rendimiento y es más ampliable que los *firewalls* con *proxy* a nivel de aplicación. ASA hace un seguimiento de la dirección de origen y de destino, de los números de secuencia del protocolo TCP, de los números de puerto y de otros indicadores TCP de cada paquete. Se permite el acceso a través del *firewall* sólo si existe una conexión adecuada para validar el paso, proporcionando a las organizaciones un acceso transparente a los usuarios internos y externos autorizados, al tiempo que protege las redes internas de accesos no autorizados. Tiene disponibles hasta 8 puertos Fast Ethernet o 3 puertos Gigabit Ethernet. Proporciona 330 Mbps de transferencia de datos con la habilidad de manejar más de 280,000 sesiones simultáneas.

El modelo PIX 525 permite realizar comunicaciones privadas seguras a través de Internet o de cualquier red IP. Integra las características clave de las VPN (conexión en túnel, cifrado de datos, seguridad y *firewall*) para proporcionar plataformas seguras y con capacidad de ampliación a fin de aceptar mejor y con mayor rentabilidad la conexión de acceso remoto, de oficina remota y extranet utilizando servicios públicos de datos. PIX 525 proporciona a los usuarios una total implementación de los estándares IPsec. IPSec garantiza la confidencialidad, la integridad y la autenticidad. Para conseguir un cifrado de datos seguro, la implementación de Cisco de IPSec es compatible con los algoritmos DES de 56 bits y 3DES de 168 bits.

Utiliza mecanismos de inspección especializados para las múltiples aplicaciones de hoy en día. Además, los administradores pueden crear fácilmente políticas de seguridad personalizadas para el tráfico del *firewall* utilizando los métodos de control de acceso y las más de 100 aplicaciones predefinidas, servicios y protocolos que reconoce el *firewall*.

Las capacidades integradas de protección contra intrusión pueden proteger las redes corporativas de muchos ataques populares como negación de servicio, paquetes malformados, inundación, falsificación de IP, además de las más de 55 firmas de diferentes ataques. En caso de registrar algún ataque puede bloquearlo y notificar al administrador inmediatamente.

Algunos modelos de la serie 525 poseen capacidades contra caídas de sistema que proveen protección continua a la red corporativa. Entre dos equipos configurados con esta característica existe comunicación continua y sincronización de datos de configuración. En el caso de existir una caída de sistema las sesiones son automáticamente controladas por el *firewall* de respaldo con transparencia completa para los usuarios.

Algunas características adicionales:

- Sistema operativo propietario que elimina los riesgos de seguridad asociados con sistemas operativos de propósito general.
- Incluye filtrado de contenido para Java y ActiveX.
- Soporta el estándar IPsec.
- Provee soluciones de terceros para filtrado de URL, de contenido y protección contra virus entre otras.
- Acepta la creación de políticas de seguridad basadas en VLANs (Virtual Local Area Networks, Redes de Área Local Virtual).
- Contiene soporte para servicios dinámicos de ruteo OSPF (Open Shortest Path First, Abrir la Ruta más Corta Primero).
- Entrega seguridad en los ambientes que utilizan NAT.
- Soporta balanceo de cargas.
- Entrega reportes históricos y en tiempo real.

Nokia/CheckPoint IP440

Este producto, también conocido como *Firewall-1*, es multiplataforma es decir puede ser instalado en distintos sistemas operativos como son: Windows, Linux, Solaris entre los más comunes. Pero principalmente se integra con los equipos de seguridad Nokia, obteniéndose de esta fusión un dispositivo de propósito específico. Tiene la característica de ser escalable, trabajar como *cluster* y trabajar como una sola entidad además de soportar VPN, adicionalmente se puede actualizar esta solución de seguridad estando el equipo en producción, lográndose así no detener ningún servicio fundamental para el desarrollo de las empresas.

El *Firewall-1* sumado con el sistema de seguridad de Nokia permite un flujo más rápido de los paquetes que pasan a través de éste hacia el segundo, reduciéndose así la saturación por paquetes, observando una notable mejora en la comunicación con la red pública.

Esta solución está integrada por los siguientes elementos: Un dispositivo Nokia con sistema operativo IPSO, el IPSRD (Ipsilon Routing Deamon, Demonio de Ruteo Ipsilon), el *software* de CheckPoint *Firewall-1* y la interfaz de administración del equipo Nokia llamado Voyager.

Sistema operativo IPSO

Este es un sistema operativo UNIX basado en FreeBSD. El nombre de IPSO proviene de la versión Ipsilon, desarrollada por los ingenieros de Nokia. IPSO fue creado para mejorar las capacidades de ruteo y mejorar las funcionalidades de *Firewall-1*. Cabe destacar que fueron removidas algunas de las características innecesarias de este Unix, con el fin de facilitar la administración del sistema.

IPSRD

El demonio (también llamado proceso o programa) de ruteo Ipsilon, es un programa propietario de Nokia desarrollado para mejorar el ruteo. La política de ruteo implementada por IPSRD reside en una base de datos dentro del sistema. A través de la interfaz Voyager se configura, se mantiene el ruteo y la base de datos.

Firewall –1

El *firewall* de CheckPoint posee de dos componentes principales: el módulo del *firewall* y el módulo de administración. El primero corre en el *firewall* de Nokia y es donde se alojan o implementan las políticas de seguridad, el módulo de administración puede funcionar en el mismo dispositivo Nokia o en una estación de trabajo externa. En el módulo de administración se definen y se mantienen las políticas de seguridad.

Voyager

El Voyager es una interfaz desarrollada por Nokia basado en HTML, la cual a través de un navegador el administrador se comunica con el *software* de ruteo, configura las interfaces del dispositivo, define los protocolos de ruteo, configura las políticas de ruteo para el *firewall*, puede monitorear el tráfico de la red y observar el comportamiento tanto como del *hardware* (utilización de CPU, memoria RAM, estado de las interfaces y espacio en disco) como del ruteo.

El *Firewall-1* de CheckPoint incorpora algunos beneficios de seguridad como control de accesos, autentificación, administración con dispositivos de terceros, traducción de direcciones de red (NAT), seguridad de contenidos (antivirus, URL y Java/ActiveX), balanceo de cargas, auditoría y una administración integral de la seguridad de la empresa. Además puede adicionársele varios elementos de seguridad propietarios como son: VPN-1 SecuRemote, VPN-1 Pro, SmartDefense, SmartView Reporter y FloodGate-1.

Los elementos mencionados se pueden integrar junto con los sistemas de Nokia para formar una sólida solución de seguridad. Nokia propone sistemas de acuerdo al tamaño de la empresa. Actualmente, la empresa tiene una dimensión considerada de tipo mediano, por lo que la recomendación que propone Nokia para este tipo de red es el modelo IP440.

El dispositivo IP440 de Nokia posee puertos que soportan una alta densidad, un número de conexiones adecuado para los clientes de una empresa mediana, usando la interfaz con la tecnología 10/100 Mbps Ethernet o Gigabit Ethernet. En esta plataforma se integra el *Firewall-1* de CheckPoint, además que tiene la facilidad de configurarse en alta disponibilidad.

Características técnicas del dispositivo Nokia IP440

- Compatibilidad con los protocolos de Internet: IP, ICMP, ARP, RIP, OSPF, IGMP.
- Soporte a redes LAN: Ethernet 10/100, Ethernet Gigabit, Fibra Multi-modo.

- Soporte de redes WAN: PPP, Frame Relay, HDLC Cisco, T1/E1, ATM, V.35/X.21.
- Ancho de Banda: 507 Mbps del *firewall* y 115 Mbps para VPN.
- Administración: SNMP, TELNET, FTP, SSH, HTTP, SSL (Secure Socket Layer, Capa Segura de Localidad) y utilidades de línea de comando.
- Alta disponibilidad: Protocolo VRRP (Virtual Routing Redundancy Protocol, Protocolo de Redundante de Ruteo Virtual), modo *cluster* y disco espejo.
- Seguridad: SSH (Secure Shell, Seguridad del Interprete de Comandos), SSL, control de listas de accesos, administración del tráfico, autentificación centralizada, IPsec, cliente de DNS, NTP (Network Time Protocol, Protocolo de Tiempo de Red) cliente y servidor.
- Estándares soportados: IPsec, PPTP, L2TP, GRE (Generic Routing Encapsulation, Encapsulamiento Genérico de Ruteo).

En la tabla 4.4 podemos comparar características generales de los tres modelos que mencionamos anteriormente.

Características	***NetScreen-204***	***Cisco PIX 525R***	**Nokia IP440 (Check Point)**
Rendimiento *Firewall*	400 Mbps	370 Mbps	185 Mbps
Funcionamiento 3DES VPN	200 Mbps	~ 70 Mbps con tarjeta aceleradora	~ 45 Mbps con tarjeta aceleradora
Número de Interfaces	4	2 a 6	4 a 16
Desempeño en Alta Disponibilidad (HA)	Sí	No	Sí
Administración de Tráfico	Sí	No	No
Desactivación NAT	Sí	No	Sólo clientes CP hacia FW-1
VPN a cualquier interfaz	Sí	No	Sí
Modo Transparente	Sí	No	No
Suplementos Extras	No necesario	Licencia 3DES: $3,000 USD Tarjeta VPN: $7,500 USD	Tarjeta VPN: $1,000 USD

Tabla 4.4. Comparación de características generales.

Analizando las características ya mencionadas de los modelos propuestos podemos observar que el *firewall* NetScreen-204 es el modelo más conveniente por las ventajas que proporciona.

4.2.3 Comparación de antivirus

La revista PC World publicó, en su edición de septiembre de 2001, un análisis comparativo realizado a los principales productos antivirus.

Se evaluaron siete de los antivirus más importantes: F-Secure, Mc Afee VirusScan, Norman Virus Control, Panda Antivirus Platinum, Sophos Antivirus p/Windows, Symantec Norton Antivirus y Trend Micro PC-cillin.

Para evaluar la eficacia de estas aplicaciones se probó su habilidad para encontrar virus, destruirlos y reparar el daño que causan. Se descargaron en el disco duro todas las firmas (cadenas identificadoras) y 352 archivos infectados con 225 virus y seis Troyanos, tomados de un directorio compilado por WildList Organization International. Los resultados obtenidos con esta evaluación se resumen en la tabla 4.5.

La tabla muestra información valiosa sobre de las características técnicas de los antivirus más importantes dentro del mercado de la seguridad. Con base en estas características se puede tomar una decisión para una buena elección de esta herramienta. Nuevamente cabe señalar que en la propuesta que se presenta ya no se contempló la instalación de un antivirus, porque la empresa cuenta con una solución corporativa instalada.

4.2.4. Comparación de productos anti-*spam*

En el mercado existen varios productos anti-*spam*, los más usados son: Sopho Pure Message, IntelIdeas y Cymcom System.

Sophos *PureMessage*

Es una solución completa, que permite tener un mayor control del tráfico de correo electrónico en empresas. Algunas de sus características son:

- Permite establecer políticas de seguridad mediante diversas herramientas de administración.
- Revisa cada mensaje que pasa por el servidor de correo electrónico.
- Ofrece un nivel extra de protección contra virus.
- Permite a las empresas controlar el uso del correo electrónico (brechas de confidencialidad, responsabilidad legal, pérdida de productividad y mala reputación).

Programa	F-Secure 5.21	McAfee VirusScan 5.13	Norman Virus Control 5	Panda Antivirus Platinum 6.23	Sophos Antivirus para Windows 95/98/Me	Symantec Norton Antivirus 2001	Trend Micro PC-Cillin 2000
Precio en USD (5/27/01)	$125 Se ofrecen una versión gratuita para particulares	$29	$60	$60	$60	$40	$40
Virus ignorados en prueba de muestreo total	0/5	1/1	0/0	0/0	6/6	1/1	1/1
Virus desconocidos	1	2	6	0	14	3	10
Positivos falsos	0	0	0	0	4	0	3
Tiempo de ejecución (min : sec)	14:26	7:30	23:30	5:06	10:30	3:47	6:45
Pago anual por actualización (USD)	$62.50	$4.95	$45	$30	$60	$3.95	N/A
Actualización automática	Sí	Sí	No	Sí	No	Sí	Sí
PROs	Información excelente sobre virus	Muchas opciones de muestreo Utilitarios de respaldo	Dirección remota para redes	Ejecución rápida y perfecta Interfaz clara	Documentación excelente Licencia flexible	Rápido tiempo de muestreo Excelente actualización	Gran interfaz Enciclopedia informativa de virus
CONTRAs	Omitió virus Lenta ejecución	No actualización automática Interfaz confusa	Muy lento Interfaz confusa	El registro y actualización pudieran ser más simples	Omitió varios virus y detectó positivos falsos	Difícil de instalar y desinstalar	Falló un virus y tuvo tres positivos falsos

Tabla 4.5. Comparación de antivirus.

Fuente: CAPTAIN, Sean. "Stealth Fighters: today's best antivirus programs are tough on PC parasites but easy on users" en *PC World magazine*. Septiembre de 2001.

IntelIdeas

Es un filtro que detecta y marca los correos basura destinados a nuestro buzón. Detecta los correos independientemente del origen, idioma, servidor, etc. Sus características que de alguna manera superan a Sophos PureMessage son:

- Funcionamiento mediante la búsqueda de parámetros en los mensajes.
- Sin revisión por parte de agente humano alguno.
- No afecta a la velocidad de servicio.
- No necesita modificar la instalación de su actual servidor de correo.
- No necesita modificar los clientes de correo de sus usuarios.
- No necesita invertir tiempo en la instalación del sistema.
- Evita la preocupación por las implicaciones legales de tener el material ilegal que le ha llegado en los correos basura.
- Tiene una efectividad cercana al 98 %.
- Su tarifa está dada en función del servidor de correo único y del número de usuarios.
- Es competitivo en costos.
- Disponible desde un céntimo de euro al día por usuario.
- Desde 1 usuario hasta 4000.

Cincom *System*

Es otra opción contra los correos *spam*. Cincom System ha adoptado los siguientes puntos para todas las comunicaciones electrónicas:

- El correo se enviará a un solo destinatario y concernirá a una sola persona.
- La dirección del remitente será una dirección electrónica aceptada por Cincom y controlada por un empleado de la misma. La dirección del remitente deberá tener una relación pertinente con el contenido del mensaje enviado.
- La comunicación por e-mail siempre presentará un encabezado o un tema congruente con el contenido de dicha comunicación.
- Aplica igualmente una política muy estricta en materia de protección de datos personales.
- Cincom se compromete a suministrar información fidedigna y concerniente a la empresa determinada, además de soluciones, productos y servicios que se consideren pertinentes y ventajosas para el destinatario.

4.2.5. Comparación de productos anti-*spyware*

Existen herramientas importantes y que se actualizan constantemente para localizar archivos spyware, algunas opciones existentes son: Ad-aware 6.0 Build 162, BPS Spyware & Adware Remover 7.1 y SpyBot Search & Destroy 1.2.

Ad-aware 6.0 Build 162

Con este software podremos eliminar de forma segura la mayoría de programas *spyware* que existen actualmente en Internet. Ad-aware es considerado uno de los mejores en su categoría. Ejecutándolo periódicamente se puede mantener el perfecto estado de los sistemas.

BPS Spyware & Adware Remover 7.1

Es una de las herramientas básicas para los sistemas de cómputo. Este software nos permite desde eliminar el *spyware* hasta monitorear en tiempo real la entrada de dichos programas en nuestro sistema. Es un eliminador de programas espías.

SpyBot Search & Destroy 1.2

SpyBot no sólo nos permite eliminar los programas *spyware*, sino que también nos ayuda a inmunizar el sistema contra los mismos. Además, detecta una gran cantidad de *dialers*, *adware* o cualquier otro tipo de aplicaciones "espía". También es conocido como inmunizador de sistemas.

En la tabla 4.6 se presentan las características generarles de cada uno de los *softwares* antes mencionados.

Criterios	Ad-ware 6.0 Build 162	BPS Spyware & Adware Remover 7.1	SpyBot Search & destroy 1.2
Puntuación	Muy buena	Muy buena	Buena
Ventajas	Actualización automática de la base de datos. Totalmente en castellano. Interfaz gráfica fácil de usar. Posibilidad de ejecutarlo a través de línea de comandos. Gran rapidez en el análisis y eliminación de spyware. Soporte de plug-ins.	La mayoría de utilidades se encuentran en castellano. Monitor en tiempo real de spyware y adware. Actualización automática del programa. Selección individual de componentes a eliminar.	Totalmente en castellano. Facilidad de uso, así como un nivel avanzado para usuarios expertos. Capacidad de inmunizar el sistema frente a algunos controles ActiveX.
Desventajas	Sólo se encarga de eliminar el software spyware en nuestro sistema, no lo detecta, ni previene su instalación. Opciones avanzadas únicamente en sus versiones de pago.	La versión de demostración sólo se puede probar durante cinco días	Presenta algunos problemas de estabilidad.

Tabla 4.6. Comparación de anti-spyware.

Una vez que se han comparado las tecnologías más comunes en el mercado de la seguridad informática y de las redes, es preciso establecer cuales son los costos de estas soluciones, con la finalidad de elegir las que se adapten a las necesidades propias de la empresa y a la red misma.

4.2.6 Costos

Una vez que se ha hecho una indagación del mercado, tanto de las diferentes tecnologías de seguridad como de los fabricantes de éstas, es necesario hacer una evaluación de los costos que cada equipo tiene en el mercado de la seguridad informática. En la tabla 4.7 se presentan los costos actuales (Noviembre 2003) de los modelos de *firewalls* seleccionados para la integración del sistema de seguridad, cabe señalar que estos equipos tienen la opción ser configurados para brindar alta disponibilidad.

Descripción del producto	Cantidad	Precio Unitario M.N.	Costo
Checkpoint Firewall-1 NG Feature Pack 1 *Software*	1	$ 39,500.00	$ 39,500.00
Equipo Nokia IP440	2	$55,000.00	$110,000.00
Equipo Cisco PIX 525	2	$72,500.00	$145,000.00
Equipo NetScreen 204	2	$62,500 .00	$125,000.00

Tabla 4.7. Precios de firewalls comerciales.

También en la tabla 4.8 se muestran los costos de los equipos IDS que también fueron evaluados y considerados dentro de la solución de seguridad.

Descripción del producto	Cantidad	Precio Unitario M.N.	Costo
Cisco IDS 4250	1	$197,580.75	$197,580.75
NetScreen IDP 100	1	$200,330.00	$200,330.00
Sleuth9 IPS	1	$485,000.00	$485,000.00

Tabla 4.8. Precios de IDS comerciales.

De las tablas anteriores se eligieron los equipos NetScreen como los equipos que reúnen las características técnicas ideales para el aseguramiento de la red corporativa. Esta propuesta se presentó a los directivos del corporativo para su evaluación, especialmente a los directivos de compras, logística, informática, administración y desarrollo de proyectos. La respuesta obtenida contempla la implementación de la propuesta a largo plazo, es decir, se decidió su desarrollo en etapas, siendo la primera la implementación de un *firewall* en alta disponibilidad. La segunda etapa consiste en la instalación y configuración de un

sistema IDS y Filtros. Esta medida se tomó principalmente debido a que se tiene destinado un presupuesto bien definido por la empresa, y que como primer paso solamente contempla el aseguramiento de la red corporativa frente a la red pública. Se consideró también la implementación de las siguientes etapas en un futuro.

La medida elegida como sistema de seguridad en la primera etapa es un *firewall*, con base en las necesidades del corporativo y el grado de funcionalidad que proporciona. Pero entendemos que no es suficiente este elemento de red para asegurar que los servicios de la empresa no se vean interrumpidos en algún momento por alguna intrusión. Aunque una necesidad prioritaria del corporativo, y por tanto de este trabajo, es buscar una solución de seguridad que posea una alta disponibilidad, con el fin de mantener siempre los servicios en línea.

En la segunda etapa se implementará un sistema IDS, el cual adhiere seguridad a la red, es decir, esta solución complementaría la anterior, ya que en el momento de la implementación de esta segunda etapa ya se tendrán políticas bien definidas que sólo necesitarán el apoyo de herramientas que detengan ataques que un *firewall* no pueda contener.

Por tanto, de acuerdo a los argumentos planteados previamente, el desarrollo del proyecto descrito en el presente trabajo se limitará a tener como propósito la elección de un *firewall*, configurado en alta disponibilidad como una sólida solución de seguridad en redes.

Terminada la fase del análisis del estado actual y la determinación de una propuesta de solución para la red corporativa continuaremos con el diseño e implementación del sistema de seguridad.

4.3. PROPUESTA DE SOLUCIÓN PARA LA EMPRESA

De acuerdo a las tablas de costos para las soluciones de seguridad presentadas, en la propuesta final únicamente se contemplará un *firewall* como una solución de seguridad con la característica de alta disponibilidad, ya que la empresa no cuenta con los suficientes recursos para implementar más tecnología que le brinde una mayor seguridad.

4.3.1. Justificación de la selección

El *firewall* del fabricante NetScreen Technologies se caracteriza por ser la solución de *hardware* basado en ASICs (Aplication Specific Integrated Circuit, Circuitos Integrados Específicamente Diseñados) sobre el que se ejecuta un sistema operativo de propósito específico (ScreenOS). Gracias a la especialización del *hardware* y del *software*, el rendimiento y la seguridad de estos dispositivos resultan considerablemente superiores a los de generaciones precedentes, ya que no sufre la limitación en el rendimiento de los

procesadores de propósito general, ni se ve afectado por las vulnerabilidades presentes en los sistemas operativos de propósito general.

Este dispositivo de seguridad de NetScreen no sólo se trata de un *firewall*, sino que incorpora dos funcionalidades adicionales que le permiten actuar como *gateway* VPN y gestor de tráfico. La integración de esta triple funcionalidad en un sólo dispositivo permite el ahorro de costos directos (adquisición de menor número de equipos) e indirectos (menos horas para su instalación, configuración y gestión al no tratarse de productos de distintos fabricantes que pueden plantear problemas de compatibilidad). También, con este equipo, se tiene la posibilidad de una conexión en alta disponibilidad.

La inmensa mayoría de los dispositivos capaces de establecer túneles VPN presentes en el mercado definen una VPN mediante unas reglas específicas. ScreenOS permite esa configuración, pero también otra en la que para definir una VPN sólo es preciso asociar una interfaz (llamada interfaz túnel) a una zona de seguridad, encargándose ésta del cifrado y descifrado de información sin necesidad de definir reglas específicas.

La gestión de tráfico se basa en "*traffic shaping*", que consiste en la asignación del ancho de banda adecuado para cada usuario y aplicación. Para clasificar el tráfico se especifica la cantidad de ancho de banda garantizado, el ancho de banda máximo, y la prioridad asignada a cada clase de tráfico.

El *firewall* de NetScreen posee un rendimiento muy superior a los productos análogos de otros fabricantes y dependiendo de las necesidades, soporta arquitecturas de alta disponibilidad activo/activo (puede tener dos o más dispositivos que comparten el tráfico entrante y saliente a la organización y que no se ven afectados por el fallo de alguno de estos dispositivos manteniendo el estado de las sesiones). También es un dispositivo NEBS que soporta configuraciones de alta disponibilidad no sólo a un nivel de chasis sino también de procesadores, fuentes de alimentación y ventiladores.

ScreenOS de NetScreen ofrece una gran flexibilidad en el diseño del diagrama de red de la arquitectura de seguridad. Permite crear varias zonas de seguridad y configurar políticas para regular el tráfico de zonas internas y zonas externas. Se puede asociar una o más interfaces (tanto físicos como lógicos mediante subinterfaces) para cada zona. Una zona de seguridad es una entidad que agrupa interfaces que transportan tráfico de un nivel de seguridad equivalente y rompe con la limitación de otros productos, donde la asignación de niveles de seguridad a las interfaces es permanente y predefinida (comúnmente red externa, interna y DMZ).

La mayoría de los *firewalls* poseen un único dominio de ruteo y no permite direccionamiento de diferentes redes. NetScreen resuelve estas limitaciones introduciendo el concepto de ruteo virtual, habilitando así que un dispositivo pueda poseer varios dominios de ruteo con políticas de ruteo completamente independientes.

Los equipos NetScreen ofrecen ventajas sobre las otras marcas, por ejemplo:

Cisco PIX no ofrece las siguientes características:

- *Desempeño en HA*. Los túneles VPN deben ser renegociados cuando falla el primer PIX.
- *Modo transparente*. No se ofrece en la línea de productos PIX, muchos ambientes necesitan una integración "limpia" entre redes existentes.
- *Túneles VPN en todas las interfaces*. Los túneles sólo pueden ser terminados en la interfaz externa.
- *Desactivación NAT*. No es posible realizar un túnel sobre dispositivos NAT o PAT.
- *Aceleración VPN integrada por hardware*. Se requiere de un costoso componente adicional.
- *Administración de tráfico*. Los clientes no pueden maximizar su ancho de banda.
- *Desempeño*. El equipo PIX 525 ofrece un bajo desempeño de *firewall* y VPN.
- *Precio*. El equipo PIX posee un alto costo, especialmente cuando se integran los componentes adicionales.

Nokia/CheckPoint no ofrece las siguientes características:

- *Sistema operativo y FW/VPN integrado*. Las licencias y mantenimientos de CheckPoint son una sobrecarga que vuelve su costo fuera del alcance de pequeñas y medianas empresas.
- *Amplio número de protecciones de firewall y facilidad de configuración*. Solamente son soportadas 10 protecciones; requiere de un conocimiento sofisticado de las localidades de memoria.
- *Servidor DHCP incorporado*. Requiere de dispositivos externos.
- *Modo transparente*. No se ofrece en la línea de productos Nokia, muchos ambientes necesitan una integración "limpia" entre redes existentes.
- *Aceleración VPN integrada por hardware*. Se requiere de un componente adicional.
- *Desempeño*. IP530 e IP440 ofrecen muy bajo desempeño en VPN, incluso con tarjetas aceleradoras; IP440 tiene un desempeño bajo para el mercado al que está destinado.
- *Precio*. El equipo tiene un alto costo, especialmente después de adicionar las licencias de CheckPoint.
- *Solución efectiva y confiable*. Nokia está causando confusión con el cese de su tecnología Crypto Cluster, su solución VPN previamente recomendada.

Una vez que se justifica la elección del *firewall* NetScreen 204, como una solución robusta de seguridad para la red de datos, y que además cubre con las necesidades que la empresa requiere, se procede hacer una descripción de las características técnicas de dicho equipo.

4.4. DESCRIPCIÓN DEL FIREWALL NETSCREEN 204

Los productos de seguridad de NetScreen se basan en arquitecturas de *hardware* innovadoras que integran circuitos integrados personalizados. Las características principales, tanto físicas como técnicas, son:

NetScreen-204 es un dispositivo de seguridad de red con un chasis diseñado para *rack*, y que cuenta con cuatro puertos Ethernet de interfaz 10/100 BaseT. La figura 4.5 muestra un equipo NetScreen-204.

Las características del panel delantero de NetScreen-204 incluyen: una pantalla LED de exhibición del estado de sistema, orificio de recuperación del sistema, un puerto de consola, un puerto de módem, ranura para tarjeta Compact Flash e interfaces de Ethernet.

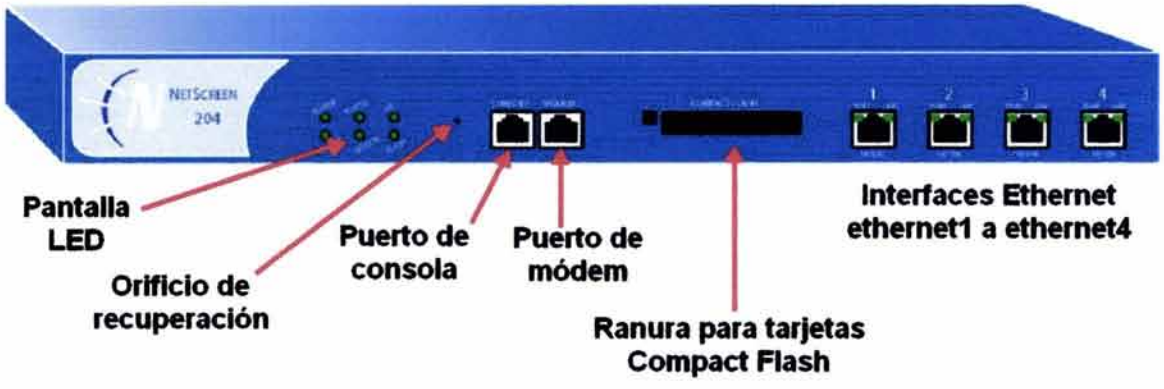

Figura 4.5. NetScreen-204 (Panel delantero).

El color de los LED's de estado del sistema muestran el status cuando se inicializa el sistema y la operación propia del equipo.

Pantalla LED

El panel delantero tiene una pantalla LED (ver figura 4.6) de exhibición del estado de sistema, que contiene seis LEDs. La información revelada por cada LED se describe en la tabla 4.9.

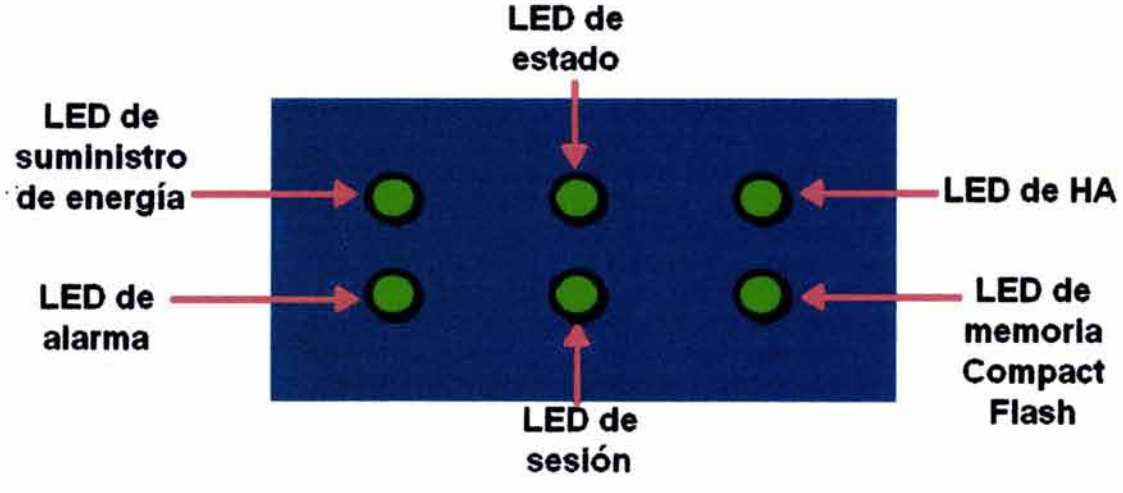

Figura 4.6. Pantalla LED.

Restablecimiento de parámetros predeterminados

Existe una forma para reestablecer los parámetros predeterminados de fábrica del sistema. El fabricante adicionó al equipo un orificio de recuperación, que consiste en un interruptor que reajusta el dispositivo a su configuración original. Para utilizar este interruptor se necesita establecer una conexión por emulador de terminal y pulsar en el *switch* ubicado en el orificio por un periodo de cuatro a seis segundos. El dispositivo advierte de la operación y solicita efectuar el proceso por segunda vez antes de llevar a cabo la recuperación. El dispositivo se restaura a la configuración original de fábrica, por tanto, se pierde cualquier ajuste previo de la configuración. Como consecuencia, la tabla de políticas y el servicio de VPN quedan inoperantes.

Puertos de consola y modem

El puerto de consola es un conector serial RJ-45, sirve para que los programas emuladores de terminal realicen la configuración y la administración localmente. El puerto de módem es un conector serial RJ-45, sirve para establecer sesiones remotas de la consola usando conexiones *dial-up* a través de un módem a 9600 bps vía un cable RS-232.

Ranura para tarjetas Compact Flash

NetScreen-204 soporta tarjetas Compact Flash con una variedad de capacidades de memoria. NetScreen ha probado SanDisk de 96 MB y de 512MB. El dispositivo de NetScreen detecta automáticamente la presencia de una tarjeta Flash y registra la bitácora de sistema en él.

LED	Propósito	Color	Significado
Power	Suministro de Energía	Verde continuo	La fuente de alimentación está funcionando correctamente
		Negro	Falla de la fuente de alimentación
Status	Estado del Sistema	Ámbar continuo	Al inicio del encendido
		Verde continuo	En el arranque y mientras realiza el diagnóstico
		Ámbar intermitente	Durante el arranque
		Verde intermitente	Operación normal
		Rojo intermitente	Error detectado
HA	Estado en modo de Alta Disponibilidad	Verde continuo	La unidad es el dispositivo (principal) primario
		Verde intermitente	Miembro redundante del grupo no encontrado
		Ámbar continuo	La unidad es el dispositivo de respaldo
		Negro	Modo HA no habilitado

Tabla 4.9. Estado del dispositivo indicado por LEDs. (Continúa)

LED	Propósito	Color	Significado
Alarm	Alarma del Sistema	Rojo continuo	Alarma crítica: -Falta del componente de hardware o del módulo del software (tal como un algoritmo criptográfico) -Ataques al *firewall* detectados
		Ámbar continuo	Alarma importante: -Memoria baja (menos del 10% restante) -Alta utilización del CPU (más del 90% en uso) -Máximo número de sesiones -Número máximo de túneles VPN alcanzado -Estado HA cambiado o miembro redundante del grupo no encontrado
		Negro	No hay alarmas
Sesión	Utilización de Sesiones	Naranja continuo	La utilización de la sesión está entre 70% y 90%
		Rojo continuo	La utilización de la sesión es mayor del 90%
		Negro	Operación normal
Flash	Estado de la Tarjeta de Memoria	Verde continuo	La tarjeta está instalada pero no hay actividad
		Verde intermitente	Se detectó actividad de lectura/grabación
		Negro	La ranura de tarjeta Flash está vacía

Tabla 4.9. Estado del dispositivo indicado por LEDs.

