UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

A R A G Ó N

ESTRATEGIA DE SEGURIDAD A PARTIR DEL SISTEMA OPERATIVO LINUX EN LOS SERVIDORES DE LA GERENCIA DE TECNOLOGÍA INFORMÁTICA DEL INSTITUTO MEXICANO DEL PETRÓLEO

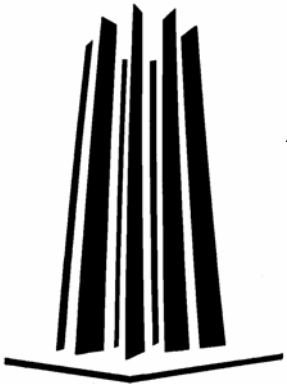
T E S I S P R O F E S I O N A L

Que Para Obtener el Título de

INGENIERO EN COMPUTACIÓN

Presenta:

C L A U D I A M O N T E J A N O G O N Z Á L E Z



Asesor de tesis: Ing. Rodolfo Vázquez Morales

México 2005

Agradecimientos

Durante el tiempo en el que llevé a cabo este trabajo, recibí apoyo y ayuda de diversas personas a quienes deseo expresarles mi más profundo agradecimiento.

Primeramente, quiero agradecer a mis padres por siempre estar junto a mí motivándome para terminar mi carrera, sin su apoyo yo no sería lo que soy. Gracias por permitirme tener los estudios que me servirán para salir adelante en la vida; y gracias también por todo su amor. Los quiero mucho.

En segundo lugar, deseo expresar mi más sincero agradecimiento a mi asesor de tesis, el Ing. Rodolfo Vázquez Morales, por haber tenido siempre la paciencia de escuchar mis dudas y apoyarme con grandes ideas; finalmente todos sus comentarios fueron tomados en cuenta para el enriquecimiento de la tesis. Gracias también por haberme dado la oportunidad de descubrir el lado humano de su persona, además del maestro, un gran amigo.

Luego, quiero expresar mi agradecimiento a Javier por soportar cada momento de desesperación que tuve durante el desarrollo de la tesis, reconozco que fuiste muy paciente conmigo. Gracias por ayudarme con algunas ideas y por corregir todos los errores de gramática y de escritura que tuve. Te amo.

No quiero dejar de mencionar también a mis grandes amigos, compañeros de la carrera, porque finalmente este trabajo forma parte de su motivación. Espero verlos muy pronto en el mismo lugar que yo. Los quiero.

Por último, quiero agradecer a mis revisores por haber corregido mi trabajo y permitirme enriquecerlo con sus ideas.

Índice de Contenido

Introducción

El Instituto Mexicano del Petróleo (IMP), al igual que muchas otras organizaciones del sector público y privado, ha sido víctima de los riesgos que supone contar con una conexión a Internet para realizar las diversas transacciones que justifican su entorno de negocios. Pero lo que realmente importa no es saber cuáles son los riesgos que presenta hacer uso de Internet, sino cuáles son los riesgos de no contar con equipos asegurados de manera adecuada. En este sentido, el IMP está consciente de que necesita realizar un análisis exhaustivo de la problemática que presenta, así como de los controles que implantará para darle solución.

Como parte de los usuarios que diariamente trabajan con un sistema de cómputo en el IMP y como víctima de la inseguridad que conllevan dichos equipos, surge una propuesta de solución que pretende mitigar los riesgos y las vulnerabilidades que presentan las infraestructuras informáticas soportadas bajo la plataforma de Microsoft y hacer conciencia de que la situación económica actual del Instituto exige no hacer demasiados gastos en recursos informáticos.

De manera personal, se propone una estrategia de seguridad que parta de la primera línea de seguridad: una adecuada configuración del sistema operativo que soporta la infraestructura informática. Partiendo de este aspecto se comprende que la seguridad estaría conformada básicamente por una configuración del sistema operativo que permita cerrar todos los puntos de entrada para cualquier tipo de intrusión maliciosa. Así mismo, se pretende cubrir las vulnerabilidades propias del sistema operativo, con el antecedente de que, como cualquier otro software, el sistema operativo también presenta fallas y errores de programación que llegan a ser muy peligrosos para la seguridad de los sistemas. La seguridad de cualquier equipo de cómputo, ya sea servidores o estaciones de trabajo, se complementa siempre con herramientas que hacen uso de las funciones mismas del sistema operativo para incrementar el nivel de seguridad de éste.

La razón para la elección de Linux como la plataforma de las diversas aplicaciones con las que cuenta la Gerencia de Tecnología Informática del IMP son varias: en primer lugar, porque se trata de un sistema operativo con un nivel de seguridad muy por encima de la plataforma Microsoft; en segundo lugar, porque permite una configuración personalizada que se adapta de manera adecuada a las necesidades de las diferentes aplicaciones, además de contar con un gran número de expertos que le brindan soporte desde cualquier parte del mundo y en cualquier momento; y por último, porque Linux es un sistema operativo libre y de código fuente abierto, por lo que no representa ningún tipo de gasto por su utilización.

Muchas empresas en México, y especialmente instituciones de gobierno, no confían aún en el software llamado libre por diversas circunstancias; pero lo realmente cierto es que durante años se ha conservado la costumbre de utilizar la plataforma Microsoft porque representa una aplicación muy fácil de manejar y aprender. En mi opinión, se vuelve bastante interesante y sobre todo muy útil descubrir la funcionalidad de cada herramienta y de todo el software que se encuentra disponible, ya sea libre o comercial, en todo el mundo porque de esta manera se evita hacer ciertos prejuicios que influyen de manera determinante en el entorno de trabajo, y sobre todo en la seguridad de los sistemas.

Abstract

The Instituto Mexicano del Petróleo (IMP), as many others organizations from the public and private sector, has been affected by the issues of having an Internet connection in order to realize many transactions which justify its businesses environment. It does not really matter to know which the risks of using Internet are, but which the risks of improperly assured equipment are. In this way, the IMP is conscientious of the need of fulfill an exhaustive analysis about the trouble it presents, as well as the controls that it will implant to give it a solution.

As a part of users who daily work with a computer system in the IMP and suffer the insecurity of the equipment, it surges a solution proposal that pretends to mitigate risks and vulnerabilities in informatic infrastructures supported under Microsoft platform and to make conscience of the current economical situation of the IMP demands to avoid too many expenses on informatic resources.

In a personal way, a security strategy that parts from the first security line, is proposed: a proper configuration of the operating system that supports the informatic infrastructure. Starting from this aspect, it is understood that security would be conformed basically by an operating system configuration which allows to close all the entry points of any kind of malicious intrusion. Also, it should cover the own vulnerabilities of the operating system, having the preceding that, as any other software, the operating system also has programming faults and errors which could be very dangerous for systems security. Security of any computer equipment, servers or workstations, is always complemented with tools that use the same operating system's functions to increase their security level.

The reasons to choose Linux as the platform of diverse applications of the IMP's Informatic Technology Gerency are several. Firstly, because it is about a high security level operating system, much better than Microsoft platform; secondly, because it allows a customized configuration that adapts according

with different applications needs, in addition of having a huge number of experts who offer support from any part in the world at any time; finally, because Linux is a free open source operating system, so it represents no kind of expense for using it.

A lot of enterprises in Mexico, and specially governmental institutions, still do not trust in the called free software for diverse circumstances; but the true is that during years the custom of using Microsoft platform has been preserved because it represents a very easy application to manage and learn. In my opinion, it gets quite interesting and overall very useful to discover the functionality of each tool and all the available software, free or commercial, in the whole world because in this way certain prejudices can be avoid which influence in a very determining way in the work environment, and also in the systems security.

Entorno del problema

Introducción

El Instituto Mexicano del Petróleo (IMP) es un organismo público descentralizado de interés científico, técnico, educativo y cultural cuya función es buscar la independencia científica y tecnológica en el área petrolera; creado en 1965 por decreto del entonces presidente Gustavo Díaz Ordaz para desarrollar investigación y tecnología para la industria petrolera nacional.

Dentro del Instituto Mexicano del Petróleo se encuentra una organización estructurada en diferentes programas, dentro de los cuales se encuentran las Direcciones Ejecutivas, y en un nivel más abajo, la Gerencia de Tecnología Informática (GTI), la cual cuenta con diversas áreas, pero el área en la cual se centra el siguiente trabajo es de Seguridad de la Información.

Uno de los retos más importantes del actual gobierno consiste en mejorar el contacto y los servicios que brinda a la ciudadanía, sin aumentar desmedidamente su presupuesto. Es por ello que conceptos como optimización de la administración, productividad con disminución de costos y capacitación costeable que permita añadir valor a la atención que hoy en día reciben los ciudadanos por parte de las instituciones gubernamentales, son prioritarios en los planes de los funcionarios. Por esta razón, es que es un requerimiento y una necesidad que los sistemas informáticos, así como toda su infraestructura de red, sean seguros. Así mismo, con el objetivo de minimizar los gastos en

informática y en el pago de licencias por el uso del software, la Gerencia de Tecnología Informática y las áreas de Matemáticas Aplicadas y Computación, Soporte Informático y Seguridad de la Información tomaron la decisión de emprender nuevos controles de seguridad sobre los servidores y la red que componen dichas áreas haciendo uso de herramientas libres y software gratuito; todo esto con el fin de minimizar los riesgos y las amenazas que las áreas antes mencionadas han estado presentando recientemente por ataques externos de personas malintencionadas. El objetivo principal que se persigue en estas áreas es detectar y corregir las posibles deficiencias en su infraestructura informática, haciendo un análisis exhaustivo en cuestión de seguridad.

La Alternativa de Solución

Como parte de un apoyo personal hacia la GTI se propone realizar una reestructuración en la configuración que actualmente opera en los servidores de dicha gerencia, siguiendo con una estrategia de seguridad que se plantea para que sea implantada y la cual establece una migración total del sistema operativo que soporta toda la infraestructura informática de dichas áreas. Esta propuesta comprende la migración de Microsoft Windows hacia Linux como el principal sistema operativo y soporte del 80% de los servidores que componen la GTI haciendo uso de herramientas complementarias de distribución libre.

Unix es un sistema operativo que tiene sus orígenes a finales de los años 60 y fue desarrollado en los laboratorios Bell de ATT culminando finalmente en 1983 con la versión 1 del sistema V de Unix. Durante este tiempo, y desde entonces, muchas organizaciones han hecho sus propias variantes sobre la fórmula Unix y ahora funcionan docenas de sistemas operativos diferentes que utilizan sus mismos componentes básicos y sus principios. Linux es uno de ellos. Desarrollado como un proyecto de colegio universitario por Linus Torvalds, Linux ha emergido como una de las variantes más populares de Unix en los años recientes y su versión más popular hoy en día se llama Linux Red Hat. La popularidad de Linux ha llegado al punto de expandirse más allá del mercado tradicional de Unix: los profesionales de los equipos y los aficionados técnicos. Esto es debido en parte a la reacción en contra de Microsoft, que, según piensan algunos, está a punto de alcanzar el monopolio de los sistemas operativos. Cuando se paga una versión "comercial" de Linux como Red Hat, se obtiene no sólo el sistema operativo y el código fuente en CD-ROM, sino también diversas aplicaciones, documentación del producto y soporte técnico, que con frecuencia faltan en las versiones gratuitas.

Todo esto ha contribuido en gran medida a que Linux sea un sistema operativo que comienza a expandirse de manera considerable en ambientes de trabajo y es por ello que también diversos fabricantes comienzan a vender sus equipos con alguna de las diferentes versiones de Linux como un sistema

operativo estándar; por ejemplo, Unix puede ejecutarse en diversas plataformas de hardware y muchas de las variantes de Unix son versiones propietarias creadas por fabricantes específicos para ejecutarse en sus propias plataformas hardware. Solaris de Sun Microsystems, HP-UX de Hewlett-Packard, AIX de IBM e IRIX de Silicon Graphics son ejemplos de sistemas operativos que se venden junto con una estación de trabajo construida por el mismo fabricante.

Existen varios factores que han contribuido a la adopción del sistema Linux, uno es la falta de madurez y de soluciones disponibles en el mercado, pero el principal aspecto es la seguridad. Por lo general, el software presenta agujeros desde su nacimiento, como Microsoft, pero la ventaja de Linux es que se pueden resolver más rápido porque no depende de un proveedor. Además sus usuarios constantemente están trabajando en mejorar la plataforma. Por supuesto que Linux implica gastos sólo si el cliente no comprende el modelo de negocio porque el código abierto permite un ambiente de creatividad más fuerte, pero no implica que todo sea gratis. Podemos ver en Linux un gran paso hacia la tecnología que se mueve hacia los servicios a usuarios al considerar la comunicación con otras plataformas. La causa del éxito de Linux es la participación de los desarrolladores que están por todas partes, usándolo y aportando elementos y funcionalidades al sistema operativo; además de su capacidad de crecimiento con servidores formando clusters, para conseguir alto rendimiento o alta disponibilidad en cualquier servicio y sin costo adicional de software. La plataforma Linux está lista ya para correr aplicaciones de misión crítica porque desde 1999 ha probado ser un sistema operativo seguro para aplicaciones de negocios.

En México, las soluciones basadas en código abierto son cada vez más aceptadas en empresas e instituciones, tanto en sistemas sencillos como en los de misión crítica. Cabe mencionar que entre las compañías que utilizan Linux se encuentran Acer, AOL, Banco de México, El Sitio, IBM, La Jornada, Prodigy y Radio Red, así como PEMEX, la UNAM y el IFE. También la página de la presidencia opera con Linux y otras herramientas de código abierto como GNU, MySQL y PHP.

Recursos de la Organización

El Instituto Mexicano del Petróleo tiene en su haber un registro de casi 5000 computadoras que son utilizadas en las diferentes áreas antes mencionadas, de las cuales casi 120 están destinadas para los diferentes proyectos del laboratorio de Matemáticas Aplicadas y Computación, y todas ellas cuentan con tarjetas de red Ethernet conectadas a la Intranet del propio Instituto.

La Intranet sigue las normas del cableado estructurado y la topología utilizada es tipo estrella con 5 switches enlazados en forma redundante, esto es,

semejando una topología de malla en la cual se cuenta con más de un camino para evitar fallas y pérdida de continuidad. La conexión del Backbone se realiza por medio de fibra óptica con una velocidad de transmisión de 622 Mbps con tecnología ATM, lo mismo que el cableado vertical. Por otro lado, el cableado horizontal lo constituye cable de par trenzado categoría 5 con tecnología Ethernet y Fast-Ethernet, el cual puede alcanzar una velocidad de transmisión de 100 Mbps.

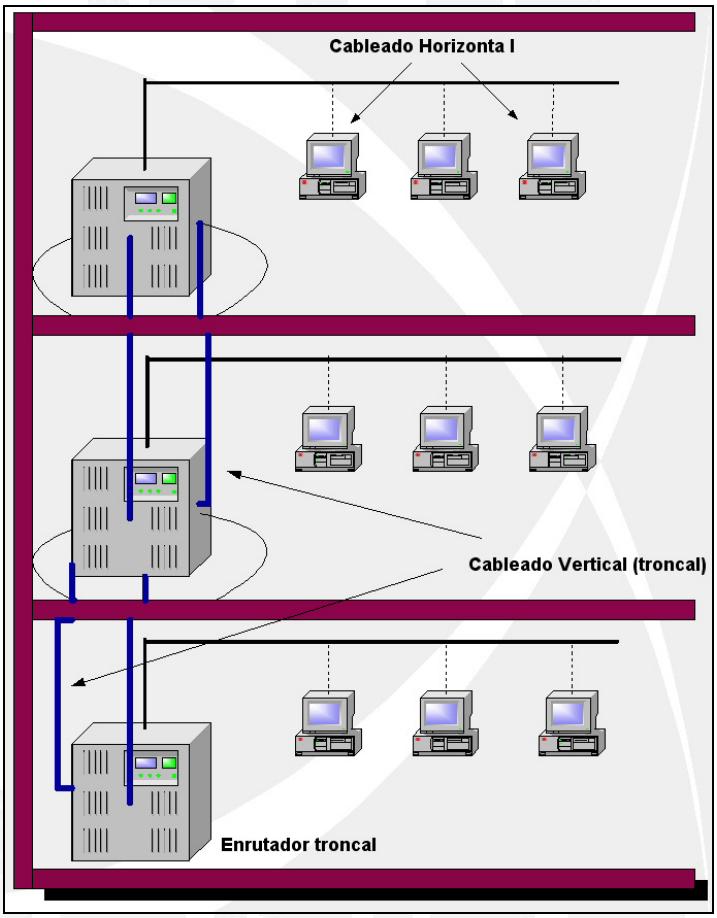


Fig. 1 Sistema de Cableado Estructurado para un edificio genérico

Problemática Encontrada

Desde el inicio de mi estancia en el Instituto, hace casi 6 meses, me he percatado de forma indirecta de la problemática que tiene la GTI en el ámbito de la seguridad.

Se tiene registro de que, en varias ocasiones, el Instituto ha sido atacado con bombas lógicas y en muchas más, la red ha sido infectada con diversos virus interrumpiéndose la operabilidad del mismo por periodos largos de tiempo. Todos los usuarios, sin distinción, que cuentan con una PC personal se

encuentran conectados a la red interna del Instituto y a Internet sin ninguna restricción sobre las páginas Web que consultan. Se les está permitido el acceso a los servidores de correo externo y al uso del Messenger del portal T1MSN para el intercambio de mensajes instantáneos y archivos. Del mismo modo, se les permite que compartan cualquier recurso, carpeta, archivo, e incluso las unidades de disco duro que tengan en su PC en la red interna. Todo esto hace más fácil la propagación de virus informáticos, pero sobre todo hace que no se tenga un control sobre la información propia de la gerencia. Esto quiere decir, que cualquier persona puede tener acceso a ella.

Además de esto, la GTI presenta varias deficiencias en su propósito de contar con un nivel adecuado de seguridad que respalde sus objetivos:

- *No se cuenta con una metodología de seguridad adecuada, es decir, actualmente los controles de seguridad que se tienen implantados no se encuentran respaldados por una metodología desarrollada.*
- *No se tiene realizado un análisis de riesgos actuales en los equipos de cómputo, en los servidores ni en la red.*
- *No se cuenta con un manual de políticas y procedimientos actualizado y que vaya acorde con los procesos que actualmente se desarrollan.*
- *Tampoco se tiene desarrollado un plan de contingencias adecuado a los riesgos y vulnerabilidades actuales de la operación.*
- *El soporte que se tiene que dar a los usuarios por medio de los distintos servidores, pareciera que es insuficiente para la carga de clientes conectados, lo que hace lentos los procesos.*

Visión de la Mejora

Después de poner en claro los riesgos actuales en cuestión de seguridad informática por los que atraviesa la Gerencia de Tecnología Informática del IMP, queda claro que se hace necesaria la aplicación de medidas que ayuden a proporcionar cierto grado de fiabilidad en los actuales procesos que se llevan a cabo en dicha gerencia. Los objetivos principales en la GTI, como parte de la estrategia actual de seguridad informática son:

- *La protección del sistema operativo y aquellos aplicativos que sean instalados en los servidores*
- *Establecer políticas para aplicación de revisiones de software, particularmente de seguridad, de manera continua en servidores y estaciones de trabajo*
- *Establecimiento de políticas a escritorios de usuarios*

- *Establecimiento de metodologías para administración de cambios en servidores críticos sin comprometer la operación en producción*

De acuerdo a los puntos que se pretende considerar, queda establecido que cualquier estrategia de seguridad que se desee implantar en una infraestructura informática debe comenzar por hacer un análisis de riesgos y vulnerabilidades, tanto en los procesos como en la operación, para determinar con exactitud en qué situación se encuentran la institución y los servicios que presta. Pero, debido a que toda infraestructura informática es soportada por un sistema operativo, cuando se habla de una estrategia de seguridad, lo primero que se debe tomar en cuenta para la protección de los datos, es precisamente la configuración del sistema operativo.

CAPÍTULO 1
Elementos de una Infraestructura Informática

Introducción

Todas las organizaciones hacen uso de recursos informáticos que les permiten desarrollar sus actividades administrativas, los cuales forman una amplia infraestructura que hace posible la manipulación del activo más valioso con el que cuentan: la información. Esa infraestructura tiene un gran soporte en el sistema operativo con el cual interactúa. Por eso es importante dar una visión general de los sistemas operativos y su evolución en entornos de trabajo, pero sobre todo de los aspectos de seguridad que el mismo sistema operativo implementa para proteger a las infraestructuras informáticas.

Es cierto que cada elemento que conforma una infraestructura informática cuenta con sus propias generalidades y características, también que tiene sus propias problemáticas y su propio nivel de seguridad implementado, el cual se complementa siempre con la seguridad que le brinda su principal soporte: el sistema operativo.