La tabla 4.10 es una lista de la configuración de las terminales del adaptador RJ45-DB9. Para emplear un puerto estándar del UART, la consola y los puertos del módem deben utilizar esta configuración.

DB9	Señal	Abreviación	DTE	DCE	RJ-45
1	Data Carrier Detect	DCD	In	Out	NC
2	Received Data	RD	In	Out	3
3	Transmitted Data	TD	Out	In	6
4	Data Terminal Ready	DTR	Out	In	7
5	Signal Ground	SGND	N/A	N/A	4
6	Data Set Ready	DSR	In	Out	2
7	Request To Send	RTS	Out	In	8
8	Clear To Send	CTS	In	Out	1
9	Ring Indicator	RI	In	Out	NC

Tabla 4.10. Configuración del adaptador para el puerto de módem.

Interfaces Ethernet

Cada puerto de Ethernet es una interfaz 10/100 de detección automática con dos LED. El LED izquierdo indica el tráfico de la red, y el LED derecho indica una comunicación activa de la red.

Fuentes de alimentación

El equipo NetScreen-204 puede tener una fuente de AC o una fuente de DC. La fuente de DC puede funcionar con una o dos alimentaciones de DC, que se extienden de 36V a 72V. Cuando se utilizan dos alimentaciones se comparte la carga. Si una alimentación falla, la otra asume automáticamente la carga completa.

La figura 4.7 muestra el panel trasero de un dispositivo NetScreen-204 (con una fuente de corriente de AC).

Figura 4.7. Panel trasero.

El fusible interno para la fuente de DC es un fusible de 3.1 A @ 250 V de acción rápida. Este no es reemplazable. Cada dispositivo NetScreen-204 utiliza un fusible de 2.5 A de acción lenta clasificado para 250 voltios.

Las especificaciones se muestran en la tabla 4.11. En esta tabla se muestran las dimensiones del equipo, las especificaciones eléctricas, la temperatura óptima de operación y el peso del equipo.

Dimensiones	
Altura:	1.73 pulgadas
Profundidad:	10.8 pulgadas
Ancho:	17.5 pulgadas
Peso:	8 libras
Especificaciones eléctricas	
Voltaje AC:	100-240 V +/- 10%
Voltaje DC:	36 a 72 VDC
Potencia AC:	45 W
Potencia DC:	50 W

Tabla 4.11. Especificaciones. (Continúa)

Temperatura	En operación	Sin operar
Altitud normal 0 - 3,660 metros	0°-50° C	-40°-70° C
Humedad relativa	10-90%	5-95%
Sin condensación	10-90%	5-95%

Tabla 4.11. Especificaciones.

Una vez que se han mostrado las especificaciones propias del equipo, es importante también mencionar en el siguiente punto, las características técnicas de este elemento de seguridad de red.

4.4.1. Características técnicas

En la tabla 4.12 se enlistan las características técnicas del *firewall*.

Máximo Desempeño y Capacidad	NetScreen 204
Desempeño de *firewall*	400 Mbps
Desempeño 3DES	200 Mbps
Sesiones concurrentes	128,000
Sesiones nuevas/segundo	13,000
Políticas	4,000
Interfaces	4 10/100 Base-T
Modo de Operación	**NetScreen 204**
Modo en capa 2 (modo transparente)	Sí
Modo en capa 3 (modo ruteo/NAT)	Sí
NAT	Sí
PAT	Sí
Políticas basadas en NAT	Sí
IP virtuales	4
IP mapeadas	4,000
Usuarios soportados	Sin restricción
Firewall	**NetScreen 204**
Número de ataques de red detectados	31
Ataques de red detectados	Sí
Protecciones DoS y DDoS	Sí
Reensamblado de paquetes TCP	Sí
Protección contra paquetes malformados	Sí
Inspección profunda de paquetes	Sí
Anomalías de protocolo	Sí
Firmas de estado	Sí

Tabla 4.12. Características técnicas. (Continúa)

Protocolos soportados	HTTP, FTP, SMTP, POP, IMAP, DNS
Número de ataques de aplicación detectados	más de 250
Inspección de contenidos	Sí
Antivirus externos (Trend Micro)	Sí
Antivirus embebido (Trend Micro)	No
Filtrado Malicioso URL	hasta 48 URLs
Filtrado externo URL (Websense)	Sí
VPN	**NetScreen 204**
Túneles VPN concurrentes	hasta 1,000
Interfaces de túnel	hasta 256
Encripción DES, 3DES y AES	Sí
Autentificación MD5 y SHA-1	Sí
Prevención de repetición de ataques	Sí
Acceso remoto	Sí
L2TP dentro de Ipsec	Sí
Ipsec NAT traversal	Sí
Compuertas redundantes VPN	Sí
Monitor de túnel VPN	Sí
Autentificación de Usuario en *Firewall* y VPN	**NetScreen 204**
Base de datos interna - límite de usuarios	hasta 1,500
Autentificación XAUTH en VPN	Sí
Autentificación basada en Web	Sí
Administración de Sistema	**NetScreen 204**
WebUI (HTTP y HTTPS)	Sí
Línea de comandos (consola)	Sí
Línea de comandos (telnet)	Sí
Línea de comandos (SSH)	Sí
Administrador de Seguridad NetScreen	Sí
Administración completa desde VPN	Sí
Implementación Rápida	Sí
Monitoreo y Bitácoras	**NetScreen 204**
Bitácoras en servidores	Externo, hasta 4 servidores
Correo electrónico (dos cuentas)	Sí
NetIQ WebTrends	Externo
SNMP	Sí
MIB estándar y personalizado	Sí
Seguimiento de rutas (traceroute)	Sí
Virtualización	**NetScreen 204**
Zonas de seguridad personalizadas	4
Ruteadores virtuales (VRs)	2
Soporte VLAN	32
Ruteo	**NetScreen 204**
Ruteo dinámico OSPF/BGP	2
Ruteo dinámico RIP	2

Tabla 4.12. Características técnicas. (Continúa)

Rutas estáticas	256
Ruteo basado en la fuente	Sí
Alta Disponibilidad (HA)	**NetScreen 204**
Activo/Activo	Sí
Activo/Pasivo	Sí
Interfaces redundantes	Sí
Sincronización de configuración	Sí
Sincronización de sesión para *firewall* y VPN	Sí
Detección de falla de dispositivo	Sí
Detección de falla de enlace	Sí
Autentificación para nuevos miembros HA	Sí
Encripción de trafico de HA	Sí
Asignación de Direcciones IP	**NetScreen 204**
Estáticas	Sí
Cliente DHCP, PPPoE	Sí
Servidor DHCP interno	Sí
Repetidor DHCP	Sí
Administración	**NetScreen 204**
Base de datos de administradores locales	20
Base de datos de administradores externos	RADIUS/LDAP/SecurID
Redes de administración restringidas	6
Niveles de Administrador, Usuario y Superusuario	Sí
Actualización de software	TFTP/WebUI
Administración de Tráfico	**NetScreen 204**
Ancho de banda garantizado	Sí
Ancho de banda máximo	Sí
Prioridad sobre el uso del ancho de banda	Sí
Estampa DiffServ	Sí
Memoria Externa	**NetScreen 204**
CompactFlash	Sí
Bitácoras de eventos y alarmas	Sí
Configuración de sistema desde archivo	Sí
Software ScreenOS	Sí
Dimensiones	**NetScreen 204**
Alto/Ancho/Largo	1.73/17.5/10.8 pulgadas
Peso	8 libras
Voltaje de alimentación (AC)	90 a 264 VAC, 45 watts
Voltaje de alimentación (DC)	36 a 72 VDC, 50 watts

Tabla 4.12. Características técnicas.

Una vez que conocemos las características del equipo a utilizar, procedemos con la instalación y configuración de políticas requeridas en nuestra red corporativa.

4.5. INSTALACIÓN Y CONFIGURACIÓN

Para hacer una instalación adecuada, se deben tener presentes las características técnicas del mismo, posteriormente en la configuración se determinan los servicios a los que pueden acceder los usuarios remotos en la red.

4.5.1. Instalación

Requisitos generales de instalación

Para que el dispositivo de NetScreen se instale y funcione de forma correcta, se debe asegurar que la alimentación de CA (corriente alterna) está preparada antes de comenzar la instalación del *hardware*.

- Comprobar la alimentación de CA para asegurar que se está recibiendo alimentación "limpia" (sin picos ni ruidos). Si fuera necesario, se debe instalar un regulador de voltaje.
- Elegir una toma de CA donde la temperatura ambiente oscile entre 32 y 104 °F (entre 0 y 40 °C). El dispositivo de NetScreen está diseñado para ser utilizado en un entorno de oficina normal. Si las condiciones fueran más extremas, es necesario comprobar que las condiciones de alimentación, temperatura y humedad cumplen las especificaciones de cada plataforma NetScreen.
- El equipo NetScreen dependen de los sistemas de seguridad eléctrica instalados en cada edificio, para evitar cortocircuitos, sobretensiones y problemas relacionados con la falta de tomas de tierra. Se debe asegurar que los sistemas de seguridad eléctrica del edificio estén correctamente instalados para proteger el dispositivo.

Precauciones

El equipo NetScreen puede colocarse sobre una mesa o montarse en un *rack*. La ubicación del chasis y el diseño del *rack* del equipo ya existente o de la sala de cableado es muy importante para poder utilizar el sistema correctamente. Si los equipos se colocan a muy poca distancia entre sí, la ventilación será inadecuada, por lo que algunas áreas el equipo serán inaccesibles para el mantenimiento del sistema durante apagones o fallos de este último.

Cuando se planifique la distribución del entorno y la toma de CA del equipo, se deben tomar en cuenta ciertas precauciones:

- Asegurar que la habitación en la que se utilice el sistema disponga de una circulación de aire suficiente. Los equipos eléctricos generan calor. Es posible que la temperatura natural del aire no sea suficiente para refrigerar el equipo con temperaturas de funcionamiento apropiadas sin un sistema de ventilación adicional.
- Elegir la ubicación de una zona seca, limpia, bien ventilada y con aire acondicionado.

Montaje en *rack* del equipo

La siguiente información ayudará en el montaje adecuado de una configuración en *rack* del equipo.

- No apilar ni colocar en equilibrio el equipo sobre otros dispositivos para evitar tropiezos con los cables y permitir la circulación de aire.
- Instalar el dispositivo en un *rack* abierto siempre que sea posible. Si se instala el dispositivo en un *rack* cubierto, se debe asegurar que se dispone de una ventilación adecuada. Verificar que el *rack* no esté excesivamente congestionado, ya que cada unidad genera calor. Un *rack* cubierto debe disponer de piezas laterales con rejillas y de un ventilador para suministrar aire de refrigeración.
- Cuando se monte un chasis en un *rack* abierto, verificar que el soporte para *rack* no bloquee los puertos de entrada y escape.
- En un *rack* cubierto con ventilador en la parte superior, el exceso de calor generado por el equipo situado junto a la parte inferior del *rack* puede desplazarse hacia arriba y hacia los puertos de entrada del equipo situado por encima, en el *rack*. Verificar que se proporcione la ventilación apropiada para el equipo en la parte inferior del *rack*.

Alimentación de energía

Existen tres tipos de alimentación de voltaje que hay que considerar en la instalación del equipo: alimentación de CA, de CC y redundante.

- Alimentación de CA

  * El equipo está diseñado para conectarse a sistemas de alimentación TN (Tierra-Neutro). Un sistema de alimentación TN es un sistema de distribución eléctrica que dispone de un punto conectado directamente a la toma de tierra. Las partes conductoras externas de la instalación se encuentran conectadas a ese punto por medio de conductores de puesta a tierra de protección.
  * Verificar que el dispositivo de NetScreen esté conectado a una fuente de alimentación de CA equipada con un dispositivo de protección contra sobretensiones.

- Alimentación de CC

  * Conectar las entradas de alimentación de CC únicamente a una fuente de CC que cumpla con las normas de seguridad para SELV (Safety Extra Low Voltage, Voltaje Bajo por Seguridad) establecidas por los estándares UL 1950, CSA 950, EN 60950 e IEC 60950.
  * Incorporar al cableado fijo un dispositivo de desconexión de dos polos al que pueda accederse fácilmente.
  * Utilizar únicamente conductores de cobre para realizar la conexión a la terminal de CC.

* Se debe asegurar que ningún fragmento desprotegido del cable de entrada de CC salga del conector del terminal eléctrico. Los cables desprotegidos pueden conducir una cantidad de electricidad potencialmente peligrosa.

- Alimentación redundante

* El equipo NetScreen incluye una fuente de alimentación redundante opcional, se deben conectar cada una de las dos entradas a fuentes de alimentación diferentes. Si la conexión no se realiza de este modo, el equipo NetScreen puede quedarse completamente sin suministro de corriente en caso de que fallara una de las fuentes de alimentación.

Trabajo con láseres

Ciertos equipos de NetScreen están equipados con puertos de fibra óptica y emiten radiaciones que podrían ser nocivas para el ojo humano. Tener en cuenta lo siguiente:

- Para evitar la exposición a estas radiaciones, no fije la mirada en la abertura de un puerto de fibra óptica. Cuando no hay ningún cable conectado, la abertura del puerto podría emitir radiaciones invisibles.
- Los puertos de fibra óptica (por ejemplo, en módulos GBIC y mini-GBIC) se consideran puertos láser de Clase 1 o puertos LED de Clase 1.
- Verificar que estos productos cumplan con las normas de Clase 1 de IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2 y 21CFR1040.

Ya que el *firewall* ha sido instalado de acuerdo a las recomendaciones dadas por el fabricante, el paso siguiente consiste en la configuración lógica del equipo.

4.5.2. Configuración

Una vez que el equipo está colocado en el *rack* o escritorio se procede a realizar su configuración, la cual debe reflejar las políticas de seguridad que se desean en nuestra red corporativa.

Modos operacionales

El NetScreen-204 soporta dos modos operacionales del dispositivo: el modo transparente y modo de ruteo.

Modo transparente

En este modo, el dispositivo de NetScreen-204 opera como un puente en la capa 2. El modo transparente es otra de las cualidades en donde las direcciones internas de la LAN son respetadas y no son tomadas para traducción.

En este modo, las direcciones de red de las zonas Vl-Seguras, Vl-DMZ, y VI-No Seguras son 0.0.0.0, haciéndolo así invisible a la red. Sin embargo, puede seguir operando como VPN, *firewall* y administrador de tráfico de acuerdo a la configuración establecida.

Modo de ruteo

En este modo, el equipo NetScreen-204 opera en la capa 3. Se puede configurar cada interfaz que usa una dirección de IP y una máscara de subset para implementar NAT.

Cuando la interfaz implementa servicios NAT, el dispositivo traduce la dirección IP de origen de cada paquete de salida en la dirección de IP del puerto de red no confiable. También reemplaza el número del puerto de origen con un valor generado al azar.

Cuando la interfaz no implementa servicios NAT, la dirección IP origen y el número de puerto en cada encabezado de paquete permanece inalterado. De esta manera, para que se tenga acceso a la Internet, los *host* locales deben contar con direcciones IP ruteables.

Interfaces del NetScreen-204

Cada equipo NetScreen-204 tiene cuatro interfaces ethernet, además de contar con interfaces lógicas (no físicas) que desempeñan funciones de administración y de capa 2 (ver tabla 4.13).

Tipo de interfaz	Descripción
Interfaces Ethernet	**ethernet1,** se liga a la zona de seguridad de **Vl-Trust.**
	ethernet2, se liga a la zona de seguridad de **VL-DMZ.**
	ethernet3, se liga a la zona de seguridad de **Vl-Untrust.**
	ethernet4, en NetScreen-204, se liga a la zona **HA.**
Interfaces de la Capa 2	**vlan1,** especifica una interfaz lógica usada para mantenimiento y para el tráfico en VPN mientras el dispositivo de NetScreen está en modo transparente.
	v1-trust, especifica una interfaz lógica en la capa 2 ligada a la zona de Vl-Trust.
	v1-untrust, especifica una interfaz lógica en la capa 2 ligada a la zona de Vl-Untrust.
	v1-dmz, especifica una interfaz lógica en la capa 2 ligada a la zona de Vl-DMZ.
Interfaces Túnel	**tunnel.**n especifica una interfaz de túnel lógica. Esta interfaz es para el tráfico de VPN.

Tabla 4.13. Interfaces predeterminadas.

Conexión del dispositivo como una compuerta de seguridad

Hay muchas maneras de conectar el dispositivo al sistema de la red. En la mayoría de los casos, el dispositivo sirve como una sola entrada de seguridad que protege una LAN, (normalmente se conecta al dispositivo de un *switch* o un *hub*).

Ejemplos de conexión

En este ejemplo (ver figura 4.8), el dispositivo se conecta a la LAN a través del ethernet1 (en la zona de seguridad confiable). El equipo se conecta externamente a un ruteador a través del ethernet3 (en la zona de seguridad no confiable).

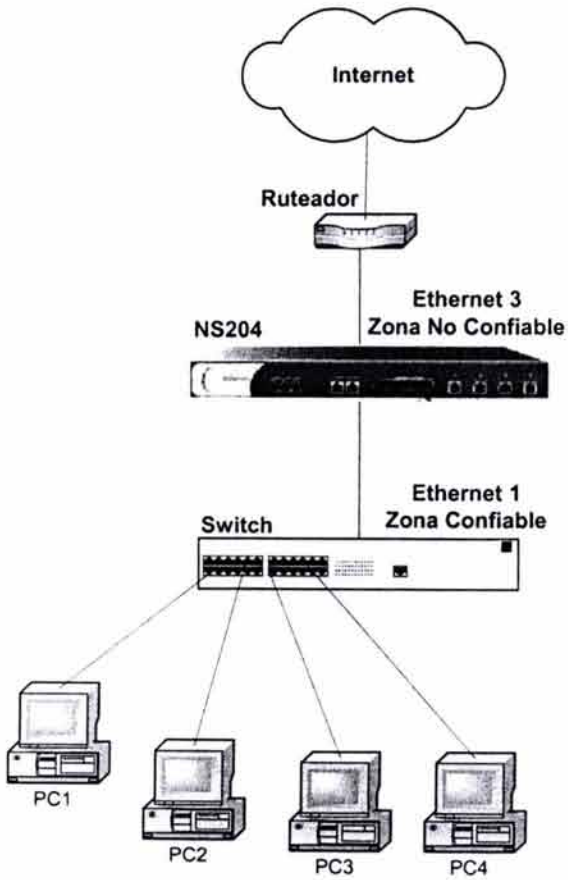

Figura 4.8. Primer ejemplo de conexión.

En la figura 4.9, el dispositivo se conecta a una LAN a través del ethernet1 (en la zona de seguridad confiable) y a un DMZ protegido a través del ethernet2 (ligado a la zona de seguridad DMZ). El equipo se conecta externamente a un ruteador a través del ethernet3 (en la zona de seguridad no confiable).

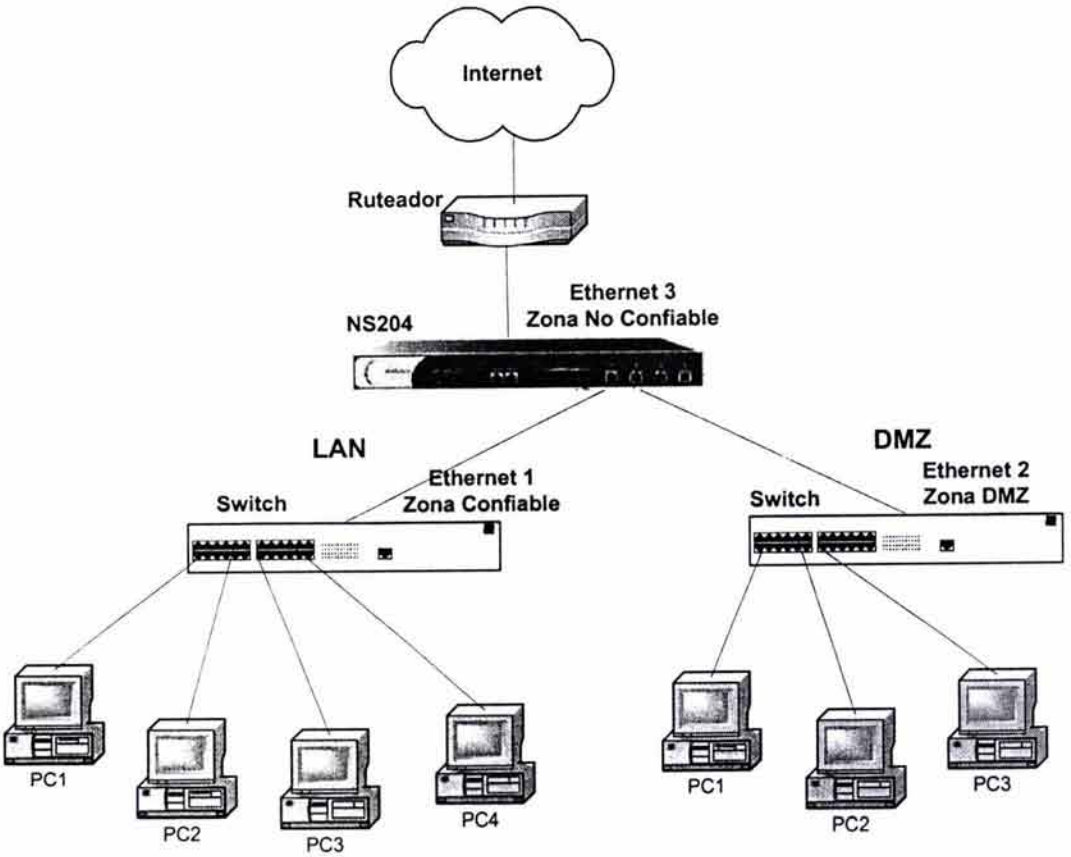

Figura 4.9. Segundo ejemplo de conexión.

Cabe señalar que en este tipo de conexión se incluye una zona desmilitarizada. El objetivo de dicha zona es exponer sólo los equipos que dan servicios a la red pública y que cuentan con un direccionamiento diferente al usado en la red privada, con el único propósito de no exponer otros sistemas a la red pública.

Conexión del equipo

El equipo tiene cuatro interfaces ethernet. La dirección IP predeterminada de la VLAN1 y la máscara de subred de estas interfaces es 192.168.1.1/24.

Para establecer las conexiones de red del dispositivo se debe considerar que:

- El lugar en el que se va a instalar el dispositivo, en un *rack* o en el escritorio.
- Confirmar que la conexión de la alimentación esté apagada ("0" presionado).
- Conectar el cable de la alimentación a la toma de corriente.
- Conectar el dispositivo a la red.
- Encender el dispositivo, luego encender los demás dispositivos de la red. (Si todos los cables se conectan correctamente, la luz de enlace para cada conexión se enciende).

Para conectar dos dispositivos en HA (ver figura 4.10):

1. Se debe asegurar que todos los interruptores de suministro de corriente estén apagados.
2. Conectar un cable 10/100 BaseT desde el ethernet4 en el dispositivo 1 al puerto del ethernet4 del dispositivo 2.
3. En el equipo 1, conectar un cable 10/100 BaseT del ethernet1 al "*switch* 3".
4. En el equipo 1, conecte un cable 10/100 BaseT del ethernet2 al *switch* "DMZ".
5. En el equipo 1, conecte un cable 10/100 BaseT del ethernet3 al "*switch* 1".
6. En el equipo 2, conecte un cable 10/100 BaseT del ethernet1 al "*switch* 4".
7. En el equipo 2, conecte un cable 10/100 BaseT del ethernet2 al *switch* "DMZ".
8. En el equipo 2, conecte un cable 101100 BaseT del ethernet3 al "*switch* 2".
9. Cablear los "*switch* 3" y "*switch* 4".
10. Cablear los "*switch* 1" y "*switch* 2".
11. Cablear los "*switch* 1" y "*switch* 2" a los ruteadores.
12. Encender todos los equipos.

Conexión y Configuración

Para establecer la primera sesión con el dispositivo NetScreen-204, se debe utilizar un emulador de terminal a través del conector RJ-45/DB9 del puerto serie.

Estableciendo una conexión de alta disponibilidad

Para asegurar el flujo de tráfico continúo en caso de una falla del sistema, se pueden conectar y configurar dos equipos de NetScreen en un grupo redundante. Los equipos mantienen simultáneamente la información de la red, configuraciones y sesiones existentes. Si un dispositivo falla, el otro toma el control del tráfico de la red. La interfaz de HA (High Availability, Alta Disponibilidad) predefinida es el ethernet4. La figura 4.10 muestra una configuración típica en HA.

Conexión con el emulador de terminal

Para establecer una sesión inicial:

1. Conectar la terminal DB9 del cable RJ-45/DB9 al puerto serial de la PC.
2. Conectar la terminal RJ-45 del cable RJ-45/DB9 al puerto de consola del dispositivo.
3. Iniciar la sesión entre la PC y el dispositivo utilizando un programa de emulación de terminal. Los parámetros son:

    - Velocidad de transferencia: 9600.
    - Sin paridad.
    - 8 bits de datos.
    - Un bit de paro.
    - Sin control de flujo.

4. Presionar ENTER para ver el inicio de sesión.

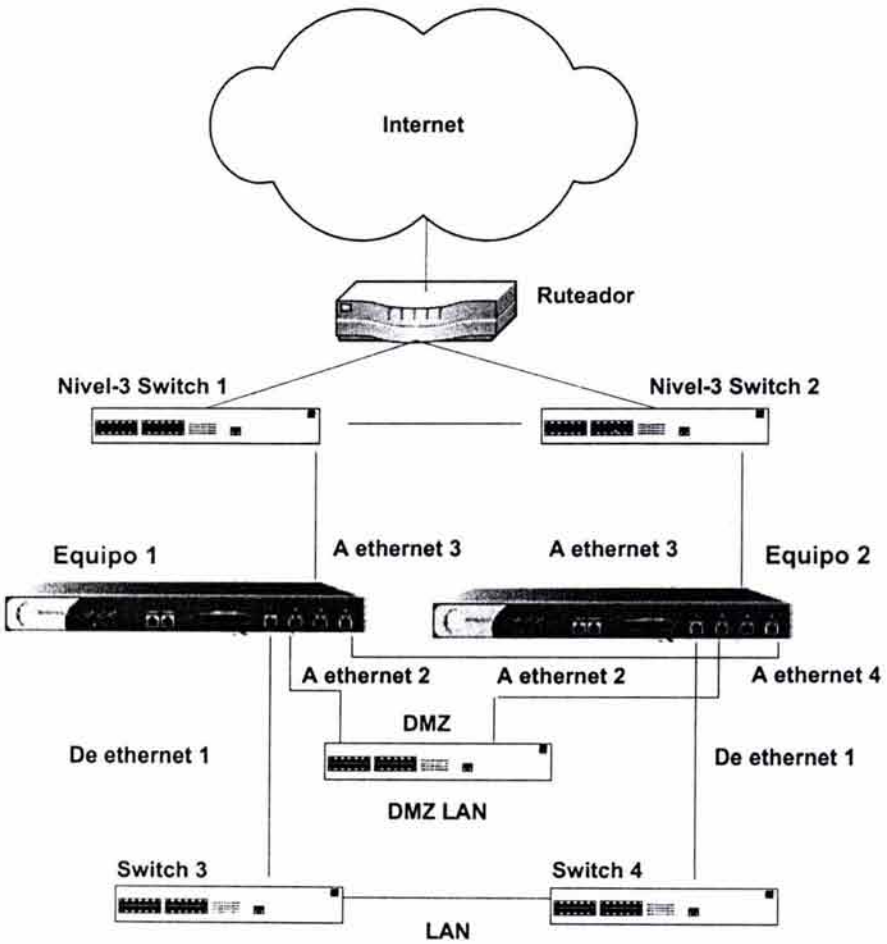

Figura 4.10. Ejemplo de conexión en HA.

5. Escribir como nombre de usuario `netscreen`.
6. Escribir como contraseña `netscreen`.

Cambiar el nombre de usuario y la contraseña

Para realizar esta operación escribir los siguientes comandos:

```
set admin name nombre_de_usuario
set admin password contraseña
save
```

Configuración de las direcciones IP del las interfaces

A través del CLI (Command Line Interface, Interfaz de Línea de Comando) se pueden ejecutar comandos para definir la dirección IP y máscaras de subred para la mayoría de las interfaces físicas.

Para empezar el proceso de configuración, es aconsejable ver los parámetros de los puertos existentes ejecutando el siguiente comando:

```
get interface
```

Este comando despliega el nombre del puerto, la dirección IP, la dirección MAC, y otra información útil.

Configuración de la dirección IP de la interfaz de administración

Para que una interfaz trabaje tal como una interfaz de administración, se deben poner las direcciones IP y su máscara en el mismo rango de dirección que la PC de administración (o LAN). Para configurar la interfaz ethernet1 como interfaz de administración se sigue el siguiente procedimiento:

1. Determinar las direcciones IP y los enmascaramientos para su PC (o LAN).
2. Asignar la dirección IP y la máscara a la interfaz ethernet1, ejecutando el siguiente comando:
   `set interface ethernet1 ip` *direccion_ip/máscara*
3. Habilitar la administración en la interfaz ethernet1 ejecutando el siguiente comando:
   `set interface ethernet1 manage`
4. Para confirmar la nueva interfaz, ejecutar el siguiente comando:
   `get interface ethernet1`

Configuración de la dirección IP de la interfaz de la zona no confiable

El equipo NetScreen-204 normalmente se comunica con dispositivos externos a través de una interfaz a una zona no confiable (como el ethernet3). Para permitirle a una interfaz comunicarse con dispositivos externos, debe asignarle una dirección de IP pública. Para configurar la dirección IP y la máscara en ethernet3 se sigue el siguiente procedimiento:

1. Escoger una dirección IP pública y una máscara que no se use.
2. Para asignar la dirección IP y la máscara se ejecuta el siguiente comando:
   `set interface ethernet3 ip` *direccion_ip/máscara*
3. Para confirmar el nuevo puerto, ejecutar el siguiente comando, (optativo):
   `get interface ethernet3`

Autorizando tráfico

El equipo NetScreen-204 no permite tráfico hacia el interior o exterior, ni permite el tráfico al DMZ. Para permitir o negar el tráfico se deben crear políticas de acceso. Con el siguiente comando de CLI se crean políticas que permiten el tráfico de cualquier tipo.

```
set policy from trust to untrust any any any permit
save
```

Configurando el dispositivo para telnet y sesiones de WebUI

Además de los programas del emulador de terminal, se puede usar Telnet (o *dialup*) para establecer sesiones de consola al dispositivo. Además, se pueden realizar sesiones de administración usando el NetScreen WebUI, una aplicación basada en web.

Inicio de sesión por Telnet

Para establecer una sesión de Telnet con el dispositivo de NetScreen-204 se sigue el siguiente procedimiento:

1. Conectar un cable de RJ-45 del puerto ethernet1 al *switch*, ruteador, o *hub* en la LAN.
2. Abrir una sesión de Telnet, especificando la dirección IP actual para ethernet1.
3. Escribir el nombre de usuario (el valor predeterminado es netscreen).
4. Escribir la contraseña (el valor predeterminado es netscreen).

Inicio de sesión por dial-up

Cada dispositivo NetScreen-204 proporciona un puerto para módem, lo que permite establecer una sesión remota por medio de una conexión *dialup* a través de un módem de 9600.

Estableciendo una sesión de administración por WebUI

Para acceder al equipo NetScreen-204 con la aplicación WebUI se siguen los siguientes pasos:

1. Conectar la PC (o el *hub* de la LAN) al puerto ethernet1 usando un cable ethernet.
2. En el navegador Web, se debe escribir la dirección IP de la interfaz ethernet1.
3. El software WebUI de Netscreen despliega un campo para insertar el nombre de usuario y otro para la contraseña (los valores predeterminados son netscreen).

Configuración del modo de alta disponibilidad

Para implementar una configuración en alta disponibilidad, es necesario realizar los siguientes pasos:

1. Configurar la zona e interfaz confiable en la unidad maestra.

2. Configurar la zona e interfaz no confiable en la unidad maestra.
3. Habilitar la alta disponibilidad en la unidad maestra.
4. Apagar la unidad maestra.
5. Configurar la zona e interfaz confiable en la unidad esclavo.
6. Configurar la zona e interfaz no confiable en la unidad esclavo.
7. Habilitar la alta disponibilidad en la unidad esclavo.
8. Apagar la unidad esclavo y encender las dos unidades.
9. Verificar que este funcionando la alta disponibilidad.

1. Configurar la zona e interfaz confiable en la unidad maestra

Para definir una interfaz confiable y relacionarla con una zona confiable, se asigna una dirección IP a la interfaz como sigue:

```
ns204→ set interface ethernet1 zone trust
ns204→ set interface ethernet1 ip 172.30.60.1/24
ns204→ set admin sys-ip 0.0.0.0
```

Para verificar que la configuración de la interfaz fue realizada, se solicita con el comando *get* a la interfaz ethertnet1 y nos despliega la siguiente información:

```
ns204→ get interface ethernet1
Interface ethernet1:
   number 0, mode nat, up/full-duplex, zone Trust
   vr trust-vr
   ip 172.30.60.0/24  mac 0010.db18.0370
   manage ip *172.30.40.23 mac 0010.db18.0370
   ping enabled, telnet enabled, SCS enabled, SNMP enabled
   web enabled, ident-reset disabled, SSL enabled
   bandwidth: physical 100000 kbps, configured 0 kbps,
   current 0 kbps
     total configured gbw 0 kbps, total allocated gbw 0 kbps
```

2. Configurar la zona e interfaz no confiable en la unidad maestra

Para definir una interfaz no confiable y relacionarla con una zona no confiable, se asigna una dirección IP a la interfaz. Esto se puede realizar desde la CLI o en la WebUI, de la siguiente forma:

En la CLI:

```
ns204→ set interface ethernet3 zone untrust
ns204→ set interface ethernet3 ip 148.225.135.9/24
```

En la WebUI:
Interfaces >> Physical >> Edit (ethernet2): escribir lo siguiente y pulsar en Save
IP address: 0.0.0.0
Netmask: 255.255.255.0
Manage IP: 0.0.0.0

Zone Name: Untrust

Cabe hacer mención que en la implementación no se está considerando crear una zona DMZ, por lo que la interfaz ethernet 2 no se configura.

3. Habilitar la alta disponibilidad en la unidad maestra

Para definir una interfaz en alta disponibilidad y relacionarla con una zona de alta disponibilidad se hace de la siguiente manera:

En la CLI:

```
ns204-> set interface ethernet4 zone ha
ns204-> set ha interface ethernet4
ns204-> set ha group 1
System change state to Passive (0)
ns204(S) -> System change state to Active (0) [Enter]
ns204-> set ha priority 1
ns204-> set ha monitor interface ethernet1
ns204-> set ha monitor interface ethernet2
```

Nota: el dispositivo con el número más cercano a 1 es la unidad maestra, un valor de 0 deshabilita la alta disponibilidad y apaga los puertos dedicados a alta disponibilidad.

Para verificar que la configuración de alta disponibilidad fue realizada, se solicita con el comando *get ha* y nos despliega la información siguiente:

```
ns204-> get ha
version:9.2.2
state: master(0.0.62)
group id:1 priority:1 ha interface:ethernet4/
ha mac: 0010db180378 virtual mac: 0010dbff0100
encryption: disable password:
authentication: disable password:
arp count: 5 time ratio: 8
ha mode: normal
session sync: on
slave linkup: on
link hold time: 3
HA monitor interface:
       ethernet1 ethernet3
```

En la WebUI:
Configure >> HA: escribir lo siguiente, después pulsar en Apply:
HA Port: ethernet8
Group ID: 1
Priority: 1

Nota: no es posible definir una interfaz de monitoreo en la WebUI.

4. *Apagar la unidad maestra*

Para evitar que se generen alarmas como las que se muestran a continuación, y se detecten conflictos entre las dos unidades, se aconseja apagar la unidad maestra antes de terminar de configurar la unidad esclavo.

```
ns204→ get alarm event
Date            Time      Module      Level  Type
Description
2001-03-11 05:08:35 system crit 00031 Detect IP conflict
(172.30.60.1) on
                                                    interface
ethernet1
2001-03-11 05:08:35 system crit 00031 Detect IP conflict
(172.30.60.1) on
                                                    interface
ethernet1
2001-03-11 05:08:34 system crit 00031 Detect IP conflict
(172.30.60.1) on
```

5. *Configurar la zona e interfaz confiable en la unidad esclavo*

Para definir una interfaz confiable y relacionarla con una zona confiable, se asigna una dirección IP a la interfaz de la siguiente manera:

```
ns204→ set interface ethernet1 zone trust
ns204 . set interface ethernet1 ip 172.30.60.1/24
ns204→ set admin sys-ip 0.0.0.0
```

Verificar la configuración de la interfaz ethernet1 ejecutando el siguiente comando:

```
ns204→ get interface ethernet1
Interface ethernet1:
   number 0, mode nat, up/full-duplex, zone Trust
   vr trust-vr
   ip 172.30.60.1/24  mac 0010.db18.0370
   manage ip *172.30.40.23 mac 0010.db18.0370
   ping enabled, telnet enabled, SCS enabled, SNMP enabled
   web enabled, ident-reset disabled, SSL enabled
    bandwidth: physical 100000 kbps, configured 0 kbps,
   current 0 kbps
     total configured gbw 0 kbps, total allocated gbw 0 kbps
```

6. *Configurar la zona e interfaz no confiable en la unidad esclavo*

Para definir una interfaz no confiable y relacionarla con una zona no confiable, se asigna una dirección IP a la interfaz. También es posible realizarlo en la CLI y en la WebUI.

En la CLI:

```
ns204→ set interface ethernet3 zone untrust
ns204→ set interface ethernet3 ip 148.225.135.9/24
```

En la WebUI:
Interfaces >> Physical >> Edit (ethernet3): escribir lo siguiente y pulsar en Save:
IP address: 0.0.0.0
Netmask: 255.255.255.0
Manage IP: 0.0.0.0
Zone Name: Untrust

7. *Habilitar la alta disponibilidad en la unidad esclavo*

Para definir una interfaz para alta disponibilidad y relacionarla con una zona de alta disponibilidad se realiza lo siguiente:

En la CLI:

```
ns204→ set interface ethernet4 zone ha
ns204→ set ha interface ethernet4
ns204→ set ha group 1
System change state to Passive (0)
ns204(S) → System change state to Active (0) [Enter]
ns204→ set ha priority 1
ns204→ set ha monitor interface ethernet1
ns204→ set ha monitor interface ethernet2
```

Nota: el dispositivo con el número más cercano a 1 es la unidad maestra, un valor de 0 deshabilita la alta disponibilidad y apaga los puertos dedicados a alta disponibilidad.

Verificar la configuración de alta disponibilidad con el comando:

```
ns204→ get ha
version:9.2.2
state: master(0.0.62)
group id:1 priority:1 ha interface:ethernet4/
ha mac: 0010db180378 virtual mac: 0010dbff0100
encryption: disable password:
authentication: disable password:
arp count: 5 time ratio: 8
ha mode: normal
session sync: on
slave linkup: on
link hold time: 3
HA monitor interface:
       ethernet1 ethernet3
```

En la WebUI:
Configure >> HA: escribir lo siguiente, después pulsar en Apply:
HA Port: ethernet8

Group ID: 1
Priority: 1

Nota: no es posible definir una interfaz de monitoreo en la WebUI.

8. *Apagar la unidad esclavo y encender las dos unidades*

9. *Verificar que esté funcionando la alta disponibilidad*

Se conecta un cable de consola a la unidad esclavo y se hace Telnet hacia la unidad maestra. En la unidad maestra se ejecuta el comando *get ha* para confirmar cuál es su estado de operación, tal y como se muestra:

```
ns204(M) → get ha
version:9.2.2
state:master(0.0.62)
group id:1 priority:1 ha interface:ethernet4/
ha mac: 0010db180378 virtual mac: 0010dbff0100
encryption:disable password:
authentication: disable password:
arp count: 5time ratio: 8
ha mode: normal
session sync: on
slave linkup: on
link hold time: 3
HA monitor interface:
       ethernet1 ethernet3
```

En la unidad esclavo también se ejecuta el comando *get ha*, igualmente para verificar su estado de operación, como se muestra en las siguientes líneas:

```
ns204(S) → get ha
version:9.2.2
state: slave(0.0.62)
group id:1 priority:100 ha interface:ethernet4/
ha mac: 0010db1802e8 virtual mac: 0010dbff0100
encryption: disable password:
authentication: disable password:
arp count: 5 time ratio: 8
ha mode: normal
session sync: on
slave linkup: on
link hold time: 3
HA monitor interface:
       ethernet1 ethernet3
```

Nota: Se debe comparar la unidad maestra con la esclavo, las diferencias son el estado de la alta disponibilidad, la prioridad y la dirección MAC de alta disponibilidad.

En la unidad maestra escribir *set ha check*, con este comando se enviará la información de la unidad maestra a la unidad esclavo y se hará una comparación entre las dos configuraciones para verificar su buen funcionamiento.

```
ns204(M) → set ha check
config checksum 73864007 to slave
```

En este momento la unidad de respaldo desplegará en la consola:

```
ns204(S) → local config 772883502  remote config 73864007
```

Nota: los números local config y remote config deben ser iguales.

En este caso, se deben sincronizar la configuración de la unidad maestra a la unidad esclavo usando el comando: *save config ha-master*

```
ns204(M)→ save config ha-master
download configuration from master
ns204(S) → Get Master configuration successfully.
Save local configuration successfully.
Please reset system now.

ns204(S) → reset
System reset, are you sure? y/[n] y
In reset ...
```

Nota: si aparece la pregunta: "Configuration modified, save? y/n", se debe responder "n".

```
ns204(M) → set ha check
config checksum 73864007 to slave

ns204(S) → local config 73864007  remote config 73864007
```

Nota: Ahora las configuraciones de la unidad maestro y esclavo son iguales, con esto se asegura un funcionamiento adecuado de alta disponibilidad.

En la figura 4.11 se muestra el esquema final de la implementación del *firewall* NetScreen-204 en alta disponibilidad, así como sus conexiones hacia la red pública y también hacia la red corporativa. En este esquema se describen también las direcciones definidas para cada interfaz del equipo.

4.6. CONFIGURACIÓN DE POLÍTICAS

Actualmente se considera que la principal causa de problemas de seguridad con *firewalls* se debe a problemas de configuración, diseño y definición de políticas robustas.

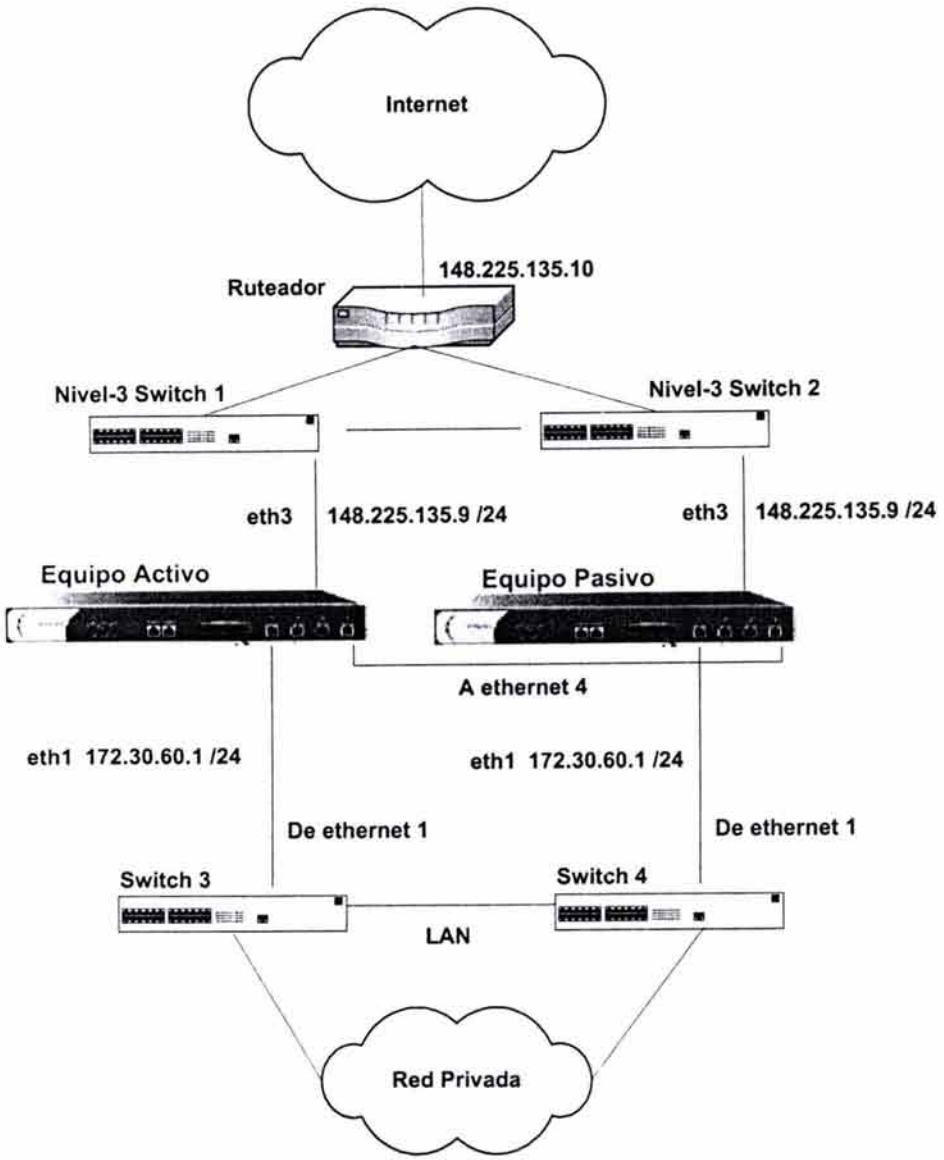

Figura 4.11. Esquema final de alta disponibilidad.

Las vulnerabilidades a nivel aplicación y sistema operativo subyacente tienen gran impacto aunque suelen ser escasas, y pueden ser resueltas aplicando los parches y actualizaciones correspondientes.

El objetivo del establecimiento de una buena definición de políticas nos permitirá aceptar, negar, encriptar y autentificar toda las conexiones, ya sea tanto de entrada como de salida para cada una de las interfaces *Trust*, *Untrust*, y *DMZ* respectivamente. Una buena

definición de políticas le permitirá al administrador mayor control sobre las conexiones que se establezcan a través del *firewall*.

En la tabla 4.14 se muestran las políticas configuradas en el *firewall* de la interfaz *Untrust* a la Interfaz *Trust*. En estas políticas se definen claramente cuales son los servicios que serán permitidos desde cualquier punto de la red externa, con esta definición aseguramos que solamente se utilicen los servicios definidos, y de otra forma negar los que no están definidos explícitamente en la política.

ID	Fuente	Destino	Servicio	Acción
1	Cualquiera	WEB Server 1	HTTP, HTTPS	Permitida
2	Cualquiera	WEB Server 2	HTTP, HTTPS, PING, P8080, P8081	Permitida
3	Cualquiera	Mail Server	POP3, MAIL, HTTP	Permitida
4	Cualquiera	FTP Server	FTP, PING, TRACEROUTE	Permitida

Tabla 4.14. Políticas de la interfaz Untrust a la Interfaz Trust.

Las políticas de la tabla anterior fueron definidas en el *firewall* de acuerdo a los requerimientos establecidos por la empresa. Es decir, el mundo exterior sólo tendrá la posibilidad de usar únicamente los servicios que se definieron para cada servidor de aplicación, cualquier otra petición que se haga a dichos servidores mostrados en la tabla serán negados. Cabe hacer mención que los usuarios que hagan peticiones hacia los servidores, lo harán a través del mecanismo de traducción de direcciones de red. El NAT permite traducir una dirección interna en una dirección válida en Internet.

Es importante tener muy claro las políticas que se definen en el *firewall*, para que desde el mundo exterior accesen los usuarios a los servicios. Es también importante conocer cuáles son los puertos que las aplicaciones utilizan, ya que el mal uso de estos puertos o una mala programación en las aplicaciones pueden abrir puertas, y es donde los intrusos toman ventajas para hacer una conexiones no autorizadas, lo que puede provocar el hurto, la modificación o la simple consulta de información etiquetada como confidencial o que no está permitida su modificación u alteración.

En la tabla 4.15 se muestra las políticas definidas de la interfaz *Trust* a la interfaz *Untrust*.

ID	Fuente	Destino	Servicio	Acción
1	WEB Server 1	Cualquiera	Cualquiera	Permitida
2	WEB Server 2	Cualquiera	Cualquiera	Permitida
3	Mail Server	Cualquiera	Cualquiera	Permitida
4	FTP Server	Cualquiera	Cualquiera	Permitida
4	Redes Internas	Cualquiera	Cualquiera	Permitida

Tabla 4.15. Políticas de la interfaz Trust a la interfaz Untrust.

Las políticas de la tabla anterior también fueron definidas dentro del *firewall*, y en la cual se muestra que todos los servidores y redes internas tendrán permitido usar cualquier tipo de servicio hacia cualquier destino de la red externa, en este caso hacia Internet sin restricción alguna. Cabe destacar que de las políticas definidas anteriormente están tomadas de la premisa de "Todo lo que no está explícitamente permitido, está negado".

Cuando se termina de definir cuales son las políticas que se implantarán, es necesario implementarlas dentro de la configuración del *firewall*.

4.7. CONFIGURACIÓN FINAL DEL *FIREWALL*

En esta etapa de configuración del *firewall*, para nuestro caso la configuración de NetScreen-204, se establecen los parámetros con los cuales el *firewall* entra en operación. Estos parámetros se definen en el archivo de configuración del NetScreen-204. Además se establecen todas las políticas de seguridad, la configuración de las interfaces del equipo, la alta disponibilidad, habilitar las firmas de ataque más comunes definidas por el fabricante del *firewall*, así como la definición de la cuenta del administrador y las tablas de ruteo.

Configuración de la cuenta de administrador

```
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set clock "timezone" -6
set admin format dos
set admin name "netscreen"
set admin password nPYrEFr+Co0GcavFYsUBPEItTRDhCn
set admin user "nsadmin" password
"nNXIIZrmMKNEcS0Bos7C5ICtgJCHZn" privilege "all"
set admin manager-ip 172.30.40.23 255.255.255.255
set admin manager-ip 172.30.40.24 255.255.255.255
set admin auth timeout 10
set admin auth server "Local"
```

Configuración de puertos personalizados

```
set service "P8081" protocol tcp src-port 0-65535 dst-port
8081-8081 group "other"
set service "P8080" protocol tcp src-port 0-65535 dst-port
8080-8080 group "other"
```

Configuración de las zonas Trust, Untrust y DMZ

```
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
```

```
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "DMZ" tcp-rst
set zone "MGT" block
set zone "MGT" tcp-rst
```

Configuración de las firmas contra ataques más comunes definidas en el *firewall*

```
set zone Untrust screen icmp-flood
set zone Untrust screen udp-flood
set zone Untrust screen winnuke
set zone Untrust screen port-scan
set zone Untrust screen ip-sweep
set zone Untrust screen tear-drop
set zone Untrust screen syn-flood
set zone Untrust screen ip-spoofing
set zone Untrust screen ping-death
set zone Untrust screen ip-filter-src
set zone Untrust screen land
set zone Untrust screen syn-frag
set zone Untrust screen tcp-no-flag
set zone Untrust screen ip-bad-option
set zone Untrust screen ip-timestamp-opt
set zone Untrust screen ip-loose-src-route
set zone Untrust screen icmp-fragment
set zone Untrust screen icmp-large
set zone Untrust screen syn-ack-ack-proxy
set zone Untrust screen block-frag
set zone V1-Untrust screen tear-drop
set zone V1-Untrust screen syn-flood
set zone V1-Untrust screen ping-death
set zone V1-Untrust screen ip-filter-src
set zone V1-Untrust screen land
```

Configuración de las interfaces físicas

```
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface "ethernet4" zone "HA"
unset interface vlan1 ip
```

Configuración del direccionamiento IP en las interfaces

```
set interface ethernet1 ip 172.30.60.0/24
set interface ethernet1 route
set interface ethernet2 ip 0.0.0.0/0   # No se usará Zona
Desmilitarizada
set interface ethernet2 route
set interface ethernet3 ip 148.225.135.9/28
```

```
set interface ethernet3 nat
set interface ethernet4 ip 0.0.0.0/0
set interface ethernet4 route

unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip

set interface vlan1 ip manageable
set interface ethernet1 ip manageable
set interface ethernet2 ip manageable
set interface ethernet3 ip manageable
```

Configuración de direcciones NAT a los servidores internos

```
set interface ethernet2 manage web
set interface "ethernet3" mip 148.225.135.11 host
172.30.60.100 netmask 255.255.255.255 vr "trust-vr"
set interface "ethernet3" mip 148.225.135.12 host
172.30.60.101 netmask 255.255.255.255 vr "trust-vr"
set interface "ethernet3" mip 148.225.135.13 host
172.30.60.102 netmask 255.255.255.255 vr "trust-vr"
set interface "ethernet3" mip 148.225.135.14 host
172.30.60.103 netmask 255.255.255.255 vr "trust-vr"
```

Configuración de las redes internas dentro del *firewall*

```
set domain ledaxis.com
set hostname ns01
set address "Trust" "172.30.60.0/24" 172.30.60.0
255.255.255.0
set address "Trust" "172.30.0.0/24" 172.30.0.0 255.255.255.0
set address "Trust" "172.30.10.0/24" 172.30.10.0
255.255.255.0
set address "Trust" "172.30.20.0/24" 172.30.20.0
255.255.255.0
set address "Trust" "172.30.30.0/24" 172.30.30.0
255.255.255.0
set address "Trust" "172.30.40.0/24" 172.30.40.0
255.255.255.0
set address "Trust" "172.30.50.0/24" 172.30.20.0
255.255.255.0
set address "Trust" "172.35.0.0/28" 172.35.0.0
255.255.255.240
set address "Trust" "172.35.1.0/28" 172.35.1.0
255.255.255.240
set address "Trust" "172.35.2.0/28" 172.35.2.0
255.255.255.240
set address "Trust" "172.35.3.0/28" 172.35.3.0
255.255.255.240
set address "Trust" "172.35.4.0/28" 172.35.4.0
255.255.255.240
```

```
set address "Trust" "172.35.5.0/28" 172.35.5.0
255.255.255.240
set address "Trust" "172.35.6.0/28" 172.35.6.0
255.255.255.240
set address "Trust" "172.35.7.0/28" 172.35.7.0
255.255.255.240
set address "Trust" "172.35.8.0/28" 172.35.8.0
255.255.255.240
set address "Trust" "172.35.9.0/28" 172.35.9.0
255.255.255.240
set address "Trust" "WEB Server1" 172.30.60.100
255.255.255.255 "Pagina WEB"
set address "Trust" "WEB Server2" 172.30.60.101
255.255.255.255 "Pagina WEB Distribuidores"
set address "Trust" "FTP Server" 172.30.60.102
255.255.255.255 "Servidor FTP"
set address "Trust" "Mail Server" 172.30.60.103
255.255.255.255 "Servidor de Correo"
set firewall log-self
set snmp name "ns01"
```

Configuración de servidores y servicios permitidos

```
set group address "Trust" "GrupoInterno"
set group address "Trust" "GrupoInterno" add "WEB Server1"
set group address "Trust" "GrupoInterno" add "WEB Server2"
set group address "Trust" "GrupoInterno" add "FTP Server"
set group address "Trust" "GrupoInterno" add "Mail Server"

set group service "WEB Server1"
set group service "WEB Server1" add "HTTP"
set group service "WEB Server1" add "HTTPS"

set group service "WEB Server2"
set group service "WEB Server2" add "HTTP"
set group service "WEB Server2" add "HTTPS"
set group service "WEB Server2" add "P8081"
set group service "WEB Server2" add "PING"
set group service "WEB Server2" add "P8080"
set group service "FTP Server"
set group service "FTP Server" add "PING"
set group service "FTP Server" add "TRACEROUTE"
set group service "FTP Server" add "FTP"

set group service "Mail Server"
set group service "Mail Server" add "POP3"
set group service "Mail Server" add "MAIL"
set group service "Mail Server" add "HTTP"
```

Configuración de políticas de la zona Untrust a la zona Trust

```
set policy id 2 from "Untrust" to "Trust"  "Any"
"MIP(148.223.138.11)" "WEB Server1" Permit log count
set policy id 3 from "Untrust" to "Trust"  "Any"
"MIP(148.223.138.12)" "WEB Server2" Permit log count
set policy id 4 from "Untrust" to "Trust"  "Any"
"MIP(148.223.138.13)" "FTP" Permit log count
set policy id 5 from "Untrust" to "Trust"  "Any"
"MIP(148.223.138.14)" "Mail Server" Permit log count
set policy id 6 from "Untrust" to "Trust"  "Any" "ANY" "ANY"
Deny log count
```

Configuración de la zona Trust a la zona Untrust

```
set policy id 7 from "Trust" to "Untrust"  "GrupoInterno"
"Any" "ANY" nat dip-id 2 Permit log count
```

Configuración de alta disponibilidad

```
set nsrp cluster id 3
set nsrp rto-mirror sync
set nsrp vsd-group id 0 priority 100
set nsrp vsd-group id 0 preempt
set nsrp encrypt password abc123
set nsrp auth password "abc123"
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set scs enable
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set dns host dns1 172.30.60.50
set dns host schedule 00:00
set vrouter "untrust-vr"
exit
```

Configuración de ruteo

```
set vrouter "trust-vr"
unset add-default-route
set route  172.30.0.0/24 interface ethernet1 gateway
172.30.60.1
set route  172.30.10.0/24 interface ethernet1 gateway
172.30.60.1
set route  172.30.20.0/24 interface ethernet1 gateway
172.30.60.1
set route  172.30.40.0/24 interface ethernet1 gateway
172.30.60.1
set route  172.30.50.0/24 interface ethernet1 gateway
172.30.60.1
```

```
set route  172.35.0.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.1.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.2.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.3.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.4.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.5.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.6.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.7.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.8.0/28 interface ethernet1 gateway
172.30.60.1
set route  172.35.9.0/28 interface ethernet1 gateway
172.30.60.1
set route  0.0.0.0/0 interface ethernet3 gateway
148.225.135.10
exit
```

Una vez configurado el *firewall* NetScreen 204, se procede a verificar la instalación a través de la obtención de una serie de resultados.

4.8. RESULTADOS

Como parte final de la implementación del sistema de seguridad en alta disponibilidad, el siguiente paso es hacer una comprobación de que la configuración se haya realizado de una forma correcta, y para tal efecto se muestran en los siguientes apartados los resultados finales.

4.8.1. Resultados de los servicios

Esta prueba se realizó con base en registros que genera el *firewall* cuando este se encontró productivo durante los tres días de prueba. Cabe señalar que las bitácoras fueron llevadas a un repositorio para generar reportes con una herramienta llamada *Webtrends*.

En la tabla 4.16 se muestran los resultados o estadísticas generales, obtenidos apartir de las bitácoras durante el periodo o ventana de pruebas.

En la figura 4.12 se muestra que en primer lugar, el mayor tráfico lo genera el servidor de correo usando el protocolo SMTP. La empresa presta el servicio de correo electrónico para los clientes que soliciten este servicio. Siendo este servicio el más usado.

Resultados del *Firewall*	
Fecha del Reporte	Lunes 03 Noviembre, 2003 - 13:34:19
Lapso de tiempo de la prueba	11/03/2003 00:00:00 - 11/05/2003 23:59:59
Número de eventos	773,153
Número de bytes totales de conexiones hacia Internet	1,416,714k
Número de bytes totales de conexiones hacia la red corporativa	106,875k
Promedio de número de eventos por día	1,932,884
Promedio de bytes por día de las conexiones hacia Internet	3,541,787k
Promedio de bytes por día de las conexiones hacia la red corporativa	26,718k
Porcentaje de ancho de banda debido al protocolo SMTP	52.55%
Porcentaje de ancho de banda debido al protocolo HTTP	16.63%
Porcentaje de ancho de banda debido al protocolo FTP	3.03%
Porcentaje de ancho de banda debido al protocolo TELNET	0.00%
Porcentaje de ancho de banda debido a otras actividades	53.7%

Tabla 4.16. Resultados del firewall.

Figura 4.12. Gráfica del uso del ancho de banda por protocolo.

El segundo protocolo más usado es HTTP, ya que por este protocolo se establecen el mayor número de conexiones, y lo vemos como un tráfico normal, ya que casi todos los servicios se basan en este protocolo. Otro de los protocolos más comúnmente usado es el protocolo FTP para la transferencia de archivos, de un *host* a otro, ya sea dentro o fuera de la red de datos.

Por último mencionaremos al protocolo ICMP, este protocolo es usado para verificar que los equipos contesten dentro de la red, a través de las utilerías PING y TRACEROUTE. El uso de TELNET no está permitido usarse de la red externa hacia la red interna, es por eso que en la gráfica no se muestra ninguna conexión de este tipo, sin embargo este servicio es muy empleado al interior de la red, debido a que los desarrolladores hacen las respectivas modificaciones a los aplicativos usando esta utilería.

Dentro de los protocolos que no se mencionan pero que sin embargo tienen un elevado uso se encuentran: NetBios, ARP, UDP entre otros. Estos protocolos están inherentes en la red de datos. Estos son protocolos de equipos de comunicación como ruteadores y switches, también existen *hosts* con sistemas operativos que generan tráfico de tipo *broadcast*.

4.8.2. Resultados de detección de ataques

En esta parte se presentan los resultados los distintos ataques que se hicieron programados al *firewall* con *software* que se puede adquirir de forma gratuita en Internet. Los ataques que se realizaron fueron: ataque de barrido de puertos (*port scanning*) y ataque de negación de puertos (*ping of death*). En la figura 4.13 se muestra el número de eventos de la prueba.

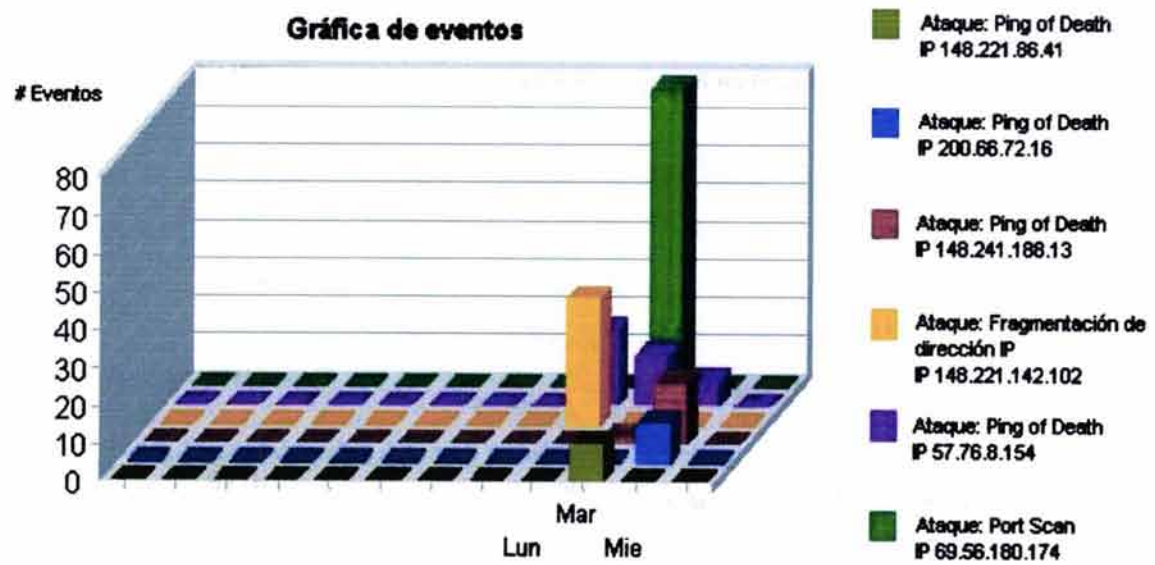

Figura 4.13. Gráfica de ataques.

La prueba de ataques se realizó hacia la interfaz *Untrust* del *firewall*. Estos ataques fueron programados de manera que realmente se pudiera observar que el *firewall* estaba actuando en contra de estos. Las herramientas de ataque utilizadas para esta prueba fueron: *Nmap* y el programa *Ping of Death*, éstas pueden ser obtenidas de una forma gratuita en el sitio ***www.packetsecuritystorm.org***

Observando la tabla 4.17 podemos comentar que se hizo un mayor énfasis en el uso de la herramienta *Nmap* para verificar que puertos del *firewall* se encuentran abiertos. Con la herramienta *Ping of Death* se realizaron algunas pruebas de ataques de bombardeo de paquetes ICMP, con el fin de ver el comportamiento del *firewall* en una situación de ataque.

En la tabla 4.17 se da un resumen del número de eventos o ataques que se realizaron para hacer la prueba con el equipo puesto en producción.

Resumen de Ataques al *Firewall*			
	Descripción	**Número de Eventos**	**% Total**
■ 1	**Ataque: Port Scan** **Dirección IP 69.56.180.174**	79	42.74%
■ 2	**Ataque: Ping of Death** **Dirección IP 57.76.8.154**	41	32.69%
3	**Ataque: Fragmentación de IP** **Dirección IP 148.221.142.102**	34	10.84%
■ 4	**Ataque: Ping of Death** **Dirección IP 148.241.188.13**	18	8.18%
■ 5	**Ataque: Ping of Death** **Dirección IP 200.66.72.16**	11	2.91%
■ 6	**Ataque: Ping of Death** **Dirección IP 148.221.86.41**	10	2.64%
	Número total de eventos críticos	**193**	**100%**

Tabla 4.17. Resumen de ataques al firewall.

Para las pruebas se utilizó un servidor con sistema operativo *Windows 2000* en el cual se simularon varias direcciones IP públicas. Lo más importante que arrojaron estos resultados fue que el *firewall* logró detectar y detener dichos ataques, además se generaron alarmas dentro del mismo y bitácoras donde se registraron cada uno de los eventos.