1.1 Arquitectura de una infraestructura informática

Una arquitectura como la que se muestra en la figura 1.1 esta compuesta por diversas máquinas, barreras, redes, comunicaciones, hardware adicional y es con la que suele encontrarse "el hacker" cuando navega por Internet, y para

él representa su campo de batalla, con todos y cada uno de los obstáculos que encuentra y que su mente abierta está dispuesta a traspasar.

Toda esta arquitectura computacional es soportada por un Sistema Operativo que se encarga de controlar y regular las acciones y procesos dentro de ella. Aunque esta es sólo una visión de la arquitectura, porque se debe tener en cuenta que cada organización cuenta con su propia arquitectura y visión informática dependiendo de las necesidades de su objetivo como empresa y de su implementación de seguridad informática; sin embargo, toda arquitectura computacional está compuesta por al menos una base de datos, una red LAN, un servidor, un sistema de información que procesa los datos contenidos en la base de datos y los hace productivos y por supuesto, un Sistema Operativo base como soporte de toda esta infraestructura.

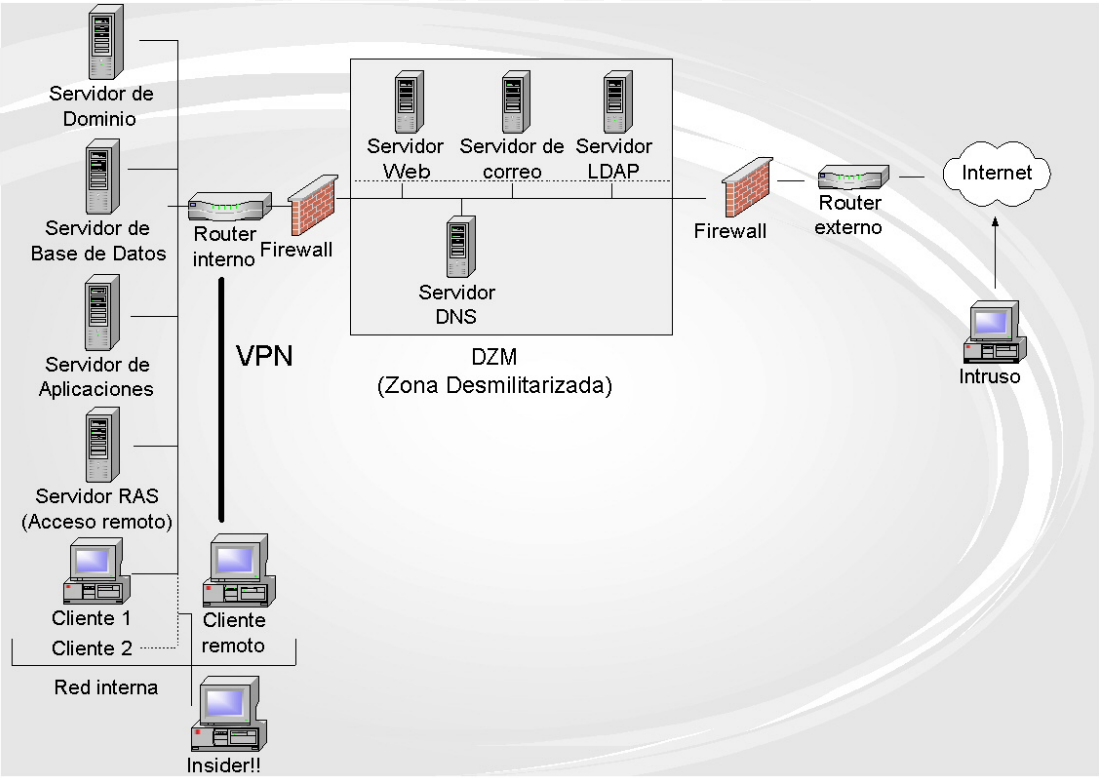


Fig. 1.1 Visión gráfica de la arquitectura informática que nos rodea

1.2 El Sistema Operativo como Elemento Básico de Información

Un sistema operativo es un programa que controla la ejecución de programas de aplicación y actúa como una interfaz entre el usuario y el hardware de una computadora.
Se define al sistema operativo como una conexión de programas de control, de administración y servicio que controlan todos los aspectos del ambiente en el

que funcionan los programas de aplicación, los cuales ejecuta junto con el hardware.
Un sistema operativo es un factor fundamental en la administración de recursos de una computadora, ya que bajo este nombre se agrupan todos los programas que permiten a los usuarios la utilización del sistema de cómputo. Los sistemas operativos están entre las piezas más complejas de software hasta ahora desarrollados.

El hardware y el software que se usan para proporcionar aplicaciones a un usuario pueden verse de manera jerárquica o por capas (fig. 1.2). El usuario final ve un sistema computacional en términos de una aplicación programada como un conjunto de instrucciones de máquina responsables por completo del control del hardware de la computadora; para esto se cuenta con utilerías, las cuales implementan funciones usadas con frecuencia y que ayudan en la creación del programa, la administración de archivos y el control de dispositivos de E/S. El programa de sistema más importante es el sistema operativo.

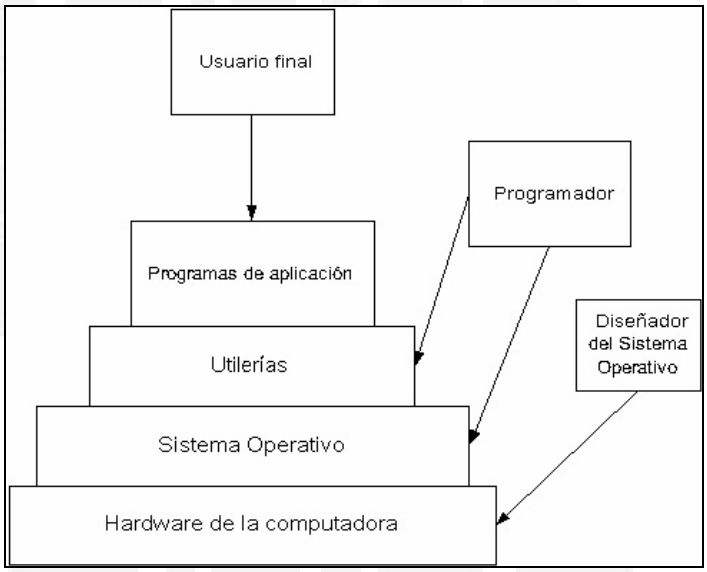


Fig. 1.2 Capas de un sistema computacional

El sistema operativo proporciona servicios en las siguientes áreas:

- **Creación del programa**. *El sistema operativo proporciona facilidades y servicios, como editores y depuradores, para ayudar al programador en la creación de programas; estos servicios son parte de las utilerías que en realidad no son parte del sistema operativo pero son accesibles mediante él.*
- **Ejecución del programa**. *Para ejecutar un programa las instrucciones y los datos deben cargarse en la memoria principal, los dispositivos de E/S deben inicializarse y otros recursos deben prepararse y el sistema*

operativo es el que se encarga de manejar todas estas tareas por el usuario.

- **Acceso a dispositivos de E/S**. *Cada dispositivo de E/S requiere su propio conjunto individual de instrucciones o señales de control para su correcta operación y es el sistema operativo el que se encarga de todos estos detalles para que el programador solo piense en términos de lecturas y escrituras simples.*

- **Acceso controlado a archivos**. *En el caso de archivos, el control debe incluir una comprensión tanto de la naturaleza del dispositivo de E/S (unidad de disco, etc.) como del formato de archivo en el medio de almacenamiento; sobre todo en el caso de un sistema con múltiples usuarios simultáneos.*

- **Acceso al sistema**. *El sistema operativo controla el acceso a todo el sistema y a recursos específicos del mismo. La función de acceso debe proporcionar protección de recursos y datos desde usuarios no autorizados y debe resolver conflictos en el caso de disputas por recursos (en el caso de un sistema público o compartido).*

- **Detección de errores y respuesta a ellos**. *Pueden ocurrir varios errores mientras corre un sistema de cómputo y el sistema operativo se ve precisado a emitir la respuesta que elimina la condición de error, con el menor impacto sobre las aplicaciones que corren.*

- **Contabilidad**. *Un buen sistema operativo recopila estadísticas del uso de los diferentes recursos y monitorea los parámetros de ejecución, como tiempo de respuesta. Esta información es útil para anticipar la necesidad de mejoras futuras y para ajustar el sistema con el fin de mejorar el rendimiento.*

Al administrar los recursos de la computadora (movimiento, almacenamiento y procesamiento de datos), el sistema operativo controla sus funciones básicas, las cuales son:

- *El SO es un programa ejecutado por el procesador.*
- *El SO con frecuencia abandona el control y debe depender del procesador para que le permita recuperarlo.*

El sistema operativo dirige al procesador en el uso de otros recursos del sistema y en la temporización de la ejecución de otros programas. Más aún, el procesador mismo es un recurso y el sistema operativo debe determinar qué

tanto tiempo de procesador va a dedicarse a la ejecución de un programa particular de usuario.

1.2.1 Funciones del Sistema Operativo

Básicamente los sistemas operativos realizan las siguientes funciones:

1. *Decidir cuáles usuarios pueden tener acceso a los recursos del sistema y durante cuánto tiempo (Restringir el acceso).*
2. *Impedir que el sistema sufra un colapso si algún dispositivo causara alguna falla.*
3. *Ayudar en la elaboración y ejecución de programas de usuario.*
4. *Administrar y llevar registro de los recursos como memoria, procesador, dispositivos de E/S e información.*
5. *Autoprotección contra el usuario y la protección de cada usuario contra los demás.*
6. *Reportar al procesador la entrada de programas e instrucciones a la memoria.*
7. *Asignar memoria a los programas, guardando su dirección absoluta, dónde comienza y su tamaño.*
8. *Suministrar un medio de ejercer control después de que se interrumpe un programa, salvando el estado del programa interrumpido y determinando la rutina requerida a procesar.*
9. *Proporcionar una bitácora de lo que sucedió durante el proceso de un programa y el tiempo requerido para cada programa.*
10. *Tratamiento de errores.*

El sistema operativo es una interfaz genérica que se asienta entre las aplicaciones del software y el hardware subyacente. Sin los archivos que aporta el sistema operativo, cada paquete de software tendría que escribir detalles en bajo nivel de cómo almacenar archivos o comunicarse con otras aplicaciones. El sistema operativo suministra a sí mismo un medio de abstraer recursos, de modo que sean independientes del hardware. Otra función importante del sistema operativo comprende la carga y ejecución de programas, y la gestión del espacio de memoria para los múltiples procesos.

1.2.2 Tipos de sistemas operativos

En esta sección se discuten ciertas características de los diferentes tipos de sistemas operativos, en general, las propiedades generales, aplicaciones típicas y requerimientos básicos de cada uno, con el fin de comprender los requisitos clave y la estructura de los sistemas operativos más modernos. Además se da una descripción breve de las principales ventajas y problemáticas que presentan cada uno de ellos con el fin de hacer un análisis comparativo entre

cada uno de ellos, aunque algunos de estos sistemas operativos ya no se utilicen muy comúnmente.

1.2.2.1 Procesamiento en serie

Con las primeras computadoras, desde los últimos años cuarenta hasta la mitad de la década de los cincuentas, el programador y/o usuario interactuaba de manera directa con el hardware de la computadora; no había sistema operativo. Estas máquinas eran operadas mediante interruptores de consola que tenía luces de exhibición o, tal vez, a través de un teclado hexadecimal, alguna forma de dispositivo de entrada (por ejemplo, un lector de tarjetas) y una impresora.

Los programas para la máquina se podían desarrollar traduciendo manualmente secuencias de instrucciones en código binario o cualquier otro cuya base es siempre una potencia entera de 2. Se arrancaban los programas cargando el registro contador de programa con la dirección de la primera instrucción y se obtenían los resultados de la ejecución examinando los contenidos de los registros relevantes y las posiciones de memoria. Si el programa proseguía hasta su culminación normal, la salida aparecía en la impresora; pero si un error detenía el programa, las luces indicaban la condición de error.

Con el tiempo, se desarrollaron varias herramientas de software para intentar hacer más eficiente el procesamiento serial, que incluían bibliotecas de funciones comunes, ligadores, cargadores (los cuales transferían la información desde el dispositivo de entrada a la memoria), depuradores y rutinas de manejo de E/S. Los dispositivos de E/S también tuvieron su evolución al dar paso a las tarjetas perforadas, cintas de papel y traductores de lenguaje.

Este modo de operación no es obviamente muy eficaz; ejecutar el sistema de la computadora puede requerir la carga manual frecuente de programas y datos, y todo esto repercute en la baja utilización de los recursos del sistema. La productividad de los usuarios es baja, especialmente en entornos multiusuario; e incluso este procesamiento es muy lento con herramientas como editores y depuradores y se eleva con la carga manual de programas y datos.

1.2.2.2 Sistemas por Lotes Simples o tipo Batch

El paso lógico en la evolución de los sistemas operativos fue automatizar la secuencia de operaciones involucradas en la ejecución de un programa y en los aspectos mecánicos del desarrollo de programas. La idea era incrementar la utilización de los recursos y la productividad del programador reduciendo o eliminando los tiempos muertos provocados por las operaciones manuales muy largas en comparación.

El primer sistema operativo por lotes, que fue el primer sistema operativo existente en cualquier clase, fue desarrollado en la mitad de los años cincuentas por General Motors para usarlo en la IBM 701.
La idea central detrás del esquema de procesamiento por lotes fue el uso de una pieza de software llamada "monitor". Con el uso de este sistema operativo el usuario ya no tenía acceso directo a la máquina. Más bien, se proponía el trabajo en tarjetas o cinta a un operador de computadora, quien hacía lotes de los trabajos reunidos de manera secuencial y colocaba el lote completo en un dispositivo de entrada para que lo usara el monitor.
Cada programa estaba construido para regresar al monitor cuando completaba el procesamiento, en ese momento el monitor cargaba el siguiente programa de forma automática. Los trabajos son procesados típicamente en el orden de admisión, según el modelo de una cola (el primero en llegar es el que será primeramente procesado).
El procesamiento por lotes requiere que estén reunidos en forma de un trabajo el programa, los datos y las órdenes del sistema apropiadas. Este tipo de sistemas pueden servir muy bien para programas que no requieran interacción y para aquellos con tiempos de ejecución largos; algunos ejemplos de estos sistemas incluyen programas de nóminas, de pronósticos, de análisis estadísticos y asimilación de grandes datos científicos.
Los sistemas por lotes no necesitan ningún gestor de dispositivo de tiempo crítico, desde el momento en que no puede estar en ejecución más de un programa a la vez. Además, como el acceso a los archivos también es serial se necesita poca protección y ningún control de concurrencia de acceso a archivos.
Uno de los mayores problemas que presentan estos tipos de sistemas, es que debido los retardos en el tiempo total de ejecución y a la depuración fuera de línea, no son muy convenientes para el desarrollo de programas.

1.2.2.3 Sistemas por Lotes Multiprogramados

La ejecución concurrente de programas, es decir, reasignación de los recursos de un sistema de cómputo dinámicamente entre una colección de programas activos en diferentes estados de ejecución es a lo que se le conoce como multiprogramación.
Un instante de un programa en ejecución se llama proceso *o* tarea*. Un sistema operativo multiproceso o multitarea se distingue por sus habilidades para soportar dos o más procesos activos simultáneamente. El término* multiprogramación *denota un sistema operativo que, además de soportar procesos concurrentes múltiples, permite que residan simultáneamente en la memoria primaria las instrucciones y los datos procedentes de dos o más procesos disjuntos.*
En efecto, la operación multiproceso es uno de los mecanismos que un sistema operativo multiprogramado emplea en gestión de la totalidad de los recursos del sistema, incluyendo la unida de proceso central (CPU), la memoria y los dispositivos de E/S. Un sistema operativo de multiprogramación monitoriza el

estado de todos los programas activos y recursos del sistema. Se activa el sistema operativo para proporcionar ciertos servicios cuando ocurre un cambio de estado importante, o cuando es llamado explícitamente; los requerimientos del entorno específico al que se va a servir influyen en la elección de los objetivos y las estrategias del sistema operativo asociado.

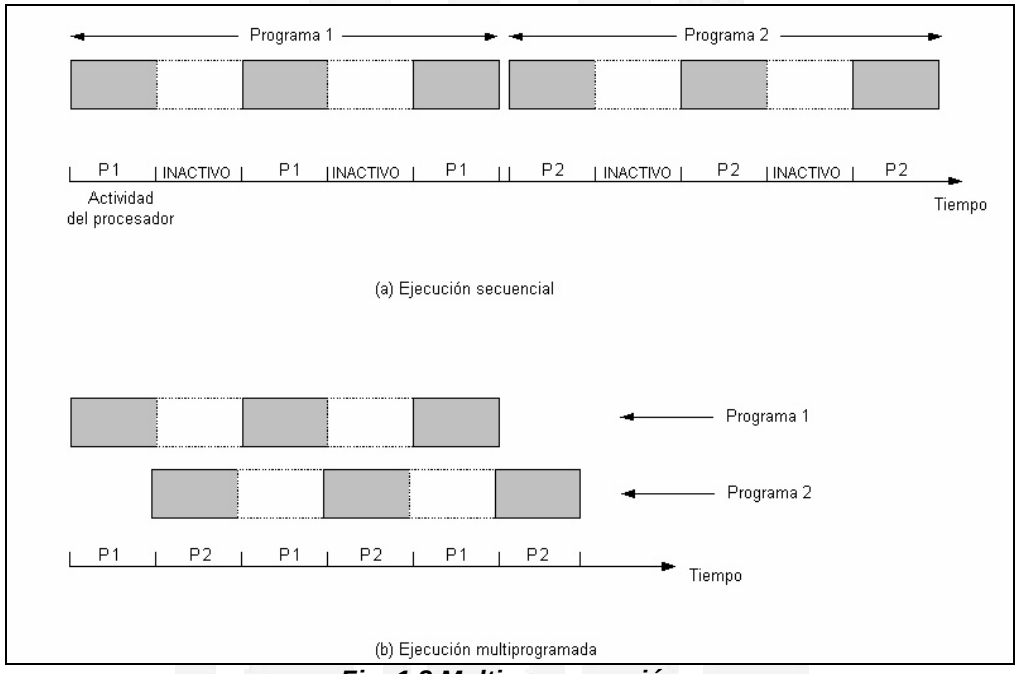


Fig. 1.3 Multiprogramación

El multiprocesamiento crea la posibilidad de cierto tipo de conflictos que no se presentan en los sistemas de un solo procesador. Es necesario ordenar secuencialmente el acceso a una localidad de memoria compartida, para que dos procesadores no traten de modificarla al mismo tiempo, con la posibilidad de alterar inadecuadamente su contenido. El orden secuencial también es necesario cuando un procesador desea modificar una localidad que otro procesador desea leer.

1.2.2.4 Sistemas de Tiempo Compartido

El uso de la multiprogramación es bastante eficiente, sin embargo, era deseable proporcionar un modo en que el usuario interactuara en forma directa con la computadora. Esta opción no estaba disponible en los años sesentas y para cambiar esto se descubrió otra técnica llamada "tiempo compartido", reflejando el hecho de que múltiples usuarios comparten el tiempo del procesador. Uno de los primeros sistemas de tiempo compartido desarrollados fue el CTSS (Compatible Time-Sharing System), desarrollado por el Instituto Tecnológico de Massachussets para la IBM 709 en 1961.

La técnica básica es tener múltiples usuarios que acceden al mismo tiempo a un sistema de microcomputadoras por medio de dos o más terminales, con el sistema operativo intercalando la ejecución de cada programa usuario en tiempo máquina. Un ejemplo típico lo encontramos en una aplicación bancaria con cientos de terminales funcionando bajo el control de un programa único y accediendo a una base de datos común.
Uno de los objetivos principales de los sistemas multiusuario en general, y de los sistemas de tiempo compartido en particular, es un buen tiempo de respuesta de las terminales; éstos últimos tratan con frecuencia de proporcionar un reparto equitativo de los recursos comunes para dar la ilusión a cada usuario de poseer la máquina solo para él.
Es importante señalar que los sistemas de tiempo compartido incorporan tanto la multiprogramación como la operación multiusuario, ya que aunque se asocia frecuentemente con la multiprogramación, las operaciones multiusuario no implican ni tienen implícita la multitarea.
El gestor de memoria en un sistema de tiempo compartido proporciona el aislamiento y la protección de los programas residentes. Y, el gestor de archivos debe proporcionar protección y control en el acceso, dada la posibilidad de concurrencia y de conflictos al tratar de acceder a los archivos. Esta tarea se acomoda a los requerimientos de los archivos compartidos por ciertos usuarios o grupos de usuarios.

El tiempo compartido y la multiprogramación originan nuevos problemas para el sistema operativo. Si están múltiples trabajos en la memoria, entonces deben protegerse de interferir uno con otro. Con múltiples usuarios interactivos, el sistema de archivos debe protegerse de manera que únicamente los usuarios autorizados tengan acceso a un archivo particular. Debe manejarse la contención de recursos, como impresoras y dispositivos de almacenamiento masivo.

1.2.2.5 Sistemas de Tiempo Real

Los sistemas operativos de tiempo real se utilizan en entornos donde se deben aceptar y procesar en tiempo breve y sin tiempos muertos un gran número de sucesos, en su mayoría externos al sistema de la computadora; y por el contrario, son asuntos secundarios la conveniencia del usuario y la utilización de recursos.
No es raro para este tipo de sistemas esperar el proceso súbito de miles de interrupciones por segundo sin perder un solo suceso. Tales requerimientos no pueden abordarse normalmente solo con la multiprogramación y usualmente ponen su confianza en ciertas estrategias y técnicas específicas para hacer su trabajo. Procesos claramente definidos y controlados por el programador se encuentran en sistemas de tiempo real. El proceso se activa al ocurrir un suceso externo, señalado por una interrupción y se consigue el multiproceso planificando los procesos independientes unos de otros. Se asigna a cada

proceso un cierto nivel de prioridad que corresponde a la importancia relativa de los sucesos que sirve.
En los sistemas de tiempo real, el gestor de memoria está, en comparación, menos solicitado que en los sistemas operativos antes mencionados debido a que muchos procesos residen permanentemente en memoria para proporcionar tiempos de respuesta muy rápidos. Además, el gestor de archivos se encuentra sólo en grandes instalaciones de sistemas y debe satisfacer muchos de los requerimientos de protección y control de acceso, ya que su objetivo principal es la velocidad de acceso, más que la utilización eficaz del almacenamiento secundario.
Ejemplos de las aplicaciones de tales sistemas incluyen control industrial, equipamiento telefónico conmutado, control de vuelo, aplicaciones militares y simulaciones en tiempo real.

1.2.2.6 Sistemas Combinados

Como podemos ver, los diferentes tipos de sistemas operativos están optimizados, o al menos muy acoplados para servir a las necesidades de ciertos entornos específicos. Sin embargo, en la práctica un entorno dado puede no encajar exactamente en ninguno de los modelos descritos anteriormente. Por esta razón, algunos sistemas operativos comerciales proporcionan una combinación de los diferentes esquemas hasta ahora descritos.
Por ejemplo, un sistema de tiempo compartido puede soportar usuarios interactivos mientras incorpora también un monitor por lotes bastante maduro. En otras palabras, se puede usar el procesamiento por lotes como relleno para mejorar la utilización del procesador mientras se realiza un completo servicio así mismo.
De igual manera, algunos sucesos de tiempo crítico, tales como recepción y transmisión de paquetes de datos en una red, se pueden manejar con el modelo de tiempo real en sistemas que por otra parte proporcionan servicios de tiempo compartido a sus usuarios de terminales.

1.2.3 Problemáticas de los Sistemas Operativos

El tamaño de un sistema operativo caracterizado por completo y la dificultad de las tareas que dirige han conducido a tres problemas infortunados pero bastante comunes. Primero, de manera crónica, los sistemas operativos tardan en entregarse y esto favorece a los nuevos sistemas operativos y las mejoras de sistemas viejos; segundo, los sistemas tienen defectos latentes desde su inicio que muestran en acción debido a que son liberados en muchas ocasiones con la finalidad de ganar el mercado sabiendo las vulnerabilidades que presentan, por lo cual deben repararse y volverse a trabajar; y, finalmente,

con frecuencia el rendimiento no es el que se espera cuando se implementa, pues siempre existen mejoras que deben hacérsele.

A todos los programas, tarde o temprano, se les descubre algún error; y si ese programa es el propio sistema operativo, los errores se convierten en algo muy serio, pues son aprovechados por cualquier persona con dudosas intenciones permitiéndoles tener el control total sobre el sistema. Continuamente están apareciendo nuevos agujeros en la seguridad que son aprovechados por los crackers por medio de sofisticados canales de comunicación. El resultado es que cuando aparece un programa que se aprovecha de un nuevo fallo en un sistema operativo (llamado comúnmente exploit*), todas las máquinas que utilizan ese sistema operativo son vulnerables a ese exploit.*

Si este sistema operativo es propietario, es decir, que es propiedad y está controlado por una empresa, por una persona o por una institución, significa normalmente que el programa es "cerrado": ni está disponible, ni se puede leer, ni puede ser modificado por otros. Todo esto trae como consecuencia que todo software cerrado sea vulnerable al exploit hasta que la empresa o institución decida asignar los recursos necesarios para corregir el error y publicar esa corrección a todos los que usen ese sistema operativo propietario.

1.2.4 Seguridad que debe brindar el Sistema Operativo

En la economía actual, la masiva utilización de la computación, las comunicaciones para transferir y almacenar información y sobre todo el uso de Internet, está sujeta a amenazas que ponen en riesgo uno de los activos más importantes de una organización, es decir, su información y el cumplimiento de sus objetivos de negocio.
Los sistemas operativos seguros han sido materia de gran preocupación entre los expertos en seguridad de computadoras. Se han hecho esfuerzos considerables para definir y desarrollar lo que se llama un sistema operativo seguro. Los conceptos incorporados en un sistema así están más allá de las necesidades de un sistema de cómputo comercial típico.

Es evidente que la línea de seguridad comienza con el sistema operativo, es decir, el sistema operativo constituye la base para la implementación de cualquier medida de seguridad. Todos los sistemas operativos tienen vulnerabilidades y de nada sirve implementar una serie de herramientas si el sistema operativo que soporta la infraestructura computacional es vulnerable. Es por esto que se comienza a definir una estrategia de seguridad a partir del sistema operativo. Posteriormente se complementa la línea de la seguridad con toda una gama de herramientas que apoyan de manera específica la seguridad que brinda el sistema operativo.

El sistema operativo, como administrador de los recursos computacionales, es un elemento estratégico en la protección de servidores de Internet e Intranet

y el administrador debe conocer los posibles puntos de riesgo e implementar las soluciones antes de verse afectado, a través de mecanismos de diagnóstico, pruebas de penetración, análisis de riesgos y vulnerabilidades, detección de intrusos, análisis de tráfico y rastreo de puertos.

Gran parte del trabajo en seguridad y protección en lo que se relaciona con sistemas operativos puede agruparse en las siguientes tres categorías:

- **Control de acceso**. *Regula el acceso del usuario al sistema total, subsistemas y datos, así como el acceso a procesos de varios recursos y objetos dentro del sistema.*

- **Control del flujo de información**. *Regula el flujo de datos dentro del sistema y su entrega a usuarios.*

- **Certificación**. *Se relaciona con probar que los mecanismos de acceso y control de flujo se desempeñen de acuerdo con sus especificaciones y que hagan cumplir la protección y las políticas de seguridad deseadas.*

Los niveles y técnicas de seguridad que son utilizados varían dependiendo del sistema operativo sobre el cual se trabaje; va a ser muy diferente que se este frente a sistemas Microsoft Windows 9x y Xp, que ante un 2000 Server o servidores Unix/Linux, los cuales son capaces de dar servicio a cientos de usuarios. Para cada máquina los tipos de acceso y técnicas de autenticación son distintos, al igual que los permisos sobre los datos a utilizar.

El software de control de acceso debe estar diseñado para que las terminales de usuario no puedan obtener acceso directo a las funciones del sistema operativo. Estas funciones incluyen acceso a las librerías de programas y a las diversas tablas del sistema. Debe haber un buen mecanismo para revisar la ocurrencia de cualquier operación inusual.
Los sistemas operativos más propensos a ser atacados son todos aquellos que tienen un Shell*, y con los que un usuario externo puede llegar a conectarse, para hacerse de la cuenta del administrador del sistema y de esta manera tener el control total sobre la máquina asaltada. El malicioso utilizará, en muchos casos, programas que circulan por Internet, que permiten tener el control de la máquina y que explotan errores en este tipo de sistemas operativos.*
Para los fines de esta tesis, trataremos la seguridad desde el punto de vista de sistemas operativos con tecnología Unix/Linux.

1.3 Redes e Internet

Las redes en general, consisten en un conjunto de ordenadores o computadoras que están unidas por un medio físico de transmisión de datos compartiendo recursos, distribuyendo el procesamiento de una tarea particular o intercambiando mensajes. No tan sólo la red es el medio de comunicación, sino que es un conjunto de elementos que hacen posible la existencia de los sistemas distribuidos mediante el intercambio y procesamiento de datos.
Las primeras redes utilizaban enlaces individuales, como las conexiones telefónicas para unir dos sistemas, pero tan pronto la primera PC de IBM impactó en el mercado en 1980 como herramienta empresarial, la solución más eventual fue la red de área local (LAN, Local Area Network). Una LAN tiene, generalmente, acotada su zona de operación dentro de un único edificio o, a lo más, en un campo de edificios adyacentes por las propiedades eléctricas de los cables utilizados para construirlas y por el número relativamente pequeño de computadoras que pueden compartir un único medio de transmisión. En la mayor parte de los casos, una LAN es una red de banda base con conmutación de paquetes construida mediante cables de cobre (par trenzado) que usan corrientes eléctricas estándar para transmitir señales. Otras alternativas son el cable de fibra óptica, el cual utiliza pulsos de luz para codificar datos binarios, ondas de radio, rayos infrarrojos y microondas.
Las LAN conectan computadoras utilizando varios tipos de configuraciones de cableado llamadas topologías, que dependen del tipo de cable usado y de los protocolos utilizados por los equipos.

Las topologías más comunes son las siguientes:

- **Bus**. *Consiste en un cable que va desde una computadora hasta la siguiente como una guirnalda, asemejando una tira de luces para árbol de Navidad. Cada señal transmitida por una computadora viaja a lo largo de la red en ambas direcciones hasta todas las demás. Sus desventajas se reflejan en que al haber una falla del cable en cualquier punto divide la red en dos impidiendo la comunicación desde un extremo a otro, pero sobre todo, encontrar un defecto de conexión en una red grande de este tipo puede ser problemático y llevar mucho tiempo. En cualquier caso, por diversos motivos la topología de bus no es la mejor opción. Por ejemplo, con una tecnología cliente-servidor (quizá en una intranet) las redes en bus proporcionan un rendimiento muy pobre; los* backbones *en bus convencionales sólo gestionan las transmisiones de una en una y presentan una alta tasa de colisiones, lo que es incompatible con las órdenes de transacciones cliente-servidor o las conexiones constantes entre hosts. Un gran tráfico web sobre una red tipo bus podría dar lugar a una degradación del rendimiento. Por último, la topología de bus es muy sensible a escuchas.*

- **Anillo**. *Esta topología es funcionalmente equivalente a la de bus con los dos extremos conectados entre sí, de modo que las señales viajan de una computadora a la siguiente en una propagación circular de nodo en nodo y en un solo sentido. Y al igual que en la topología de bus, mantiene al menos dos puntos de fallo: el servidor y el cable; si cualquiera de ellos deja de funcionar, todas las estaciones de trabajo pierden la conexión a la red. Además, en la topología en anillo las máquinas trabajan como repetidores por lo que si falla una estación de trabajo podría no haber comunicación entre el servidor y las demás estaciones. Y, como se puede deducir, esta topología ofrece varias entradas para los agresores, llevando a cabo ataques de denegación de servicio muy fácilmente y, de la misma manera, es muy vulnerable a escuchas electrónicas.*

- **Estrella**. *Esta topología utiliza un cable distinto para cada computadora que llega hasta un dispositivo central llamado* hub *o concentrador. El concentrador es el que propaga las señales que entran por cualquiera de sus puertos hacia todos los demás equipos. Una red en estrella es más tolerante a fallas que una de bus porque una interrupción en un cable afecta solamente al dispositivo al que está conectado el cable, no a la totalidad de la red. Por otro lado, las redes en estrella ofrecen ventajas de seguridad sobre las dos anteriores. Con un hardware de red avanzado se puede llevar a cabo una refinada segmentación y proteger el flujo de datos de cada estación de trabajo contra escuchas mediante cifrado. De las desventajas que presenta esta topología la más notoria es que su rendimiento puede empeorar bajo grandes cargas, sobre todo si se utilizan hubs de acceso por contienda en lugar de switches que separan los anchos de banda. Esto se debe a que cada transmisión debe pasar a través de una estación central.*

- **Malla**. *En esta topología se buscan muchos caminos para conectar a todos los equipos, es decir, cada máquina esta conectada individualmente con todas las demás computadoras que forman la red, de modo que si falla un camino se dispone de otro. La desventaja principal de esta topología es su costoso mantenimiento.*

Antes de elegir una topología, hay que tener en cuenta ciertos factores:

- *Si las estaciones de trabajo van a tener un software local.*
- *La convivencia de distintos sistemas operativos entre los segmentos de red*
- *Los protocolos que van a funcionar en la red*
- *Los requisitos de ancho de banda y distancia*

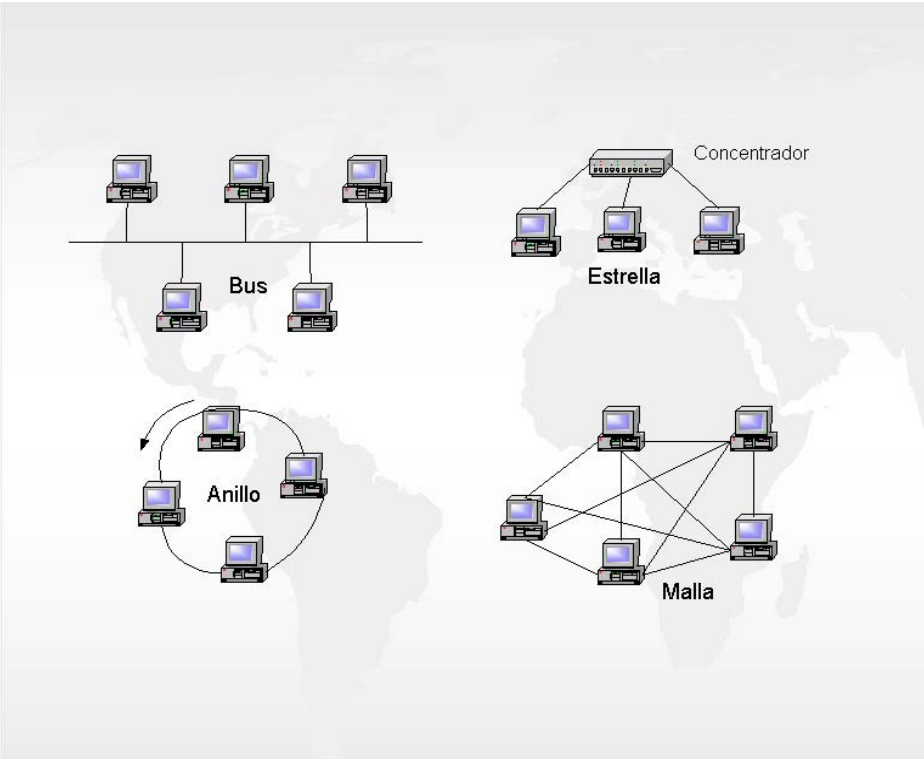


Fig. 1.4 Topologías comunes de cableado

1.3.1 Modelo de Referencia OSI

Las comunicaciones de red tienen muchos niveles y pueden ser difíciles de entender incluso para el administrador de red experto. El modelo de referencia de Interconexión de Sistemas Abiertos (Open Systems Interconnection u OSI) es un concepto teórico que separa las comunicaciones de red en siete niveles diferentes. Cada computadora de la red utiliza una serie de protocolos para realizar las funciones asignadas a cada nivel. En la parte más alta de la pila de protocolos o niveles está la aplicación que demanda un recurso localizado en cualquier otro sitio de la red y en la parte más baja, medios de transmisión, como los cables.

Los protocolos, que definen las comunicaciones entre las computadoras de una red, son lenguajes estandarizados que tienen en común los programas de dichas computadoras. Estos protocolos definen cada parte del proceso de comunicación, desde las señales transmitidas por los cables de red hasta los lenguajes que permiten que aplicaciones de máquinas diferentes intercambien mensajes. Además, los protocolos deben asegurarse de que las transmisiones alcanzan los destinos correctos y a su debido tiempo. Cada nivel del modelo OSI proporciona un servicio a los niveles que están directamente por encima y por debajo del mismo.

» **Nivel físico**. *Este nivel define el medio físico utilizado para transmitir los datos de una computadora a otra. El nivel físico incluye el tipo de tecnología utilizada para transportar los datos, el tipo de equipo que implementa esa tecnología, las especificaciones de instalación del equipo y la naturaleza de las señales que codifican los datos transmitidos. Uno de los estándares de nivel físico más usado para LAN es Ethernet, el cual define también cómo instalar el cable, incluyendo la longitud máxima de los segmentos y la distancia desde las fuentes de alimentación. Así, se puede ver que el nivel físico abarca mucho más que el tipo de cable porque se debe conocer todas las especificaciones que afectan al proceso como los estándares IEEE 802.3.*

» **Nivel de enlace**. *Este nivel es un intermediario entre la red física y la pila de protocolos de la computadora. Además, los protocolos de enlace incluyen un mecanismo de detección de errores y un indicador que especifica el protocolo de red que debe usar el sistema receptor para procesar los datos incluidos en el paquete. El protocolo de enlace de datos es el encargado de controlar el acceso al medio compartido e impedir un exceso de colisiones. Es necesario que el protocolo de enlace esté íntimamente relacionado con el nivel físico porque los mecanismos de control de acceso al medio dependen considerablemente del tamaño de las tramas y de la longitud de los segmentos de cable.*

» **Nivel de red**. *El protocolo del nivel de red es el principal portador, desde el origen hasta el destino, de los mensajes generados en el nivel de aplicación. Esto significa que, a diferencia del protocolo de enlace que solo se ocupa de que el paquete llegue a su próximo destino en la red local, el protocolo del nivel de red es responsable de todo el camino recorrido por el paquete, desde el sistema de origen hasta el destino final. El protocolo del nivel de red realiza funciones de direccionamiento, enrutamiento por Internet, fragmentación de paquetes, reensamblaje y comprobación de errores entre el sistema de origen y el de destino. Un protocolo del nivel de red acepta datos del nivel de transporte y los encapsula en un datagrama, añadiendo su propio encabezado. El protocolo más popular del nivel de red es el Protocolo de Internet o IP.*

» **Nivel de transporte**. *Una vez alcanzado el nivel de transporte, el proceso de llevar los paquetes a su destino ha dejado de ser una preocupación. Una de las funciones principales del protocolo de transporte es identificar tanto el proceso del nivel superior que generó el mensaje en el sistema origen, como el que recibirá el mensaje en el sistema destino. Por ejemplo, los protocolos de transporte del conjunto TCP/IP utilizan en sus encabezados números de puerto para identificar servicios de niveles superiores. Otras funciones que puede realizar el nivel de transporte son*

la detección y corrección de errores, el control de flujo, el asentimiento de recepción de paquetes y otros servicios de conexión.

- **Nivel de sesión**. *No hay protocolos independientes que operen exclusivamente en el nivel de sesión. En cambio, la funcionalidad de este nivel está incorporada en diversos protocolos, cuyas funciones caen también en la jurisdicción de los niveles de presentación y aplicación. NetBIOS (Network Basic Input/Output System), o Sistema básico de entrada/salida de red y NetBEUI (NetBIOS Extended User Interface), o Interfaz de Usuario Extendido de NetBIOS son dos de los mejores ejemplos de estos protocolos. La frontera del nivel de sesión es también el punto en el que se terminan todas las preocupaciones sobre la transmisión de datos entre dos sistemas. El nivel de sesión no se ocupa necesariamente de la seguridad, ni del proceso de inicio de sesión; en su lugar, las principales funciones de este nivel están relacionadas con el intercambio de mensajes entre los dos sistemas terminales (control y separación del diálogo).*

- **Nivel de presentación**. *El nivel de presentación gestiona el uso de una sintaxis de transferencia admitida por las dos computadoras conectadas, de modo que sistemas terminales de tipos diferentes se puedan comunicar. Las aplicaciones generan peticiones de recursos de red usando su propia sintaxis nativa, pero la sintaxis de la aplicación que recibe la petición, en el sistema destino, puede ser diferente en ciertos sentidos. La capa de presentación se responsabiliza de presentar los datos a la capa de aplicación. En ciertos casos, la capa de presentación traduce los datos directamente de un formato a otro. Una técnica habitual para mejorar la transferencia de datos consiste en convertir todos los datos a un formato estándar antes de su transmisión. Las normas OSI definen la Abstract Syntax Representation, Revision 1 (ASN.1 -Representación de sintaxis abstracta, revisión 1) como sintaxis estándar para los datos a nivel de la capa de presentación. Aunque el conjunto de protocolos TCP/IP no defina formalmente una capa de presentación, el protocolo External Data Representation (XDR -Representación de datos externos), utilizado por el sistema de archivos de red (NFS -Network File System), cumple una función similar. Otras funciones que pueden corresponder a la capa de presentación son la encriptación y desencriptación, así como la compresión y descompresión de datos.*

- **Nivel de aplicación**. *Como nivel superior de la pila de protocolos, el nivel de aplicación constituye el origen y destino de todos los mensajes transmitidos por la red. Todos los procesos analizados en las secciones previas son iniciados por una aplicación que demanda acceso a un recurso localizado en un sistema de la red. En la mayor parte de los casos, la distinción entre peticiones de archivos de la unidad de discos*

local y peticiones de archivos de red, la efectúa realmente un elemento del sistema operativo. Sin embargo, otras aplicaciones están diseñadas específicamente para acceder a recursos de red. Por ejemplo, cuando se ejecuta un cliente de FTP, la aplicación misma es inseparable del protocolo del nivel de aplicación que usa para comunicarse con la red.