4.8.3. Resultados de alta disponibilidad

Actualmente la solución de seguridad se encuentra configurada en alta disponibilidad como *Activo - Pasivo*, es decir todo el tráfico fluye por un solo equipo. El equipo que se encuentra *Pasivo* tiene la misma configuración del equipo *Activo*, una señal

de latido (*Heartbeat*) verifica el estatus de ambos equipos. Cuando alguna de las interfaces del equipo falla, entonces es cuando la señal de *Heartbeat* toma acción para hacer el cambio de equipo. En la tabla 4.18 se muestra la matriz de pruebas para validar el funcionamiento de la alta disponibilidad.

Para realizar las pruebas de alta disponibilidad, se hizo la desconexión física de los cables de red para emular un fallo en la comunicación.

Se tuvieron resultados satisfactorios, ya que al hacer el cambio de control de *Activo-Pasivo*, éste se realizó en un periodo no mayor a los 6 segundos. De lo anterior puede interpretarse como una ventaja, ya que los servicios no se ven afectados en el momento del fallo para cualquiera de las interfaces, y lo que es más, se maximiza el tiempo de operación de los servicios siendo éste uno de los objetivos de nuestra propuesta.

Prueba	*Firewall* Activo			Evento Programado	Observaciones
#	Interfaces				
	Trust	Untrust	HA		
	Ethernet1	Ethernet3	Ethernet4		
1				Fallo en la Interfaz Trust por desconexión física	Se verifica con esta prueba que el control pasa al *firewall* Pasivo y continúa la operación normal del equipo. Sólo se registra el cambio en bitácoras, ahora el Pasivo tiene el control.
2				Fallo en la Interfaz Untrust por desconexión física	Se verifica con esta prueba que el control pasa al *firewall* Pasivo y continúa la operación normal del equipo. Sólo se registra el cambio en bitácoras, ahora el Pasivo tiene el control.
3				Fallo en la Interfaz HA por desconexión física	Se verifica con esta prueba que el control se mantiene en el *firewall* Activo. No hay suspensión de servicios, pero genera alarmas en el repositorio de bitácoras de forma continua, haciendo referencia al fallo de la interfaz.

Tabla 4.18. Matriz de pruebas para verificar alta disponibilidad.

4.8.4. Esquema final de la implementación

Durante el proceso de instalación y configuración del equipo, la red corporativa tuvo que ser modificada con el fin de integrar al nuevo elemento que proveerá la seguridad y control de tráfico de servicios. En el diagrama de la figura 4.14 muestra el estado final de la red corporativa, ya con la solución de seguridad integrada. Esta solución esta pensada para brindar alta disponibilidad en el equipo de *firewall*.

Con este capítulo damos por terminado el desarrollo del proyecto de seguridad en alta disponibilidad propuesto para una red corporativa. Por último resta exponer nuestras conclusiones que se generaron a partir del presente trabajo.

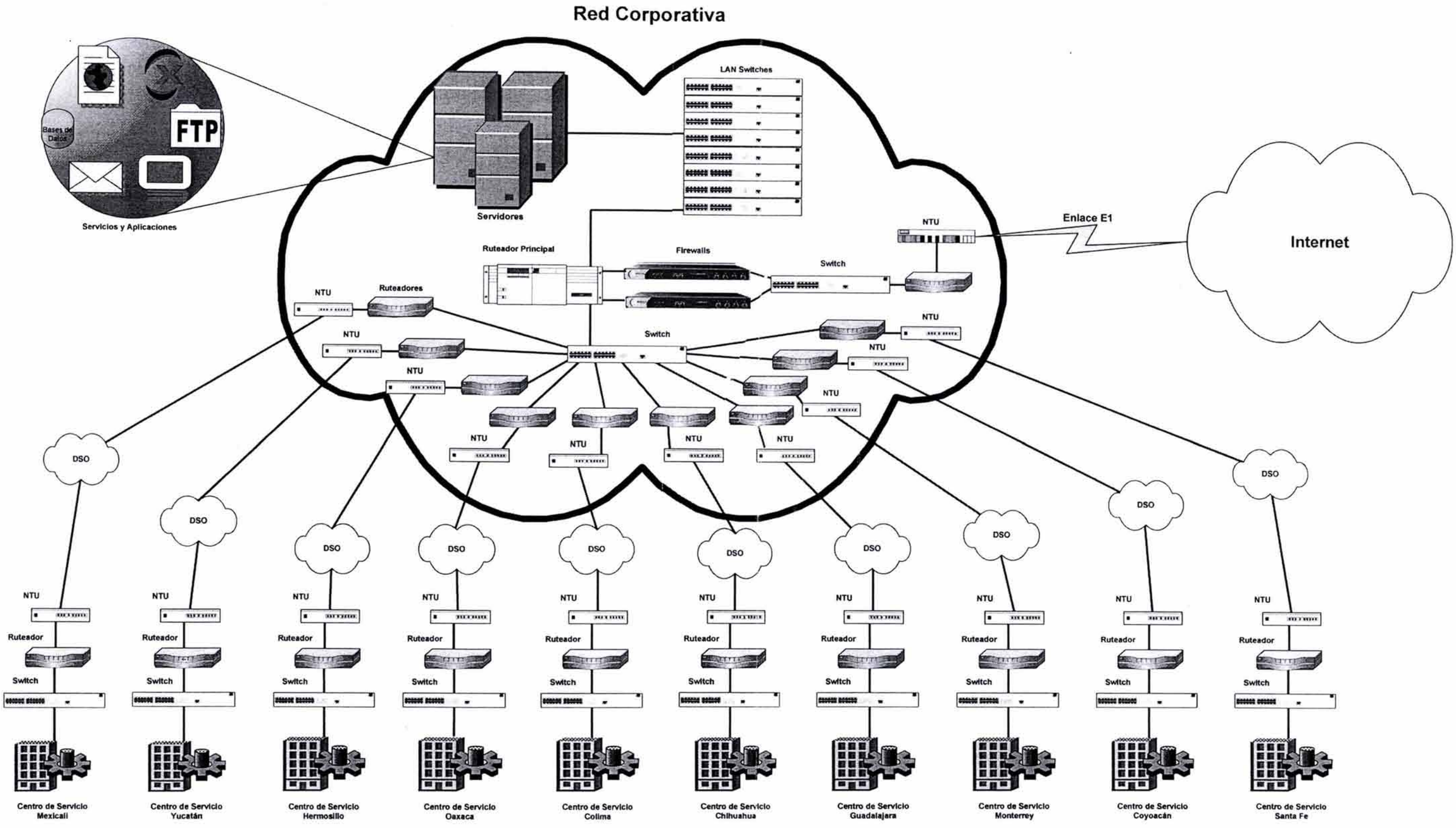

Figura 4.14. Esquema final de la implementación.

RESULTADOS Y CONCLUSIONES

En este capítulo se presentan los resultados del sistema de seguridad en alta disponibilidad y, finalmente, se establecen las conclusiones del trabajo.

El propósito de establecer un plan de seguridad informática, realizable a partir de las recomendaciones planteadas, es proteger la información y los activos del corporativo, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos y las responsabilidades que debe asumir los empleados mientras permanezcan en la organización. Llevar a cabo dicho plan requiere un alto compromiso de la institución, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función de un ambiente dinámico.

Con el fin de implementar el sistema de seguridad para la red corporativa, se realizaron diversas actividades directa o indirectamente involucrados con nuestro objetivo principal. Las actividades realizadas contemplaron la auditoría y el análisis de información de la operación actual de la red, la generación de recomendaciones y finalmente el diseño e implementación de una propuesta de solución para la seguridad en las comunicaciones de red, abarcando su instalación, configuración y posterior preparación de resultados de su implementación.

Auditoría

La primera acción realizada fue la de definir los objetivos y alcances de la auditoría, a fin de conocer el estado de la red corporativa y sus estrategias de seguridad existentes. Para llevar a cabo esta tarea, fue necesaria la recopilación y revisión de fuentes de información, debido principalmente a que necesitábamos conocer los procedimientos involucrados en su elaboración. Asimismo se efectuaron reuniones con los directivos del corporativo directamente relacionados, para que generáramos un plan de trabajo de manera conjunta y para la obtención de los permisos necesarios. Una vez conseguidos los permisos, se procedió a retomar los datos requeridos con los cuestionarios elaborados.

La red corporativa por asegurar, contaba ya con algunos lineamientos de seguridad como las llamadas políticas de red, que les permitían a los usuarios y administradores cubrir ciertos puntos concernientes a la seguridad de la red tanto física, lógica y administrativa. Sin embargo, no se podía determinar su grado de seguridad sin antes llevar a cabo la auditoría.

Análisis de información

El levantamiento de la información del estado de la red corporativa arrojó datos como el tipo de red, su topología, diseño de las conexiones, el número de usuarios, las normas tomadas en cuenta para su construcción, el número de centros de servicio y su direccionamiento; la forma de comunicación con Internet; el tráfico en la red, el ancho de banda utilizado por protocolo, volumen de tráfico por día y las políticas de seguridad físicas y técnico administrativas.

Lo anterior nos permitió tener un panorama general de los servicios, y en un análisis posterior, conocer las vulnerabilidades de los sistemas existentes. Parte de esta información se realizó en conjunto con los encargados del área de sistemas.

Recomendaciones

En esta parte se procedió a la ubicación de las debilidades de los lineamientos empleados por el corporativo para su red. De igual manera se generaron las recomendaciones para cada uno de los puntos analizados. Posteriormente fue presentado un informe a los directivos del corporativo con los resultados de la auditoría y las recomendaciones planteadas.

Diseño e implementación

Después de realizar la auditoría de seguridad para la red corporativa, y haber planteado las recomendaciones con base en los datos obtenidos durante las actividades de la primera etapa, se planteó una propuesta que integrara las tecnologías de seguridad adecuadas para las comunicaciones de red, involucrando el factor económico, que en este caso llegó a ser elevado. La propuesta presentada a los directivos del corporativo encargados del proyecto, sugiere la instalación de varias tecnologías de seguridad utilizadas actualmente y disponibles en el mercado, como son la implementación de *firewalls* configurados para proporcionar alta disponibilidad, instalación de un sistema de detección de intrusos y, finalmente, el uso de aplicaciones de filtrado. En esta solución se integran: encripción 3DES, NAT, PAT, detección de ataques, filtrado URL, soporte de túneles VPN, autentificación de usuarios, soporte SNMP y VLAN, funciones de ruteo, servidor DHCP, administración del ancho de banda, zonas DMZ y alta disponibilidad, siendo esta última la solución requerida para garantizar a los usuarios la continuidad de los servicios.

Al decidirse la implementación de un *firewall* por considerarse primordial para el corporativo, se procedió a evaluar y comparar equipos similares que pudieran satisfacer los requisitos requeridos. Para tal efecto, se tomaron en cuenta características generales a cubrir, para después requerir información adicional de varios equipos a las compañías del sector y elegir el más conveniente a los aspectos planteados, actividad que nos llevó la mayor parte del tiempo en esta etapa.

Una vez determinado el equipo que se iba a utilizar, continuaron los trámites necesarios en el corporativo para su adquisición, y en la compañía que proporcionó el equipo a través de sus representantes regionales. Durante el lapso de tiempo que duró el envío, empezaron también los acuerdos para la capacitación del personal destinado a administrar el equipo, así como los requerimientos y adecuaciones necesarias para su instalación conforme a las recomendaciones del fabricante. Por último se procedió a su instalación e interconexión. Al instalar el *firewall* en alta disponibilidad, surgió la necesidad de redefinir cierta parte de la red corporativa, ya que los *firewalls* deben ser la línea de separación entre la red no segura (Internet) y la red segura (red corporativa).

Posteriormente a la instalación del equipo, se generaron las cuentas de los administradores con diferentes privilegios para cada uno; después empezó el proceso de configuración descrito en el trabajo. Adicionalmente se generó la tabla de ruteo, basado en su mayor parte en las direcciones existentes de la red corporativa. Finalmente se implementaron en el equipo las políticas consideradas a partir de los requerimientos de seguridad.

La implementación de una política de seguridad informática en una empresa implica un gran desafío porque se debe estar preparado y dispuesto a reaccionar con rapidez, ya que las amenazas y las vulnerabilidades están cambiando constantemente, y cada vez se producen con mayor frecuencia.

Una vez concluido el desarrollo del presente trabajo, la última etapa consistió en la preparación de pruebas que abarcan los aspectos de servicios, detección de ataques y el modo de alta disponibilidad. En esta etapa también fue necesaria la petición de permisos especiales a los directivos de logística para la realización de algunas de estas pruebas.

Al realizar la evaluación y comparación de los resultados obtenidos con las expectativas que se tenían al inicio del proyecto, consideramos que éstas fueron cubiertas, ya que al revisar las bitácoras que nos proporciona el equipo instalado, nos indica que éste cumple con las necesidades planteadas por el corporativo. Esto lo podemos aseverar sólo para una parte de la propuesta, ya que ésta no fue implementada en su totalidad, por razones exclusivamente del corporativo. La empresa, que se mostró muy conforme con las recomendaciones sugeridas, reveló su intención de poner en práctica las recomendaciones de seguridad generadas que quedaron pendientes.

Respecto al trabajo aquí presentado, nuestras conclusiones son:

1. La instalación de los *firewalls* en alta disponibilidad proporcionó a la red corporativa los siguientes beneficios:

- Control de accesos a la red corporativa.
- Centralización de la administración de algunas políticas de seguridad.
- Reforzamiento de las políticas de seguridad del corporativo.
- Fácil monitoreo de la seguridad de las comunicaciones de red.
- Enmascaramiento de las IPs internas.
- Protección y detección de ataques conocidos por el *firewall*.
- Generación de alarmas en caso de detección de ataques.
- Monitoreo del uso del ancho de banda.
- Creación de registros de uso de servicios.

2. No se realizó la implementación de los elementos adicionales contemplados inicialmente en la propuesta, debido a la decisión tomada por el corporativo de implementarla parcialmente. De este modo se puede decir que el trabajo del aseguramiento de la información de la red corporativa no ha finalizado, por esta razón recomendamos su desarrollo lo antes posible. De la misma manera recomendamos seguir perfeccionándolo conforme a las posibilidades económicas del corporativo y a la tendencia de las nuevas tecnologías de seguridad, con el fin de mantener el sistema actualizado y fuera del alcance de cualquier riesgo o amenaza que pudieran surgir a futuro.

3. Considerando los elementos de juicio obtenidos durante las tareas efectuadas, se ha determinado que si bien existen prácticas tendientes a garantizar un adecuado nivel de

seguridad del sistema informático y de comunicaciones, las mismas no son suficientes ni se encuentran ordenadas en su totalidad bajo un cuerpo normativo.

4. Las recomendaciones propuestas en el presente trabajo pueden ser consideradas como un medio para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de tal forma que permitan a la empresa desarrollarse de una manera más eficiente.

5. Llevar a cabo las recomendaciones expuestas permitirá reducir el ambiente de riesgo vigente, disponer de las medidas de control interno necesarias, disminuir el grado de exposición de los sistemas que se procesan, incrementar la confiabilidad, integridad y disponibilidad de la información y optimizar los procesos orientados al cumplimiento de los objetivos del corporativo.

6. A lo largo del presente trabajo pudimos advertir que para la seguridad de una red de datos y servicios, no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos de la información y los activos de una organización. Sin embargo, la comunicación con los usuarios de la red es un punto clave para hacer que estas políticas sean efectivas y gradualmente se genere una "cultura de la seguridad".

7. Asimismo, podemos afirmar el aprendizaje de nuevos conceptos al desarrollar un trabajo sobre un tema vigente y la aplicación de la teoría asimilada a lo largo de la carrera en un caso práctico, por lo que las expectativas personales también fueron cubiertas favorablemente.

8. Por último, esperamos que este trabajo genere la inquietud para que futuras investigaciones o proyectos profundicen en el campo de la seguridad informática.

BIBLIOGRAFÍA

- **Libros**

BACE, Rebecca. *An Introduction to Intrusion Detection*. Infidel Inc. for ICSA Inc. EEUU. 1999.

BLACK, Uyless. *Redes de Computadores*. Alfaomega. 1995.

BORGHELLO, Cristian Fabián. *Seguridad Informática, sus Implicancias e Implementación*. Documento PDF. Universidad Tecnológica Nacional. Septiembre 2001.

CERINI, María Dolores, PRÁ, Pablo Ignacio. *Plan de Seguridad Informática*. Documento PDF. Facultad de Ingeniería, Universidad Católica de Córdoba, Argentina. Octubre 2002.

COMER, Douglas. *TCP/IP, Vol. 1*. Prentice Hall. 1996.

FEIBEL, Werner. *The Encyclopedia of Networking, 2nd edition*. Documento PDF. Network Press. EEUU. 1996.

FEIT, Sidnie. *TCP/IP*. Editorial Osborne - McGraw Hill. EEUU. 1998.

FERNADEZ, Carlos M. *Seguridad en Sistemas Informáticos*. Ediciones Díaz de Santos S.A. España. 1988.

GLENDALE SYSTEMS.COM Ltd. *Information Security Policies V 2.0*. Documento PDF. RUSecure. Mayo 2001. http://www.eon-commerce.com/rusecure

GONCALVES, Marcus. *Firewalls Complete, Beta Book*. Editorial McGraw Hill. EEUU. 1997. http://www.ods.com.ua/win/eng/security/firewall

GONZÁLEZ GÓMEZ, Diego. *Sistemas de Detección de Intrusiones, versión 1.0*. Documento PDF. Julio 2003. http://www.dggomez.arrakis.es/secinf/ids/html/index.htm

HANCE, Olivier. *Leyes y Negocios en Internet*. McGraw Hill. México. 1996.

HUERTA VILLALÓN, Antonio. *Seguridad en Unix y redes*. (Versión 2.1). Documento PDF. Julio 2002. http://www.kriptopolis.com

KLANDER, Lars. *A Prueba de Hackers*. Editorial Anaya Multimedia. EEUU. 1998.

LEVIN, Ricardo. *Virus Informáticos*. McGraw Hill. España. 1992.

LÓPEZ FIGUEROLA, Santiago. *Teoría de las Redes Informáticas*. Documento PDF. Agosto 2003.

LUCENA LÓPEZ, Manuel José. *Criptografía y Seguridad en Computadores*. Universidad de Jaén. 3a edición. Documento PDF. España. Mayo 2003. http://wwwdi.ujaen.es/~mlucena

MCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hackers, Secretos y Soluciones para la Seguridad en Redes*. Traducción: GÓMEZ BASTIDA, Fulgencio. McGraw Hill. España. 2000. http://www.hackingexposed.com

MORALES VÁZQUEZ, José María. *Cortafuegos. Comparativa entre las Distintas Generaciones y Funcionalidades Adicionales*. Documento PDF. Curso de Experto Universitario en Seguridad y Comercio Electrónico, Programa de Postgrado UNED. 2002.

NORTHCUTT, Stephen, NOVAK, Judy. *Detección de Intrusos, Guía Avanzada*. Prentice Hall. 2a edición. España. 2001.

PINO CABALLERO, Gil. *Introducción a la criptografía*. Editorial RA-MA.

POYATO, Chelo, COLL, Francisco, MORENO, David. *Recomendaciones de Seguridad. Definición de una Política de Seguridad*. Documento PDF. España. 15 de diciembre de 2000. http://www.rediris.es/cert

RODRÍGUEZ, Adolfo, GATRELL, John, KARAS, John, PESCHKE, Roland. *TCP/IP Tutorial and Technical Overview*. Documento PDF. IBM Redbooks. Agosto 2001. http://ibm.com/redbooks

SGARRO, Andrea. *Códigos secretos*. Editorial Pirámides.

STALLINGS, William. *Network and Internetwork Security*. 2a Edición. Prentice Hall. EEUU. 1998.

TANENBAUM, Andrew S. *Redes de Computadoras*. 2a Edición. Editorial Prentice Hall. EEUU. 1997.

- **Manuales**

ARCERT. *Manual de Seguridad en Redes*. Documento PDF. Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina. Argentina. 1998. http://www.arcert.gov.ar

CHECKPOINT. *VPN-1 / Firewall –1, Management I NG FP-1, Student Edition.*

CHECKPOINT. *VPN-1 / Firewall –1, Management II NG FP-1, Student Edition.*

CHECKPOINT. *Introduction to Firewall -1, Management Student User Guide. Version 4.1. Revision A.*

COOB, Stephen. *Manual de Seguridad para PC y Redes Locales*. Ed. McGraw Hill.

DGSCA. *Guía para pruebas en áreas de cómputo*. Documento PDF. Departamento de Control de Calidad y Auditoría Informática. Marzo 2000.

- **Revistas y publicaciones**

CAPTAIN, Sean. "Stealth Fighters: today's best antivirus programs are tough on PC parasites but easy on users" en *PC World magazine*. September 2001.

DGSCA. *Vista general del libro naranja.* Documento PDF. Departamento de Control de Calidad y Auditoría Informática. Marzo 2000.

HERNÁNDEZ, Roberto. "Firewalls: Seguridad en las redes e Internet" en *Boletín de Política Informática*. N° 2. España. 2000.

LIMA DE LA LUZ, María. "Delitos Electrónicos" en *Criminalia*. N° 1–6 Año L. Ediciones Porrúa. México. Enero–Julio 1984.

PÉREZ IGLESIAS, Santiago. "Análisis del Protocolo IPSec: el estándar de seguridad en IP" en *Comunicaciones de Telefónica I+D*. N° 23, Noviembre 2001.

- **Internet**

Nota: Por el continuo movimiento de las direcciones de Internet es posible que alguna de las direcciones especificadas a continuación no se encuentren disponibles para consulta.

CISCO SYSTEMS, Inc. *Why You Need a Firewall?* Septiembre 28, 2002. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch2.htm

CORNELL SECURITY SEMINAR. *Firewall Deployment Considerations*. Agosto 29, 2001. http://www.cit.cornell.edu/computer/security/firewall/seminar-aug01/

DEPARTMENT OF DEFENSE. *Green Book*. Library N° S225, 994. EEUU. 1985. http://www.doe.gov

DEPARTMENT OF DEFENSE. *Orange Book.* Library N° S225, 711. EEUU. 1985. http://www.doe.gov

HOWARD, John D. *Thesis: An Analysis of security on the Internet 1989–1995.* Carnegie Institute of Technology. Carnegie Mellon University. EEUU. http://www.cert.org

MEINEL, Carolyn. *The Happy Hacker.* http://www.happyhacker.org. Traducción Equipo de Kriptopolis.com. http://www.kriptopolis.com/hacker

MONSERRAT COLL, Francisco Jesús. *Seguridad en los protocolos TCP/IP.* España. 14 de septiembre de 1998. http://www.rediris.es/ftp

MXCERT. *Guía Básica de Seguridad.* Coordinación de Emergencia en Redes Teleinformáticas. México. http://www.mxcert.org.mx/recursos

NOKIA. *Nokia and CheckPoint security appliances.* http://www.nokia.com/nokia/0,,3352,00.html

PHONEBOY'S FireWall-1 FAQ. *Essential Check Point FireWall-1 NG.* Septiembre 09, 2003. http://blog.phoneboy.com/

ROSTECK, Tanja S. *Hackers, rebeldes con causa.* 1996. http://www.geocities.com/ Silicon Valley/Pines/7347

STERLING, Bruce. *La Caza de Hackers.* Traducción de la versión original en inglés por Kriptopolis.com. España. 1999. http://www.kriptopolis.com

VALVERDE, José R. *Cortafuegos en Internet.* España. 2000. http://www.rediris.es/cert/doc

VALVERDE, José R. *Definición de una Política de Seguridad.* España. 2000. http://www.rediris.es/cert/docu_rediris/recomendaciones/html/recomendaciones.htm

VICOMSOFT Ltd. *Firewall Software for Internet Security: Why wait to be hacked?* http://www.firewall-software.com/index.html

Organismos

CERT Internacional: http://cert.org
CERT Argentina: http://www.arcert.gov.ar
CERT México: http://www.mxcert.org.mx
CSI (Computer Security Institute): http://www.gocsi.com
EFF (Electronic Frontier Foundation): http://www.eff.com
ICSA (International Computer Security Association): http://www.icsa.net
IETF (Internet Engineering Task Force): http://www.ietf.org

ISO (International Standard Organization): http://www.iso.ch
NIST (National Institute of Standards and Technology): http://www.nist.gov
NSA (National Security Agency): http://www.nsa.gov:8080
PGP International: http://www.pgpi.com–http://www.pgpinternational.com–http://pgp.org
Policía Electrónica Española: http://www.mir.es/policia/uiti
Red Iris: http://www.rediris.es–http://www.rediris.es/cert

Empresas

Ernst & Young, S.L.: http://www.ey.com
Microsoft Corporation: http://www.microsoft.com
Network Associates Inc.: http://www.nai.com
NIC Internacional: http://www.nic.com
Norton Symantec: http://www.symantec.com
Packet Storm: http://packetstorm.securify.com
Panda Software: http://www.pandasoftware.es
RSA Labs: http://www.rsa.com
Seguridata: http://www.seguridata.com
Steganos: http://www.steganos.net
SUN Microsytems: http://www.sun.com
Technet: http://www.microsoft.com/technet
Verisign: http://www.verisign.com
Zone Labs: http://www.zonelabs.com

Direcciones varias

http://esp.sophos.com/products/pm/
http://mssimplex.com/antivirus.htm
http://virusmd.com
http://web.mit.edu/kerberos/www/papers.html
http://www.350cc.com
http://www.alerta-antivirus.es
http://www.arrakis.com
http://www.asc.unam.mx
http://www.astalavista.box.sk
http://www.bsa.org
http://www.buscalaw.com
http://www.consealfirewall.com
http://www.crn.com/sections/special/champs/champs02.asp?ArticleID=33962
http://www.cybercursos.net
http://www.cybersnot.com/iebug.html
http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html
http://www.etcetera.com.mx
http://www.hack3r.org
http://www.hackersmag.com/revistas
http://www.hexagono.com

http://www.iec.csic.es/criptonomicon
http://www.infohack.org
http://www.javasoft.com/security
http://www.kriptopolis.com
http://www.lafirmadigital.com
http://www.lainfeccion.com
http://www.linux.org.es
http://www.microsoft.com/security
http://www.netsearch–ezine.com
http://www.newhackcity.net/win_buff_overflow
http://www.ntbugtraq.com
http://www.nwnetworks.com/iesf.html
http://www.paisvirtual.com/informatica/redes/er_pako/zines.htm
http://www.pgp.com
http://www.phrack.com
http://www.securiteam.com
http://www.terra.es/tecnologia/articulo/html/tec8966.htm
http://www.toxyn.org
http://www.trouble.org/survey
http://www.virusattack.com.ar

APÉNDICE A

GLOSARIO

A

AES (Advanced Encryption Standard): Avance del Estándar de Encripción, se refiere a los sistemas operativos del futuro que encriptarán todos los ficheros que guardan en el disco duro de manera automática.

AH (Authentication Header): Cabecera de Autentificación, se puede utilizar de dos modos: en modo de transporte y en modo túnel. Dependiendo del modo, la cabecera se situará en diferentes lugares.

ANSI/TIA/EIA 568: Este estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

ARP (Addres Resolution Protocol): Protocolo de Resolución de Direcciones, permite mantener asignaciones de pares formadas por las direcciones IP y las direcciones físicas.

ASA (Adaptive Security Algorithm): Algoritmo de Seguridad Adaptable, tecnología CISCO, está basado en estado y orientado a conexión, crea flujos de sesión basados en: direcciones origen y destino, números de secuencia TCP, números de puerto y banderas TCP.

AVPD (Anti-Virus Product Developers Consortium): Desarrolladores de Productos Antivirus, es un foro para el intercambio de información entre los líderes desarrolladores de productos, y soporta un estándar de la industria para la prueba y certificación de productos antivirus.

B

Backbone: Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

BBS (Bulletin Board System): Sistema de Mensajería Electrónica, se trata de un equipo informático al que se accede a través de la línea telefónica. En éste los usuarios intercambian información y software.

BGP (Border Gateway Protocol): Protocolo de Pasarela Frontera, se encarga de mover paquetes de una red.

BIOS (Basic Input Output System): Sistema Básico de Entrada Salida, es un programa residente en la memoria permanente del sistema electrónico. Se encarga de controlar las interacciones entre el hardware del conjunto informático. Es el programa diseñado por el fabricante para "poner en marcha" el sistema.

B-ISDN (Broadband ISDN): ISDN de banda amplia, conjunto de servicios, capacidades e interfaz que soportan una red integrada y una interfaz de usuario a velocidades mayores que la de la ISDN.

Bomba Lógica: Programa ilegítimo contenido dentro de un sistema y ante un hecho o fecha prevista "explota" causando daño al sistema que lo contienen u a otro.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Se identifican por una dirección broadcast.

Buffer: Área de almacenaje temporal, por lo general en la RAM. Su objetivo es de actuar como un área propia, necesita el permiso de la CPU antes de la transferencia de datos a un dispositivo.

C

Caballo de Troya: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar daño.

CCITT (International Consultative Committee of Telegraph and Telephone): Comité de Consultoría Internacional para Telefonía y Telegrafía, organización internacional responsable por el desarrollo de estándares de comunicación. Actualmente se conoce como UIT-T.

CERT (Computer Emergency Response Team): Equipo de Emergencia de Internet, dirigido por expertos en diagnósticos y resolución de problemas de seguridad.

Cluster: Con este término se identifica una sección física dentro de un disco de almacenamiento. Agrupa uno o varios sectores del disco que se encuentran consecutivos o adyacentes.

Código Rojo: Virus creado por el grupo internacional de virus conocido como 29A. Utiliza un agujero de seguridad para obtener acceso a los servidores web y continúa buscando nuevos sistemas vulnerables.

CRN (Computer Reseller News): Noticias De Distribuidores de Computadoras, es la revista líder que provee noticias y análisis de la industria para proveedores de productos que integran soluciones de tecnología.

CSMA/CD (Carrier Sense Multiple Access / Collision Detection): Acceso Múltiple por Percepción de Portadora / Detección de Colisiones, mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora.

D

DARPA (Defense Advanced Research Projects Agency): Agencia de Proyectos de Investigación Avanzada para la Defensa, agencia gubernamental de E.U. que financió la investigación y la experimentación con Internet. Antiguamente denominada ARPA, volvió a utilizar ese nombre a partir de 1994.

DES (Data Encryption Standard): Estándar de Encripción de Datos, es un sistema que se puede catalogar como un cifrado en bloque que es a la vez un cifrado producto de transposiciones y sustituciones. Su variante 3DES, es el resultado de aplicar de manera iterativa este estándar.

DHCP (Dynamic Host Configuration Protocol): Protocolo de Configuración Dinámica del Host, protocolo que proporciona un mecanismo para asignar direcciones IP de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

Direccionamiento IP: Conjunto de 32 dígitos binarios (cuatro bytes) o 12 decimales organizados en cuatro grupos de números con valores comprendidos entre 0 y 255, mediante los cuales se reconocen las máquinas entre ellas al establecer una conexión.

DMZ (Demilitarized Zone): Zona Desmilitarizada, referente una red de computadoras o computadora que divide la zona de red pública e interna.

DNS (Domain Name Service): Servidor de Nombres de Dominio, servicio de búsqueda de IPs de dominios, almacenadas en bases de datos. En Internet los equipos conectados se reconocen por su IP.

DoD (Department of Defense of the United States): Departamento de Defensa, organización gubernamental de los E.U. responsable por la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

DoS (Denial of Service): Negativa de Servicio, acciones que impiden a cualquier sistema funcionar de acuerdo con su propósito.

DS0: (Digital Signal): Señal Digital 0, es un canal digital de 64 kbps.

E

E1: Esquema de transmisión digital de área amplia, que lleva datos a una velocidad de 2,048 Mbps. Las líneas E1 pueden ser dedicadas para el uso privado de carriers comunes.

Encriptar: Codificar, cifrar. Es un término que se refiere a la aplicación de una serie de operaciones matemáticas o algoritmos a un texto legible, para convertirlo en algo

totalmente inteligible, de manera que se impida su comprensión por parte de personal no autorizado. En el proceso de desencriptado la información vuelve a su estado original.

ESP (Encapsulating Security Payload): Seguridad del Encapsulado de la Carga Útil, protocolo IP 50, de la familia IPSec que incluye las características de AH y agrega, opcionalmente, la confidencialidad de los datos.

Ethernet: Protocolo de comunicación. Tecnología estándar para la instalación de redes LAN Esta tecnología fue creada y desarrollada por Xerox.

Extranets: Red cooperativa que usa la tecnología de Internet para vincular actividades comerciales con proveedores, clientes u otros negocios. Las partes cooperativas o el público en general pueden acceder a la información.

Exploits: Programa que aprovecha un bug de un sistema, es decir, abusa de algún error de un sistema operativo para conseguir aumentar los privilegios de un usuario o la caída del sistema.

F

FDDI (Fiber Distributed Data Interface): Interfaz de Datos Distribuida por Fibra, estándar de LAN, que especifica una red de transmisión de tokens de 100 Mbps que utiliza cable de fibra óptica, usa una arquitectura de anillo doble para brindar redundancia.

Finger: Programa o comando que muestra información sobre un usuario específico. Normalmente, su identidad, tiempo de conexión y ubicación.

Frame Relay: Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales entre dispositivos conectados. Es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FTP (File Transfer Protocol): Protocolo de Nivel de Usuario, permite la transferencia de archivos entre computadoras.

Fuerza Bruta: Se basa en aprovechar diccionarios para comparar las palabras almacenadas en él con las contraseñas del sistema y obtenerlos.