Las interacciones entre los protocolos que operan en los distintos niveles del modelo de referencia OSI pueden ser extremadamente complejas. En la figura 1.5 se muestra la interacción entre los protocolos más comúnmente utilizados.

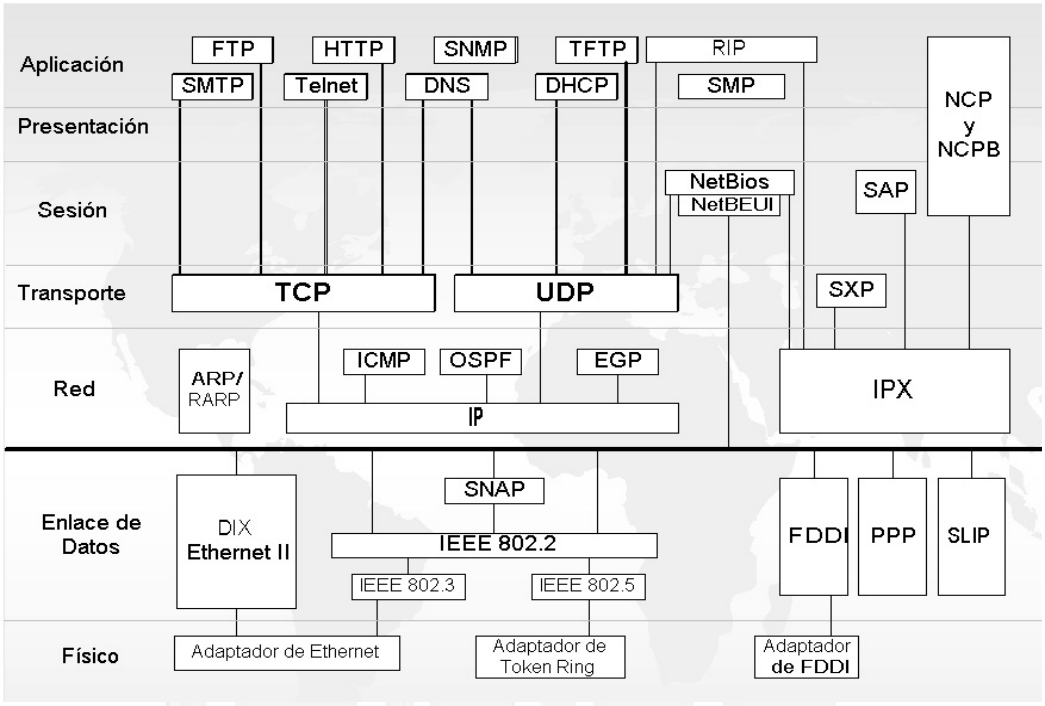


Fig. 1.5 Protocolos de red y modelo OSI

1.3.2 Problemáticas de las Redes

1. *Falta de continuidad (fallas en los medios de transmisión)*
2. *Mala planeación y diseño de la red*
3. *Crecimiento (aumento del número de nodos)*
4. *Un gran número de colisiones (cuellos de botella)*
5. *Lentitud en el servicio (sobrecarga de información)*
6. *Ancho de banda insuficiente para el número de usuarios*
7. *Difícil mantenimiento en redes muy grandes*
8. *Control de la seguridad en la red (intrusiones)*

Mejorar el rendimiento de una red implica contar con un buen diseño de la misma desde el principio, es decir, contemplar lo que se requiere para resolver

la primera necesidad del usuario, los crecimientos que se pueden alcanzar y tratar de proponer equipos en una solución que permita cambios tecnológicos.
*Debe considerarse que a mayor número de usuarios, es menor la posibilidad de transmitir información; dicho de otra forma, a mayor número de usuarios mayor cantidad de colisiones, lo cual derivará en una red lenta. Esto nos lleva a que las redes extremadamente grandes se deben segmentar en pequeños grupos para que, de esta manera, sea posible reducir la disputa por el medio de transmisión. El rendimiento de las redes también depende de los protocolos que se elijan para transportar la información, tanto del usuario como de las actualizaciones de la red, se deben escoger protocolos confiables y que generen poco tráfico (*overhead*). Sin embargo, la mejor estrategia para el rendimiento de la red es el monitoreo, pues si se hace de forma continua será capaz de modificar los patrones reales de comportamiento y lograr que se ajusten de manera adecuada con un alto grado de oportunidad.*

Por otro lado, cuando hablamos de la seguridad de una red, debemos tomar en cuenta que la red representa el punto de entrada para cualquier intruso que desee perjudicar las actividades que se realizan dentro de una organización. Por eso mismo, lo primero que se debe proteger de la infraestructura informática es la red, utilizando reglas de filtrado para que direcciones no conocidas no se puedan conectar a la misma. Los routers *son puntos críticos de ataques, una pasarela a través de la que los usuarios se comunican con el exterior y viceversa, por lo que si se consigue colapsar los routers, switches o hubs se puede denegar el servicio a muchos usuarios. La medida que puede tomarse para esto consiste en aislar el hardware de red de los usuarios locales que no tengan necesidad de tener acceso a él.*

1.3.3 Internet

La red Internet, una red que engloba miles de redes en todo el mundo, se desarrolló a partir de un experimento impulsado a principios de los años 70 por el Departamento de Defensa de los Estados Unidos, ya que se había definido el protocolo TCP/IP. Aunque parezca extraño, la idea era garantizar mediante este sistema la comunicación entre lugares alejados en caso de ataque nuclear; ahora, el TCP/IP sirve para garantizar la transmisión de los paquetes de información entre lugares remotos, siguiendo cualquier ruta disponible. Poco a poco todos los fabricantes de ordenadores personales y redes fueron incorporando el TCP/IP en sus sistemas operativos de modo que en la actualidad cualquier equipo está listo para conectarse a Internet.
En Internet las comunicaciones concretas se establecen entre el ordenador personal desde el que se accede y los servidores que hay en la red y proporcionan información. El fundamento principal sigue siendo TCP/IP, un protocolo de transmisión que asigna a cada máquina que se conecta un número específico, llamado número o dirección IP, el cual actúa como un número telefónico único, por ejemplo: 192.55.26.11. Toda Internet funciona a través del

protocolo TCP/IP y razones históricas hacen que esté muy ligado al sistema operativo Unix y todas sus variantes.
Los servicios más usuales que ofrece Internet son:

1. **Correo electrónico**. *El buzón de correo electrónico sirve para recibir y enviar mensajes a otros usuarios, por lo que nunca hay dos nombres iguales de dirección electrónica. El correo electrónico sirve también para enviar texto o archivos codificados como texto (gráficas u hojas de cálculo, etc.).*

2. **World Wide Web (WWW)**. *La WWW puede definirse como hipertexto, que es un sistema de enlaces de unos lugares a otros; multimedia, que hace referencia al tipo de contenidos que puede manejar (Texto, gráficos, video, sonido y otros) e Internet, la base sobre la que se transmite la información. El aspecto exterior de la WWW son las conocidas "páginas Web" situadas en servidores de todo el mundo y a las que se accede mediante un programa denominado "navegador" (browser) que emplea un protocolo llamado HTTP, una ventana muestra al usuario la información que desea.*

3. **FTP**. *Es un sistema de transmisión de archivos en el que enviar y recibir archivos de gran tamaño de un lugar a otro de Internet es rápido y más cómodo que mediante el correo electrónico. Los servidores FTP también se emplean para la distribución de software de demostración, revistas electrónicas, etc. Los servidores FTP pueden ser privados pero por lo general son públicos y se accede a ellos mediante un URL (Localizador Uniforme de Recursos) de acceso (que indica el directorio donde se encuentran los archivos).*

4. **Telnet**. *Sirve para conectarse de forma remota a un ordenador (generalmente Unix) desde un programa terminal. Se puede trabajar con ese ordenador como si se estuviese sentado frente a una terminal local, aunque se encuentre en la otra punta del mundo.*

5. **Buscadores**. *Son una novedosa categoría de servicio. Se trata de sistemas (motores de búsqueda) que organizan la información de Internet y permiten buscarla por palabras y/o por contexto.*

Desde el punto de vista de la arquitectura de una infraestructura, Internet representa el punto de enlace más importante para toda la red local de una organización puesto que es desde el acceso a Internet que se tiene conexión con muchos sitios de la red local y los mismos servidores. Además, es importante destacar que los ataques externos hacia la seguridad provienen precisamente de Internet, por esta razón se considera indispensable proteger toda la infraestructura informática utilizando barreras que impidan el acceso a la red

interna a personas no autorizadas o haciendo uso de la encriptación de datos que viajan a través de la red con el fin de que la confidencialidad de la información no se vea alterada.

1.3.4 Seguridad en Redes e Internet

En cualquier tipo de red, y por supuesto en Internet, la seguridad es siempre un factor que se debe tomar en cuenta a la hora de administrar la propia red y sus computadoras. Dicho de manera muy simple, todos los mecanismos de seguridad proporcionados por los diversos componentes de una red están diseñados para proteger el hardware, el software y los datos del sistema de daños accidentales o del acceso no autorizado. El objetivo del proceso de administración de seguridad es proporcionar a los usuarios acceso a todos los recursos que necesitan, mientras se les aísla de los que no necesitan. Hay muchos mecanismos diferentes de seguridad en la red media, algunos de los cuales son invisibles para los usuarios e incluso para los administradores, y muchos de ellos son proporcionados por el propio sistema operativo que maneja la red.
Hay dos formas básicas de seguridad que se pueden aplicar al sistema de archivos de los equipos conectados a una red:

a) *Control de acceso, por medio de permisos otorgados por el propio administrador*
b) *Cifrado de datos, por medio de encriptación*

Internet es un medio por el cual se publica una infinidad de información y es por eso que también se convierte en un blanco perfecto para ataques que ocasionan contaminación por virus, alteración o pérdida de registros en diversos sitios Web. Aunado a esto, cabe mencionar que Internet conecta diversas instituciones comerciales, gubernamentales, académicas, etc. a nivel mundial por lo que la inseguridad en esta enorme red no puede estar garantizada, lo único que la salva es la implementación de diversos mecanismos de seguridad transitando por ella, aunque no se vuelve segura completamente.
El factor que diferencía a las redes de tipo educativo de otras de carácter financiero, militar o de empresas privadas o públicas, es que su objetivo es estar abiertas al cambio de experiencia; por ejemplo, que los alumnos puedan consultar sus datos académicos desde su casa a través de Internet hace muy difícil la conciencia de los problemas de seguridad por la excesiva apertura que supone.

1.4 Bases de Datos

Una base de datos es un conjunto o colección de datos almacenados de forma no volátil (no se pierden), estructurados y relacionados entre sí, los cuales suelen sufrir actualizaciones (altas, bajas, cambios y consultas). Dichos datos no tienen significado por sí solos, pero en conjunto y después de ser procesados producen información productiva. El contenido de una base de datos engloba a la información concerniente (almacenadas en archivos) de una organización, de tal manera que los datos estén disponibles para los usuarios. El objetivo de almacenar y organizar datos en una base de datos es representar las relaciones entre las distintas entidades de interés para la empresa o institución; además, organizar los datos de esta forma facilita la integración de las áreas dentro de la empresa. Para la mayoría de las empresas la única forma eficaz de lograr el nivel de apoyo deseado a los sistemas de información es mediante la administración de bases de datos.

Una base de datos esta formada por tablas estructuradas y relacionales:

- **Tabla**. *Entidad que tiene características propias o atributos que definen a la entidad. Todas las entidades son diferentes.*
- **Campos**. *Son los atributos de la entidad o tabla.*
- **Registros**. *Son los datos almacenados estructuradamente en los campos de una entidad.*
- **Relación**. *Es la característica de que dos o más entidades tengan al menos un atributo o campo en común.*

Normalmente la definición de base de datos se realiza en forma de requerimientos u objetivos que ésta debe cumplir. Los requisitos que debe cumplir un buen sistema de base de datos son:

- **Acceso múltiple**. *Diversos usuarios pueden acceder a la base de datos, sin que se produzcan conflictos ni visiones incoherentes.*
- **Flexibilidad**. *Se podrán utilizar distintos métodos de acceso, con tiempos de respuesta razonablemente pequeños.*
- **Confidencialidad y seguridad**. *Se debe controlar el acceso a los datos (a nivel de campo), impidiéndolo a los usuarios no autorizados*
- **Protección contra fallos**. *Deben existir mecanismos concretos de recuperación en caso de fallo de la computadora o servidor.*
- **Independencia física**. *Debe ser posible cambiar el soporte físico de la base de datos (modelo de discos, por ejemplo), sin que esto repercuta en la base de datos ni en los programas que la usan.*
- **Independencia lógica**. *Es posible modificar los datos contenidos en la base, las relaciones existentes entre ellos o incluir nuevos datos, sin afectar a los programas que las utilizan.*
- **Redundancia controlada**. *Los datos se almacenan una sola vez.*

- **Interfaz de alto nivel**. *Existe una forma sencilla y cómoda de utilizar la base, desde un lenguaje de programación de alto nivel.*
- **Interrogación directa (query)**. *Existe una utilidad que permite el acceso a los datos de forma convencional.*

1.4.1 Sistema Manejador de Bases de Datos

Un Sistema Manejador de Bases de Datos (DBMS) es un programa que hace posible la creación, empleo y el mantenimiento de bases de datos. Sin embargo, como es independiente de la aplicación puede utilizarse en una gran variedad de entornos. Esto es, no depende de ningún programa de aplicación o archivo específico, pero se puede usar para hacer que los datos estén disponibles para varios programas de aplicación. Un DBMS se define por sus peculiaridades, las cuales incluyen las aptitudes para desarrollar estructuras de datos, definir datos e interrogar y actualizar la base de datos después de que ha sido creada, así como de manejar las definiciones de la estructura de almacenamiento.
En el procesamiento de los datos según se especifica en los programas de aplicación, el DBMS funge como una interfaz entre el programa y los datos almacenados. El proceso ocurre de la siguiente manera:

1. *Los programas de aplicación y/o sistemas de información solicitan ayuda al DBMS para recabar los datos requeridos para el procesamiento. Todas las solicitudes de ayuda se hacen por medio de los comandos del lenguaje de manipulación de datos.*
2. *El DBMS acepta y examina la solicitud. Se efectúa una comparación con el fin de asegurarse de que los datos que se solicitan hayan sido definidos con acierto en el esquema y en subesquema.*
3. *El DBMS solicita operaciones de entrada/salida del sistema operativo de la computadora.*
4. *El sistema operativo a su vez accede al dispositivo de almacenamiento secundario correspondiente para transferir los datos al buffer (memoria auxiliar) de entrada/salida del sistema de cómputo.*
5. *El DBMS lleva los datos de buffer al área de trabajo del usuario según lo solicitado en los comandos iniciales para el manejo de datos*
6. *Los datos en el área de trabajo del usuario se procesan de acuerdo con las instrucciones contenidas en el programa de aplicación o sistema de información correspondiente.*

1.4.2 Problemáticas que Presentan las Bases de Datos

1. *Duplicidad de los datos, es decir, redundancia*
2. *Falta de integridad de los datos*
3. *Tiempos largos de respuesta o consultas*

4. *Incompatibilidad de las plataformas y el DBMS*
5. *Mala visión del crecimiento de la base de datos, definición del espacio*
6. *La migración de la base de datos hacia otra plataforma o DBMS*
7. *Diseño de un mal esquema de respaldos y replicación*
8. *Falta de indexación.*
9. *La seguridad de los datos, establecimiento de permisos y accesos*
10. *Mala planeación del espacio para la segmentación (creación de temporales)*

Todas estas problemáticas que presentan las bases de datos son, en la mayoría de las veces, ocasionadas por la mala administración y planeación del administrador. Sin embargo, el Sistema Manejador de la Base de Datos puede causar ciertos problemas si desde un principio no se diseña adecuadamente la base de datos.
La configuración lógica de una base de datos tendrá un enorme efecto sobre su rendimiento y facilidad de administración. Como producto final de una aplicación de bases de datos, se tendrá una herramienta que administre información (un sistema de información, por ejemplo), por lo que el objetivo principal será configurar la base de datos de manera que los objetos queden separados por uso (segmentación).

1.4.3 Aspectos de Seguridad

En tanto que las medidas de respaldo ayudan a proteger contra la pérdida de los datos, las medidas de seguridad están orientadas a preservar la información impidiendo cualquier intromisión que pudiera conducir a la destrucción de archivos y de bases de datos. En otras palabras, la seguridad se refiere al acceso ilegal a los archivos de la computadora, ya sea físicamente o por infiltración (hacking) en un sistema en línea, con el propósito de destruir, modificar o tener acceso a los datos sin permiso. La confidencialidad o privacía entraña el derecho de controlar la distribución o la divulgación de los datos.
Everest identificó en 1972 tres estrategias de protección para las bases de datos: el confinamiento (alojamiento de los datos en una ubicación física a la que no tengan fácil acceso personas no autorizadas), la reglamentación (determinar quién debe tener acceso a los datos) y el cifrado de la información.
Cada medida de protección implica una transacción en términos de costos y beneficios. La seguridad de los datos es costosa puesto que requiere equipo y tiempo. Por ello el personal de sistemas y los directivos tiene que decidir hasta qué punto el costo de la seguridad excede al valor de los datos que protegen.

Y dado que las bases de datos son el producto de los sistemas de información y otras aplicaciones, expondremos ahora todo lo que a ellos se refiere.

1.5 Sistemas de Información

Los sistemas de información son sistemas hechos por el ser humano, los cuales interactúan con una o más computadoras o son controlados por ellas para realizar una tarea específica; para ello están estrictamente relacionados con el hardware, el software, los programas de aplicación, las personas o usuarios que operan el sistema, los datos con los cuales trabaja el sistema y los procedimientos que son las políticas formales e instrucciones de operación del sistema. Todos ellos se interrelacionan con la finalidad de soportar las operaciones y la toma de decisiones oportunas y eficaces de una organización. Los sistemas de información son sistemas computarizados que optimizan la recolección, transferencia y presentación de la información de una organización, a través de una estructura integrada de bases de datos y flujos de información, los cuales proporcionan a los responsables de las decisiones informes sobre pedido y capacidad de consulta, así como informes periódicos de rutina.
Estos sistemas normalmente están relacionados unos con otros, puesto que las salidas de un sistema pueden ser transacciones de entrada para otro sistema y algunas veces comparten una base de datos que ayuda a reducir la redundancia de los datos y permite a las distintas áreas coordinar sus actividades con mayor eficiencia. Los sistemas de información se clasifican del siguiente modo:

- **Sistemas de Procesamiento de Transacciones**. *Estos sistemas procesan los datos referentes a las actividades de la empresa, por ejemplo, ventas y movimientos de almacén e inventarios. Las cinco razones para el procesamiento de las transacciones son la clasificación, cálculo, distribución u ordenación, resumen y el almacenamiento de los datos.*

- **Sistemas de Información Gerencial**. *También llamados sistemas de reportes de gerencia se enfocan al apoyo para la toma de decisiones cuando los requerimientos de información pueden ser identificados de antemano. En otras palabras, la información que un administrador o un usuario final necesita puede ser determinada después de un análisis minucioso de la situación.*

- **Sistemas de Apoyo a Decisiones**. *No quiere decir que estos sistemas tomen decisiones por sí mismos, sino que ayudan a los administradores y otros profesionistas a tomar decisiones inteligentes y documentadas. Son sistemas operacionales y se conocen también como sistemas de procesamiento de transacciones, por ejemplo, sistemas de nómina, de inventarios, etc. No sólo recuperan y exhiben los datos sino que también realizan varios tipos de análisis matemáticos y estadísticos de los mismos.*

Además tienen la capacidad, en la mayoría de los casos, de presentar la información en una variedad de formas gráficas o reportes.

- **Sistemas basados en el conocimiento**. *También llamados sistemas expertos, se asocian con el campo de la Inteligencia Artificial. Un sistema experto es un programa de cómputo que utiliza hechos (datos) almacenados y reglas para imitar a un experto humano. Están diseñados para recomendar una decisión específica, sugerir acciones o hacer predicciones.*

- **Agentes de software**. *Los agentes de software, al igual que los sistemas expertos, son un tipo de Inteligencia Artificial y son sistemas que reaccionan para satisfacer las exigencias de una meta determinada.*

Importancia de los sistemas de información:

1. **La información**. *La mayoría de los trabajadores en la actualidad pasan el tiempo creando, distribuyendo o utilizando información. La información es el activo más valioso de toda organización y debe estar a la altura de las tareas que se realizan y de las decisiones que se toman.*
2. **El ritmo rápido de cambio**. *Mantenerse al día es una preocupación continua de la gerencia para trazar el curso a seguir por sus respectivas organizaciones, departamentos u oficinas que les permitirán lograr las metas y los objetivos en forma apropiada.*

3. **La creciente complejidad de la administración**. *Debido en parte al ritmo de vida de una organización y en parte al alcance y dimensión de las tareas administrativas, el trabajo de la gerencia está creciendo en complejidad; por la seguridad de los trabajadores, la calidad de los productos o servicios ofrecidos y una competencia real. Todo lo anterior, añade una nueva dimensión a la toma de decisiones administrativas.*

4. **La interdependencia de las unidades de la organización**. *Dado que todas las actividades están relacionadas, los éxitos y los problemas en una parte de la organización afectan a las actividades en otras partes de la misma. Es evidente que las organizaciones también son sistemas, cuyas áreas persiguen objetivos comunes. La información es el ingrediente que mantiene unidos a las áreas del sistema organizacional.*

5. **El mejoramiento de la productividad**. *La productividad es la aptitud para incrementar la eficacia de un proceso. Los sistemas de información computarizados, desarrollados y utilizados adecuadamente, pueden mejorar la productividad aumentando el volumen de trabajo realizado y la velocidad con la cual se ejecutan las transacciones.*

6. **El reconocimiento de la información como un recurso**. *La información es reconocida como un recurso para la organización. Tiene valor porque influye en la manera como opera la empresa. Carecer de información vital puede ocasionar que los administradores cometan errores, pierdan oportunidades y se enfrenten a graves problemas de rendimiento. Los sistemas de información también son un recurso que hace posible lograr nuevos niveles de eficacia.*

Un sistema de información efectivo que puede producir la información correcta para la persona indicada en el tiempo necesario, apoyando la toma de decisiones correcta, se ha vuelto uno de los factores competitivos más importantes en estos días.

Al diseñar un nuevo sistema es necesario considerar la flexibilidad que presentan las estructuras de datos, para asegurar que la información siempre estará disponible con un adecuado nivel de seguridad. Algunos medios físicos proporcionan seguridad por sí solos, pero en los sistemas de actualización en línea pueden establecerse algunos procesos adicionales y software complementario para controlar los accesos y las actualizaciones de los datos almacenados.

En el futuro, las organizaciones desarrollarán estrategias bajo las cuales los sistemas de información serán considerados en toda la organización y no sólo para tareas individuales. Muchos de los recursos necesarios para lograrlo están ya preparados. Los sistemas de bases de datos, los métodos de comunicación de datos y el continuo surgimiento de estándares de comunicación de datos facilita aún más esta tendencia.

"Como administrador de recursos, el Sistema Operativo de un sistema computacional, es un elemento estratégico en la protección de todo tipo de servicios de infraestructura informática, así como de las aplicaciones que son usadas con mayor frecuencia por un usuario final".

CAPÍTULO 2
Seguridad Informática

Introducción

Una vez descritas las características de los sistemas operativos y de los componentes de una infraestructura informática, es indispensable resaltar la importancia del aspecto que más repercute sobre ellos: su seguridad. La seguridad informática es la mayor preocupación que hoy en día enfrentan todas las organizaciones y por eso es fundamental dar a conocer los aspectos más importantes que la constituyen, así como sus diferentes niveles, sus elementos y sus aplicaciones, considerando las aplicaciones y servicios que brindan los sistemas informáticos.

A pesar de que siempre se persigue que las infraestructuras informáticas cuenten con un nivel de seguridad muy alto, es imposible que exista un sistema cien por ciento seguro, siempre habrá riesgos que pongan en peligro la integridad de la información.

2.1 Visión Global de la Seguridad Informática

Con la introducción de la computadora y la automatización de procesos se hizo evidente la necesidad de herramientas que permitieran proteger archivos y todo tipo de información que se almacena en los ordenadores. Podemos entender como seguridad una característica de cualquier sistema (informático o

no) que nos indica que está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Para ello debe ser capaz de predecir los posibles ataques y problemas que pudieran surgir y con ello garantizar que el sistema pueda estar en funcionamiento las 24 horas al día, los 365 días del año, si es que fuera necesario. El nombre genérico para la descripción de las herramientas diseñadas con el fin de proteger datos y desalentar los hurtos y malos usos de dicha información es seguridad informática*.*

"La implementación de seguridad total en un sistema tendría un coste infinito, valorado en horas de trabajo y recursos económicos para la empresa" [1].

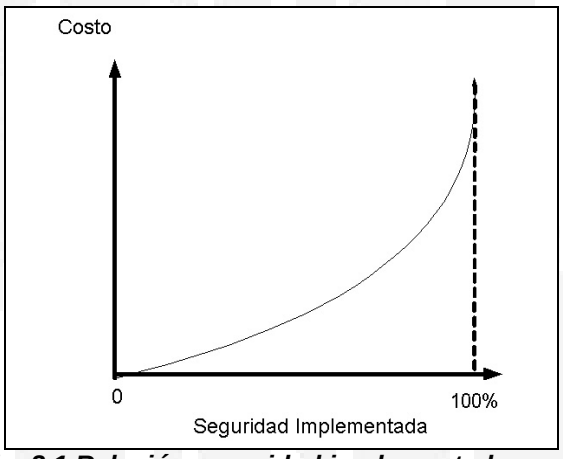


Fig. 2.1 Relación seguridad implementada-coste

Es inconcebible en términos de costo económico proteger, monitorear, auditar y actualizar en tiempo real un sistema de cómputo, por lo que lo que se tiende a realizar, y se hace en realidad, es estudiar las posibles debilidades conocidas de nuestras máquinas y sobre ellas aplicar las medidas de seguridad correspondientes. Además, periódicamente estas medidas deben ser revisadas y reajustadas si otras vulnerabilidades han aparecido o han sido dadas a conocer. Entonces procedemos a decir que un sistema es fiable, es decir, es un sistema que se comporta tal y como se espera de él; para nosotros será un sistema que, tras revisarlo y estudiarlo ha sido protegido de las amenazas conocidas que pudieran actuar sobre él. Pero no se debe de olvidar que un sistema 100% fiable no existe, ni existirá por las razones antes mencionadas.

El principal desafío (y riesgo) para la seguridad está representado no por la tecnología sino por la gente involucrada, desde un administrador sin una preparación adecuada o sin la suficiente experiencia, hasta un guardia de seguridad que ni siquiera tiene acceso lógico al sistema, pero que deja acceder a todo el mundo a la sala de operaciones, pasando por supuesto por la gran mayoría de usuarios, que no están conscientes de que la seguridad también les concierne a ellos. Obviamente todos los sistemas de cómputo son vulnerables a

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

desastres, accidentes, sabotaje y mala planeación. Por lo tanto es necesario, decidir qué información no debería estar disponible para todos. Esto es, la clasificación de información sensitiva requiere ser formalizada.

A grandes rasgos se entiende que la seguridad consiste básicamente en garantizar tres aspectos:

1. **Confidencialidad**. *Implica que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a él y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades externas.*

2. **Integridad**. *Consiste en que el contenido del sistema computacional, es decir, que los datos puedan ser modificados únicamente por el personal debidamente autorizado. La modificación incluye escritura, cambios, cambio de estado, borrar y crear nuevos datos a partir de los actuales.*

3. **Disponibilidad**. *Indica que toda aquella información contenida en el sistema permanezca accesible (disponible) para todo el personal autorizado. La disponibilidad es lo contrario de la negación del servicio.*

Ahora, los cuatro elementos principales a proteger en cualquier sistema informático son:

1. **El hardware**. *Es el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes) o tarjetas de red. El hardware es el más vulnerable para atacar y el menos dócil para aceptar controles automáticos. Sus principales amenazas incluyen daños accidentales y deliberados al equipo y por supuesto, robo.*

2. **El software**. *Es el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones; éste es muy fácil de borrar, sobre todo el software de aplicación. El software también puede alterarse, modificarse o dañarse para volverlo inútil. Los virus computacionales y cualquier tipo de ataque relacionado con ellos caen en esta categoría.*

3. **Los datos**. *Es el conjunto de información lógica que manejan el software y el hardware, como paquetes que circulan por un cable de red o entradas de una base de datos. Los aspectos de seguridad con respecto a datos son muy amplios, pues abarcan la confidencialidad, la integridad y la disponibilidad; por ejemplo, la destrucción de archivos accidental o maliciosa, la lectura no autorizada de archivos de datos, etc.*

4. **Las líneas de comunicación y las redes**. *Se consideran dentro de este rubro las líneas telefónicas y las redes de comunicación.*

Generalmente en las auditorías de seguridad se habla de un quinto elemento a proteger, los fungibles *(elementos que se gastan o desgastan con el uso continuo, como papel de impresora, tóners, cintas magnéticas, diskettes, etc.)*

Por otro lado, la seguridad global debe implementarse en distintos módulos:

- **Canales de comunicación**. *Protección de los canales de comunicación externos a través del cifrado de la información, firmas digitales, VPN, etc. Ya que el canal de comunicaciones es sensible a la posibilidad de que la red esté monitoreada (*sniffers*), pudiéndose así realizar una modificación de la información capturada o una suplantación de identidad.*

- **Arquitecturas externas de acceso público**. *Protección de los sistemas de acceso público como los servidores Web, de correo, de aplicaciones, DNS, etc. Las acciones para proteger estos servicios suelen realizarse mediante políticas de seguridad en los* router, *implementación de* firewall *e IDS (Sistemas de Detección de Intrusos).*

- **Arquitecturas internas de acceso privado**. *Protección de sistemas, redes y aplicaciones. Implementación de seguridad para el* host, *redes, políticas de usuarios, accesos a bases de datos seguras, protección antivirus, troyanos, etc.*

- **Seguridad física de los sistemas de IT (Tecnologías de la Información)**. *Protección de sistemas físicamente. Implementación de medidas biométricas como puede ser la verificación de voz, escritura, huellas digitales, patrones oculares (retina e iris) o geometría de la mano entre otras.*

La seguridad informática ya no sólo es una serie de herramientas, sistemas, fórmulas matemáticas (criptografía) y protocolos, sino también un conjunto de obligaciones legales que están establecidas en nuestro ordenamiento jurídico, como la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico LSSI. En esta ley se exige al prestador de servicios una responsabilidad sobre los contenidos almacenados, ya que se otorga el mismo valor jurídico a contratos firmados electrónicamente que a otros con soporte documental y cuya pérdida o variación de su integridad podrían llevar de la mano sanciones tanto administrativas como judiciales.

Los tipos de amenazas a la seguridad de un sistema computacional o red se identifican mejor observando la función del sistema que va a proporcionar

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

información. En general, existe un flujo de información desde una fuente (un archivo o una región de la memoria principal) a un destino (otro archivo o un usuario). Son cuatro las categorías de amenazas:

- **Interrupción**. *Una parte del contenido del sistema se destruye, se torna inutilizable o ya no está disponible. Esta es una amenaza a la* disponibilidad. *Algunos ejemplos incluyen la destrucción de un equipo de hardware, como un disco duro, el rompimiento de una línea de comunicación o la deshabilitación del sistema de administración de archivos.*

- **Intercepción**. *Una parte no autorizada consigue acceder al contenido del sistema. Esta es una amenaza a la* confidencialidad *y la parte no autorizada podría ser una persona, un programa u otra computadora. Los ejemplos en este caso incluyen intervención de las conexiones para capturar datos en una red y la copia ilícita de archivos o programas.*

- **Modificación**. *Una parte no autorizada o intruso no sólo consigue acceder a nuestro sistema si no que altera en forma indebida una parte del contenido del sistema, es decir los datos y la información almacenada. Esta es una amenaza a la* integridad. *Los ejemplos incluyen cambiar valores en un archivo de datos, alterar un programa de manera que se ejecute en una forma diferente y modificar el contenido de mensajes que se transmiten en una red.*

- **Fabricación**. *Un intruso o malhechor inserta objetos falsificados en el sistema y es también una amenaza a la integridad. Los ejemplos incluyen la inserción de mensajes impuros en una red o la adición de registros a un archivo.*

Los mecanismos de seguridad se dividen en tres grandes grupos:

1. *Los mecanismos de* **prevención** *son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema Unix en la red.*

2. *Los mecanismos de* **detección** *son aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como Tripwire.*

3. *Los mecanismos de* **recuperación** *son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su*

funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional.

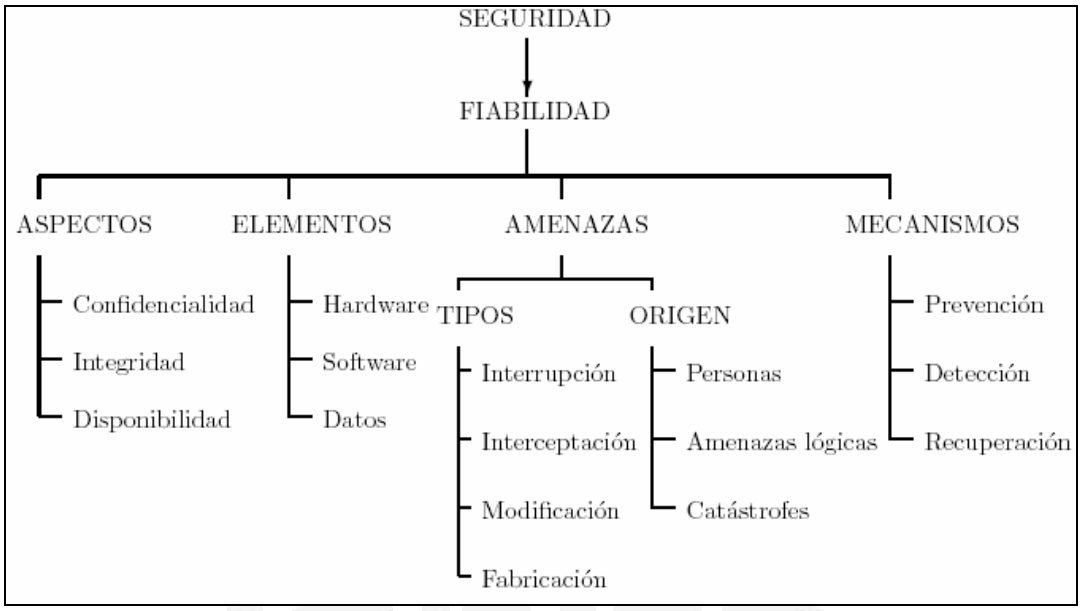


Fig. 2.2 Visión global de la seguridad informática

2.2 Riesgos y Vulnerabilidades

Podemos definir el riesgo como la posibilidad de que ocurra algún evento negativo en contra de una organización, derivado de factores como su propio personal, su actividad, su situación económica, la asignación de sus recursos financieros o la tecnología utilizada en sus procesos. Así, el riesgo es definido como:

Riesgo = valor del activo * amenaza * vulnerabilidad

Donde:

- **El valor del activo** *es la importancia de la información para la estrategia de la empresa. En un ambiente computacional, los posibles activos sujetos a evaluación serían los servicios.*

- **Las amenazas** *son los sucesos o las acciones que podrían tener un impacto negativo en la disponibilidad, integridad o confidencialidad de la información. Por* amenaza *se entiende cualquier persona, lugar o cosa con suficiente potencial para obtener acceso a los recursos y causar daños. Su origen se sitúa en dos fuentes principales: los humanos y las catástrofes.*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

» **La vulnerabilidad** *es la ausencia, inadecuación o incoherencia de las utilidades y los procesos implementados para proteger el valor del activo frente a las amenazas identificadas. Una* vulnerabilidad *(punto vulnerable) es un punto donde se manifiesta una amenaza para un activo, algo así como una debilidad. Las vulnerabilidades casi siempre se deben a fallas tecnológicas en la implementación del software o del hardware, o bien al diseño o la arquitectura del sistema. De cierto modo, una vulnerabilidad es un punto débil o un agujero en la seguridad que aprovechan los atacantes maliciosos para obtener acceso a la red o a los recursos de ésta.*

Los equipos de cómputo que habitualmente se utilizan están sujetos a riesgos de que ocurra alguna eventualidad que los dañe y el costo de asumirla puede ser muy alto si se considera que muchas veces no basta con reponer el equipo. Es evidente que la exposición de cualquier organización al riesgo también esta directamente relacionada con sus actividades, y su solución de seguridad debería depender precisamente de esa base de actividades. Para valorar los riesgos de seguridad, no basta con buscar agujeros en el sistema, en la red y en el software de aplicación. Hay que comenzar por conocer el riesgo.

Existen dos tipos de riesgos: riesgos externos y riesgos internos.

1. **Riesgos externos**. *Se definen como todos aquellos que se presentan en el ambiente físico y social que rodea una instalación de procesamiento de información. Los riesgos externos pueden ser naturales como las inundaciones, terremotos, incendios, erupciones volcánicas, etc.; o provocados por el hombre como explosiones, bombas, sabotaje, robos, fraude, etc.*

2. **Riesgos internos**. *Los riesgos internos se generan desde la misma empresa y es más fácil que se presenten ya que el conocimiento de los procedimientos internos de operación hace más sencillo el camino de alguna persona interesada en dañar a la institución. Los riesgos internos pueden ser robo (de material, de información y/o de recursos), sabotaje, destrucción de datos o equipos, huelgas, fraudes, etc.*

2.2.1 Análisis de Riesgos

El objetivo general del análisis de riesgos es cuantificar los riesgos a que están sujetos los activos de una empresa, la pérdida esperada y el costo de tomar medidas de control. Este costo debe ser menor a la pérdida esperada. Un proceso de análisis de riesgos permite establecer dónde se requiere mayor seguridad y los costos de implantar las medidas necesarias, es decir, debe evaluar y comparar las necesidades y los costos para ser una excelente

herramienta de administración mediante la cual puedan determinarse las prioridades y los recursos adecuados a fin de reducir los accidentes.

Los objetivos específicos de un análisis de riesgos son:

1. *Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas, los cuales dependerán del tipo de riesgo considerado. Se debe tomar en cuenta que muchas veces se incrementa la pérdida por la interrupción de labores o bien que puede existir una pérdida de oportunidades para la empresa si ésta toma mucho tiempo. Los recursos actualmente disponibles ayudarán a contrarrestar los gastos y deben considerarse dentro del análisis.*

2. *Determinar cuáles son los activos existentes por medio de un inventario detallado. Además se deben evaluar los costos de las pérdidas potenciales y cuantificar los costos de reposición y reparación.*

3. *Llevar a cabo un minucioso análisis de los riesgos y vulnerabilidades: identificar las fuentes, alcances, métodos y amenazas potenciales; estimar la probabilidad de cada ocurrencia. También se deben identificar las debilidades potenciales y todos los tipos de amenazas y vulnerabilidades.*

4. *Identificar, definir y revisar todos los controles de seguridad ya existentes (las defensas existentes), así como los recursos del sistema.*

5. *Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados. Definir cuáles son las medidas a implantar y las ventajas y desventajas de cada decisión.*

Existen otros enfoques, no cuantitativos, del análisis de riesgos. Las técnicas de simulación, por ejemplo, intentan probar ciertos riesgos que existen en el procesamiento de datos, determinando cuáles son las medidas existentes y dónde son necesarios controles adicionales.
Las técnicas cualitativas únicamente indican, en términos relativos y sin llegar a una cuantificación, la pérdida que ocasionaría cierta eventualidad, comparada con otra.
Generalmente un enfoque cuantitativo es adecuado para un equipo de cómputo grande y centralizado. Por otro lado, un enfoque cualitativo es más adecuado para una red distribuida o con pequeños subsistemas, ya que permite fragmentar el riesgo y los problemas pueden ser localizados más fácilmente.