G

Gateway: Se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro.

GBIC (Gigabit Interface Converter): Convertidores de Interfaz Gigabit, es un transmisor-receptor que convierte las señales eléctricas utilizadas entre los adaptadores del transportador anfitrión y las señales eléctricas u ópticas convenientes para la transmisión.

H

Host: Sistema Central, computadoras que permiten a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, TELNET, FTP.

HTML (HyperText Markup Languaje): Lenguaje de Marcado de Hipertexto, lenguaje en el que se elaboran y transmiten las páginas Web para su visualización con el navegador las páginas Web.

HTTP (HyperText Transfer Protocol): Protocolo de Transferencia de HiperTexto, es un protocolo de la capa de aplicaciones con la velocidad necesaria para sistemas de información hipermediales en un ambiente distribuido y colaborativo.

Hub: Concentradores, centro de una topología en estrella. También denominado repetidor multipuerto. Es un equipo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Pueden ser activos o pasivos.

I

ICMP (Internet Control Message Protocol): Protocolo de Mensajes de Control en Internet, protocolo de Internet de la capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP.

IDS (Intruder Detection System): Sistemas de Detección de Intrusos, es el área aplicada de la seguridad informática encargada de informar de eventos que puedan tener lugar en un sistema informático y pueda ser considerado, por unas u otras razones, como parte de un intento de intrusión.

IEC (International Electrotechnical Commission): Organismo Internacional de Normalización, es el organismo que establece las normas internacionales en todos los ámbitos de la electrotecnología.

IEEE (Institute of Electrical and Electronics Engineers): Instituto de Ingeniería Eléctrica y Electrónica, organización profesional entre cuyas actividades se incluye el desarrollo de estándares para comunicaciones y redes.

IEEE 802.x: Es un conjunto de normas que definen las características físicas de las redes, dictadas por el IEEE. IEEE 802.3 define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables). IEEE 802.5 define hardware para Token Ring.

IETF (Internet Engineering Task Force): Fuerza de Tareas de Ingeniería de Internet, fuerza de tareas compuesta por más de 80 grupos de trabajo responsables por el desarrollo de estándares de Internet.

IGMP (Internet Group Management Protocol): Protocolo de Administración del grupo Internet, proporcionan un protocolo para intercambiar y actualizar información acerca de la pertenencia de hosts a grupos de multidifusión específicos.

Ingeniería Social: Son técnicas elaboradas a través del engaño de las personas en revelar contraseñas u otra información, más que la obtención de dicha información a través de las debilidades propias de una implementación y mantenimiento de un sistema.

Intranet: Red privada que utiliza las tecnologías de Internet, brinda a los usuarios la capacidad de compartir dinámicamente recursos internos de la misma forma que los usuarios de Internet lo hacen.

Internet: Sistema de redes de computación ligadas entre sí, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos y correo electrónico.

IP (Internet Protocol): Protocolo de Internet, es un conjunto de reglas o protocolos que regulan el tráfico de datos en las denominadas redes IP y/o en Internet.

i-Planet: Permite trabajar en Internet. No sólo para el chat, escuchar música, etc. Este producto permite a los colaboradores y socios de una compañía acceder a las aplicaciones internas de la empresa a través de un navegador con la debida seguridad, sin modificar las aplicaciones para que éstas sean web-enabled.

IPSec (Internet Protocol Security): Protocolo de Seguridad para Internet, es un protocolo de comunicaciones que provee de opciones avanzadas de seguridad tales como unos algoritmos de encriptación de la información más avanzados y una autentificación de usuarios más exhaustiva.

IPv4 (Internet Protocol Versión 4): Protocolo Internet Versión 4, es un protocolo de conmutación no orientado a conexión de máximo esfuerzo.

IPv6 (IP versión 6): Reemplazo de la versión actual de Ipv4. Brinda soporte para identificación de flujo en el encabezado del paquete, que se puede usar para identificar flujos.

IPX/SPX (Internetwork Packet Exchange-Sequenced Packet Exchange): Conjunto de protocolos de bajo nivel utilizados por el sistema operativo de la red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

IRC (Intenet Relay Chat): Charla o Conferencia en Internet, protocolo de Internet para la transmisión de comunicaciones simultaneas en tiempo real a través de servidores IRC.

IRQs (Interruption Request): Petición de Interrupción, recursos que utiliza un dispositivo cuando necesita detener el proceso que está realizando la PC.

ISO (International Organization for Standarization): Organización Internacional para la Estandarización, organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia OSI y protocolos estándares para varios niveles de este modelo.

J

Java Script: Lenguaje de programación orientado a la elaboración de pequeñas aplicaciones, funcionales en la red (applets) capaces de operar bajo cualquier plataforma a través de navegadores WWW.

K

Kernel: Núcleo o parte esencial de un sistema operativo. Provee los servicios básicos del resto del sistema.

L

LAN (Local Area Network): Red de Área Local, es una red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña. Conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada.

LCP (Link Control Protocol): Protocolo de Control de Enlace, protocolo que proporciona un método para establecer, configurar, mantener y terminar una conexión punto a punto.

L2TP (Layer To Tunneling Protocol): Protocolo Tunneling de Dos Niveles, es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet.

Logs: Son archivos de informe que se crean mientras y/o tras haberse realizado una acción con el fin de mostrar lo que ha acontecido durante la realización de la misma. Los log de un monitor de sistema muestran todo lo que se ha ejecutado en un sistema, quién ha accedido a ese sistema, qué ha hecho, cuánto tiempo, etc.

Logging: Es un archivo donde se guarda todo lo acontecido en la página errores, accesos, etc.

Login: Procedimiento de identificación de usuario ante un sistema informático previo la entrada o uso del sistema. Este login más la contraseña, permiten acceder a información o usos restringidos.

M

MAC (Media Access Control): Control de Acceso al Medio, es la inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos.

MAN (Metropolitan Area Network): Red de Área Metropolitana, es una red que cubre una gran área geográfica y que promete alta velocidad de comunicación a grandes distancias.

MAU (Multiple Access Unit): Unidad de Acceso Múltiple, es un dispositivo utilizado en redes Ethernet e IEEE 802.3 que proporciona una interfaz entre el puerto AUI de una estación y el medio común de Ethernet. Esta puede ser incorporada a una estación, o puede ser un dispositivo separado, lleva a cabo funciones de la capa física, incluyendo la conversión de datos digitales de la interfaz Ethernet, la detección de colisiones, y la inyección de bits en la red.

Mbone (Multicast Backbone): Es un sistema de Multicast para la red IP. Permite la transmisión de información desde un emisor a múltiples receptores. Las aplicaciones que más se usan en este ámbito son las de videoconferencia.

MIME (Multipurpose Internet Mail Extensions): Extensiones Multipropósito de Correo de Internet, conjunto de especificaciones que permite la interpretación y traducción de distintos formatos de texto y de algunos formatos de archivo por parte de los servidores de correo.

MTU (Maximum Transmission Unit): Unidad Máxima de Transmisión, indica el tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

N

NAT (Network Address Translation): Traducción de Direcciones de Red, mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. Permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a Internet transformando esas direcciones en espacio de direccionamiento en ruteable global.

NCP (Network Control Protocol): Protocolo de Control de Red, es un protocolo del Network Layer.

NEBS (Network Equipment Building System): Sistema de Construcción de equipo de Red, grupo de requerimientos técnicos con un objetivo único, hacer que los switches de las redes de comunicación sean "a prueba de balas".

NetBEUI: Protocolo de los niveles de transporte y red del modelo ISO/OSI, se integra con NetBIOS para ofrecer un sistema de comunicaciones eficiente en el entorno LAN de grupos de trabajo.

NetBIOS (Network Basic Input Output System): Sistema Básico de Entrada – Salida, protocolo del nivel de sesión, que establece y mantiene las sesiones de comunicación entre computadoras.

NetWare: Es una plataforma capaz de entregar servicios de negocio a través de cualquier tipo de red, sistemas de almacenamiento y estaciones de trabajo y, como tal, forma parte de Novell Enterprise.

NFS (Network File System): Sistema de Archivos de Red, es un servicio de red por el cual varias máquinas llamadas Clientes comparten uno o varios directorios que se encuentran físicamente en una máquina llamada Servidor.

NIC (Network Interface Card): Tarjeta de Interfaz de Red, también conocida como adaptadora o tarjeta adaptadora, es una placa de circuito instalada en un componente de equipos de informática.

Nimbda: Virus que se propaga por la red, infecta los servidores web de Microsoft, no debería afectar un servidor Linux más que en mensajes en el log.

NNTP (Network News Transfer Protocol): Protocolo de Transferencias de Noticias en Red, protocolo para la transmisión de noticias en la red, se utiliza para enviar, distribuir y recuperar mensajes de USENET.

NOC (Network Operation Center): Centro de Operación de Red, proporciona a los clientes, de forma remota, el monitoreo, control y gestión de los sistemas informáticos y de comunicaciones. Es un servicio dotado de medios humanos, tecnológicos y de infraestructura propios dedicada exclusivamente a la gestión y mejora de la operación cotidiana de la totalidad de la infraestructura de las tecnologías de la información del cliente.

NTP (Network Time Protocol): Protocolo de Tiempo de Red, protocolo desarrollado sobre el TCP que garantiza la precisión de la hora local. Puede sincronizar los relojes distribuidos en milisegundos durante períodos de tiempo prolongados.

NTU (Network Terminating Unit): Unidad de Terminación de Red, es un dispositivo que cumple funciones de gestión de ATM en el límite entre el servicio público de ATM.

NWLink: Es un protocolo de transporte, compatible con IPX/SPX/NetBIOS. Es una implementación de los protocolos de intercambio de paquetes entre redes e intercambio de paquetes secuenciados.

O

OSI (Open System Interconnection): Interconexión de Sistemas Abiertos, programa de estandarización internacional creado para desarrollar normas para redes de datos que faciliten la interoperabilidad entre equipos de diversos fabricantes.

OSPF (Open Shortest Path First): Primero la Ruta Libre más Corta, protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas y el balanceo de carga.

P

PAP (Password Authentication Protocol): Protocolo de Autentificación por Password, protocolo de comunicaciones que permite a un sistema informático verificar mediante password la identidad de quien se le conecta.

PHP: Es un lenguaje de programación orientado a servidor, es decir, que nuestra máquina no realiza ninguna operación de compilado, la máquina encargada de esto es el servidor web en el que esté puesta nuestra página.

POP (Postal Office Protocol): Protocolo para Recibir Correo Electrónico, brinda la posibilidad de que el correo electrónico sea depositado en "buzones" ubicados en algún tipo de sistema servidor de correo, y no directamente en una estación de trabajo.

POP3: Es el protocolo cliente/servidor por el cual el correo electrónico es recibido y enviado al usuario desde su servidor de Internet.

PPPoE (Point to Point Protocol over Ethernet): Protocolo Punto a Punto a través de Ethernet, es un método de administrar protocolos PPP a través de Ethernet. Proporciona autentificación de sesiones mediante el protocolo de autentifcación de contraseñas.

PPP (Point to Point Protocol): Protocolo Punto a Punto, protocolo de comunicaciones serie que opera sobre líneas de enlace telefónico rentadas y cifradas entre un cliente y un gateway o entre dos gateways.

PPTP (Point-to-Point Tunneling Protocol): Protocolo Tunneling Punto a Punto, sirve para el acceso a redes privadas virtuales, se emplea en situaciones en las que los usuarios de una red privada corporativa precisan de un acceso a la red privada desde un lugar remoto.

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Proxy: Es una aplicación o un dispositivo hardware que hace de intermediario entre los usuarios, normalmente de una red local, e Internet. Lo que hace realmente un proxy es recibir peticiones de usuarios y redirigirlas a Internet. La ventaja que presenta es que con una única conexión a Internet podemos conectar varios usuarios.

R

RARP (Reverse Address Resolution Protocol): Protocolo de Resolución de Direcciones Inverso, la función de éste protocolo complementa la función de ARP, pues permite mantener asignaciones de direcciones físicas a direcciones Internet.

RIP (Routing Information Protocol): Protocolo de Información de Enrutamiento, protocolo suministrado con los sistemas BSD de Unix. RIP utiliza el número de saltos como métrica de enrutamiento.

RJ-45: Conector estándar de 8 alambres usados en LANs.

RJ-11: Conector estándar de 4 alambres para líneas telefónicas.

RPC (Remote Process Call): Llamada de Procedimiento Remoto, base tecnológica de la arquitectura cliente/servidor. Las RPC son llamadas de procedimiento que los clientes crean o especifican y que se ejecutan en los servidores. Los resultados se devuelven a los clientes a través de la red.

Ruteador: Equipo que forma parte de las redes de comunicaciones y tiene como misión encauzar y distribuir el tráfico de paquetes de información.

Ruteo Dinámico: Permite tener conocimiento automático y sin intervención humana de las rutas de la red.

S

Servidor de archivos: Es aquel equipo que permite compartir los archivos y programas que se encuentren en sus discos. Ordinariamente funciona también como servidor de impresoras.

Servidor de dominios: Es el servidor que se encarga de verificar, a través de las cuentas de usuario, el acceso de los mismos a la red y a determinados recursos compartidos.

SLIP (Serial Line Internet Protocol): Protocolo de Conexión Serial de Internet, es usado para trasmitir paquetes IP a través de líneas de comunicación seriales.

SMTP (Simple Mail Transfer Protocol): Protocolo de Correo Simple, proporciona la capacidad de almacenamiento y reenvío del correo entre los host de los sistemas de correo de la red.

Sniffers: Monitor de red. Son programas que monitorizan la información que circula por la red con el objeto de capturar información.

SNMP (Simple Network Managment Protocol): Protocolo para la Administración Simple de una Red, permite obtener información de gestión de los dispositivos conectados a la red.

Spam: Se denomina así al correo electrónico que se recibe sin haberlo solicitado, son los llamados "correos basura". Son utilizados por las empresas para fines publicitarios.

SSH (Secure Shell): Seguridad del Intérprete de Comandos, es una aplicación de seguridad que permite la conexión entre computadoras de forma segura.

SSL (Secure Sockets Layer): Capa de Socket Segura, protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

STP (Shielded Twisted Pair): Par Trenzado Blindado, medio de cableado de dos pares que se usa en diversas implementaciones de red. Posee una capa de aislamiento blindada para reducir la interferencia electromagnética.

Super-usuario: Es un usuario especial que tiene permiso para ejecutar todas las tareas de administración del sistema. El nombre de usuario para el super-usuario es root.
Swap: Es un espacio reservado en el disco duro para poder usarse como una extensión de memoria virtual del sistema. Es una técnica utilizada para hacer creer a los programas que existe más memoria RAM de la que en realidad existe. Es el propio sistema operativo el que se encarga de pasar datos a la swap cuando necesita mas espacio libre en la RAM y viceversa.

Switch: Dispositivo que conecta computadoras. Actúa de manera inteligente, puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

T

TCP (Transmission Control Protocol): Protocolo de Control de Transmisión, es un protocolo orientado a la conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega delos paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de éstos.

TCP/IP (Transfer Control Protocol/Intenet Protocol): Protocolo de Control de la Comunicación en Internet, arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundido en la actualidad, por ser la base de Internet.

TCP wrapper: Es un programa que permite filtrar IP por los distintos puertos e indicar que programa se ejecuta en cada uno de los puertos, por lo que se pueden ver todas las aplicaciones malintencionadas que pueden conseguir los roots usando este tipo de programas.

TELNET (Tele Network): Conexión a un servidor en la que la computadora del cliente emula un terminal de manera que se configura como terminal virtual del ordenador

servidor. Es un protocolo estándar de Internet que permite al usuario conectarse a un ordenador remoto y utilizarlo como si estuviera en una de sus terminales.

TFTP (Trivial File Transfer Protocol): Protocolo de Transferencia de Archivos Trivial, es una versión simplificada de FTP que permite la transferencia de archivos de un computador a otro a través de una red.

Token Ring: LAN de transmisión de señales desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo.

Tunneling: Se trata de una técnica especialmente diseñada para imposibilitar la protección antivirus en cualquier momento. Mientras el análisis permanente, o residente, del programa antivirus que se encuentre instalado, intenta realizar detecciones el virus actúa en su contra.

T1: Servicio de portadora WAN digital que transmite datos formateados DS-1 a 1,544 Mbps a través de la red de conmutación telefónica, usando la codificación AMI.

U

UDP (User Datagram Protocol): Protocolo de Datagrama de Usuario, es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

URL (Uniform Resource Locator): Localizador de Recursos Uniforme, esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y otros servicios utilizando un explorador de Web.

UUCP (Unix to Unix Copy Protocol): Se trata de un protocolo para la transferencia de ficheros, noticias, y correo, así como para ejecutar ordenes distantes entre ordenadores.

V

VLAN (Virtual LAN): LAN Virtual, grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos.

VPN (Virtual Private Network): Red Privada Virtual, permite establecer una conexión segura a través de una red pública, o Internet.

W

WAN (Wide Area Network): Red de Área Amplia, es una red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes.

Web: Página diseñada generalmente con lenguaje HTML, y utilizadas para la publicación de información en Internet. Para poder visualizarse necesitamos el uso de navegadores.

WebSense: Es un producto de software que trabaja con una base de datos maestra. Además, dispone de una herramienta que permite generar detallados reportes del uso de la Internet, brindando así a los administradores un real control de los disponibles recursos de cómputo. Permite mejorar la productividad de los usuarios y optimizar el uso de los servidores Internet y el ancho de banda de su enlace a Internet.

WWW (World Wide Web): Red Mundial de documentos HTML interconectados entre sí y distribuidos entre servidores en todo el mundo.

APÉNDICE B

IPSec

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros). Es un estándar que aborda las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y, tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP.

Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se estipula su aplicación en la normativa de IPv6.

Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable; todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios.

Otra característica destacable de IPSec es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI (Public Key Infrastructure, Infraestructura de Clave Pública) y, aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Entre los beneficios que aporta IPSec, se encuentran:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.

- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación. Las extranets son un ejemplo.

- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.

- Ofrece al usuario a distancia el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

Es importante señalar que cuando citamos la palabra "seguro" no nos referimos únicamente a la confidencialidad de la comunicación, también nos estamos refiriendo a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad. Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente.

Descripción del protocolo IPSec

IPSec es, en realidad, un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública, algoritmos de cifrado, algoritmos de *hash* y certificados digitales X509v3.

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 (Message Digest Algorithm 5, Algoritmo de Condensado de Mensaje, versión 5) y SHA-1 (Secure Hash Algorithm 1, Algoritmo Seguro de *Hash*, versión 1), como funciones de *hash*. Además, es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA (International Data Encryption Algorithm, Algoritmo Internacional de Encripción de Datos), Blowfish, o el más reciente AES (Advanced Encryption Standard, Estándar Avanzado de Encripción), que se espera sea el más utilizado en un futuro próximo.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: *IP Authentication Header* (AH) e *IP Encapsulating Security Payload* (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.

- Un protocolo de gestión de claves *Internet Key Exchange* (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El protocolo AH

El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autentificación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo, no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

Tal como indica su nombre, AH es una cabecera de autentificación que se inserta entre la cabecera IP estándar (en IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (ver la figura B.1). AH es realmente un protocolo IP nuevo, y como tal el IANA (Internet Assigned Names Authority, Autoridad para la Asignación de Nombres en Internet) le ha asignado el número decimal 51. Esto significa que el campo Protocolo de la cabecera IP contiene el valor 51, en lugar de los valores 6 ó 17 que se asocian a TCP y UDP respectivamente.

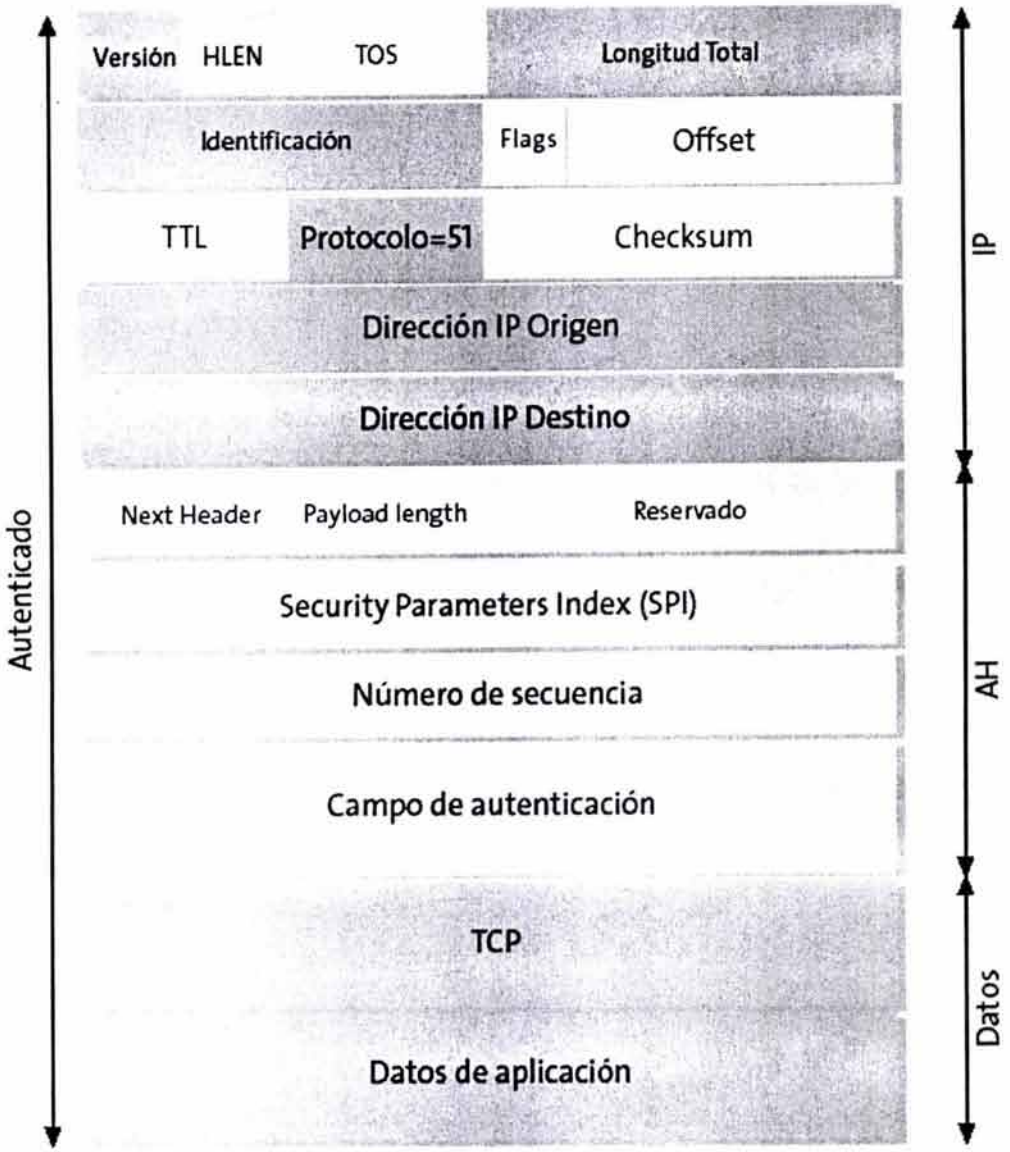

Figura B.1. Estructura de un datagrama AH.

Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: *TOS, TTL, flags, offset* y *checksum*.

El funcionamiento de AH se basa en un algoritmo HMAC (Hashed Message Authentication Code, Código de Autenticación de Mensaje con *Hash* previamente aplicado), este es un código de autentificación de mensajes. En la figura B.2 se muestra el modo en que funciona el protocolo AH.

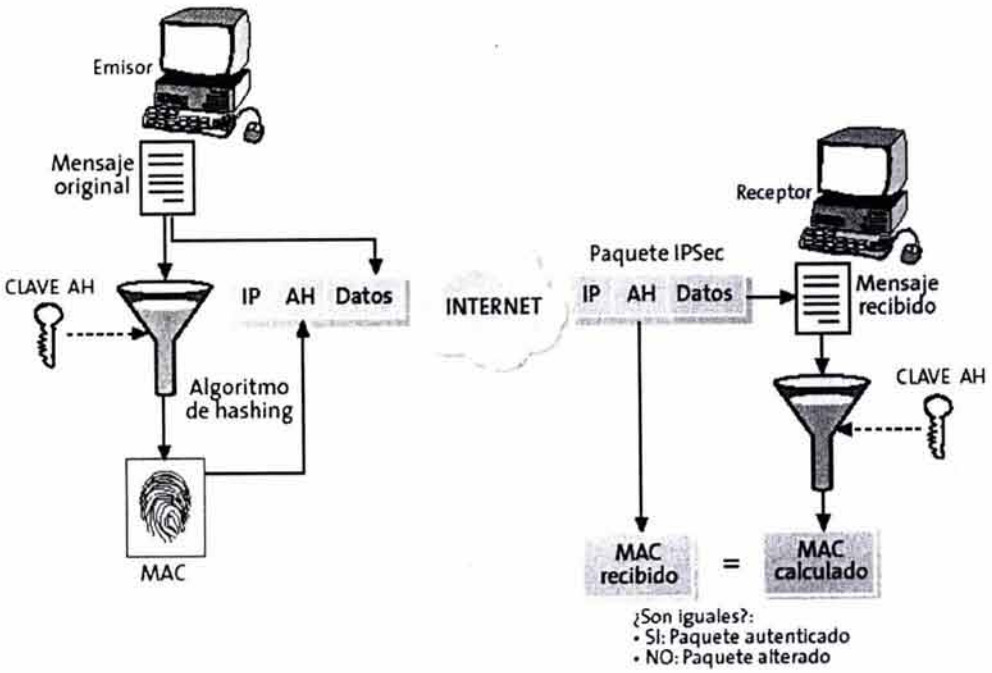

Figura B.2. Funcionamiento del protocolo AH.

El algoritmo HMAC consiste en aplicar una función *hash* a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extracto MAC (Message Authentication Code, Código de Autenticación de Mensaje) es imposible sin conocer la clave, y que dicha clave (en la figura B.2, clave AH) sólo la conocen el emisor y el receptor.

El protocolo ESP

El objetivo principal del protocolo ESP es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autentificación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo).

El IANA ha asignado al protocolo ESP el número decimal 50. Esto implica que el campo Protocolo de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, está cifrado, un atacante hipotético que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información. En la figura B.3 se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

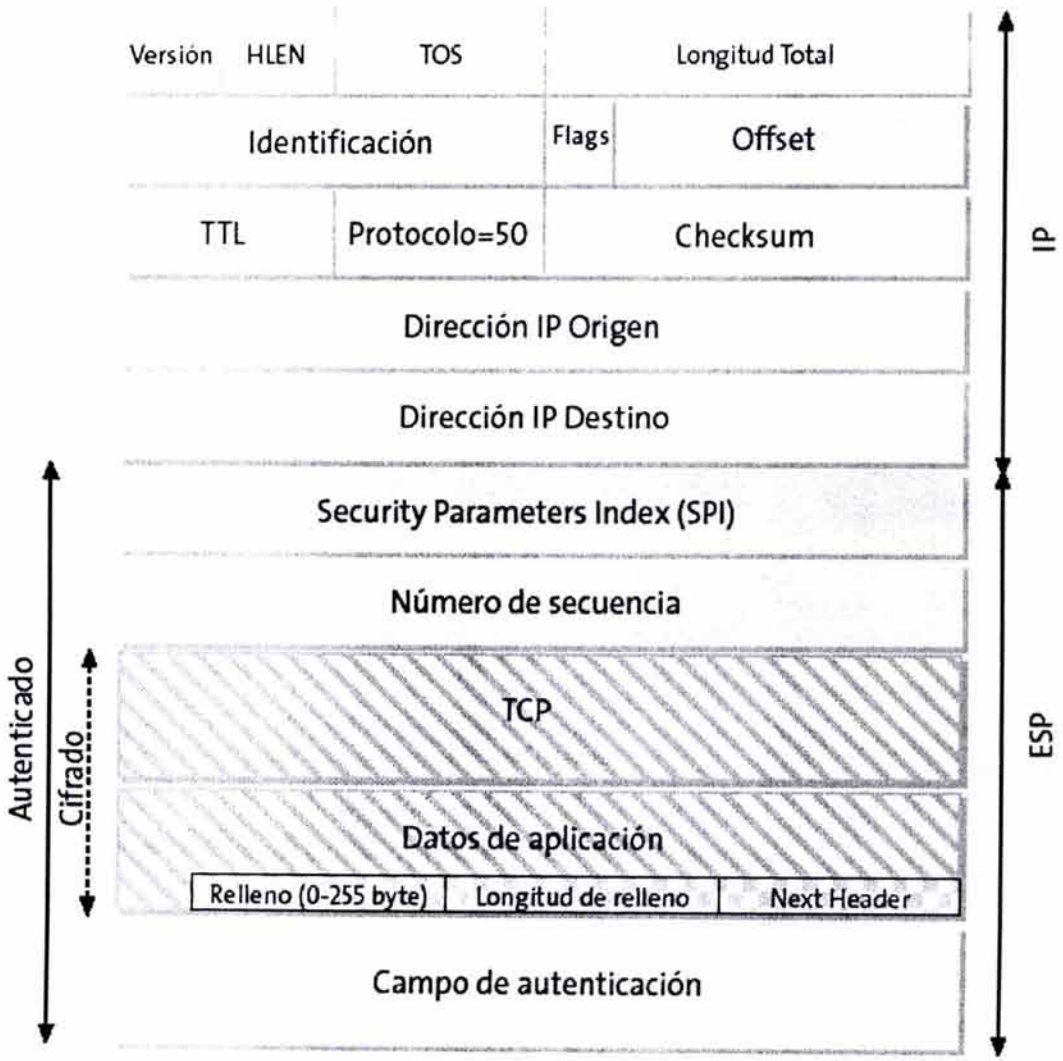

Figura B.3. Estructura de un datagrama AH.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado de bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno, tal como se observa en la figura B.3, el cual tiene una función adicional de poder añadir caracteres de relleno al campo de datos para ocultar así su longitud real y, por tanto, las características del tráfico. Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

En la figura B.4 se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra utilizando una clave determinada y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

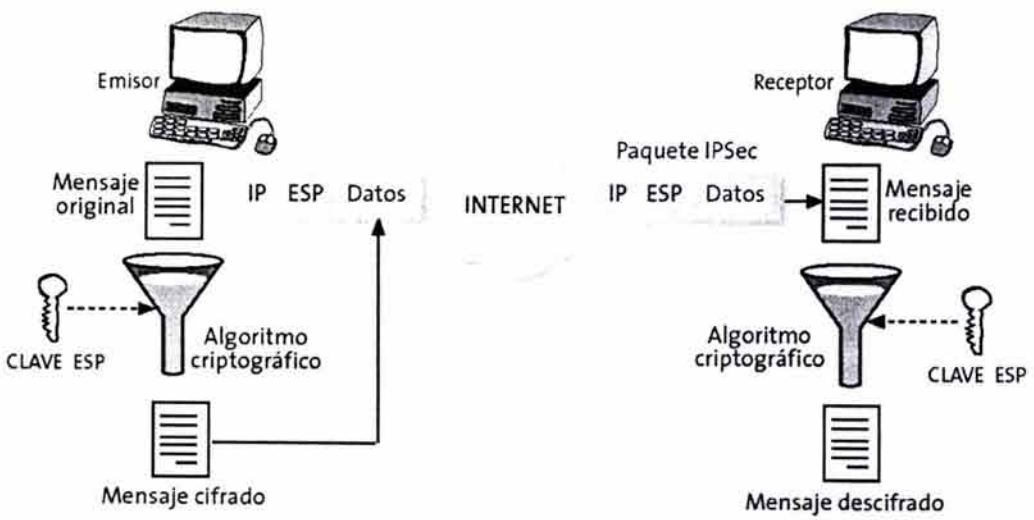

Figura B.4. Funcionamiento del protocolo ESP.

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de *hash* y en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE, que se detalla más adelante.

Los modos de transporte y túnel

El funcionamiento de IPSec permite que tanto ESP como AH proporcionen dos modos de uso:

- *El modo transporte.* En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

- *El modo túnel.* En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

La figura B.5 muestra los dos modos de funcionamiento del protocolo IPSec.

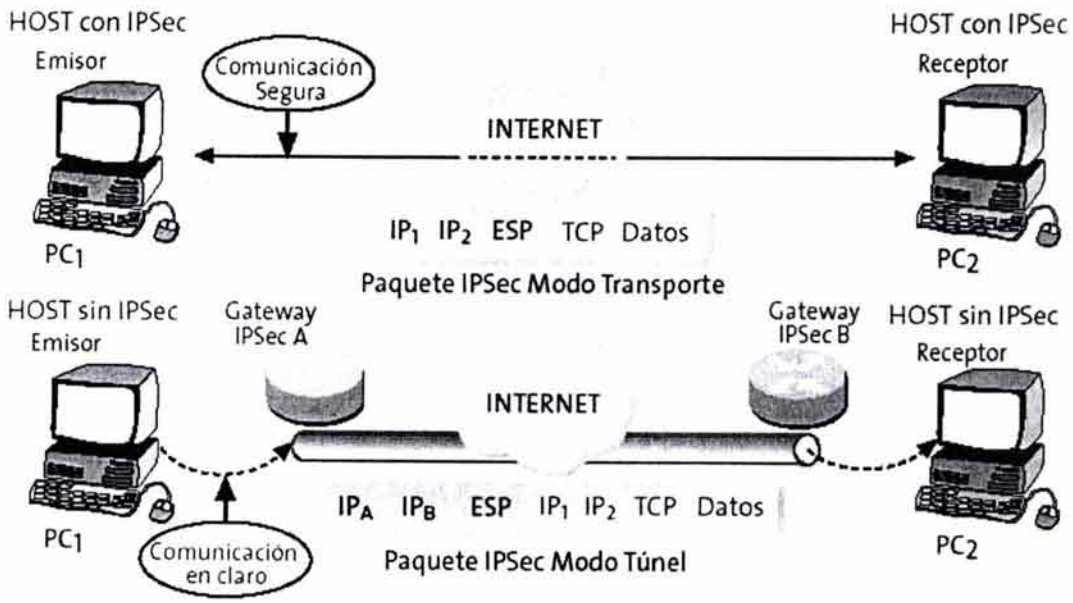

Figura B.5. Modos de Transporte y Túnel.