El método de análisis propuesto está basado en los modelos desarrollados por IBM e incluye las siguientes etapas:

1. *Asignar un valor a los datos procesados (o información) y a los servicios ofrecidos por las aplicaciones. El análisis se realiza a nivel de usuario,*

 [1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

quien es responsable de la aplicación y determina el valor de un servicio, así como la información necesaria para prestar dicho servicio. Éste análisis de valor está limitado al racionamiento de las propiedades de facilidad de acceso, carácter confidencial y autenticidad.

- *Identificar el hardware, software y recursos internos de la computadora.*
- *Asignación de valores o costos de los distintos recursos*

2. *Analizar los peligros que amenazan a los recursos computacionales. Se debe elaborar una lista de accidentes potenciales y determinar la incidencia de los mismos.*
3. *Determinar las necesidades de protección y sugerir medidas de seguridad apropiadas.*

2.3 Seguridad Física

El hardware es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial, esto implica una protección a la información de nuestro sistema, tanto a la que está almacenada en él como para la que se transmite entre diferentes equipos. Por tal motivo, la seguridad física debe ser el primer objetivo.

Básicamente la seguridad física de los equipos de cómputo se basa en:

1. **Ubicación del site y/o de los servidores, así como el acceso a ellos**. *Casi todos los sistemas de computación son vulnerables a ataques en su propio sitio de ubicación y se ha estimado que el 80% de las intrusiones provienen del personal interno de la organización. Es por ello que, para minimizar la probabilidad de ser víctimas de robo o usuarios malintencionados, se recomienda situar el centro de cómputo fuera de la vista y debe ser tan inaccesible como sea posible, los usuarios que no lo requieran no deben saber dónde se encuentra el almacén de información ni mucho menos el área de servidores. En ocasiones merece la pena llevar un registro escrito de acceso y ordenar que incluso el personal autorizado firme al entrar y al salir.*

El centro de operaciones de red (NOC) es el área donde se encuentran los servidores y debe ser restringida y cumplir con los siguientes requisitos:

- » *Debe encontrarse dentro de un espacio alejado del público, de preferencia que no sea la planta baja del edificio*
- » *La sala y los pasillos que conducen al NOC deben ser totalmente opacos, sin puertas de cristal*
- » *Se deben mantener todos los dispositivos de almacenamiento en un lugar seguro, o aún mejor, en otro lugar distinto del NOC*
- » *Si se emplea vigilancia (circuito cerrado de TV o imágenes secuenciales instantáneas) es recomendable dirigir la señal desde la cámara hasta un VCR remoto.*

2. **Topología de la red**. *Dado que la topología de la red determina el modo en que se conectan los dispositivos de hardware y la forma en que fluye la información a través de dichas conexiones tiene claras implicaciones de seguridad. Al elegir una topología hay que tener en cuenta tres riesgos:*

    - » Punto único de fallo. *Es un punto al que se conectan uno o varios dispositivos de red*
    - » Susceptibilidad de escucha electrónica. *Es la práctica de captura furtiva del tráfico de red*
    - » Tolerancia a fallos. *En este contexto, es la capacidad de la red para dejar funcionando las demás estaciones de trabajo si una llegara a fallar*

3. **Hardware de red**. *El* router *es un punto crítico de ataque, una pasarela a través de la que los usuarios se comunican con el exterior y viceversa. Si los agresores consiguen colapsar los* routers, switches *o* hubs, *pueden denegar el servicio a mucha gente.*

4. **Contraseñas de BIOS y de consola**. *La mayoría de las arquitecturas como X86, PPC o Sparc utilizan contraseñas de BIOS-PROM, contraseñas de consola o de ambos tipos como una capa extra de seguridad para impedir el acceso a la configuración del sistema.*

5. **Controles biométricos de acceso**. *Estas herramientas autentican a los usuarios en base a sus características biológicas como son el olor corporal, las huellas dactilares, los patrones de retina e iris, la voz, el trazado de las venas, etc. Los controles de acceso biométrico no son adecuados para entornos que van más allá de una red local.*

Evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger (no es necesario hablar sólo de equipos Linux, sino de cualquier elemento físico que se pueda utilizar para amenazar la seguridad, como una toma de red apartada en cualquier rincón de un edificio de alguna organización).

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

2.3.1 Desastres Naturales

Hemos hecho referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos, sin embargo, un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su (falta de) prevención.
Los principales desastres naturales que se pueden producir son:

1. *Terremotos*
2. *Tormentas eléctricas*
3. *Tornados y huracanes*
4. *Inundaciones y humedad excesiva*
5. *Incendios y humo*
6. *Radiaciones electromagnéticas muy altas*
7. *Sobrecargas de tensión y cortes en el suministro de energía eléctrica*

2.4 Seguridad Lógica

Quizá las amenazas a la seguridad de un sistema de cómputo que se consideran las más sofisticadas están representadas por programas que explotan las debilidades de los sistemas computacionales. En este contexto, hablaremos de los programas de aplicación, así como los programas de utilerías, tales como editores y compiladores.
Las amenazas de acceso a la información son aquellos que interceptan o modifican datos en favor de usuarios que no deben tener acceso a ellos.

La seguridad lógica esta dada por:

1. *Seguridad que brinda el sistema operativo*
2. *Establecimiento de un sistema de passwords eficiente*
3. *Encriptación de archivos de datos*
4. *Creación de respaldos (Backups)*
5. *Detección y expulsión de intrusos del sistema*
6. *Control de calidad del software*
7. *Establecimiento de una política de seguridad formal*
8. *Restricciones de tiempo de acceso y conexiones concurrentes*

Por lo general, existen tres niveles de controles de acceso lógico con lo que debería contar cualquier sistema de seguridad para la información:

a) *Identificación de usuario.*
b) *Password (o contraseña) o número de autenticación de usuario. Se utiliza para autentificar que la persona es quien dijo al identificarse.*

c) Mecanismo de autorización. Son los derechos o privilegios que se tienen para acceder a diversos recursos de un sistema, los cuales son especificados por reglas de autorización dadas por el administrador.

2.4.1 Tipos de Amenazas Lógicas

Las amenazas lógicas son representadas por programas que atacan y/o explotan las vulnerabilidades de los sistemas de cómputo.

2.4.1.1 Amenazas de Acceso a la Información

Las amenazas de acceso a la información son aquellas que interceptan o modifican datos a favor de usuarios que no deben tener acceso a ellos. Entre las principales amenazas de este tipo se encuentran las siguientes:

- **Trampas**. *Una trampa es un punto de entrada secreto en un programa que permite a alguien que está enterado de la trampa obtener acceso sin atravesar los procedimientos usuales para un acceso seguro. Las trampas han sido usadas en forma legítima por programadores durante mucho tiempo para depurar y probar programas. Por lo general, la depuración y la prueba se hacen cuando el programador está desarrollando una aplicación que tiene un procedimiento de autenticación o una preparación larga, que requiere que el usuario introduzca muchos valores diferentes para correr la aplicación. Para depurar el programa, el desarrollador puede desear ganar privilegios especiales o evitar toda la preparación y autenticación necesarias. La trampa es un código que reconoce alguna secuencia especial de entrada o se activa al correrse desde un cierto identificador de usuario o con una secuencia de eventos poco probable. Las trampas resultan amenazas cuando las usan programadores sin escrúpulos para obtener un acceso no autorizado. Es difícil implementar los controles de un sistema operativo para trampas; las medidas de seguridad deben enfocarse sobre el desarrollo del programa y la actualización de software.*

- **Caballos de Troya**. *Un caballo de Troya es un programa o procedimiento útil (o que sólo lo parece) el cual contiene un código oculto que, cuando se solicita, ejecuta alguna función no deseada o perjudicial. Estos programas pueden usarse para lograr funciones en forma indirecta que un usuario no autorizado no podría lograr directamente. Otro objetivo de los caballos de Troya es la destrucción de datos. Por ejemplo, para obtener acceso a los archivos de otro usuario en un sistema compartido, un intruso puede crear un programa caballo de Troya que, cuando se ejecuta, cambia los permisos de archivo del*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

usuario que solicita, de manera que cualquier usuario puede leer los archivos. Un enfoque para seguridad contra ataques de caballos de Troya es el uso de un sistema operativo seguro. En este caso se usa un caballo de Troya para rodear el mecanismo de seguridad estándar usado por la mayoría de los sistemas operativos y de administración de archivo: la lista de control de acceso.

- **Canales secretos**. *Las características incorporadas en sistemas operativos de multinivel dan seguridad de que se evitará que un usuario privilegiado envíe información confidencial a un usuario no autorizado (sin privilegios). Un canal secreto intenta transferir la información de una manera inesperada y sutil que no impiden los controles de seguridad de multinivel ordinarios. Por ejemplo, un programa privilegiado puede tener la función de producir un resumen no privilegiado de un archivo de datos confidenciales. El sistema sólo puede comprobar que no se imprimen datos delicados. No obstante, cambiar la palabra TOTAL a TOTALES en un encabezado no se notaría, creando así un bit canal secreto. Si la palabra TOTAL o TOTALES aparece con bastante frecuencia puede comunicarse información útil. La utilidad de los canales secretos está limitada por la tasa de transferencia de información, la cual por lo general será pequeña.*

2.4.1.2 Amenazas al Servicio

Las amenazas al servicio son aquellas que explotan los defectos de servicio en las computadoras para inhibir su uso por sus propios usuarios. Los virus y sus parientes cercanos son una amenaza bastante inquietante para los administradores responsables de la seguridad, ya que desbaratan operaciones, destruyen datos y dan origen a preguntas inquietantes sobre las vulnerabilidades de los sistemas de información.

- **Virus**. *Un virus es un programa que se ejecuta en una máquina con la finalidad de alterar el correcto funcionamiento de ésta. Los virus por lo general hacen copias de sí mismos y se expanden por la red o redes a las que esté conectado el ordenador infectado, protegiéndose y ocultándose para no ser descubierto. Una vez alojado en una máquina central, el virus típico toma el control temporal del sistema operativo de la computadora. Después, cuando la computadora infectada entra en contacto con alguna otra pieza de software desinfectada, una copia fresca del virus pasa al nuevo programa. Por lo tanto, la infección puede dispersarse de una máquina a otra cuando se intercambian discos o se envían datos sobre una red. La mayoría de los virus realiza su tarea en una manera que es específica para un sistema operativo en particular; por lo tanto, están*

diseñados para aprovechar las vulnerabilidades de los sistemas operativos.

» **Gusanos**. *Los programas de gusano de red usan conexiones de red para dispersase de sistema en sistema. Una vez activo dentro de un sistema, el gusano de red puede comportarse como un virus o bacteria de computadora, o puede implantar programas caballo de Troya para ejecutar cualquier cantidad de acciones de interrupción o destructivas. Para duplicarse a sí mismo, un gusano usa alguna clase de vehículo de red; por ejemplo:*

- Función de correo electrónico. *Un gusano envía por correo una copia de sí mismo a otros sistemas.*
- Capacidad de ejecución remota. *Un gusano ejecuta una copia de sí mismo en otro sistema.*
- Capacidad de inicio de sesión remota. *Un gusano inicia una sesión en un sistema remoto como un usuario y después usa los comandos para copiarse a sí mismo de un sistema a otro*

Después, se corre la nueva copia del programa gusano en el sistema remoto donde, además de realizar cualquier función en ese sistema, continúa para extenderse en la misma forma.
En un sistema de multiprogramación un gusano también puede disfrazar su presencia nombrándose a sí mismo como un proceso del sistema o usando algún otro nombre que no puede notar el operador del sistema. Al igual que los virus, los gusanos son difíciles de encontrar, no obstante, las medidas de seguridad de red y de sistema único, si están bien diseñadas e implementadas, minimizan la amenaza de gusanos.

» **Bacterias**. *Las bacterias son programas que no dañan en forma explícita cualquier archivo; su único propósito es duplicarse ellas mismas. Un programa de bacteria típico puede no hacer nada más que ejecutar dos copias de sí mismo en forma simultánea en un sistema de multiprogramación o quizás crear dos nuevos archivos, cada uno de los cuales es una copia del archivo fuente original del programa bacteria. Después, esos dos programas pueden copiarse a sí mismos dos veces y así sucesivamente. Las bacterias se reproducen de manera exponencial y terminan por abarcar toda la capacidad del procesador, la memoria o el disco duro, negando a los usuarios el acceso a esos recursos.*

2.4.2 Tipos de Ataques Lógicos

En esta sección expondremos diferentes tipos de ataques y daremos una breve explicación de cada uno de ellos. No se pretende enumerar todos los tipos

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

de ataques existentes debido a su gran extensión y sobre todo, a que la evolución de los sistemas informáticos genera nuevos tipos y variantes cada vez más sutiles.

2.4.2.1 Ataques de Monitoreo

Como su propio nombre lo indica, estos ataques se ejecutan para observar a la víctima y a su sistema, de este modo es posible obtener información muy valiosa. El objetivo que también queda implícito en este tipo de ataque es enumerar las debilidades del sistema y obtener posibles formas de acceso al mismo.

- **Shoulder surfing**. *Consiste en espiar físicamente al usuario que será la primera víctima. Como su propio nombre lo indica, es mirar por encima del hombro a la víctima y observar cuando teclea su nombre de usuario y contraseña para acceder al sistema, de tal forma que el atacante pueda memorizarlos. Otra variante es explotar el error de olvidos de las contraseñas en el escritorio de la oficina por parte de la víctima.*

- **Decoy**. *Son programas que se implementan en el ordenador con una interfaz igual a otro de los que utiliza comúnmente el usuario, éstos requieren la autentificación del usuario mediante su login y password, donde la víctima inocentemente los introduce. El programa guarda la información en un archivo y deja ejecutar el programa que usa el usuario con normalidad. Otro tipo de estos programas son los que guardan, durante toda una sesión, las teclas pulsadas por la persona que trabaja con la computadora deseada.*

- **Scaneo**. *Es el método por el que se descubren canales de comunicación susceptibles de ser utilizados por el intruso; se envían paquetes de varios protocolos a los puertos de la máquina víctima y se deduce, según la recepción o extravío de los paquetes de respuestas, qué servicios de ella están abiertos. Existen diferentes tipos de escaneo según las técnicas, puertos objetivos y protocolos utilizados:*

    - Escaneo TCP Connect. *Es la forma básica de escaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito, cualquier otro evento significa que el puerto no está abierto o que no podemos establecer conexión con él. Estas técnicas se caracterizan por ser muy rápidas y no precisan de ningún permiso de usuario sobre la máquina atacada, por otro lado es fácilmente detectable por el administrador del sistema.*

* Escaneo TCP SYN (sincronización). *Este tipo de escaneo realiza la técnica de "la media apertura", pues nosotros como intrusos no pretendemos establecer una conexión completa. Se envía un paquete SYN (como si quisiéramos establecer una conexión real), esperamos la respuesta de la máquina víctima y, al recibir la autenticación ACK de que el puerto escaneado esta abierto, lo que hace el intruso es responder con un RST, como si no nos interesara en ese momento establecer conexión, pero guarda ese puerto de escucha en la máquina víctima como abierto. Esta técnica es muy funcional y poco ruidosa.*

* Escaneo TCP FIN. *Este tipo de escaneo se realiza cuando el intruso desea ser más sigiloso y hacer el menor ruido posible, (en la actualidad determinados* firewall *y programas de detección de intrusos pueden detectar los escaneos del tipo SYN). Esta técnica se basa en el principio de que los puertos cerrados suelen responder a los paquetes FIN con un RST, los abiertos, por el contrario, no les hacen caso y no responden, ése es el momento de registrar el puerto como abierto. Este ataque tiene nula utilidad en sistemas Windows pues siempre envía paquetes RST ante un FIN, esté o no abierto el puerto, pero es de gran utilidad en sistemas Linux/Unix.*

* Escaneo fragmentado. *Aumentando la sutileza de los paquetes enviados a los puertos de la máquina víctima, este procedimiento consiste en partir los paquetes completos de sondeo en pequeños fragmentos, con lo cual estos pequeños paquetes provocan menos ruido en las posibles herramientas de detección del administrador de la máquina objetivo.*

* Eavesdropping o sniffering. *Consiste en, una vez dentro de una red de ordenadores (habiendo conseguido algún tipo de privilegio de usuario en ella), implementar en una de las máquinas o hardware un programa espía, llamado* sniffer*, el cual registra en un fichero accesible al intruso todo el tráfico de información en la red (contraseñas en texto plano, nombres de usuarios, teléfonos, números de cuentas bancarias, etc.). Esta técnica tiene el inconveniente de que sobrecarga el funcionamiento de la tarjeta de red del ordenador huésped del* sniffer*, y además actualmente existen dispositivos inteligentes de red (Switcht) que controlan el tráfico de red y no dejan que todos los sistemas reciban los paquetes de los demás, con lo que en redes de este tipo la técnica de sniffering se complica mucho y no es nada trivial.*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

2.4.2.2 Ataques de Validación

Este tipo de técnicas tiene por objetivo suplantar al dueño o usuario de un sistema, mediante la consecución de sus cuentas de acceso y contraseñas, o suplantando la identidad de la máquina en la red.

- **Suplantación de identidad en saltos**. *También conocida como Spoofing-Looping, consiste en hacerse del nombre y contraseña de un usuario del sistema, entrar en su máquina para obtener información de la red y del resto de los equipos e ir suplantando nuevas identidades de usuarios de máquina en máquina (esto es aplicable a ordenadores conectados a Internet). Seguir el rastro a un intruso que ha realizado este tipo de ataque es muy complicado, pues requiere de la colaboración del administrador para analizar cada una de las computadoras por donde ha ido saltando el intruso.*

- **Suplantación IP**. *También conocido como IP Spoofing, en este ataque se generan paquetes de información con una dirección IP falsa en la parte del paquete TCP/IP que identifica el ordenador origen de la llamada. Si el intruso conoce la dirección IP del ordenador de una persona cualquiera en el trabajo, será suficiente alterar el paquete para incluir esa dirección, con lo cual si la máquina atacada y el administrador registran esos paquetes donde aparece la IP cambiada (origen), la persona culpada puede ser otra y no el intruso, incluso se puede pensar que el ataque proviene de una red distinta a la original, dependiendo de la IP falsa que el intruso decida incluir.*

- **Suplantación DNS (Sistema de Nombres por Dominio)**. *También llamado DNS Spoofing, consiste en la manipulación de paquetes del protocolo UDP, para engañar al servidor de dominio y que éste entregue información de sus tablas de registros a la petición de un intruso. Esto es posible si el servidor DNS tiene el método de recursión en funcionamiento.*

- **Suplantación IP Splicing-Hijacking**. *El atacante ha interceptado una conexión establecida reciente, observa el intercambio de paquetes entre el usuario original y el servidor (el ordenador víctima), y entonces suplanta al usuario emitiendo un paquete casi idéntico al que el servidor espera recibir del usuario conectado, lo suficientemente idéntico para que el servidor no note nada; en ese momento el intruso recibe la respuesta del servidor y puede seguir enviando paquetes de información habiendo suplantado al usuario original. El usuario original se queda esperando datos como si su conexión se hubiera colgado.*

- **Puertas traseras**. *Aunque el tema de establecimiento de puertas traseras es en ocasiones diferente a la suplantación de identidad, sí existe como tal en el siguiente caso: muchos programadores generan una puerta trasera para entrar en su software o máquina sin tener que pasar los procedimientos normales de validación, esta puerta consiste, por ejemplo, en un segmento de código, si esa puerta por descuido queda abierta (no se borra adecuadamente) a la finalización del trabajo, una persona que explore el código del programa puede descubrirla y utilizarla para tomar el control de la aplicación o modificarla.*

- **Utilización de Exploits**. *La detección de vulnerabilidades específicas o* bugs *en los sistemas operativos es aprovechada por los* exploits *para dar al intruso la identidad del super usuario (el administrador) y, en consecuencia, los privilegios sobre el ordenador asaltado.*

2.4.2.3 Ataques de Denegación de Servicios

La comunicación entre ordenadores se basa en protocolos y siempre se fundamenta, desde sus inicios, en la buena voluntad de establecimiento de comunicación entre las máquinas, en consecuencia estos protocolos no fueron diseñados ni están preparados para que un intruso decidiera hacer uso de ellos para otro fin que no fuera la correcta comunicación entre varios ordenadores, de ahí su debilidad y son más las facilidades para crear caos. Este tipo de ataques lo que pretenden es desbordar los recursos de una computadora víctima de forma que se interrumpan los servicios suministrados por ésta. El objetivo principal es bloquear los servicios ofrecidos por un ordenador a sus clientes (conjunto de otras máquinas que solicitan de él ese servicio).