El modo túnel es empleado principalmente por los gateways IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo. El modo túnel también es útil cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra

aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (VPN) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet. IPSec puede ser implementado bien en un *host* o bien en un equipo dedicado, tal como un router o un *firewall*, que cuando realiza estas funciones se denomina gateway IPSec.

En la parte superior de la figura B.5 se representan dos *hosts* que entienden IPSec y que se comunican de forma segura. Esta comunicación se realiza en modo transporte, por tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.

En la parte inferior de la figura B.5 se muestran dos redes que utilizan para conectarse dos gateways IPSec y, por tanto, emplean una implementación en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los gateways IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales. Sin embargo ambos PCs envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local.

Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración.

El protocolo de control IKE

Un concepto esencial en IPSec es el de SA (Security Association, Asociación de Seguridad), que es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs.

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2 (Routing Information Protocol, 2nd version, Protocolo de Información de Enrutamiento, segunda versión).

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley. ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases: el establecimiento de un canal seguro y autenticado y la negociación de parámetros de seguridad.

Establecimiento de un canal seguro y autenticado

Es la fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado.

Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autentificación.

Existen varios métodos de autentificación, los dos más comunes se describen a continuación:

- El primer método de autentificación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones *hash*, cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autentificación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autentificación mediante secreto compartido, sino autentificación basada en certificados digitales.

- En los estándares IPSec está previsto el uso de un método de autentificación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI, cuya integración se tratará con detalle más adelante.

Negociación de parámetros de seguridad

En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec.

Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

En la figura B.6 se representa en forma esquemática el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH.

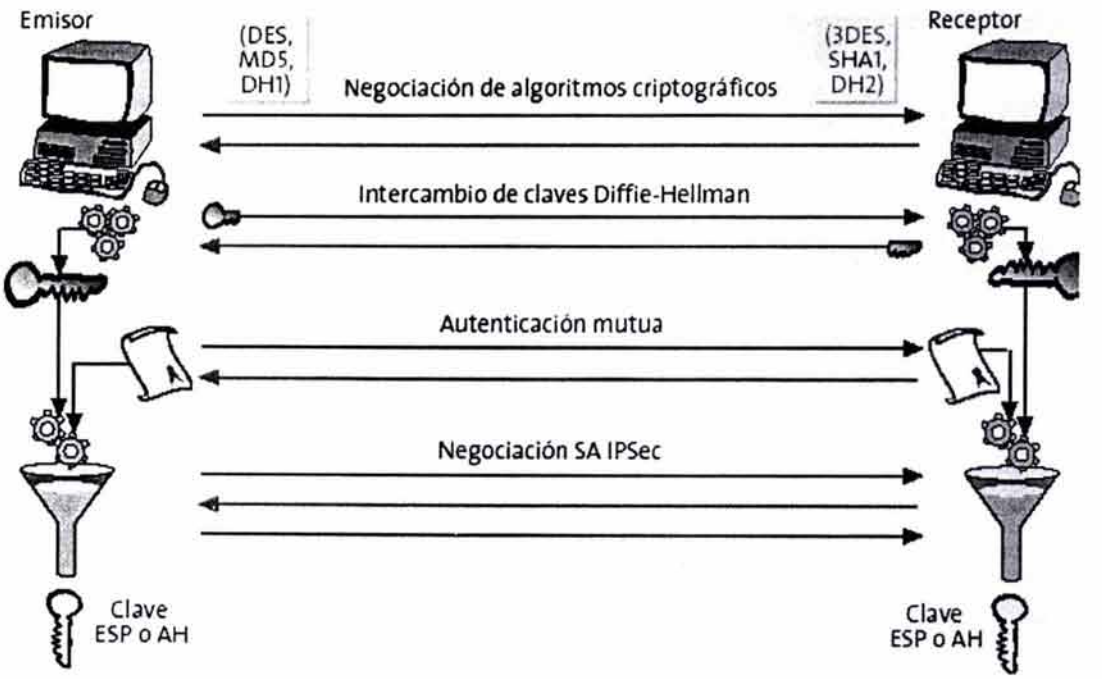

Figura B.6. Funcionamiento del protocolo IKE.

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. La existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación de IPSec en un entorno de usuarios a distancia y/o móviles.

Bajo el nombre de PKI se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y eventualmente renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec.

Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (en adelante CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3 como formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones mediante el cual los dispositivos IPSec dialogan con la PKI no está totalmente estandarizado. Esto hace que existan varias alternativas según el fabricante de que se trate.

En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta al directorio de la PKI. Típicamente, los periodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación.

Para la solicitud y descarga de certificados existe un protocolo denominado SCEP (Cisco Simple Certificate Enrollment Protocol, Protocolo Cisco de Alistamiento Simple de Certificado), que se ha convertido en un estándar de facto en las operaciones de registro y descarga de certificados para aplicaciones IPSec. SCEP es un protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados.

Servicios de seguridad ofrecidos por IPSec

Los servicios de seguridad ofrecidos por IPSec son: integridad y autentificación, confidencialidad, detección de repeticiones, control de acceso y no repudio.

Integridad y autentificación del origen de los datos

El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autentificación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se comentó anteriormente, esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

Confidencialidad

El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autentificación, ya que si no se garantiza la integridad de los datos, el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Ésta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado.

Detección de repeticiones

La autentificación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un número de secuencia incluido en la cabecera ESP o AH; el emisor incrementa dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados.

Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

Control de acceso: autentificación y autorización

Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentifican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autentificación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la

conexión IPSec. Esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen y destino, el byte "TOS" y otros campos.

No repudio

El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autentificación mediante certificados digitales. En este caso, el procedimiento de autentificación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

APÉNDICE C

CRIPTOGRAFÍA

La protección de la información se lleva a cabo variando su forma. Se llama cifrado (o transformación criptográfica) a una transformación del texto original, que lo convierte en el llamado texto cifrado o criptograma. Análogamente, se llama descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado.

Cada una de estas transformaciones está determinada por un parámetro llamado clave. El conjunto de sus posibles valores se denomina espacio de claves. La familia de transformaciones criptográficas se llama sistema criptográfico.

Para cada transformación criptográfica se definen las imágenes de cada una de las palabras de n letras. Se usará el término n-palabra en lugar de palabra de n letras.

Para evitar ambigüedades, se hacen las siguientes suposiciones:

- Se usa el mismo alfabeto para ambos textos, original y cifrado.
- Se define el cifrado de todas las posibles palabras, independientemente de si existen o no.
- Cada n-palabra se cifra en una n-palabra, teniéndose así que el cifrado no cambia la longitud del texto original.
- En general no es necesario imponer simultáneamente todas estas condiciones, aunque en algunos casos, en el procesamiento de información digital, si es recomendable, porque se trabaja únicamente con alfabeto binario. Además, debe existir el cifrado de todas las palabras posibles, si el cifrado cambiara la longitud del texto, sería necesario usar un nuevo formato para el texto cifrado.

La criptología representa una lucha entre el criptógrafo, que trata de mantener en secreto un mensaje usando para ello una familia de transformaciones, y el atacante, que intenta recuperar el texto inicial. Por lo que es necesario establecer unas reglas.

Criptografía teórica

Reglas de Kerckhoffs.

- No debe existir ninguna forma de recuperar, mediante el criptograma, el texto inicial o la clave.
- Todo sistema criptográfico debe estar compuesto por dos tipos de información:
  * Pública, como es la familia de algoritmos que lo definen. En los sistemas de clave pública, parte de la clave es también información pública.
  * Privada, como es la clave que se usa en cada cifrado particular.
- La forma de escoger la clave debe ser fácil de recordar y modificar.
- Debe ser factible la comunicación del criptograma por los medios de transmisión habituales.
- La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

Las principales desventajas del código cuando se utiliza cifrado son:

- Sólo se pueden transmitir aquellas palabras que tengan traducción asignada en el diccionario del código.
- El receptor debe tener el diccionario para poder decodificar la información.
- Su implementación, sobre todo a la hora de cambiar el código, es muy costosa.
- El criptoanálisis se puede basar en un análisis de frecuencias.
- Fuente del texto. En primer lugar hay que distinguir, según la fuente que proporciona el texto, el cifrado digital del analógico. Si dicha fuente es digital, los mensajes están constituidos por grupos de elementos pertenecientes a una colección finita denominada alfabeto. Por otro lado, se dice que la fuente es analógica si genera un conjunto continuo de valores. El cifrado de fuentes analógicas no resulta en absoluto seguro, por lo que es necesario previamente digitalizar los mensajes analógicos.

La ventaja de este sistema es la compresión de la información, siempre que las palabras de código usadas sean más cortas que las palabras originales.

Criptografía de clave privada

En los cifrados de clave privada, la seguridad depende de un secreto compartido exclusivamente por emisor y receptor.

El hecho de que sólo el emisor y el receptor tengan la posibilidad de descifrar archivos, es un aspecto ideal de la criptografía, ya que presenta algunos problemas.

La principal amenaza criptoanalítica proviene de la mala gestión de claves. Es decir, el número de claves crece al doble del número de usuarios. Para evitar un ataque, existen dos métodos básicos, los cuales son: la difusión y la confusión.

- Con el método de la difusión se consigue anular la influencia de la redundancia de la fuente sobre el texto cifrado. Hay dos formas de conseguirlo: la primera evita los criptoanálisis basados en las frecuencias de las n-palabras. La otra manera consiste en hacer que cada letra del texto cifrado dependa de un gran número de letras del texto original.

- El objetivo del método de la confusión consiste en hacer que la relación entre la clave y el texto cifrado sea lo más compleja posible, haciendo así que las estadísticas del texto cifrado no estén muy influidas por las del texto original. Eso se consigue normalmente con la técnica de la sustitución.

Dentro del cifrado de clave pública, se puede hacer otra división de cifrados, según el tipo de operación que se realiza. Dada la característica finita del alfabeto y la hipótesis de no variación de la longitud del texto, existen otras opciones para el cifrado. La llamada transposición, sustitución y producto.

- *Cifrado por transposición.* Consiste en crear el texto cifrado simplemente desordenando las unidades que forman el texto original.

- *Cifrado por sustitución.* Consiste en reemplazar las unidades del texto original según una clave.

- *Cifrado por producto.* Es la aplicación iterativa de cifrados sobre textos ya cifrados, es decir, a la composición de varios cifrados. En general, los cifrados de clave privada son cifrados producto de las dos operaciones mencionadas, sustitución y transposición.

Sustitución y transposición no resultan muy efectivos usados individualmente, sin embargo, constituyen la base de sistemas mucho más difíciles de criptoanalizar.

Con el cifrado de clave privada, tenemos la ventaja de que la velocidad de cifra es muy alta y por ello se usa para realizar la función de cifra de la información. Además, con claves de sólo unas centenas de bits obtenemos una alta seguridad pues su no linealidad y algoritmo hace que el único ataque que puede prosperar es el de la fuerza bruta.

Pero tiene aspectos en contra, como se mencionó anteriormente tiene mala gestión de claves, mala distribución de claves y no tiene firma digital.

Cifrado en bloque

Independientemente de la clasificación realizada anteriormente, los cifrados simétricos se pueden clasificar en dos grandes grupos: los correspondientes a fuentes que generan n-palabras y los correspondientes a fuentes que generan letras. En el primer caso se habla de cifrados en bloque y en el segundo de cifrados en flujo.

El cifrado en bloque opera sobre textos formados por n-palabras, convirtiendo cada una de ellas en una nueva n-palabra.

Sin duda el cifrado en bloque más conocido es el llamado DES (Data Encryption Estandar, Estándar para Encriptar Datos). Este sistema se puede catalogar como un cifrado en bloque que es a la vez un cifrado producto de transposiciones y sustituciones.

Las ventajas que ofrece el cifrado en bloque son: alta difusión de los elementos en el criptograma y es inmune, ya que no permite introducir bloques extraños sin detectarlo.

Las desventajas son: baja velocidad de cifrado al tener que leer antes el bloque completo y es propenso a errores de cifra.

Cifrado en flujo

Usa el concepto de cifra propuesto por Vernam, que cumple con sistemas de cifrado con secreto perfecto, esto es:

- El espacio de las claves es igual o mayor que el espacio de los mensajes.
- Las claves deben ser equiprobables.

- La secuencia de clave se usa una sola vez y luego se destruye.

La técnica que se emplea en el cifrado en flujo es:

- El mensaje en claro se leerá bit a bit.
- Se realizará una operación de cifra, normalmente la función XOR, con una secuencia de cifrado por bits.

Algunas de las ventajas del cifrado en flujo son: alta velocidad de cifra al no tener en cuenta otros elementos, resistente a errores, la cifra es independiente en cada elemento.

Las desventajas que presenta son: baja difusión de elementos en el criptograma, es vulnerable, pueden alterarse los elementos por separado.

Criptografía de Clave Pública

En los cifrados de clave pública no se puede calcular a partir de la de cifrado. Este tipo de cifrado comienza a ser muy conocido a través de su aplicación en los sistemas de correo electrónico seguro permitiendo cifrar e incluir una firma digital adjunta al documento enviado.

Cualquier usuario puede cifrar usando la clave pública, pero sólo aquellos que conozcan la clave secreta pueden descifrar correctamente.

Todo algoritmo de clave pública debe cumplir las siguientes propiedades de complejidad computacional:

- Cualquier usuario puede calcular sus propias claves públicas y privadas basándose en un algoritmo.
- El emisor puede cifrar su mensaje con la clave pública del receptor.
- El receptor puede descifrar el criptograma con la clave privada teniendo el mismo algoritmo.
- El criptoanalista que intente averiguar la clave privada mediante la pública se encontrará con un problema intratable.
- El criptoanalista que intente descifrar un criptograma teniendo la clave pública se encontrará con un problema.

Es más difícil diseñar un sistema de clave pública seguro, contra un ataque con texto original escogido, que un sistema de clave privada seguro frente al mismo tipo de ataque.

En la construcción de criptosistemas se pueden observar diferencias entre los algoritmos para sistemas privados y los usados en clave pública. En primer lugar, existen mayores restricciones de diseño para un algoritmo público que para uno privado, debido a que la clave pública representa información adicional que potencialmente un atacante puede usar para llevar a cabo el criptoanálisis. Normalmente, el algoritmo de clave pública basa su seguridad en la dificultad de resolver algún problema matemático conocido,

mientras que algunos algoritmos privados, como el DES, se diseñan de tal manera que las ecuaciones matemáticas que los describen son tan complejas que no son resolubles analíticamente.

En segundo lugar, existen grandes diferencias en la generación de claves. En los algoritmos de clave privada, la clave de cifrado es equivalente a la de descifrado, y viceversa, la clave se puede seleccionar de forma aleatoria. Sin embargo, en los algoritmos de clave pública, como la relación entre clave de cifrado y de descifrado no es pública, se necesita un procedimiento para calcularla.

Sistemas de clave pública más trascendentes

Algunos de los sistemas de clave pública que han tenido más trascendencia son: sistema RSA (Rivest, Shamir, Adelman, algoritmo de encriptación de clave publica desarrollado por Rivest, Shamir y Adelman), Rabin, ElGamal, Merkle-Hellman, McEliece, basados en curvas elípticas y probabilística, entre otros.

Entre las muchas aplicaciones de los sistemas de criptografía se encuentran la autenticación, la firma digital, la identificación de usuario, seguridad en redes y protocolos criptográficos.

APÉNDICE D

CUESTIONARIOS

Hardware

Características	SI	NO	N/A
Topología y protocolos de red			
Protocolos			
Conexión al exterior con Centros de servicio			
Características del servidor:			
Tipo o marca del servidor			
Capacidad de procesamiento			
Cantidad de memoria			
Capacidad de disco duro			
Puertos de red			
Dispositivos varios (CDs, cintas, escáner, switch, hub, etc.)			
UPS o sistemas de alimentación alternativa del servidor			
Servidor alternativo, espejo o de contingencia			
Servidor de datos o de impresión			
PCs:			
Cantidad			
Características particulares			
Clones			
Características generales			
Internet:			
Tipo de conexión			
Permisos o acceso de las PCs			
Página dinámica o estática			
Servidor propio o Web hosting			
Respaldo			
Disco espejo			
Terciarios:			
Dispositivos de respaldos			

Software

Características	SI	NO	N/A
Software del servidor			
Sistema Operativo			
Aplicaciones			
Motor de bases de datos			
Sistema Operativo y software de las PCs			
Aplicaciones en cada sector del corporativo			
Gestión de virus			
Detalle de aplicaciones propias			
Gestión de red física y lógica			
Licencias			

Usuarios

Características	SI	NO	N/A
Organigrama			
Responsabilidades en el área de informática			
Responsables de redes			
Responsables de bases de datos			
Responsables de aplicaciones			
Responsables de servicio técnico			
Tipo de perfiles de usuarios según sectores			
Clasificación del perfil			
Accesos del perfil a aplicaciones o datos			

Seguridad lógica

Características	SI	NO	N/A
Altas de identificación (ID):			
¿Qué datos hay en el perfil del usuario cuando se hace una alta?			
¿Se guardan los siguientes datos? :			
ID de usuario			
Nombre y apellido completo			
Puesto de trabajo y departamento de la empresa			
Jefe inmediato			
Descripción de tareas			
Consentimiento a que auditen sus actividades en el sistema y de que conoce las normas de "buen uso" del sistema			
Explicaciones breves y claras de cómo elegir su contraseña			
Tipo de cuenta o grupo al que pertenece			
Fecha de expiración de la cuenta			
Datos de los permisos de acceso y excepciones			
Restricciones horarias para el uso de recursos			
¿Que otros datos del usuario son necesarios en el ID?			
¿Que datos se guardan en la planilla del personal?			
¿El ID de usuario puede repetirse?			
¿Y si una cuenta fue borrada o eliminada, puede utilizarse un ID ya usado y eliminado para un usuario nuevo?			
Bajas de identificación (ID):			
¿Cómo se relacionan con los de Recursos Humanos (RH)?			
¿El departamento de RH se encarga de comunicar las modificaciones en el personal?			
¿Qué se hace al respecto?			
¿Cómo se actualiza la lista?			
¿Cómo se administran los despidos (o desvinculación del personal)?			
¿Se tiene en cuenta una política de despidos para evitar actos de vandalismo por posibles disgustos de los empleados desvinculados de la empresa?			

¿Hay algún historial de las cuentas que se dan de baja?			
¿Se guardan los archivos y datos de las cuentas eliminadas?			
¿Por cuánto tiempo?			
¿Qué datos se guardan?			
¿Con qué motivo?			

Mantenimiento

Características	SI	NO	N/A
¿Hay procedimientos para asignar los usuarios a un grupo de acuerdo a ciertas características?			
¿Hay procedimientos para dar de alta, baja, modificar, suspender, etc. una cuenta de usuario?			
¿Se hacen revisiones de las cuentas de usuarios?			
¿Se revisan sus permisos?			
¿Hay procedimientos para determinar los nuevos requerimientos relacionados con cambios en funciones del empleado?			
¿Cómo se mantienen actualizadas las cuentas cuando esto pasa?			
¿Se documentan las modificaciones que se hacen en las cuentas?			
¿Se lleva un historial de los cambios?			

Permisos

Características	SI	NO	N/A
¿Tienen una clasificación de los recursos (datos) en base en la sensibilidad?			
¿O en base en los tipos (base de datos, archivos de configuración, datos personales, según el departamento de la organización)?			
¿Cómo se define la sensibilidad de los objetos?			
¿Tienen distinción de los tipos de accesos que tiene cada usuario a cada recurso?			
¿Quién les asigna los permisos a los usuarios?			

ID Inactivas

Características	SI	NO	N/A
¿Después de qué período de inactividad en que el usuario no realiza acciones en el sistema, se limpia la pantalla asociada al usuario, se desconecta el usuario inactivo o pide la contraseña de nuevo?			
Antes de terminar con la sesión, ¿se avisa al usuario que será desconectado?			
Si en un determinado tiempo el usuario no responde, ¿entonces se termina la sesión?			
¿Después de qué período (días) de inactividad se pone una cuenta de usuario como inactiva, porque el usuario no se ha logeado?			
¿Este proceso es automático (del sistema operativo) o lo realiza el administrador?			

Acciones correlativas a usuarios

Características	SI	NO	N/A
¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan?			
¿Todos los usuarios tienen un perfil o pertenecen a algún grupo?			
¿El sistema genera historiales o logs de las actividades de los usuarios en el sistema, para poder seguirles el rastro?			
¿Tienen forma de asignar responsabilidades individualmente a cada usuario, identificándolo a través de su ID?			

Grupos – Roles

Características	SI	NO	N/A
¿Existen grupos de usuarios?			
¿Cómo se forman los grupos?			
¿Según el departamento del corporativo donde trabajen, o el rol que desempeñen?			
¿Por qué se hace esa clasificación?			
¿El acceso puede controlarse con el tipo de trabajo o la función (rol) del que pide acceso?			
¿Los IDs hacen referencia a una persona, o son anónimos?			
¿Hacen referencia a un grupo?			
¿Se eliminan los que vienen por default en el sistema operativo?			

Administrador

Características	SI	NO	N/A
¿Qué tipos de perfil del administrador hay?			
¿Cuántas personas y quiénes son administradores?			
¿Desde qué terminal puede logearse un administrador?			
Además de la cuenta del administrador, ¿tienen otra cuenta para las funciones comunes?			

Avisos

Características	SI	NO	N/A
¿Cuándo alguien intenta logearse, se muestran los siguientes datos?:			
Nombre de usuario			
Contraseña			
Grupo o entorno de red			
Estación de trabajo			
Fecha y hora			
¿Cuándo alguien logra logearse, se muestran los siguientes datos?:			
Fecha y hora de la última conexión			

Localización de la última conexión			
Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda			

Varios

Características	SI	NO	N/A
¿Utilizan el ID de usuario como un control de acceso a los recursos, o sólo para ingresar al sistema?			
¿Un usuario puede tener sólo una sesión abierta, de alguna aplicación, de acuerdo a sus tareas o puede tener varias?			
¿Depende de la cantidad de grupos a los que pertenece?			

Autentificación

Características	SI	NO	N/A
¿Cómo se protegen los datos de autentificación cuando están siendo ingresados por el usuario?			
¿Se muestra algún carácter en pantalla cuando se teclea la contraseña?			
¿Espacios, asteriscos, no se mueve el cursor?			
¿Cómo se guardan los datos de autentificación en disco?:			
¿Encriptados?			
¿Bajo contraseña?			
¿De qué forma se les asegura?			
¿Cómo se restringe el acceso a estos datos?			
¿Hay un control de acceso más severo con estos datos?			
¿Se les clasifica como confidencial?			
¿Quién tiene acceso a estos datos?			
¿Cómo se transfieren los datos de autentificación desde la PC que se logea hasta el servidor encargado de autentificar?:			
¿Encriptados, o sólo en texto plano?			

Alcance de la autentificación

Características	SI	NO	N/A
¿Qué alcance tienen las autentificaciones?			
¿Es una autentificación para una aplicación en particular, para toda la red, o sólo para la LAN, y otra para la WAN?			

Límites de los intentos de logeo

Características	SI	NO	N/A
¿Se bloquea al usuario después de varios intentos fallidos de autentificación, se inhabilita la cuenta o la PC?			
¿Después de cuántos intentos?			

¿Qué se hace después de la inhabilitación: se espera un tiempo y muestra nuevamente la pantalla de logeo o el administrador debe aprobar la operación de re-logeo?			

Firmas digitales

Características	SI	NO	N/A
¿Se usan firmas digitales para autentificar a los usuarios dentro del corporativo, cuando mandan mensajes internos?			
¿Y para mensajes externos?			
¿Serían necesarias para algún documento?			

Varias

Características	SI	NO	N/A
Separación de tareas: ¿se manejan los controles de acceso de manera que una persona no tenga acceso a todo, en relación con una sola transacción?			
¿Existe separación de tareas a través del control de acceso?			
Rotación de tareas: si existe rotación de tareas, ¿cómo es el mecanismo en el control de acceso para realizar esto?			
¿Se modifican los permisos?			
¿O tienen todos los permisos necesarios permanentemente?			
Vacaciones: ¿son obligatorias las vacaciones en la empresa?			
Si es así, ¿cómo se manejan las contraseñas durante los períodos de vacaciones?			
¿Qué ocurre con la cuenta del administrador en el período de vacaciones?			
¿Puede ser modificada?			
¿Cómo controlan para que no sea modificada durante su ausencia?			

Contraseñas

Características	SI	NO	N/A
¿Las contraseñas son generadas con procesos automáticos (programas de generación de contraseñas) o son creadas por los usuarios?			
¿Se usan estos programas en alguna máquina, por ejemplo en los servidores?			
¿Qué características deben tener estas contraseñas?			
¿Cuál es el conjunto de caracteres permitidos (alfa, numéricos y caracteres especiales)?			
¿Cuál es el largo mínimo y máximo de la contraseña (seis a ocho, preferentemente nueve)?			
¿La contraseña se inicializa como expirada para obligar al cambio?			
¿De qué forma se hace cumplir este requerimiento?			
¿Se pone una fecha de expiración?			
¿No se permite al usuario logearse ya que su contraseña ha expirado?			
¿Se comparan con un diccionario en línea para verificar que no sean palabras			

que existen?			
¿Se permite que contengan el nombre de la empresa, o el nombre del usuario?			
¿Dos cuentas pueden tener las mismas contraseñas?			
Si existe más de una cuenta de administrador, ¿algunas de estas (o todas) tienen la misma contraseña?			
¿La contraseña puede ser igual al ID del usuario?			

Cambios

Características	SI	NO	N/A
¿Qué procedimiento existe para el cambio de las contraseñas de los usuarios?			
¿Se puede cambiar en cualquier momento?			
¿Quién puede hacer los cambios?:			
¿El administrador?			
¿Los usuarios a través de una opción en el menú?			
¿Le tienen que avisar a alguien cuando cambian la contraseña?			
¿Tiene que pedir autorización?			
¿Qué procedimiento existe para comprobar que las contraseñas asignadas por default (por el administrador o por el sistema operativo) han sido cambiadas por el usuario?			
¿Cuál es el procedimiento para el manejo de contraseña perdidas o reveladas?			
¿Cómo se cambian?			
¿Sólo se cambia la contraseña o se cambia también la cuenta y el nombre del usuario?			
¿Con qué frecuencia es necesario cambiar la contraseña antes de que se vuelva obsoleta?			
Al modificar la contraseña de una cuenta, ¿se puede repetir la misma contraseña?			
¿Se guarda una base de datos con las últimas contraseñas de los usuarios?			
¿Cuántas contraseñas de cada usuario se guardan?			

Entrenamiento a usuarios

Características	SI	NO	N/A
¿Se entrena a los usuarios en la administración de contraseñas?			
Se les enseña a no usar contraseñas:			
¿Fáciles de descifrar?			
¿A no divulgarlas?			
¿A no guardarlas en lugares donde se puedan encontrar?			
¿A entender que la administración de contraseñas es el principal método de seguridad del sistema?			

Control de acceso lógico

Características	SI	NO	N/A
Modelos de control de acceso:			
¿Siguen algún tipo de modelo o mecanismo estándar de control de acceso?			
¿Sería factible y económico implementar uno?			
Aplicación: ¿para el control de acceso usan una aplicación?			
¿Cómo se administra?			
¿Qué características tiene?			
Esta aplicación es:			
¿Propia del sistema operativo?			
¿Es de aplicación y programas propios o comprados?			
¿Es con paquetes de seguridad agregados al sistema operativo?			

Criterios de acceso

Características	SI	NO	N/A
¿Qué criterio usan para el control de acceso?			
¿Alguno como ID de usuario?			
¿Roles?			
Localización:			
¿Existen controles de acuerdo a la localización de la información?			
Recursos:			
¿Se pide una contraseña cada vez que alguien quiera entrar a una carpeta compartida del servidor?			
¿La contraseña que los usuarios ingresan para la aplicación del corporativo sirve para explorar el sistema y así poder ver las carpetas de los servidores?			
¿Es necesario poner otra contraseña además del login?			
Tiempo:			
¿Se limita el tiempo en el que un usuario puede entrar al sistema?			
¿Cómo?			
¿Que días, horas?			
¿Con qué aplicación?			
Limitaciones a los servicios:			
¿Existen restricciones de servicio?			
¿Cómo?			
Si el acceso es desde el ruteador, ¿existen permisos diferentes a los que da la PC?			
Transacción:			
¿Se permite hacer ciertas transacciones sólo a algunos usuarios?			
¿De qué depende?			
¿Del tipo de usuario y del grupo?			
Aplicación:			
¿Se restringe el acceso a ciertos programas a ciertos usuarios?			
¿Cómo?			

Mecanismos de control de acceso interno

Características	SI	NO	N/A
¿Cuáles de estos mecanismos de control de acceso se usan?:			
Contraseñas			
Listas de control de acceso (LCA)			
¿Existe una LCA o matriz, o algo similar donde se especifiquen los usuarios y los accesos que tienen?			
¿Qué sería más conveniente, una lista o una matriz?			
¿Por qué?			
¿Con qué aplicaciones se manejan?			
¿Con alguna del sistema operativo, o con otro software?			
¿Cómo se actualiza?			
¿En forma manual o, si se modifica la lista de usuarios del sistema, se actualiza automáticamente la LCA?			
¿Con qué frecuencia se revisa y actualiza?			
¿Se usa encriptación para almacenarla?			
¿Se protege de alguna manera?			
¿Qué sería lo mejor y por qué para protegerla?			
Interfaces de usuarios restringidas:			
¿Se restringen las interfaces que ven los usuarios, (como el escritorio de Windows) de manera que los usuarios sólo vean lo que les está permitido?			
¿Cómo se hacen las restricciones?			
¿Con la vista de menús?			
¿Los usuarios sólo ven una determinada vista o ciertas tablas de las bases de datos?			
Encriptación:			
¿Se encriptan algunos datos?			
¿Cuáles?			
¿Las listas de control de acceso?			
¿Los mensajes?			
¿Las contraseñas y datos de las cuentas de usuarios?			
¿Los datos de configuración?			
¿Los datos críticos de la empresa?			
¿Los datos que están siendo transmitidos (internamente en la LAN o externamente a través de Internet o el enlace)?			
Protección de puertos:			
¿Usan dispositivos externos físicos para proteger el puerto de los intrusos?			

Control de acceso externo

Características	SI	NO	N/A
Mecanismos de control de acceso externo:			
Gateways (puertas de seguridad) o *firewalls* seguros			
Acceso de personal contratado, consultores o mantenimiento			

Autentificación basada en host:			
¿Existe una autentificación que da acceso al sistema basándose en la identidad del host que pide el acceso, y no en la identidad del usuario que quiere entrar?			
¿Existe acceso externo a los datos, desde Internet o desde el enlace?			
¿Quién tiene ese acceso?			
¿Qué procedimientos se tienen en cuenta para mantener la integridad y la confiabilidad de los datos?			
¿Se tienen en cuenta lo siguiente?:			
¿Alguna forma de identificación o autentificación?			
¿Control de acceso para limitar lo que se lee, ve, borra, modifica, etc.?			
¿Firmas digitales?			
¿Ponen las copias de seguridad de la información pública, en otro lado, no en la misma máquina?			
¿Prohíben el acceso público a bases de datos?			
¿Verifican que los programas y la información pública no tengan virus?			
¿Contraseñas one-time?			
¿Están separados los datos que se publican en Internet de los datos del interior del corporativo?			
¿Son los mismos datos o están en PCs diferentes?			
¿Usan alguna forma de acceso remoto para cambiar las configuraciones de un sistema?			

Sistema de detección de intrusos (IDS)

Características	SI	NO	N/A
¿Ha habido intentos de intrusión?			
¿Vale la pena implementar un sistema como éstos?			
¿Se usa algún software de IDS?			
¿Son tolerantes al fallo?			
¿Usan muchos recursos?			
¿Se usan herramientas de monitorización de red para encontrar intrusos?			
¿Se releen los logs de auditoría buscando pistas de IDS?			
¿Se buscan algunos de los siguientes aspectos?:			
Muchos intentos fallidos de autentificación			
Tráfico excesivo de red			
Muchas violaciones a permisos			
Si hubiera una entrada de un intruso, ¿se documenta?			
¿Qué medidas se tomarían (o tomaron) para que no ocurra más?			

Negación de servicios

Características	SI	NO	N/A
¿Se llevan a cabo algunas de las siguientes actividades?:			
¿Instalan LCA en los ruteadores?			