- **Flooding**. *Este tipo de ataque desborda los recursos del sistema. El hacker malicioso satura el ordenador víctima de mensajes que requieren establecer conexión y dar respuesta. Como la dirección del mensaje puede ser falsa (técnica de Spoofing), la máquina atacada intenta dar respuesta a la solicitud de cada mensaje, saturando su* buffer *con información de conexiones abiertas en espera de respuestas; esto impide que oiga las solicitudes de otros usuarios que sí necesitan realmente conectarse. Un ataque famoso para el cual ya están implementadas las defensas, es el* ping *de la muerte. Una manera más rudimentaria de Flooding puede ser el envío masivo de un e-mail a la cuenta de correo de todos los usuarios existentes, terminando por saturar su servicio de correo.*

- **SYN Flood**. *El cliente o atacante envía un paquete SYN pero no responde al paquete ACK produciendo en la pila TCP/IP una espera de tiempo para recibir la respuesta del ordenador atacante, si se generan muchas de estas conexiones, los procesos de la máquina víctima se ralentizan. Para*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

que este ataque tenga un efecto óptimo se debe enviar una dirección IP suplantada o inexistente, de manera que la máquina atacada no sea capaz de dar ninguna respuesta, puesto que la IP no existe. Si la IP existe, la máquina atacada terminará respondiendo con un SYN/ACK, y ante la no solicitud de conexión real de la IP atacante, finalizará dando una respuesta RST, con lo cual el ataque se pierde. Si se generan miles de estas llamadas se terminará por colapsar a la máquina atacada.

- **Connection Flood**. *El desbordamiento de conexiones tiene el mismo principio de saturar a la máquina atacada con peticiones sin buena fe, es decir, maliciosas. Por ejemplo, si un servicio Web admite 5000 conexiones, es suficiente que un atacante realice las 5000 sin nada que solicitar a la máquina víctima, con lo que otros usuarios no pueden acceder al servicio que ésta suministra. Aunque transcurrido un tiempo las conexiones se van liberando, por inactividad, tan sólo se deben seguir enviando peticiones de conexión para reemplazar las ya liberadas y dejar el servicio inoperativo.*

- **Ataque LAND**. *Las plataformas de Microsoft Windows son sensibles a esta técnica y consiste en lanzar a un puerto abierto de la máquina víctima (normalmente del 113 al 139 del NETBIOS) un paquete formado con la dirección y puerto origen igual a la dirección y puerto destino; tras varios envíos de paquetes de esta forma, la máquina deja de responder.*

- **Tormenta BROADCAST**. *Este ataque, como su propio nombre lo indica, puede ser destructivo y radica en mandar una petición ICMP a una dirección Broadcast (router de la empresa, por ejemplo), la petición ICMP lleva como IP de origen, la del ordenador que se pretende devastar en la red; ante esta petición el dispositivo broadcast lo lanzará a todas las máquinas de la red y todas simultáneamente empezarán a responder a la víctima objetivo saturándola de respuestas que no puede procesar y produciendo un colapso en su sistema.*

- **Desbordamiento NET**. *Este ataque consiste en lanzar a la red, en la que se ha incursionado el intruso, paquetes y paquetes sin sentido que empiecen a colapsar el tráfico que circula por ella, de manera que no dejemos que las transmisiones útiles de verdad circulen o reducimos su velocidad de transmisión.*

- **OOB o SUPERNUKE**. *Las plataformas Microsoft Windows son igualmente sensibles a este tipo de ataque, el cual consiste en enviar paquetes UDP modificados con la señal* Out of Band *activada, a los puertos de escucha del NETBIOS (entre el 137 y el 139), la máquina los intercepta como no*

válidos y pasa a ser inestable y se cuelga. Este ataque tiene su defensa en los parches suministrados por el fabricante y su correcta instalación.

- **TEARDROP ONE Y TEARDROP TWO**. *Este ataque se realiza enviando paquetes fragmentados con datos que se solapen entre sí, algunas implementaciones de colas IP no pueden ensamblar correctamente este tipo de paquetes y el ordenador se cuelga. Por ejemplo, enviar un paquete con los datos del 1 al 100 y después enviar otro paquete con los datos del 50 al 150, produciría este efecto en la máquina víctima. Este ataque afecta a diversas versiones de sistemas Unix, Linux y Windows.*

- **Bombardeo de e-mail**. *Como ya se explicó anteriormente, consiste en enviar muchísimas veces un mensaje idéntico a una misma dirección electrónica, saturando de esta forma la cuenta de correo del usuario atacado.*

2.4.2.4 Ataques de Modificación

- **Tampering**. *Estos ataques están relacionados con la modificación sin autorización de datos o de los programas instalados en el sistema, incluido el borrado de ficheros. Son ataques muy peligrosos sobre todo si el hacker adquirió derechos de super usuario o administrador sobre la máquina, lo cual permite ejecutar cualquier tipo de comando y, en consecuencia, borrar cualquier información en el sistema.*

- **Borrado de huellas**. *Lo vamos a considerar como un complemento de los ataques, pues incluye el modificar los ficheros* log *del sistema operativo de la máquina asaltada, donde siempre queda constancia de la visita no deseada. Cuando un hacker se dispone a abandonar una máquina asaltada, es importante la edición de estos ficheros para borrar todo rastro de la sesión iniciada y los movimientos realizados, esto permite no despertar sospechas y efectuar futuras entradas, si la vulnerabilidad del sistema sigue sin ser detectada por el administrador.*

- **Ataques Java Applets**. *Los Applets de Java no son otra cosa que ficheros ejecutables de programas y, en consecuencia, se pueden modificar para que realicen acciones específicas de asalto. Hay que decir que Java implementa fuertes medidas de seguridad por lo que será complicado llevar a cabo este tipo de ataque. Los navegadores actuales de Internet llevan implementadas Máquinas Virtuales de Java (MVJ) para ser capaces de ejecutar los applets; no obstante, estos programas pueden llegar a ser hostiles.*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

- **Ataques con Java script o Visual script**. *Son lenguajes usados para el diseño de sitios Web, los programas realizados son interpretados por el navegador. Resultan extremadamente peligrosos puesto que son capaces de iniciar aplicaciones en la máquina cliente o víctima para grabar información del disco duro, con lo cual resultan útiles para insertar virus u otro tipo de programas maliciosos en el ordenador del usuario.*

- **Ataques ActiveX**. *La visita a páginas Web nos lleva en muchos casos a la descarga de controles ActiveX, que realizan una tarea en concreto; éstos vienen acompañados de un certificado otorgado por una compañía de Auditoría Certificadora. Cuando se descarga una página con un control de este tipo, se le pregunta al usuario si confía en la autoridad que certificó el control ActiveX. Si el usuario acepta esta credencial, el control se ejecuta. Por lo general los usuarios siempre aceptan todo lo que dice pulsar SI para continuar, y es ahí donde viene el gran problema, pues los certificados se basan en la buena fe del programador que asegura que ese control no ejecuta ninguna tarea maliciosa, lo que es falso en muchas ocasiones. Se debe ser extremadamente precavido con este tipo de objetos y leer siempre cuidadosamente lo que aparece en pantalla como medida preventiva. Un ejemplo conocido es un control ActiveX que desactivaba la petición de aceptación de éstos controles en los navegadores cuando éste se ejecutaba, quedando el ordenador víctima dispuesto a aceptar la ejecución de todos los controles que encontraba en su navegación, sin preguntarle de nuevo.*

*Como se puede ver, se ha dado una noción del extenso mundo de los ataques, pero a la vez podemos deducir que las herramientas para asaltar ordenadores no sólo son programas que circulan por Internet en entornos visuales, desarrollados por expertos programadores, son también comandos individuales a nivel de consola o un conjunto de éstos (*scripts *de comandos) que se construye el intruso.*

2.5 Ingeniería Social

Definitivamente no existe un ambiente seguro de Tecnologías de Información. A pesar de los costosos y sofisticados esquemas de seguridad que existen, el usuario continúa siendo vulnerable a las técnicas de la Ingeniería Social.

Generalmente se imagina a los crackers como personas tímidas e inadaptadas socialmente y que realizan toda su actividad sin ningún tipo de contacto con otros humanos. Sin embargo, los crackers realmente peligrosos hacen uso de técnicas encaminadas a conseguir que sea el usuario mismo el que

les haga todo el trabajo sucio, es decir, tratan de embaucarlo para burlar el entorno de seguridad sobre el que trabaja con el propósito de que les resulte mucho más sencillo acceder a datos confidenciales.
Son varios los métodos que un cracker puede utilizar para conseguir que un usuario le dé información o que le facilite un acceso restringido para poder alcanzar sus objetivos.

1. **Autoridad falsa**. *Los crackers a menudo consiguen información simplemente convenciendo a la víctima de que están en una posición en la que esa información les es necesaria, diciendo que son un supervisor o un vicepresidente puesto que en empresas muy grandes es muy probable que un empleado no conozca a todos sus superiores. Hay veces en las que ni siquiera es necesario que un cracker suplante a una persona, basta tan sólo con que diga ser alguien con la autoridad necesaria para solicitar esa información o para acceder a lo que está solicitando.*

2. **Suplantación**. *La suplantación es una versión de la autoridad falsa en la que un cracker adopta la personalidad de un individuo que realmente existe, a través del teléfono, mediante un correo, en un Chat o mediante un mensaje instantáneo.*

3. **Compasión**. *Uno de los métodos más infalibles que suele utilizar un cracker consiste en hacer ver a la víctima que necesita urgentemente lo que está pidiendo para hacerle sentir compasión y verse obligado a ayudarle.*

4. **Implicación personal**. *Los crackers se dan cuenta de que obtienen una cooperación mucho mejor si se inventan una historia que afecta directamente a la persona que están intentando manipular.*

5. **Ataque al ego**. *Si se consigue que alguien se sienta bien con lo que hace será mucho más fácil manipularlo. Cuando una persona se siente elogiada bajará totalmente la guardia con tal de que las alabanzas continúen.*

6. **Profesiones poco sospechosas**. *Un cracker puede a veces acceder a áreas reservadas haciéndose pasar por alguien de la compañía de gas, de la compañía eléctrica, de la compañía telefónica o de cualquier departamento de servicios medioambientales. Esto convierte a estas profesiones en las ideales para aquellos crackers que quieren infiltrarse disfrazados.*

7. **Recompensa**. *A veces puede resultar fácil ofrecer algún tipo de recompensa para conseguir que alguien facilite alguna información.*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

2.6 Niveles de Seguridad Informática

Los niveles de seguridad son definidos utilizando el estándar más usado a nivel mundial, el TCSEC (Trusted Computer System Evaluation Criteria, Criterio de Evaluación para Sistemas de Cómputo Confiables) o también conocido como "Libro Naranja", el cual fue desarrollado a principios de los años 80 en función de las normas de seguridad de los ordenadores del Departamento de Defensa de los Estados Unidos. Los niveles hacen alusión a los diferentes tipos de seguridad que brinda el Sistema Operativo que se ejecuta en un sistema de cómputo que requiere ser protegido. Los estándares europeos ITSEC (Information Technology Security Evaluation and Certification Scheme, Esquema de Certificación y Evaluación de Seguridad de la Tecnología de Información), ITSEM (Information Technology Security Evaluation Manual, Manual de Evaluación de Seguridad de la Tecnología de Información) y los internacionales ISO (International Organization for Standardization, Organización Internacional para la Estandarización) e IEC (International Electrotechnical Commission, Comisión Electrotécnica Internacional) se han basado en ellos.

- **Nivel D**. *Este nivel no contiene ninguna subclase y clasifica a los sistemas operativos que no cumplen ninguna especificación de seguridad. Sistemas operativos clasificados en este nivel son, por ejemplo, el MS-DOS y Windows 9x.*

- **Nivel C1 o de Seguridad Discrecional**. *Son los sistemas operativos que requieren de identificación de usuarios para permitir el acceso a recursos y diferente información. Cada usuario puede manejar su información y limitar el acceso a los mismos a otros usuarios, pero existe el administrador del sistema que tiene control total de acceso. Sistemas operativos dentro de este rubro son algunas versiones iniciales de Unix.*

- **Nivel C2 o de Acceso Controlado**. *Este nivel perfecciona el C1, puede restringir más a los usuarios y sus actividades, la ejecución de comandos por parte de éstos o los accesos a determinados archivos, permitir o denegar datos a usuarios en concreto, basándose no sólo en los permisos sino en los niveles de autorización. Requiere llevar auditorías de accesos e intentos fallidos de accesos, eliminado de restos de procesos en memoria o registros temporales. Se distingue entre el sistema de seguridad propiamente dicho y los ficheros. Sistemas operativos clasificados en este nivel son VMS, Windows NT, Novell Netware.*

- **Nivel B1 o de seguridad etiquetada**. *Este nivel agrega seguridad multinivel. El dueño de un archivo no puede modificar los permisos de objetos que están bajo control de acceso obligatorio. Cada usuario tiene asignada una etiqueta con un nivel de seguridad jerárquico*

(desclasificado, confidencial, secreto, supersecreto, etc.) y unas categorías (marketing, finanzas, personal, etc.). Cada usuario tiene objetos asociados y existen controles para limitar la escalada de derecho a accesos a otros objetos. Sistemas operativos clasificados en este nivel son Digital SEVMS, SGI trusted IRIX, HP-UX BLS y algunas versiones más recientes de Unix.

- **Nivel B2 o de Protección Estructurada**. *El sistema operativo es capaz de avisar a los usuarios si sus criterios de accesibilidad o seguridad son modificados, se prepara un modelo de seguridad previo y debe comprobarse que éste se ajusta a lo previsto, se restringen canales de transmisión de datos y se implementa la existencia jerarquizada de objetos. Sistemas operativos que cumplen con esto son Cryptek VSLAN, Trusted XENIX.*

- **Nivel B3 o de Dominios de Seguridad**. *El sistema operativo monitorea las peticiones de acceso de cada usuario y las acepta o rechaza según las políticas de acceso definidas. Las estructuras de seguridad deben ser tan óptimas que permitan análisis y estudios de posibles violaciones, en cada una de ellas, rápidamente. Se deben realizar auditorías obligatorias cada cierto tiempo para detectar posibles violaciones de seguridad. Un sistema clasificado en este nivel es el XTS-300.*

- **Nivel A1 o de Protección verificada**. *Éste es el nivel máximo, un nivel B3 mejorado, cuenta con la implementación de modelos matemáticos sofisticados para garantizar que las funciones de seguridad han sido correctamente implementadas y para asegurar los procesos que realiza un usuario. Sistemas clasificados en este nivel son Boeing MLS LAN, Gemini Trusted Network Processor.*

- **Nivel A2**. *Pensando en el futuro, no ha sido formalmente definido, todavía no existen sistemas operativos en máquinas que hayan pasado la barrera del nivel A1.*

Debemos aclarar que existe una vertiente de expertos informáticos que consideran que estos niveles de implementación de seguridad están caducos o simplemente son tan difíciles de implementar en el mundo empresarial actual que no son funcionales. Esto se plasmó cuando el NIST (The National Institute of Standards and Technology, Instituto Nacional de Estándares y Tecnología) unió fuerzas con sus homólogos europeos y emprendieron la iniciativa Common Criteria *(CC) en 1993. Esta iniciativa pretende estandarizar los esfuerzos en seguridad informática para crear un nuevo estándar internacional más acorde y realista. Lamentablemente dicha iniciativa no ha tenido resultados prácticos de gran repercusión, aunque los esfuerzos continúan. En definitiva podemos*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

decir que estos niveles de seguridad presentados deben ser conocidos en el ámbito teórico y reconocer que su aplicación en la práctica es difícil.

2.7 Metodología de Seguridad

A medida que una organización crece, también se elevan de forma exponencial los riesgos en la seguridad, y cada vez se vuelve más difícil detectar y evitar posibles infiltraciones y ataques que perjudiquen las operaciones comerciales. En realidad no existe un entorno de Tecnologías de Información totalmente seguro, como tampoco hay una receta que funcione como base para establecer una metodología de seguridad para las empresas mexicanas en general.

Establecer los objetivos generales de un programa de seguridad computacional, consiste en identificar los elementos más importantes y determinar sus actividades mediante las políticas, normas, reglas, objetivos y estrategias de la empresa.

2.7.1 Ciclo de Vida de la Seguridad Informática

Cualquiera que sea el modelo de seguridad implementado en la infraestructura de tecnología de información, deberá cumplir con un proceso activo y cíclico (ver figura 2.3).

El ciclo de seguridad parte del principio fundamental del desarrollo y apego a políticas, estándares, procedimientos y métricas, ya que son éstas las que dictan el marco de acción, respuesta, responsabilidades y alcances de las medidas de seguridad aplicadas a los activos que se busca proteger.

Una vez que se tiene la base, entonces se realiza un análisis de riesgos; incluso, se puede realizar un replanteamiento o un rediseño de las políticas, estándares y procedimientos requeridos para salvaguardar la información y las operaciones críticas del negocio. Del resultado del análisis de riesgos se realiza un diseño de seguridad acorde a los recursos humanos y materiales disponibles, así como la selección e implementación de las soluciones requeridas. Una vez implementado el modelo de seguridad, es necesario el proceso de entrenamiento, no sólo del equipo técnico sino del personal que estará en contacto con la tecnología de seguridad, con el fin de alcanzar los objetivos planteados en los esquemas de monitoreo.

Finalmente se debe contemplar en todo momento un esquema de respuesta a incidentes y un plan de recuperación de desastres, los cuales deben ser procedimientos previamente analizados y probados para permitir que, en caso de que se presente un incidente, las operaciones críticas de negocio se mantengan funcionales.

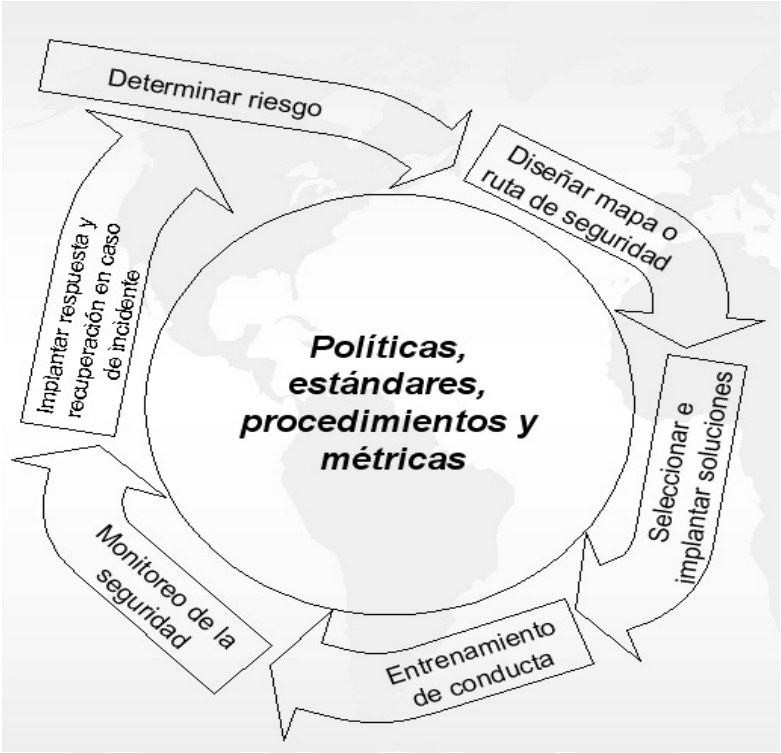


Fig. 2.3 Ciclo de vida de la Seguridad

El éxito en la aplicación del ciclo de seguridad puede ser medido de acuerdo con la forma en que cubra los procesos de alerta, protección, administración y respuesta, siempre bajo un mecanismo y control proactivo del modelo de seguridad. Si se contempla y obtiene la información en forma temprana, se tendrá la capacidad para responder preventivamente; si se cuenta con las herramientas de protección adecuadas, se detendrán las amenazas conocidas y se mantendrá la privacidad de la información; si se dispone de los mecanismos de respuesta adecuados , se tendrán los recursos humanos y/o tecnológicos, tanto internos como externos, listos para una reconfiguración del modelo de seguridad, así como claridad en los flujos de trabajo para contener el incidente; y, finalmente, si se posee un mecanismo de administración adecuado, tanto los procesos de ambiente como los de información podrán ser utilizados para el correcto y apropiado control de políticas, vulnerabilidades, incidentes y manejo de usuarios.

2.7.2 Metodología Scitum

Toda organización esta expuesta a amenazas internas y externas a su entorno que ponen en riesgo la seguridad de la información del negocio y los activos informáticos que soportan las operaciones. El problema más frecuente es que las amenazas no se conocen hasta que se materializa el riesgo y causa

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

daños en la imagen de la empresa o institución, en la oportunidad o capacidad de respuesta del negocio y en la veracidad de la información que posee, etc.

La metodología que se presenta es una de las más conocidas a nivel nacional y una de las que mejores resultados ha dado. Scitum es una empresa mexicana que por mucho tiempo ha implantado todo el ciclo de seguridad informática en diversas instituciones y organizaciones de México, el cual permite anticiparse a eventos que atenten contra la seguridad de la información.