¿Quitan los servicios de red no necesarios o no utilizados, por ejemplo: echo, etc.?			
¿Separan los datos críticos de los que no lo son, a través de lo que haya disponible?			
¿Establecen valores base para la actividad normal, en cuanto a memoria, disco, utilización de CPU o tráfico de red?			
¿Usan herramientas para detectar cambios en la configuración o en los archivos?			
¿Usan configuraciones redundantes de red y tolerantes a fallos?			

Seguridad en comunicaciones

Características	SI	NO	N/A
Configuración de la red:			
¿Cómo es la topología de la red?			
¿Existe un inventario o gráfico topológico?			
¿Incluye algo de lo siguiente?:			
switch			
ruteadores			
hub's			
modem			
PCs			
fibra óptica			
etc.			

Configuración de la red

Características	SI	NO	N/A
¿Cuántos dispositivos de esta lista hay y en que forma están ubicados y utilizados?			
¿Qué filtros tiene cada uno de estos dispositivos?			
¿Existe encriptación a nivel de hardware?			
¿Por qué pusieron un switch en lugar de un ruteador?			
¿Por el costo?			
¿Por el tamaño de la red?			

Servidor de Hosting

Características	SI	NO	N/A
¿Qué se tuvo en cuenta para elegir ese servidor de hosting?:			
precio			
medidas de seguridad			
respaldo en caso de emergencia, de caída del servidor y de pérdida de información			

¿Qué características tienen los servidores? (de mail, de Internet, de datos o aplicaciones)			
¿Causa alguna dificultad que el servidor esté físicamente lejos de los Centros de servicio?			

Comunicaciones

Características	SI	NO	N/A
Con respecto al ruteador con el que se comunican con los Centros de servicio:			
¿Pasa por un sistema de seguridad?			
¿Los datos van encriptados?			
¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a Internet?			

Recursos compartidos

Características	SI	NO	N/A
¿Se comparten los discos de las PCs en la red?			
¿Por qué?			
¿Qué carpetas comparten?			
¿Se pueden ver las carpetas de los mails de mis compañeros?			
¿Tienen contraseñas estas carpetas?			
¿Quién pone las contraseñas, el dueño de la información o el administrador?			

Configuración de puertos

Características	SI	NO	N/A
¿Se deshabilitaron los puertos que no son necesarios?			
¿Cuáles?			
¿De qué protocolos o servicios?			
¿Quién lo hizo?			
¿Se prueban los puertos de la red?			
¿Con qué herramientas?			
¿Se ha hecho una prueba de auto hackeo?			
¿Con qué herramientas se prueban o pueden probar los puertos?			

Chequeo mensual de la red

Características	SI	NO	N/A
¿Se hace algún chequeo periódico de la red y sus permisos?			
¿Qué se controla?			
¿Se documentan la ejecución y los resultados de estas pruebas?			

Acceso remoto

Características	SI	NO	N/A
¿Cómo se mantienen las máquinas con Unix?			
¿Vía acceso remoto?			
¿Quién las mantiene?			
¿Qué herramientas se usan?			
¿Cómo funciona la herramienta?			
¿Qué servicios son necesarios para el mantenimiento? (HTML, FTP, IP, DNS, TELNET)			
¿Qué es lo que se mantiene con este sistema?			
¿Cómo se aseguran que no entren llamadas, sino que solo salgan las solicitudes?			

Medidas de fiabilidad

Características	SI	NO	N/A
¿Existen medios alternativos de transmisión de datos en caso de que exista alguna contingencia con la red?			
¿Qué se haría si se cae un nodo?			
¿Está prevista esa situación?			
¿Existe una redundancia de acceso a Internet?			

Mail

Características	SI	NO	N/A
Herramientas:			
¿Con qué herramienta administran el correo en el servidor y cómo se hace?			
¿Es una herramienta del sistema operativo?			
¿Es comprada?			
¿Por qué eligieron ésa?			
¿Es configurable?			
¿Quién es el encargado de su configuración?			
¿Se checa periódicamente que la configuración sea eficiente?			
¿Con qué frecuencia?			
¿Se encuentran errores?			
¿Se actualiza a las versiones más nuevas de esta herramienta?			
¿Cómo se enteran de las nuevas versiones?			
¿El servidor de mail es el mismo que el servidor de Internet o el de aplicaciones?			
¿Con qué herramienta los usuarios leen sus mail?			
¿Lo hacen desde sus PCs?			
¿Qué configuraciones tienen estas herramientas?:			
Habilitada la vista previa			
Confirmación de lectura			
Chequeo de virus en correo entrante y saliente			

Controles ActiveX y scripts			
¿Quién las configura, los usuarios o el administrador?			
¿Todas las PCs tienen la misma configuración?			
¿Cómo las configuran?			
¿Se le deshabilitan las mismas características mencionadas anteriormente?			

Proceso de recepción y envío de mails

Características	SI	NO	N/A
¿Cómo es el proceso de recepción de mail? :			
¿El servidor baja los mails de toda la empresa a sus discos, y luego los reparte a sus destinos?			
¿Los mails se borran del servidor cuando son descargados a la máquina del usuario?			
¿O no se borran nunca del servidor?			
¿Cómo es esta política?			
¿Los mensajes están comprimidos dentro del servidor?			
¿Automáticamente se envían los mail a cada cuenta de usuario cuando llegan al servidor o se guardan en disco del servidor y se envían en un determinado momento?			
Al recibir cualquier tipo de mail, ¿existen mecanismos de filtrado que nos permiten buscan ciertas frases o palabras dentro del encabezado o cuerpo del mensaje?			
¿Podemos determinar si hay algún mail con un determinado asunto, de manera de evitar los virus o los correos no deseados?			

Espacio en disco

Características	SI	NO	N/A
¿Cómo se administra la capacidad de disco asignada a los mails? :			
¿Se asigna un espacio de disco a la totalidad del correo?			
¿Se asigna un espacio de disco a cada usuario del mail?			
¿Se asigna un espacio de disco a cada cuenta de mail?			
¿Se asigna un espacio de disco a cada departamento?			
¿Existen distintas cantidades asignadas a los usuarios de acuerdo a su perfil o grupo, o todos los usuarios tienen la misma cantidad de espacio en disco?			
¿Qué pasa si se llega al límite de espacio en disco asignado?			
¿Ha pasado alguna vez?			
¿Se le avisa al usuario correspondiente que limite el uso de su cuenta de mail?			
¿Se puede suspender solo su servicio de mail sin afectar el resto de la empresa?			
¿Cuándo se suspende la recepción de mails?			
¿Cuándo se ha llenado el servidor o antes, para poder hacer algo para vaciarlo?			
¿Existe un límite para los mensajes de salida o de entrada?			

Mail interno y externo

Características	SI	NO	N/A
¿Existen direcciones de mail para todos los empleados?			
¿Sólo algunos empleados tienen?			
¿De qué depende este servicio?			
¿Ese mail es interno o también existe una casilla para mail externo para cada empleado?			
¿Cómo funciona el mail interno, va al hosting y después al servidor de correo o va directamente al servidor de correo?			
¿Existe algún tipo de control para asegurarse que los usuarios no usan el mail del corporativo para fines personales sino para su trabajo?			
¿Se controla que no se suscriban a listas de correo o cadenas de mails con esta dirección de mail?			
¿Controlan los spams en estas direcciones?			
¿Cómo lo hacen?			
Al enviar mails hacia todos los empleados, ¿la lista se oculta o se copia oculta?			
¿Permiten el conocimiento público de las direcciones externas de mails de los empleados?			
¿Están publicadas en Internet o solo las administran sus propietarios?			
¿Existen direcciones de mails destinadas a la comunicación con el cliente, como el libro de quejas, consultas, etc.? (Ej. ventas@ledaxis.com)			
¿En dónde se encuentran?			
¿Quién las administra, el departamento correspondiente o el administrador de web?			

Correo basura

Características	SI	NO	N/A
¿Cómo se identifica el correo basura?			
¿Cómo se administra el correo basura?			
¿Con qué herramienta lo hacen?			
¿Cómo se configura?			
¿Cómo se define qué es correo basura y qué no?			
¿Qué pasa si a una cuenta llega gran cantidad de correo basura?			
¿El correo basura se elimina directamente o es posible generar logs para su posterior análisis?			
¿Qué conclusión se ha sacado de esos análisis?			
¿El correo basura se baja hasta el servidor de mails y desde ahí se elimina?			

Chat

Características	SI	NO	N/A
¿Se permiten los servicios de chat?			
¿Cuáles se usan? :			

¿Chat?			
¿Otros?			
¿Se permite bajar archivos a través de estos programas?			
¿Se usan programas de file sharing?			

Copia de seguridad

Características	SI	NO	N/A
¿Se genera una copia de seguridad de los mensajes enviados y recibidos?			
¿De todos?			
¿Se guardan en el disco?			
¿Se comprimen?			
¿Se hacen respaldo de las carpetas del SendMail?			
¿Se imprimen para su control o para que conste en algún archivo en papel?			
¿Poseen un sistema propio de mail record definido o alguna herramienta automática de gestión de mails record?			

Privacidad

Características	SI	NO	N/A
¿Prohíben el envío de archivos del corporativo u otros documentos confidenciales vía mail?			
¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales?			
¿Se exige que vaya firmado o encriptado?			
¿Se exige que la dirección de destino sea conocida o confiable?			
¿Se utiliza la firma digital en algún tipo de mensajes?			
¿Qué tipo de firma se usa?			
¿Se usa para mensajes externos e internos?			
¿Utilizan la priorización de mail para la encriptación de los mismos?			
¿Qué sería importante proteger, en el caso de mensajes internos y externos? :			
¿Integridad?			
¿Confidencialidad?			
¿No repudio?			
¿Autentificación del remitente?			
¿Se pide generalmente una confirmación de lectura en los mails salientes?			
¿En todos, sólo en los que tienen datos confidenciales, o cuando el usuario los configura?			
¿Se encriptan los datos confidenciales que se guardan en disco?			
¿Archivos con contraseñas?			
¿Archivos de configuración?			
¿Archivos top secret?			
¿Qué otros datos se encriptan?			

Virus y antivirus

Características	SI	NO	N/A
¿Cuáles de estas medidas o herramientas poseen para evitar los virus? :			
Paquetes de software antivirus			
Firewalls			
Sistemas de detección de intrusos			
Monitoreo para evaluar el tráfico de red y detectar anomalías			
Creación de un disco de rescate o de emergencia			
Procedimientos para cuando ocurra una infección con virus			
Hardware de seguridad de red dedicado			
Respaldo de datos			
¿Está habilitada alguna herramienta antivirus mientras se envían y reciben mails?			
¿Cuál?			
¿Por qué se usa esa?			
¿Están seguros que detecta los virus y los elimina correctamente?			
¿Han probado con otra herramienta?			
¿Qué precio tiene el antivirus que compran?			
¿Y las actualizaciones?			
¿Hay un antivirus instalado en cada PC (incluyendo los servidores) o hay un solo antivirus en toda la red?			
¿Qué significa que el antivirus sea corporativo?			
¿Uno para los servidores y otra versión para los clientes?			
¿En qué se diferencian?			

Mensajes infectados

Características	SI	NO	N/A
¿Se han detectado mensajes infectados?			
¿Qué problemas trajo?			
¿Era de Windows o de Unix?			
¿Cómo lo solucionaron?			
Si se encuentra un mail con virus, ¿qué se hace para que no lleguen más de esa misma persona?			
¿Se identifica la fuente del mail, para bloquearla desde el ruteador o desde el servidor correo?			
¿Se avisa al ISP para que no deje entrar más mails de esa dirección?			
¿Se observan los headers de los mails para identificar su origen verdadero?			
Si las unidades floppy están activadas en las PCs de los usuarios, ¿cómo se aseguran que los usuarios analicen los disquetes antes de abrir archivos?			
¿Se generan disco de rescate con el antivirus?			
¿Para todas las máquinas o solo para los servidores?			
¿Quién es el encargado de esto?			
¿Alguna vez han sido necesarios?			

¿Cómo es la protección contra el mail-bombing?			
¿Qué medidas se toman?			
¿Suspenden la recepción de mail cuando el servidor está ocupado en un determinado porcentaje de su capacidad?			
¿Qué procedimiento siguen en el caso de una infección con un virus?			
¿Cada cuanto se hace un escaneo total de virus en los servidores?			
¿Quién se encarga?			
¿Se hace automáticamente cada vez que hay una actualización o periódicamente?			
¿El escaneo de las máquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas?			
¿No sería más seguro que el encargado lo haga a intervalos regulares de tiempo?			
¿Qué prioridad tiene el SendMail?			
¿Cómo se realiza el download de los mails desde el servidor hasta las PCs?			
¿Cada PC se identifica según el usuario que se logea?			
¿O es según el número de terminal de la PC en la red?			
¿Se puede configurar una cuenta en otra máquina y bajar los mails desde ahí?			

Actualización de antivirus

Características	SI	NO	N/A
¿Cómo se actualizan las definiciones de virus?			
¿Quién las baja de Internet?			
¿Quién ejecuta las actualizaciones en la PCs?			
¿Cómo se enteran de las nuevas actualizaciones de virus?			
¿Cuánto tiempo lleva diseminar y actualizar el antivirus en toda la organización?			
¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?			

Documentación y normas

Características	SI	NO	N/A
¿Qué documentación existe de la red? :			
¿Diagramas topológicos?			
¿Procedimientos?			
¿Manuales?			
¿Certificados?			
¿Licencias de software?			
¿Planes de contingencia, de seguridad, etc.?			
¿Contratos? (Ej.: responsabilidades y mecanismos de transmisión al establecer una comunicación con los Centros de servicios)			
¿Cambios realizados en la configuración de la red?			
¿Qué mas?			
¿Poseen cada uno de estos elementos de documentación el corporativo? :			

Manual de uso del software y de hardware usado (del software desarrollado y del comprado)			
Diagramas de red y documentación de la configuración de ruteadores, switches y dispositivos de red.			
Procedimientos de emergencia (plan de contingencia)			
Plan de seguridad			
Manual de procesos estándares del Sistema Operativo (en especial de Unix)			
Métodos para compartir datos entre sistemas (por ejemplo con los Centros de servicio)			
¿Se han instalado correctamente todos los parches de seguridad disponibles del sistema operativo y de los programas usados?			
¿Cómo se enteran de los parches?			
¿Están suscritos a un mailing list?			
¿Hay alguna documentación donde se anote la configuración de las PCs en la red?			
¿Sus números IP, sus nodos de red, etc.?			

Ataques de red

Características	SI	NO	N/A
¿Han tenido algún ataque en la red?			
¿Qué se ha hecho para arreglarlo?			
¿Están implementados los siguientes métodos contra ataques más comunes? :			
Denial of service:			
¿Hay herramientas Anti DoS?			
¿Limitan el tráfico de red?			
¿Generan líneas de base con la actividad normal del sistema?			
¿Se hizo alguna simulación ocupando una gran cantidad de recursos de algún tipo?			
¿Instalan los parches de seguridad del sistema operativo?			
¿Implementan un sistema de cuotas?			
¿Utilizan alguna herramienta para detectar cambios en la información de configuración u otros archivos?			
Sniffing:			
¿Las líneas de comunicación se segmentan tanto como sea práctico?			
¿Los datos de logeo y otros datos sensibles son transmitidos encriptados?			
¿Las cuentas privilegiadas (como root) se logean usando contraseñas one time o shadow, contraseñas, y autentificación fuerte?			
Spoofing:			
¿Tienen alguna herramienta anti-spoofing?			
¿Los ruteadores son configurados para que rechacen los ataques de spoofing?			
¿Solo los hosts apropiados son definidos como confiables en el Unix?			
¿Y este archivo tiene los permisos restringidos?			

Por más que el acceso externo esté prohibido, ¿se configura el control de acceso para denegar cualquier tráfico de la red externa que tiene una dirección fuente que debería estar en el interior de la red interna?			
Ataque a las contraseñas:			
¿Dónde se guardan las contraseñas del sistema operativo?			
¿En el archivo /etc/passwd y /etc/group?			
¿Se checan regularmente las contraseñas para comprobar su consistencia los archivos que nombramos arriba?			

Firewall

Características	SI	NO	N/A
¿Qué firewall usan?			
¿En que máquina (servidor) se encuentra el Firewall?			
¿En una máquina dedicada?			
¿En el servidor de Internet?			

Tipos de firewall

Características	SI	NO	N/A
¿Qué tipo de firewall hay?			
¿Gateway de filtrado de paquetes?			
¿Gateway de aplicación?			
¿Gateways híbridos o complejos?			
¿Otro?			

Configuración de servicios y protocolos de red

Características	SI	NO	N/A
De todos estos servicios:			
¿Cuáles se usan en la red?			
¿Cómo están configurados?			
¿Están habilitados o prohibidos?			
¿Existen excepciones?			
¿Poseen acceso de entrada y/o salida?			
¿Que pasa con los otros puertos que quedan libres?			
¿Se desactivan completamente los siguientes servicios o protocolos?			
SUID (set user ID), RLOGIN, RSH, REXEC, SU (SuperUser), NetStar, GOPHER, TFTP, Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY.			
¿Cómo se configuran los siguientes servicios o protocolos?			
POP, MIME, HTTP, SMTP, FTP, Applets, Pruebas Cgi, Scripts Query, SHELL, NIS			

Herramientas para administración de red y protocolos

Características	SI	NO	N/A
De las siguientes herramientas o protocolos para la seguridad de la red, cuáles usan:			
Tcp-wrappers, Netlogv, Satan, AntiSniff, Cops, SafeSuite, Gabriel, Courtney, Tcplist, SSL, SHTTP, SMIME, NOCOL (Network Operations Center On-Line)			
¿Las herramientas que se usan tienen las siguientes funciones? :			
¿Pueden monitorear y filtrar peticiones entrantes a distintos servicios?			
¿Cómo lo hacen?			
¿Con qué aplicación?			
¿Indican la hora, la máquina origen (el número de IP) y el puerto de esa conexión?			
¿Pueden seguir una traza de todos los intentos de conexión tanto admitidos como rechazados?			
¿Se monitorea la red buscando ciertos protocolos con actividad inusual?			
Se controlan los siguientes:			
Conexiones TFTP			
Accesos vía RSH			
Comandos en el puerto de sendmail como vrfy, expn, etc.			
Algunos comandos de RPC como el rpcinfo			
Peticiones al servidor de NIS			
Peticiones al demonio de mountd			
¿Se llevan estadísticas de uso de los protocolos?			
¿Se puede utilizar para detectar cambios en los patrones de uso de la red, y todo aquello que nos pueda hacer sospechar que algo inusual esta pasando?			
¿Se audita el tráfico IP?			
En la captura de paquetes IP, ¿se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.?			
¿Tienen la posibilidad de filtrar paquetes por hardware o por software?			
¿Van creando una base de datos de todas las máquinas verificadas y las va relacionando entre ellas?			
¿Qué otra funcionalidad no nombramos que si tiene la herramienta usada?			
¿Que función sería muy útil al trabajar en la red?			
¿Se mantiene actualizado el software?			
¿Se investiga para mantener actualizadas las herramientas?			
¿Alguien está a cargo de ésta actividad?			
¿Se buscan herramientas nuevas que faciliten la tarea?			
¿Consultan a algún Organismo (como el CERT)?			

Elección del sistema a usar

Características	SI	NO	N/A
¿Se hicieron los siguientes cuestionarios al elegir los sistemas operativos y programas usados en el corporativo?			
¿Qué respuestas tenían?			

Para todo tipo de sistemas se debe tener en cuenta los siguientes requisitos:			
Requerimientos funcionales: ¿qué funciones debe cumplir el sistema?			
Entorno necesario: ¿Windows o Unix?			
Requerimientos de compatibilidad: ¿se ajusta a estándares internacionales, regulaciones o a programas existentes en el corporativo?			
Requerimientos de performance: respuestas por segundo, errores, etc.			
Requerimientos de interoperatividad: ¿cómo se relaciona con los demás sistemas?			
Fiabilidad: errores tolerables del sistema			
Amigable: fácil de usar			
Precio y precio adicional de mantenimiento			
Documentación y manuales propios del software			
Además hay que tener en cuenta los siguientes requisitos de seguridad:			
Identificación y autentificación			
Control de acceso			
Login			
Evaluación de protocolos			
Incorruptibilidad			
Fiabilidad			
Seguridad en la transmisión			
Respaldo de datos			
Encriptación			
Funciones para preservar la integridad de datos			
Requerimientos sobre la privacidad de datos			

Control de datos de aplicaciones

Características	SI	NO	N/A
¿Existe un control de cambios para los archivos del sistema o para las bases de datos del corporativo, que se modifique cada vez que alguien haga una modificación sobre un archivo?			
¿Existen restricciones de datos de salida, por ejemplo al portapapeles o a la impresora y otros?			
¿Cómo es el acceso a las librerías de programa (o a la carpeta "Archivos de programa")?			
¿Cómo se asegura la confidencialidad de los datos en una laptop?			
¿Qué datos hay en las laptops del corporativo, o de los usuarios?			
¿Se generan logs en cada transacción de manera de poder hacer un "undo"?			
¿Estos registran los cambios en los datos críticos del sistema?			
¿Se generan historiales de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios–gestión de configuración)?			
¿Los archivos de programa y los de trabajo se almacenan en directorios separados?			

Control de datos en el desarrollo

Características	SI	NO	N/A
¿Se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones?			
¿Las variables, parámetros y/o fórmulas de cálculo se incluyen en tablas o archivos separados de los programas, para facilitar su modificación?			
¿Existe un proceso de control de cambios para el desarrollo?			
¿Cómo se documentan estos cambios?			
¿Controlan el contenido de los archivos de entrada?			
¿Controlan que existan los archivos antes de ejecutar el programa?			
¿Se hacen controles sobre la validez de los datos ingresados manualmente?			
¿Se controla la consistencia de los datos de salida de las aplicaciones?			
¿Las aplicaciones se operan a través de menús obligatorios o es a través de comandos del sistema?			
¿Los operadores de estas aplicaciones pueden editar los datos reales del mismo?			

Seguridad de bases de datos

Características	SI	NO	N/A
¿Los archivos de la base de datos tienen control de acceso?			
¿O sólo se hacen controles en las aplicaciones?			
¿Se controlan las siguientes ocurrencias? :			
Tiempo y duración de los usuarios en el sistema			
Número de conexiones a bases de datos			
Número de intentos fallidos de conexiones a las bases de datos			
Ocurrencias de deadlock con la base de datos			
Estadísticas de entrada-salida para cada usuario			
Generación de nuevos objetos de bases de datos			
Modificación de datos			
¿Se hace alguna verificación regular de la seguridad de la base de datos?			
¿Se documentan las verificaciones incluyendo lo siguiente?			
¿Se hacen y son efectivos los respaldos y los mecanismos de seguridad?			
¿Hay algún usuario de la base de datos que no tenga asignado una contraseña?			
¿Hay algún usuario que no ha usado la base de datos por un período largo de tiempo?			
Además del administrador de datos, ¿quién tiene acceso a los archivos del software de la base de datos, a los del sistema operativo y a las tablas del sistema (FAT)?			
¿Quién puede ejecutar un editor SQL?			
¿Quién tiene acceso de lectura – escritura a los archivos de programa?			
¿Qué usuarios tienen los mismos permisos que el administrador?			
¿La base de datos tiene suficientes recursos libres para trabajar?			
¿Se borran físicamente los registros de las bases de datos cuando un usuario los elimina, o se marcan como "borrados"?			

Control de aplicaciones

Características	SI	NO	N/A
¿Todas las máquinas del corporativo tienen los mismos programas con las mismas versiones?			
¿Existe un estándar de configuración de PCs a seguir?			
¿Usan alguna herramienta como el Norton Ghost para copiar la configuración de las PCs?			
¿Existe un procedimiento para instalar las aplicaciones en las máquinas de los usuarios?			
¿Quién los instala y administra?			
¿Existen controles para realizar la instalación o la actualización de parches de las aplicaciones?			
¿Cómo se documenta la instalación o actualización del software que se instala en las máquinas?			
¿Existe algún procedimiento para encontrar programas que no deberían estar en las máquinas de los usuarios, ya sea por problemas de licencias o virus?			
¿Existe un método a seguir?			
¿Se usa algún producto para detectar estos programas?			
¿Se hacen auditorias periódicas para verificarlo?			
¿Cómo se controla a los usuarios y las aplicaciones que bajan de la Web?			
¿Cómo controlan que éstas tengan las licencias correspondientes?			
¿Se borran las versiones de prueba o demos cuando expiran?			
¿Se permiten los registros en línea de las aplicaciones?			
¿Existen métodos para autorizar y registrar software?			
¿Cómo manejan las actualizaciones del software?			
¿Existe alguna forma de configurar las PCs de manera que no se pueda instalar software nuevo sin autorización del administrador?			
¿Puede pasar que un usuario no este autorizado para modificar las carpetas c:\Windows o c:\Archivos de programa, pero otro (el administrador de sistemas) sí?			
¿Cómo se configura esto en el sistema de control de acceso del corporativo?			
¿Se usa?			

Mantenimiento de aplicaciones

Características	SI	NO	N/A
¿Cómo se etiquetan los instaladores de los programas o los drivers?			
¿Cómo se almacenan: en disco duro, en disquete, en CD, en cinta?			
¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte?			
¿Se controla el funcionamiento correcto de las aplicaciones?			
¿Se hacen verificaciones periódicas sobre el funcionamiento, la configuración, etc.?			
¿Se generan alertas?			
¿Cómo se administran las emergencias?			

¿Si se hacen cambios de emergencia, cómo se documenta?			
¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basuras y provoquen la caída del sistema?			
¿Se revisan periódicamente los sistemas para eliminar los programas o servicios innecesarios (como algunos servicios Web, FTP, HTTP)?			
¿Se buscan vulnerabilidades nuevas durante estas revisiones?			
¿Es automático el método de actualización de los Antivirus para que los mensajes en el interior y el exterior del corporativo no propaguen virus?			
¿Se programan los escaneos automáticos de virus una vez por semana?			
¿Por qué no la actualiza la aplicación automáticamente con un schedule?			
¿Existe alguna aplicación de gestión para tomar decisiones de alto nivel gerencial?			
¿Ésta obtiene datos automáticamente de las bases de datos?			
¿Existe un undelete como la papelera de reciclaje de Norton?			
¿En el servidor o en las PCs?			
¿Está habilitado el undelete de DOS?			
¿Se hace un respaldo de la configuración de los sistemas antes de hacer algún cambio de manera de poder hacer un undo?			
¿Los cambios complejos en los archivos de configuración se hacen primero (a modo de prueba) en una copia de los archivos o se hacen directamente en la configuración original?			
¿Se registran o documentan los cambios hechos a una configuración?			

Ciclo de vida

Características	SI	NO	N/A
¿Qué aplicaciones se desarrollaron en el corporativo?			
¿Una para cada área del corporativo?			
¿Qué metodología estándar usan para el desarrollo de sistemas?			
¿De qué fases consta?			
¿Qué mecanismos de seguridad manejan durante estas fases?			

Iniciación

Características	SI	NO	N/A
¿Cómo se expresan las necesidades del sistema?			

Desarrollo

Características	SI	NO	N/A
¿Se hace un análisis de riesgos antes de empezar con el desarrollo?			
¿En caso de que haya participación de terceros en el desarrollo (como en la Web, o en UNIX) el código fuente queda en el corporativo?			
¿Dejan documentación?			
¿Tienen alguna reglamentación para trabajar con terceros?			

¿Usan métricas durante el desarrollo?			
¿Les sirven?			
¿Qué miden?			
¿En qué las utilizan?			
¿Se mantienen registros de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento?			
¿Qué se guarda? :			
Sistema que afecta			
Fecha de la modificación			
Persona que realizó el cambio			
Descripción global de la modificación			
¿Qué mas?			
¿En qué momento se definen los requisitos de seguridad de un sistema?			
¿Es durante el desarrollo?			

Implementación

Características	SI	NO	N/A
¿En qué lenguajes se implementan los sistemas?			
¿Reutilizan software?			
¿Qué medidas de seguridad toman durante la implementación?			

Prueba

Características	SI	NO	N/A
¿Cómo se hace la prueba de los sistemas?			
¿Se generan planes de prueba?			
Tipos de prueba que se llevan a cabo:			
¿De unidad?			
¿De integración?			
¿Por módulos?			
¿Por sistema?			
¿Se generan escenarios de prueba para el chequeo?			
¿Se documentan las pruebas y sus resultados?			
¿Qué datos se guardan?			
¿Cómo se realiza el control de cambios del sistema?			

Instalación y mantenimiento

Características	SI	NO	N/A
¿Qué metodología usan para el mantenimiento?			

Documentación

Características	SI	NO	N/A
¿Qué documentación se generan de los desarrollos que se hacen?			
¿Se incluyen las siguientes cosas?			
Generalidades del sistema, incluyendo fecha de implementación y analísta / programador responsable			
Documentación del sistema, incluyendo sus objetivos, diagrama general, de funciones y diseños de registros			
Documentación de los programas, incluyendo objetivos, diagrama de flujo, archivos de entrada y salida que utiliza.			
Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores			
Manual de usuario			
Manual de características de seguridad			
Descripción del hardware y software, políticas, estándares, procedimientos, respaldo, plan de contingencia, descripción del usuario y del operador del sistema			

Compra

Características	SI	NO	N/A
¿Qué medidas se toman antes de comprar un sistema?			
¿Cómo es el análisis que se hace?			
¿Existe documentación de los sistemas comprados, así como los vendedores y del soporte postventa?			

Seguridad física

Características	SI	NO	N/A
Control de acceso al NOC			
¿Se hizo un análisis costo beneficio a la hora de implementar los controles?			
¿Cómo se asesoraron?			
¿Se restringe el acceso al NOC a la gente que no pertenece a esa área?			
¿Existen algunos de los siguientes métodos?			
¿Dónde?			
Tarjetas de entradas			
Guardias de Seguridad			
Llaves cifradas			
Circuito cerrado de televisión			
¿Cuál es la función de la doble puerta en la entrada?			
¿Qué tipos de autentificación se utilizan en el corporativo? Hay cuatro formas:			
Con algo que el individuo sabe (contraseña, PIN, etc.)			

Algo que el individuo procesa (un token, una smart card, etc.)			
Algo que el individuo es (controles biométricos)			
Algo que sabe hacer (como los patrones de escritura)			
¿Por qué no usan las otras?			
¿Por el costo? ¿No vale la pena?			
¿Sólo dejan entrar a aquellos que lo necesiten?			
¿Les hacen algún control de seguridad?			

Control de acceso a equipos

Características	SI	NO	N/A
¿Cómo se controlan los siguientes accesos?			
¿La BIOS tiene habilitada una contraseña?			
¿Las PCs tienen habilitados los dispositivos externos, como la unidad floppy o la lectora de CD?			
¿Cómo se controlan estos dispositivos?			
¿Cómo se controlan los virus en las unidades floppy o CDs?			
¿Qué otros peligros pueden tener?			
¿Son dispositivos booteables (se permite desde el setup de la máquina el booteo con estos dispositivos)?			
¿Ha habido robo de datos usando estos dispositivos?			
¿Existen copiadoras de CDs en la empresa?			
¿Quién tiene acceso a ellas?			
¿En qué máquinas están?			
¿Usan llave de bloqueo en las CPUs?			
¿Las CPUs y dispositivos externos extraíbles están guardados con llave?			
¿Existe algún control sobre los terceros que realizan el mantenimiento?			
¿Existen entradas no autorizadas en las PCs, como puertos no usados y no deshabilitados?			
¿Puede alguien enchufar e instalar una impresora u otro dispositivo (un zip o un disco removible) en alguna máquina?			
¿Cómo se realiza el control sobre los dispositivos que se instalan en las PCs?			
¿Se hace una revisión periódica de los mismos?			
¿Quién las hace?			
¿Cada cuándo?			
¿Qué buscan?			
¿Se apagan los servidores en algún momento?			
¿Es necesario que queden prendidos las 24 hrs?			

Utilidades de soporte

Características	SI	NO	N/A
¿Existen, se mantienen y revisan todos estos aparatos periódicamente en busca de fallas?			
Aire acondicionado (18° C a 20° C)			

Calefacción			
Humidificador en la biblioteca de cintas y NOCs			
Luz de emergencia en el NOC			
Detectores de humo, agua y calor			
Instalación de alarmas:			
Contra fuego			
Humo			
Calor			
Intrusos			
Agua			
¿Qué otras hay?			
Servidor de repuesto o redundante			
UPS ¿para mantener los servidores de red funcionando por cuántas horas?			
¿Cuántos UPS?			
¿En qué máquinas?			
Estabilizador de tensión: ¿cuántos? ¿En qué máquinas?			
Extinguidotes de incendio:			
¿Son los adecuados?			
¿Son manuales o automáticos (rociadores)?			
¿Se corta la energía eléctrica cuando se activan estos rociadores?			
¿Están en el lugar correcto?			
¿En qué lugares? ¿Cómo eligieron el lugar?			
¿Se revisan las posibles fallas eléctricas o posibles causas de incendio?			
¿Qué pasa con las máquinas cuando cae la lluvia artificial?			
¿Existen cubiertas plásticas para protección de agua?			
¿Qué pasa con los extinguidores de incendio en el NOC?			
¿Hay una sola red eléctrica?			
¿Hay un dispositivo que evite la sobrecarga de la red eléctrica?			
¿Hay hardware especial de aislamiento y protección de dispositivos magnéticos?			

Estructura del edificio

Características	SI	NO	N/A
¿Se tuvo en cuenta la seguridad de los datos y equipos en el momento de hacer la estructura de los edificios?			
NOC:			
¿Está ubicado en pisos elevados (para prevenir inundaciones)?			
¿Existe un piso o techo falso para pasar el cableado por debajo de él?			
¿El área debajo del piso o del techo falso es fácilmente accesible?			
¿Es lo suficientemente grande, anticipándose al crecimiento de la red y predispuesto a reinstalaciones?			
¿La localización del NOC, tiene paredes externas o ventanas?			
¿Está cerca del backbone?			

¿Esta permitido comer, fumar y beber dentro del NOC?			
¿En el resto de los escritorios se puede?			
Cableado:			
¿Usan cableado estructurado?			
¿Quién lo instaló?			
¿La instalación fue por parte de terceros?			
¿Usaron alguna norma para hacer el cableado?			
¿Se tuvo en cuenta el lugar de los canales de red, de manera que no sean afectados por desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos?			
¿Qué tipo de cable usan para que no haya interferencias?			
¿Qué medidas toman para las interferencias?			
¿Cómo previenen los daños o cortes en los cables?			
¿Cómo calcularon el ancho de banda de la red? ¿Es suficiente?			
Nodos de red:			
¿Son suficientes? ¿Hay de más?			
¿Cómo protegen a los que sobran?			
¿Están habilitados o no?			
¿Cómo los deshabilitan?			
¿Se conoce por dónde van las tuberías de manera que no interfieran con la red?			
¿El lugar se sitúa encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas?			
¿Esto causa molestias o interferencias?			
¿Existe un interruptor de energía de emergencia en la puerta de salida?			
¿Los muebles son de madera?			
¿Son inflamables?			

Interceptación física, visual y electromagnética

Características	SI	NO	N/A
¿Puede haber emisiones electromagnéticas desde los monitores o desde los cables UTP, que se pueden interceptar o provocar ruidos?			
Emisiones visuales: ¿se evita que los monitores puedan verse a través de las ventanas?			
Emisiones de sonido (ruido): ¿se toma alguna medida para que no afecten el funcionamiento normal?			
¿Hay ruidos que puedan causar problemas?			
¿La ubicación de las antenas de radio interfiere con los datos de alguna manera?			
¿No son necesarias las cortinas de aluminio para aislar de ruido a las señales?			
¿Usan algún otro tipo de aislamiento en algún lado?			

Sistemas móviles

Características	SI	NO	N/A
¿Si se usan laptops o PCs portátiles, se tienen en cuenta los diferentes riesgos a los que se someten los datos del corporativo?			
¿Los dueños de las laptops son conscientes de la inseguridad que generan al tener datos sensibles en ellas?			
¿Tienen en cuenta estos puntos?			
¿Se encriptan los datos en un sistema móvil?			
¿Se almacenan en lugares seguros los equipos móviles?			
¿Las laptop tienen contraseña de acceso?			
¿Cómo se maneja el trabajo desde la casa?			
¿Se hacen respaldos de los datos de los sistemas móviles?			
¿Cómo y en qué medio?			

Emergencias

Características	SI	NO	N/A
¿Cómo se procede en caso de una emergencia?			
Error físico de disco de un servidor			
Error de memoria RAM			
Error de tarjetas controladoras de disco			
Incendio total o factores catastróficos			
Durante y después de la situación de emergencia, ¿se controla el acceso al NOC?			

Clasificación de datos y hardware

Características	SI	NO	N/A
¿Existen procesos para rotular, manipular y dar de baja computadoras, sus periféricos y medios de almacenamiento removibles y no removibles?			
¿Cómo son estos procesos?			
¿Con qué se rotulan los dispositivos?			
¿Tienen un inventario de recursos de hardware y software?			
¿Existe documentación sobre los dispositivos instalados en cada máquina, su configuración, modificación, forma de mantenimiento, versión, etc.?			
¿Cómo se guarda?			
¿Es una planilla?			
¿Dónde se almacena?			
¿Quién lo actualiza?			
¿Cada cuándo?			

Respaldo

Características	SI	NO	N/A
¿Con qué frecuencia hacen los respaldos?			

¿Qué datos se almacenan? (datos y programas de aplicación y de sistemas, equipamiento, requerimientos de comunicaciones, documentación)			
Software de base y su configuración:			
¿Se hacen discos de inicio de Windows?			
¿Hay imágenes Ghost de las máquinas?			
¿Se hacen respaldos de la configuración de red?			
Software aplicativo			
Parámetros de sistema			
Logs e informes de auditorias			
Datos			
¿Qué mas?			
Respaldos del Hardware			
Modalidad externa: ¿contratan un tercero que proporcione los insumos necesarios en caso de emergencia?			
Modalidad interna: si tienen más de un local, en ambos locales deben tener señalados los equipos, que por sus características técnicas y capacidades			
¿Hay respaldos especiales (con datos distintos, o particulares)?			
¿Cada qué período de tiempo se hacen?			
¿Qué datos guardan?			
¿Qué tipo de respaldo hacen? (respaldos normales, respaldos increméntales, respaldos diferenciales)			
¿En qué áreas o datos usan increméntales, en cuáles usan normales, etc.?			
¿En qué medio se almacena? ¿Con qué dispositivo se hace?			
¿Cómo es la rotación de los medios de respaldo? ¿En una semana, un mes?			
¿Con qué aplicación se hacen? ¿Con algún tipo especial de aplicación de manejo de respaldo?			
¿Es una del sistema operativo, del administrador de archivos u otra?			
¿Utilizan archivos de tipo específicos o archivos zip, por ejemplo?			
¿Hay herramientas de respaldo automáticas, o sea que a través de una agenda hacen las copias?			
¿Quién es el encargado o el responsable?			
¿Los hace el administrador de sistemas?			
¿Tienen formalizados los procedimientos de respaldo?			
¿Existe un procedimiento escrito?			
¿Si falta el responsable del respaldo, quién los hace?			
¿Existen procedimientos escritos para recuperar archivos respaldo, o un plan de respaldo?			
¿Hacen pruebas periódicas de recuperación de respaldos?			
¿Quién puede levantar los archivos de los usuarios, los respaldos de Mis Documentos, cualquier otro usuario?			
¿Qué PC o máquina es la que tiene mayor prioridad?			
¿Cómo son las prioridades?			
¿Qué determinó la prioridad de las máquinas: un análisis de impacto, o la confidencialidad de la información?			
¿Los respaldos se almacenan dentro y fuera del edificio?			

¿Estos lugares son seguros?			
¿Cómo se rotulan e identifican?			
¿Hay documentación escrita sobre los respaldos hechos, sus modificaciones, fechas, etc.?			
¿Se necesita algún dispositivo (llaves, tarjeta) para entrar al almacén de cintas?			
¿Se crean discos de inicio de Windows?			
¿Hay información afuera de la red interna de la empresa que sea valiosa?			
¿El web host tiene datos importantes de usuarios?			
¿Se hacen respaldos de estos datos?			
¿Dentro del corporativo o por el Web host?			
¿Hay respaldos de las páginas web y de sus actualizaciones?			
¿Existen procedimientos automáticos para que, en caso que un usuario cometa un error en la base de datos, ésta pueda volverse a su estado anterior?			
¿Cómo se hace?			

Administración del NOC

Características	SI	NO	N/A
¿Se realizan las siguientes verificaciones en el sistema? Diariamente:			
¿Extraen un logístico sobre el volumen de correo transportado?			
¿Extraen un logístico sobre las conexiones de red levantadas?			
Semanalmente:			
¿Extraen un logístico sobre los intentos de ingresos del exterior a la red interna?			
¿Extraen un logístico con las conexiones externas realizadas desde nuestra red?			
¿Obtienen un logístico sobre los downloads de archivos realizados y quién los realizó?			
¿Obtienen gráficos sobre tráfico en la red?			
¿Obtienen logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino)?			
Mensualmente:			
¿Realizan un seguimiento de todos los archivos logísticos a fin de detectar cambios en las estadísticas obtenidas (realizados en comparación con los archivos del mes anterior, por ejemplo)?			
¿Existe un programa que haga estas comparaciones?			
¿Se usa?			
¿Da buenos resultados?			
¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?			
¿Cómo harían el aviso de las políticas de seguridad?			
¿A través del mailing?			
¿Con charlas o reuniones?			
¿Exposición en transparencias?			

¿Por una notificación expresa a cada empleado?			
¿Cómo funciona el boletín mensual que les entregan a los usuarios?			
¿Qué temas tratan?			
¿Se entrena a los usuarios y administradores?			
¿Quién es el encargado?			
¿Por qué?			
¿Se tienen en cuenta los delitos no tecnológicos?			
¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de o realizar un reporte?			
¿Existe un tipo de feedback o buzón de sugerencia de cambios de los usuarios?			
¿Existe un plan de sistemas formal?			
¿Quién los hace?			
¿Sobre la base de qué estudios definen las cosas por hacer?			
¿Existe un plan estratégico de sistemas?			
¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información?			
¿Existe una planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información?			
Deberá incluir como mínimo el detalle de:			
Los procesos a realizar			
Los controles que se efectúan			
Los mecanismos de registros de problemas y hechos			
Los procedimientos sobre cancelaciones y re-procesos en cada una de las actividades			
Las relaciones con otras áreas			
Los mecanismos de distribución de la información			
¿Existe documentación detallada sobre el equipamiento informático?			
¿Incluye los siguientes datos?			
Distribución física de las instalaciones			
Inventario de "hardware" y "software" de base			
Número de serie de hardware			
Número de licencia de software			
Inventario de insumos			
Diagramas topológicos de las redes			
Tipos de vínculos			
Ubicación de nodos			
Trabajos de mantenimiento y entrada del personal externo			
¿Se tienen en cuenta tanto al centro de procesamiento de datos principal, como de los secundarios, redes departamentales, sucursales y al centro, alternativo para contingencias?			
¿Se actualiza la lista de activos?			

¿Existe algún manual de seguridad, para el personal de seguridad o para los usuarios?			
Existe alguno de los siguientes documentos:			
Plan de contingencia			
Plan de continuidad			
Plan de seguridad			
Detalla las funciones y privilegios de la seguridad			
Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.			
Security Features User's guide: asiste a los usuarios del sistema, describe como usar las protecciones, las responsabilidades de la seguridad del sistema			
¿Es automático el método de actualización de los antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus?			
¿Se programan los escaneos automáticos de virus?			
¿Cada cuánto tiempo?			
¿Por qué no se actualiza la aplicación automáticamente con un schedule?			
¿Cómo se etiquetan los instaladores de los programas o los drivers?			
¿Se almacenan en disco duro, en disquete, en CD, en cinta?			
¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basura y provoquen la caída del sistema?			
Todas estas tareas ¿Son realmente útiles?			
¿Se dan en la práctica?			

Responsabilidad del equipo de seguridad

Características	SI	NO	N/A
¿Cómo se administran las emergencias?			
¿Si se hacen cambios de emergencia, cómo se documenta?			
¿Quién es el encargado de la seguridad?			
¿Y de una política de seguridad y su administración?			
¿Quién se encarga de administrar la estructura de seguridad una vez implementada?			
¿Existe un sólo responsable del NOC?			
¿Qué privilegios (o accesos) se les dan a las personas recién contratadas en el NOC?			
¿Cuál es la diferencia de permisos entre los desarrolladores y los administradores?			
¿Quién asigna los permisos a los distintos roles o grupos?			
¿Quién es el encargado de informar a los ejecutivos de la empresa sobre la administración de seguridad, actividad de seguridad de la información, y riesgos?			
¿Se realizan informes periódicos?			
¿Son a pedido de alguien o a modo de auto evaluación?			

¿Quién es el encargado de recomendar la separación de tareas y responsabilidades para las funciones de IT?			
¿Quién es responsable de asegurar que los sistemas de seguridad física están en su lugar?			
¿Existe en los empleados y altos ejecutivos una conciencia sobre su importancia de la seguridad?			
Todas estas tareas ¿Son realmente útiles?			
¿Se dan en la práctica?			

Auditorías y revisiones

Características	SI	NO	N/A
¿Se hacen auditorías en la empresa?			
¿Qué objetos se auditan? Para cada clase de objetos, ¿qué accesos se auditarán?			
Archivos y directorios			
Claves del registro			
Servicios			
Objetos del kernel			
Impresoras			
¿Qué actividades se monitorizan?			
Monitoreo del sistema general			
Monitoreo de reinicio de los sistemas			
Monitoreo de colapsos del sistema			
Monitoreo de fallas de hardware			
Monitoreo de procesos			
Monitoreo de aplicaciones			
Gestión de red: ¿Para el monitoreo de la red se utilizan aplicaciones propias de Unix?, como:			
Monitores de tráfico de red			
Monitores de rendimiento			
Monitores de control de cantidad de archivos abiertos			
Monitores de usuarios conectados al servidor			
Aplicación de monitoreo gráfico de la red			
¿Qué otra clase de eventos se auditarán?			
¿Con qué tipo de herramientas se hace el monitoreo?			
Escáner de puertos y vulnerabilidades			
Analizadores del sistema de archivos			
Analizadores de logs de eventos			
Analizadores de registro			
Analizadores de listas de control de acceso			
Sniffers de paquetes			
Herramientas para craquear contraseñas			
Escáner de seguridad integral			
¿Se hacen verificaciones aleatorias para verificar el cumplimiento de los requerimientos y procedimientos de seguridad?			

¿Sería útil?			
¿Cuánto se monitoreo? (Monitorear tiene un impacto directo en el performance del sistema)			
¿Cómo hacen para que los recursos alcancen?			
¿Cómo hacen con cada uno de los cuellos de botella?			
Carga de CPU			
Memoria disponible			
Performance del sistema de disco			
Ancho de anda de la red			
¿Cuándo se eliminan los logs para evitar llenar el disco?			
¿Tienen un tamaño máximo?			
¿Qué pasa con la información que se obtiene de las auditorías? ¿Pasa algo de lo siguiente? Se solicita la información y se ve que:			
No tiene y se necesita			
No se tiene y no se necesita			
Se tiene la información pero:			
No se usa			
Es incompleta			
No esta actualizada			
No es la adecuada			
Se usa, está actualizada, es la adecuada y está completa			
¿Las auditorías permiten rastrear las acciones de cada usuario?			
¿Que se audita?			
¿Se audita según las acciones, las maquinas o los usuarios?			
¿Cada uno de estos activos en particular se audita o depende de los sectores y/o máquinas y/o sensibilidad de la información?			
¿Las auditorías soportan investigaciones luego de los hechos, con datos sobre cómo, cuándo y por qué cesaron las operaciones normales?			
¿Se reúne información de las auditorías para formar perfiles de los usuarios del sistema?			
¿Observan, por ejemplo, patrones en los usuarios, como las terminales que utilizan, horas de acceso, y permisos que solicitan, para determinar qué acciones son inusuales y deben ser investigadas?			
¿Se usan herramientas automáticas para revisar los registros de auditorías en tiempo real?			
¿Debido a que no hay herramientas que generen warnings ni alarmas, se revisan los logs de auditorías periódicamente?			
¿Qué se revisa?			
¿La aplicación es en tiempo real?			
¿La aplicación es del sistema operativo, es un programa desarrollado por ustedes o es un programa comprado?			
¿Se deberían utilizar chequeos aleatorios, con frecuencias más bajas, para hacer auditorias manuales y/o mensuales de este tipo?			

¿Se generan historiales de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios–gestión de configuración)?			
¿Se investiga la actividad sospechosa?			
¿Se toman acciones?			
¿Se documentan la ejecución y los resultados de estas pruebas?			

Logs

Características	SI	NO	N/A
¿Está controlado el acceso a los logs en línea de auditoria?			
¿Cómo se identifica qué tipo de log es generado?			
¿Se almacenan en diferentes carpetas los que son generados por diferentes programas?			
¿Los logs se almacenan externamente al corporativo?			
¿Los almacenamientos externos de logs de auditorías se retienen por un período de tiempo?			
¿Está controlado el acceso a estos logs, también?			
¿Hay demasiada información guardada?			
¿Los archivos largos de logs hacen más difícil encontrar irregularidades?			
Los logs de los eventos deberían contener los siguientes campos:			
Fecha y hora			
Tipo (severidad del evento)			
Fuente (el componente que disparó o logeo el evento)			
Categoría (subgrupo de eventos de seguridad)			
ID del evento (número único que identifica el evento)			
Usuario (nombre del usuario relacionado con el evento, si hay)			
Computadora (máquina donde se logeó el evento)			
Descripción (datos como mensajes de error, asociados con el evento)			
Datos (datos binarios asociados con el evento)			
Análisis de los logs de auditoria:			
¿Qué datos son los más importantes o los más leídos?			
¿Cuánto tiempo lleva hacer los análisis?			
¿Es necesario mejorar los análisis?			
¿De qué forma, y cuál es la falla?			
¿Por qué no se analizan los logs, aunque sea los que posean alguna conducta irregular?			
¿Es totalmente necesario un sistema automático de monitoreo y análisis de logs que emita alarmas ante determinados eventos?			
¿Por qué esto no se da en la realidad?			
¿Es mucho trabajo?			
¿No vale la pena?			
¿No hay gente que se dedique a esto?			

Línea de base

Características	SI	NO	N/A
¿Se hace una línea de base del performance de los servidores y de la red?			
¿Qué medidas se toman?			
¿Qué datos se recogen para hacer la línea?			
¿A qué intervalo de tiempo se toman estos datos?			
¿Con qué frecuencia se tomarán las líneas base?			
¿Se hacen nuevamente las líneas de base si se modifica alguna configuración en el sistema?			
¿Cuándo se actualizan las líneas de base?			
¿Cómo se guardan?			
¿Dónde?			
¿En qué formato?			

Responsabilidades de los encargados de seguridad

Características	SI	NO	N/A
¿Quién administra, desarrolla e implementa los procedimientos de auditoría y revisión?			
¿Quién conduce la auditoría?			
¿Quién selecciona los eventos de seguridad a ser auditados?			
¿Quién administra la documentación sobre los resultados?			
¿Quién se encarga de monitorear y reaccionar a los avisos (warnings) y reportes?			
¿Quién hace verificaciones aleatorias para verificar el cumplimiento de los requerimientos y procedimientos de seguridad?			
¿Quién se encarga de reunir datos de las auditorías para formar perfiles de los usuarios del sistema?			
¿Quién revisa los reportes de auditorías buscando anomalías?			
¿Hay separación de tareas entre los que administran el control de acceso y los que hacen las auditorías, o son las mismas personas?			
¿Quién se encarga de buscar nuevas herramientas que faciliten la auditoría?			

Auditorías del servidor

Características	SI	NO	N/A
CPU del servidor usado			
¿Qué trabajos usan más el CPU?			
¿Quién usa más el CPU?			
¿En qué momento se usa más el CPU?			
¿Cuánto tiempo el CPU permanece usado en un 100%?			
Memoria del servidor usada			
¿Qué trabajos usan más memoria?			
¿Quién usa más memoria?			
¿En qué momento se usa más la memoria?			

¿Cuánto tiempo la memoria permanece usada en un 100%?			
Datos del servidor usados			
¿Qué datos son los que consumen más tráfico, memoria o CPU?			
¿Qué datos se usan más?			
¿Qué datos se modifican más?			
¿Quién entra a cada dato?			
Aplicaciones del servidor usadas			
¿Qué aplicaciones consumen más recursos?			
¿Qué aplicaciones se usan más?			
¿Qué aplicaciones se cuelgan más veces?			

Auditorías de control de acceso

Características	SI	NO	N/A
¿Se generan logs de auditoria del control de acceso?			
¿Cuándo se almacenan, y ante qué eventos?			
¿Se almacenen cuando ocurre alguno de estos eventos?			
Login exitoso			
Login fallido			
Procedimientos de cambios de contraseñas satisfactorio			
Procedimientos de cambios de contraseñas fallido			
Bloqueo de un usuario			
Modificación en bases de datos			
Utilización de herramientas del sistema			
Modificación de ciertos datos (como datos de configuración, datos críticos, datos de otros usuarios)			
Acceso a Internet			
Alertas de virus			
¿Dónde se almacenan?			
¿Quién tiene acceso a los logs?			
¿Por cuánto tiempo permanecen guardados?			
¿Se borran cuando expira ese tiempo o se genera una estadística comprimida de los mismos y se guarda un análisis de ellos solamente?			
¿Qué datos se almacenan en los logs?, ¿Se almacenan los siguientes datos? Para todos los eventos:			
Fecha y hora del evento			
Tipo de evento			
ID de usuario			
Origen del evento			
Acceso a Internet:			
Páginas visitadas			
Cookies guardadas			
Archivos descargados			
Servicios utilizados			

Aplicaciones utilizadas			
Modificación de ciertos datos:			
Datos modificados			
Valor anterior			
¿Por cuánto tiempo se guarda el valor anterior de los datos?			
¿Se hace alguna comprobación antes de efectuar el cambio definitivo?			
¿Qué se hace si se modifica algún valor de la configuración del sistema?			
Login fallido:			
Motivo del fallo			
Procedimientos de cambios de contraseñas:			
Contraseña anterior			
Contraseña nueva fallida			
Aplicación usada			
Motivo del fallo			
Lockeo de un usuario:			
Motivo del lockeo del usuario			
Aplicación que realiza el lockeo			
Modificación en bases de datos:			
Datos modificados			
Valor anterior			
Aplicación usada			
Utilización de herramientas del sistema:			
Herramienta usada			
Rastreo de acciones del usuario con esa herramienta			
Modificaciones realizadas			
¿Las estadísticas que genera son buenas?			
¿Faltan datos por analizar que son importantes para la administración del control de acceso?			
Prestar especial atención con los logs que fueron generados con el ID de Administrador, ¿hay irregularidades en estos logs?			
¿Se han controlado alguna vez?			

Auditorías de redes

Características	SI	NO	N/A
Correo:			
¿La herramienta de administración de correo genera logs de auditoria?			
¿Qué contienen?			
¿Quién los administra?			
¿Cada cuanto se leen?			
Se generan avisos cuando:			
Se está por llenar el espacio asignado para el correo			
Hay muchos mensajes de la misma dirección fuente			
Hay muchos mensajes para la misma dirección destino			

Hay muchos mensajes con el mismo encabezado, o cuerpo, o archivo adjunto			
Hay posibles virus			

Correo

Características	SI	NO	N/A
¿Hay SPAM?			
¿Se baja el performance del correo?			
¿Hay algún problema para enviar o recibir los mensajes?			
¿Hay muchos mensajes entrantes o salientes, más de lo normal?			
¿Cuándo más?			

Mantenimiento – Monitoreo

Características	SI	NO	N/A
¿Usan herramientas de monitorización de red?			
¿Se hace algún análisis periódico de la red y sus permisos?			
¿Qué datos se pueden ver?. Datos:			
¿Programas que se ejecutan en las PCs y servidores?			
¿Qué prioridades tienen los trabajos?			
¿Qué prioridades tienen los usuarios?			
¿Con qué reglas de trabajos se están corriendo?			
¿El estado de cada trabajo (en cola, ejecutándose, esperando una respuesta del operador, etc.)?			
¿Desde dónde se ejecuta el programa (usuario, ID, terminal)?			
¿Porcentaje de CPU y memoria (recursos) usado por programa?			
¿Y por terminal?			
¿Y por usuario?			
¿Colas de impresión de cada usuario?			
¿De cada impresora?			
¿De cada terminal?			
¿Trabajos programados por cada usuario?			
¿Por cada terminal?			
¿Dispositivos conectados a la red?			
¿El estado de los dispositivos?			
¿Dispositivos con problemas?			
¿Qué usuario está asignado (o usando) cada dispositivo?			
¿Qué trabajo lo está ocupando?			
¿Se monitorea a los puertos de la red?			
¿Se puede ver si hay intentos de intrusión?			
Alertas de virus:			
Tipo y nombre del virus			
Archivo infectado (nombre, ubicación etc.)			
Antivirus usado			

Acciones llevadas a cabo			
Resultado de las acciones (satisfactorio o no)			
Estadísticas de red:			
¿En qué parte de la línea el tráfico es más intenso?			
¿Quién de las terminales usa más tráfico de red?			
¿Gráfica del uso de la red por terminal?			
¿Se discrimina el tráfico ocupado por mail, datos, aplicaciones, mensajes, Internet, etc.?			
¿Cuántos intentos de intrusión hubo?			
¿Cuántos intentos de otros ataques?			
Internet:			
¿Páginas más visitadas por usuario?			
¿Tiempo promedio de estadía en Internet?			
¿Recursos usados por Internet?			
Mail:			
¿Cantidad de datos que se mueven diariamente vía mail?			
¿Mensualmente?			
¿Anualmente?			
¿Cantidad de mail enviados y recibidos por usuario?			
¿Por departamento?			
¿En toda el corporativo?			
¿Controles para saber si un usuario en particular excede el promedio de mail diarios?			
¿Mensajes infectados, salientes y entrantes?			
¿Se usan estadísticas para controlar el mail bombing?			
Virus:			
¿Cantidad de mails infectados en un determinado tiempo?			
¿Direcciones fuentes que envía más mails infectados?			
¿Cantidad de archivos infectados por extensión?			
Alarmas – Avisos:			
¿Se generan avisos ante virus?			
¿Se generan avisos ante intrusos?			
¿Se generan avisos ante poco espacio en disco de servidores o de PCs?			
¿Se generan avisos ante poca disponibilidad de CPU o de memoria en los servidores?			
¿Cuándo más?			
¿Quién se encarga de procesar y/o monitorear los datos generados por la herramienta?			
¿Cómo se actúa en consecuencia?			
¿Existe algún procedimiento específico?			
¿Qué datos parecen faltar al monitor de red que serían útiles para la administración de la red?			

Plan de contingencias

Características	SI	NO	N/A
¿Existe un plan de contingencias?			
¿Cómo es?			
¿Es formal?			
¿Quién lo desarrolló?			
¿Ha habido alguna contingencia que justifique el desarrollo del plan?			
¿Se desarrolló un previo análisis de riesgo antes de realizar el plan de contingencias?			
¿El plan de contingencias se desarrolló sólo en base en el área de cómputo, o se tuvieron en cuenta otras áreas del corporativo?			
¿Cuáles?			
¿Por qué esas áreas?			
¿El plan de contingencias incluye un Plan de recuperación de desastres?			
¿El plan de contingencias incluye un Plan de reducción de riesgos?			
¿Se definen las responsabilidades y funciones de las personas en el plan de contingencias?			
¿Existe entrenamiento para los responsables del plan de contingencias?			
¿Y para los usuarios?			
¿Poseen las acciones defensivas en caso de violación interna o externa?			
¿Hay algún tipo de mecanismo de reportes o historial, para el manejo de incidentes?			
¿Documentan el plan de contingencias?			
¿Contiene todos estos datos? :			
Objetivo del plan			
Modo de ejecución			
Tiempo de duración			
Costos estimados			
Recursos necesarios			
Evento a partir del cual se pondrá en marcha el plan			
Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades			
¿Existe alguna copia del plan de contingencia fuera de la empresa?			
¿Está protegida en caja de seguridad?			
¿Cada cuándo se actualiza?			
¿Se hacen pruebas del plan?			
¿Con qué frecuencia?			
¿Anualmente?			
¿Se mantiene actualizado de acuerdo a nuevos puestos y funciones, o amenazas?			

Plan de recuperación de desastres

Características	SI	NO	N/A
¿Cuánto cuesta un plan de recuperación de desastres?			

¿Tiene relación con la información a recuperar?			
¿O a cualquier costo salva la información crítica?			
¿En el caso de que haya un plan, cada miembro del equipo tiene una responsabilidad asignada?			
¿O la responsabilidad es del Departamento de Sistemas?			
¿Se dividen las acciones correctivas en equipos de trabajo?			
¿Cómo forman esos equipos?			
¿Dependen del desastre ocurrido?			
¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia?			

Antes del desastre

Características	SI	NO	N/A
Identificación de las funciones críticas			
¿Cuáles serían los datos críticos a proteger en la organización, en el momento de un desastre?			
¿Cuáles serían los elementos de hardware y de software críticos a proteger en la organización, en el momento de un desastre?			
¿Cómo se ordenarían según la importancia?			
Constitución del grupo de desarrollo del plan			
¿Quién sería le responsable del plan de emergencias, de su implementación y puesta en práctica?			
¿El Jefe de Sistemas?			
En cada área que cubrirá el plan debe haber un líder del plan de contingencia.			
¿Quién sugiere, el Jefe de cada área?			
¿Alguien de más bajo rango?			
¿Por qué?			
Sistemas de información:			
¿Existe un responsable de la información, en cada área de la empresa?			
¿Conocen sus responsabilidades?			
¿Los responsables que figuran en la documentación, son los que ejercen realmente el papel de responsables de la información?			
¿Qué funciones tienen que cumplir?			
¿Están identificados todos los sistemas de información y sus características (como si fuera un inventario de los sistemas)?			
¿Qué datos se almacenan de los sistemas? Se sugiere almacenar:			
Nombre			
Lenguaje			
Departamento del corporativo que genera la información (dueño del sistema)			
Departamentos del corporativo que usan la información			
Volumen de archivos con los que trabaja			
Volumen de transacciones diarias, semanales y mensuales que maneja el sistema			

Equipamiento necesario para un manejo óptimo del Sistema			
La(s) fecha(s) en las que la información es necesitada con carácter de urgencia			
El nivel de importancia estratégica que tiene la información de este Sistema para el corporativo			
Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando			
Actividades a realizar para volver a contar con el Sistema de Información			
¿Se puede dar un orden de importancia a los sistemas de la lista de arriba?			
Equipos de cómputos:			
¿Se mantiene un inventario de los equipos de cómputos?			
Se debería incluir:			
Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, ruteadores, bridges			
Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones			
Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivados fuera de línea, respaldo, bases de datos, dueño designado de la información			
Configuración de los equipos (y sus archivos de configuración)			
Ubicación de los equipos y de los datos			
Nivel de uso Institucional de los equipos			
¿Existen pólizas de seguros para los equipos en el caso de siniestros?			
¿Cómo son estos seguros?			
¿Las PCs o equipos se categorizan según su importancia?			
¿Existe una relación de las PCs requeridas como mínimo para cada Sistema permanente del corporativo?			
¿Está actualizada siempre?			
Respaldo:			
¿Existen procedimientos para realizar respaldo?			
¿Están incluidos en el plan de contingencia?			
Definición de los niveles mínimos de servicio:			
¿Cuáles son las contingencias o problemas que pueden ocurrir?			
¿Cuáles serían los peores problemas a los que se puede ver sometida el corporativo?			

Antes del desastre

Características	SI	NO	N/A
¿Cuáles serian las peores contingencias?			
¿Cuáles serían las más probables?			
¿Cuáles son las que ocurren más a menudo?			
¿Cuales son las que no ocurren nunca?			

¿Se pueden nombrar algunas funciones o servicios que funcionen como los niveles críticos de servicio para cada una de las contingencias nombradas arriba?			
¿Qué opinión tiene el jefe de cada área en cuanto a los niveles críticos de su área?			
¿Qué recursos se necesitan para que funcione este servicio?			
¿Cuáles son las prioridades de procesamiento que tendrán estas funciones o servicios críticos en caso de una emergencia?			
Evaluación de la relación costo / beneficio de cada alternativa:			
¿Qué costo tendría cada uno de los niveles críticos de servicio que se determinaron arriba?			
Entrenamiento:			
¿Entrenan al personal de alguna manera ante un siniestro?			
¿Simulan siniestros para entrenar al personal?			

Durante el desastre

Características	SI	NO	N/A
¿Poseen un plan de emergencia?			
¿Se tienen en cuenta los distintos escenarios posibles?			
¿Se incluyen los siguientes puntos? :			
¿Vías de salida?			
¿Plan de evacuación del personal?			
¿Plan de puesta a buen recaudo de los activos?			
¿Ubicación y señalización de los elementos contra el siniestro?			
¿Existen funciones y equipos con funciones claramente definidas a ejecutar durante el siniestro?			

Después del desastre

Características	SI	NO	N/A
Después de ocurrido el siniestro o desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción			
Evaluación de Daños: ¿se realizan las siguientes actividades después de que ha ocurrido algún desastre?			
¿Evalúan la magnitud del daño que se ha producido?			
¿Qué sistemas se están afectando?			
¿Qué equipos han quedado no operativos?			
¿Cuáles se pueden recuperar?			
¿En cuánto tiempo?			
¿Qué más se evalúa o debería evaluarse, según sus experiencias?			
Ejecución de Actividades:			
¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia?			

Para cada tipo de emergencia, de las enumeradas arriba, ¿Qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal?			
Evaluación de Resultados:			
¿Se evalúan los desempeños de las personas, y del Plan, luego del desastre?			
¿Se genera una lista de recomendaciones para minimizar los riesgos?			
Retroalimentación del Plan de Acción:			
¿Se evalúa el desempeño del personal durante el desastre?			
¿Se tiene en cuenta la información que se obtiene luego de una emergencia para retroalimentar el Plan?			
¿Se reordena la lista de personal afectado en tareas de emergencia, con esta experiencia obtenida?			
¿Se modifican las prioridades?			
¿Qué elemento tenía demasiada prioridad?			
¿Qué actividades faltaron incluir en el plan de emergencia?			
¿Qué se mejoraría?			
¿Cuál hubiera sido el costo de no haber tenido el plan de contingencias?			
¿Qué se hubiera perdido?			