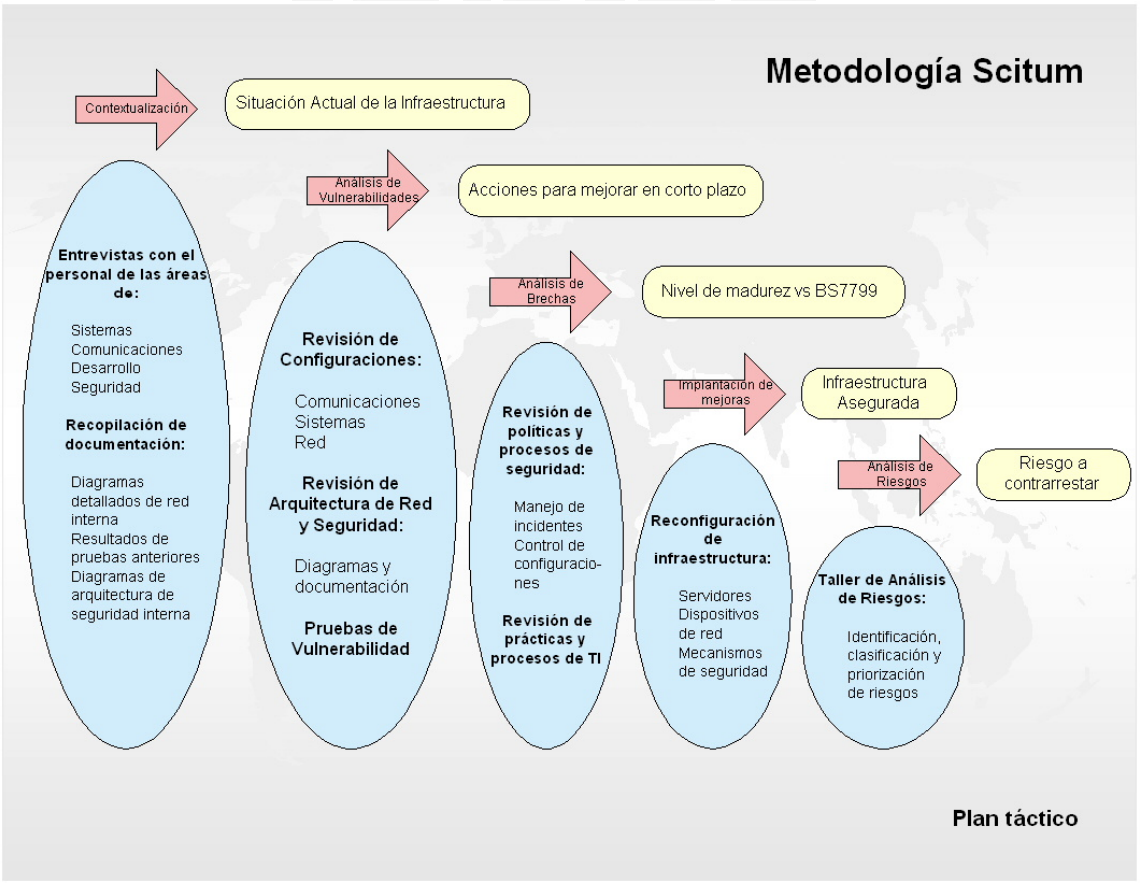


Fig. 2.4 Proceso de la Metodología Scitum

1. *Detección de necesidades.*
   - *Quién soy y cuál es mi objetivo como empresa*
   - *Qué tipo de información manejo*
   - *Con qué infraestructura cuento*
   - *Qué servicios se requieren para tomar decisiones adecuadas*

2. *Análisis de riesgos y vulnerabilidades*
   - *La posibilidad de que una vulnerabilidad sea explotada*

- *Identificar lo que se pretende proteger (clasificación de riesgos y vulnerabilidades)*
- *Cuánto cuesta proteger y/o no proteger (perder información y/u operación)*

3. *Establecer políticas y procedimientos de manera formal*
   - *Encaminadas al recurso humano (de operación y usuarios)*
   - *Trabajar con la documentación adecuada y total*

4. *Programas de concientización del personal*
   - *Debe contener datos y estadísticas de ataques*
   - *Estadísticas de rendimiento*
   - *Estadísticas de fallas y afectaciones*
   - *Probablemente también incluya un análisis de costos*

5. *Configuración de la infraestructura*
   - *Se hace una comparación con el análisis de las necesidades*
   - *Nacen los planes de contingencia*
   - *Poner en marcha la recuperación*

Symantec y Novell han propuesto una solución de tecnologías integradas de seguridad en redes y ambas compañías coinciden en que al tener funciones múltiples, los esquemas de seguridad total pueden proteger más eficientemente contra riesgos en todos los niveles de la red. Las tecnologías idóneas para esta integración son las siguientes:

- **Autenticación y autorización**. *Garantiza la identidad de cada usuario, desde la simple protección de passwords hasta la implementación de soluciones biométricas como huellas digitales, uso de tarjetas inteligentes, etc.*
- **Filtrado de contenidos**. *Identificación y eliminación del tráfico no deseado. Diversas soluciones de software, incluso suites que integran antivirus y desfragmentadores de disco, entre otros, se encargan de evitar el despliegue de sitios Web que no son de incumbencia para los objetivos de trabajo de una organización.*
- **Protección antivirus**. *Una infección por virus extendida representa una amenaza para el negocio. Todos los puntos de entrada de los virus pueden estar completamente protegidos y los puntos de entrada potenciales deben identificarse todos los días para que ningún bicho sea transmitido en los sistemas de la organización.*
- **Manejo de la vulnerabilidad**. *Descubre los agujeros que existan en la seguridad y sugiere mejoras.*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

- **Firewalls**. *Controlan el tráfico de las redes al seleccionar la información que entra y sale de las mismas, para garantizar que no ocurran accesos no autorizados. Un buen firewall debe proporcionar una protección integrada frente a amenazas internas y externas, al tiempo que garantiza el acceso de empleados, clientes y socios a la información de la compañía.*
- **Detección de intrusos**. *Detecta el acceso no autorizado y proporciona alertas e informes que se pueden analizar en cuanto a la identificación de la configuración y el programa de trabajo de la máquina. Existen soluciones eficaces que detectan, monitorean y expulsan a usuarios no autorizados.*
- **Redes Privadas Virtuales (VPN)**. *Su implementación protege las conexiones fuera del perímetro, lo que le permite a las organizaciones comunicarse en Internet de manera segura. Además, encripta los datos antes de enviarlos a una red pública. Resulta más rentable para conectar de forma segura a usuarios remotos y organizaciones.*
- **Protocolos de seguridad**. *Resuelven los problemas de autenticación. Entre los más comunes destacan SSL (Secure Sockets Layer) o IPSec (Internet Protocol Security); este último resuelve muchos de los problemas que se generan en la autenticación y confidencialidad de los datos.*
- **Gestión de certificados**. *Garantizan la seguridad de las transacciones de e-Business. Las compañías que realizan este tipo de transacciones tiene que saber con quién están tratando y que éstas son seguras, fiables y legalmente vinculantes.*

Symantec indica que al combinarse todas estas tecnologías, la protección será más completa, al mismo tiempo que ayudará a reducir la complejidad y los costos. Otra ventaja es que se pueden implementar en todos los niveles de red, ofreciendo mayor protección a los recursos patentados y disminuyendo los riesgos. Novell, por su parte, considera la protección biométrica como una de las tecnologías que mayores adeptos está ganando en el mundo, debido a su efectividad ya que es una excelente alternativa para grandes redes que operan en misiones muy críticas.

2.8 Planes de Contingencia

Ya que no puede lograrse la seguridad total, ni con el mejor y más completo programa, es muy importante tener la capacidad de recuperarse de una contingencia. Sin esta capacidad, cualquier organización o empresa dependiente del procesamiento de datos está asumiendo un gran riesgo de destrucción.

Un plan de contingencia es un plan escrito en el que se detallan acciones, procedimientos y recursos que deben usarse durante un desastre que ocasione

destrucción parcial o total de la operación y/o los servicios que brinda un área informática o de procesamiento. En éste escrito se definen qué tareas son críticas, quién es el responsable de todos los aspectos del proceso de recuperación y cómo va a funcionar la organización mientras este proceso ocurra.
Un plan de contingencias completo mitigará los efectos de desafortunados desastres y permitirá una respuesta rápida, una transferencia del procesamiento crítico a otras instalaciones y una eventual recuperación.

Una de las claves en el desarrollo de un plan de contingencias recae en una adecuada evaluación de posibles riesgos que envuelven el entorno informático y establecer el impacto que pueden causar en caso de que se presenten. Así, la concepción del plan de contingencias debe tener un alcance tal que permita una completa recuperación de la pérdida eventual, según el tiempo que de antemano se haya considerado para ello.
Debemos entender la operación "normal" de un sistema como un desarrollo en condiciones normales (cotidianas), lo que implica ciertas normas y estándares.

2.8.1 Metodología de Desarrollo

A continuación se describe la metodología de William Toigo, la cual consta de seis etapas y de cada una se desprenden sus principales tareas:

1. **Etapa de definición y arranque**
   a) *Se deben definir los objetivos principales del plan de contingencias*
   b) *Se debe seleccionar la metodología más adecuada*
   c) *Se debe contar con la aprobación de la Dirección*
   d) *Se diseñan y elaboran cuestionarios de sondeo*

2. **Etapa de análisis de riesgos**
   a) *Recolección de datos*
      - *Inventario de hardware, software, aplicaciones, bases de datos y telecomunicaciones.*
      - *Se obtiene el "grado crítico" de los sistemas, tanto desde el punto de vista de los usuarios como del de los técnicos.*
      - *Se determina la "tolerancia" a una falla o desastre, expresada como un valor en pesos (es la pérdida de ingresos de la empresa) debida a una suspensión en la operación.*
      - *Identificación de amenazas a la operabilidad normal, clasificándolas por su origen, procedencia o simplemente por observación de lo que sucede en el entorno.*
   a) *Análisis de datos*
      - *Habiendo hecho toda la recolección de datos, resta analizar todos éstos y formular un conjunto de objetivos específicos para guiar el desarrollo de la capacidad de recuperación.*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

3. **Etapa de protección a la instalación.** *En esta sección se discuten varias estrategias comunes de prevención de desastres y de protección que se pueden poner en práctica.*

    a) Detección de fugas de agua
    b) Protección contra fuego e incendios
    c) Eliminación de contaminantes y disminución de su impacto
    d) Fallas en el suministro eléctrico
    e) Control de acceso físico

4. **Etapa de almacenamiento fuera del Site,** *esto incluye el análisis y clasificación de los datos, la revisión de los procedimientos de respaldo existentes, la evaluación y selección de un proveedor de espacio de almacenamiento y la formalización de agendas para el mantenimiento actualizado de datos en el site externo.*

5. **Etapa de estrategia de respaldo de sistemas.** *En esta etapa nuevamente se hace uso de los resultados del análisis de riesgos. Hay que saber:*
    a) Qué aplicaciones son críticas o vitales
    b) Cuál es la configuración mínima de hardware para correr los sistemas
    c) Cuántos usuarios tienen los sistemas
    d) Cuáles son los requerimientos de la empresa

Existen muchas estrategias de respaldo de los sistemas de cómputo, pero debe analizarse cada caso para determinar cuál es la más conveniente.

6. **Estrategia de respaldo de redes.** *Una actividad preliminar consiste en revisar el análisis de riesgos para identificar dependencias en redes, el grado crítico de los servicios de red y el nivel mínimo de servicio requerido para la continuidad del servicio. Existen varias opciones para recuperar las redes que han tenido fallas.*
    a) Para sistemas de comunicación interna:
        » *Es importante adquirir software apropiado para diagnóstico y recuperación de problemas de redes*
        » *En el caso de una falla del conmutador hay dos opciones: instalar suficientes líneas directas para las funciones dependientes de las telecomunicaciones y comprar un segundo conmutador y tenerlo de respaldo*
    b) Para equipo periférico de las computadoras:
        » *Tener hardware redundante almacenado para reemplazo inmediato cuando falla un dispositivo crítico.*
    c) Para redes de área local (LAN):
        » *La solución reside en el software usado para crear y controlar la red, protegiéndolas contra pérdidas catastróficas*

debidas a fallas en los nodos, pérdida de la integridad de los medios de comunicación, etc.

Además de las fallas en redes, otro escenario de contingencia que puede ser considerado por el diseñador del plan consiste en la falla de la compañía telefónica y las estrategias de recuperación consisten básicamente en instalar otros medios de comunicación alternativos.

7. **Etapa de toma de decisiones en caso de emergencia.** *Se refiere a tres proyectos fundamentales para la recuperación de emergencias: evacuación, recuperación y reinstalación de las actividades normales. Deben tomarse las siguientes consideraciones:*
   a) Es imposible predecir todos los escenarios y tomar todas las decisiones por adelantado, por eso, resulta inútil diseñar procedimientos muy rígidos.
   b) Sin embargo, el plan es necesario para coordinar las acciones de recuperación ya que sin él, sería más lenta y el desastre causaría daños mayores a la empresa.
   c) En esta fase deben diseñarse los equipos que llevarán a cabo el plan de contingencia (estos mismos equipos pueden tener diferentes funciones durante la evaluación, la recuperación y la reinstalación de actividades normales).
   d) Después de diseñarse, deben formarse los equipos. Asimismo debe hacerse el directorio telefónico de estas personas y de todas las que tengan alguna relación con este plan.
   e) Pueden diseñarse uno o varios diagramas de flujo de Manejo de Emergencias que describan la secuencia en la cuál se realizarán las tareas de recuperación.

8. **Etapa de mantenimiento y pruebas.** *El plan de contingencias es un documento "vivo" y cambiante, por lo que requiere de mantenimiento. Antes de aprobar el plan se debe dar entrenamiento específico a todos los miembros del equipo de recuperación en las tareas que realizarán en caso de desastre.*
   a) Los objetivos principales de las pruebas son:
      - » *Asegurar que el plan pueda aplicarse exitosamente recuperando lo que sea posible*
      - » *Las pruebas sirven como una herramienta de auditoría*
      - » *Las pruebas pueden revelar información útil acerca del desempeño de los sistemas a un nivel de emergencia*
      - » *Las pruebas son una forma de entrenar y además pueden utilizar sus resultados para corregir el plan o agregarle aspectos no considerados originalmente*
   b) Para hacer las pruebas:
      - » *Debe establecerse un escenario*
      - » *Deben definirse los objetivos de la prueba*

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

- *Deben definirse reglas*
- *Se deben designar participantes y observadores*
- *Se deben documentar los resultados*

Independientemente de la metodología que se elija para el desarrollo del plan de contingencias, o que se desarrolle una propia, existen ciertas constantes que deben aparecer en cualquier plan de éste género, no sólo para sistemas, sino para cualquier otra área o empresa de cualquier giro o tamaño que resida en cualquier lugar.

2.9 Auditoría Informática

La auditoría informática es la revisión que se hace a la suficiencia de controles establecidos en el ambiente informático con la finalidad de disminuir riesgos y garantizar la seguridad, confiabilidad y exactitud de la información y de los procesos. Es importante destacar que la auditoría informática esta enfocada a disminuir riesgos, más no a eliminarlos; esto es, sugiere diversas soluciones, no las impone y su misión principal es fomentar medidas preventivas y de corrección en apoyo al control informático para los riesgos mayores inherentes a la operación. Además, la auditoría informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel mundial.

Los objetivos principales de la auditoría informática son:

1. *Asegurar que la función de auditoría cubra y proteja los mayores riesgos y vulnerabilidades existentes en el medio informático del negocio.*
2. *Asegurar que los recursos de informática (hardware, software, telecomunicaciones, servicios, personal, etc.) sean orientados al logro de los objetivos y las estrategias de las organizaciones.*
3. *Asegurar la formulación, elaboración y difusión formal de las políticas, controles y procedimientos inherentes a la auditoría que garanticen el uso y aprovechamiento óptimo y eficiente de cada uno de los recursos informáticos en el negocio.*
4. *Asegurar el cumplimiento formal de las políticas, controles y procedimientos definidos en cada proyecto de la auditoría mediante un seguimiento oportuno.*
5. *Asegurar que se den los resultados esperados por el negocio.*

La auditoría informática debe ser respaldada por un proceso formal que asegure su entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Al igual que otras funciones en el

negocio, la auditoría en informática efectúa sus tareas y actividades mediante una metodología

Para los administradores de sistemas Linux/Unix, una de sus mayores tranquilidades al auditarlos reside en el sistema log*, el cual registra cualquier acción o procedimiento junto con una serie de información adicional sobre éste para su posterior análisis, esto es, ayuda al diagnóstico de errores y a la prevención de catástrofes puesto que dificulta una intrusión.*
El sistema de log *en entornos Linux/Unix funciona a nivel de sistema operativo, a nivel de aplicación e incluso, a nivel de protocolo.*

"Más que un inhibidor, la seguridad debe ser vista como un habilitador de negocios".

"La seguridad es una filosofía y conforme aumenta la dependencia entre el negocio y la tecnología, la seguridad de la información se vuelve más crítica para su supervivencia".

[1] **"Hacker, la Biblia"**, *Carlos Míguez Pérez, ediciones Anaya Multimedia, Madrid 2003.*

CAPÍTULO 3
Aspectos Estratégicos en la Configuración del Sistema Operativo

Introducción

La seguridad es hoy en día una gran realidad dentro de cualquier entorno informático y ésta comienza con una adecuada configuración del sistema operativo que soporta a las distintas infraestructuras informáticas. Por esta razón, es importante mencionar a detalle los elementos que conforman la arquitectura de seguridad de Linux, sistema operativo que se ha elegido para que sea la plataforma principal de los servidores que se encuentran en la Gerencia de Tecnología Informática del Instituto Mexicano del Petróleo. Los aspectos principales que conforman la seguridad de Linux permiten cumplir con un esquema bastante aceptable dentro de los niveles de seguridad establecidos, lo cual marca una gran diferencia con los sistemas operativos de la plataforma Microsoft.

3.1 Generalidades de Linux

Linux es un sistema operativo, multiusuario, multitarea, de tiempo compartido y totalmente orientado a la red que trabaja con tecnología cliente-servidor. Linux fue creado originalmente por Linus Torvalds en la Universidad de Helsinki, Finlandia, basado en una pequeña implementación de Unix para PC denominada Minix y el cual apareció por primera vez en Internet a finales de 1991. Linus hizo que el código fuente fuera de libre distribución (open source) y

animó a otras personas a colaborar en su desarrollo con el fin de que se realizaran cambios, se ejecutaran reparaciones de errores, se instalaran parches y se realizaran mejoras, todo con la única intención de que el software funcione cada día mejor.
Como resultado de todo ello el software por completo se desarrolla rápida y eficazmente.
Las características más importantes de Linux son:

- **Multitarea**. *Desde su concepción, Linux fue diseñado completamente como un sistema multitarea por lo que puede administrar dos o más procesos o tareas de forma simultánea; éstas tareas las controla con base en su propia eficiencia (versión del kernel), en la cantidad de memoria RAM disponible en la computadora, en la velocidad del procesador y en la capacidad y velocidad del disco duro.*

- **Multiusuario**. *Linux es un sistema operativo capaz de responder a las solicitudes de varios usuarios que emplean una misma computadora simultáneamente, pero que tienen necesidades diferentes (y durante cada sesión también se pueden realizar varias tareas). Con esto, el sistema operativo lleva el control de sus actividades, les asigna espacio del disco duro a cada uno, les permite entrar a sus cuentas o permisos y les restringe el acceso a los distintos programas, utilerías, documentos, espacios, etc.*

- **Multiplataforma**. *Linux es soportado por computadoras personales con procesador 386, 486, Pentium, Pentium Pro, Pentium II, III y 4, Amiga o Atari, pero además existen versiones para plataformas como Alpha y Power PC.*

- **Sistema de archivos**. *Linux tiene la capacidad de operar con diversos sistemas de archivos como la FAT de DOS, la VFAT de Windows 9x, la OS2/FS o la ISO9660.*

- **Red**. *Linux ha sido desarrollado como un sistema operativo para trabajo en red, cuyo protocolo principal es TCP/IP; actualmente soporta también los protocolos SLIP/PPP, PLIP, NFS, Telnet, TNP, SMTP, IPX, AppleTalk, etc., y puede trabajar con casi todas las tarjetas de red existentes en el mercado.*

- **32 bits reales**. *Linux corre a 32 bits reales en una computadora personal y a 64 en una Alpha; su kernel opera en el modo protegido del procesador y sus librerías emplean el enlace dinámico, con lo que varios programas o utilerías pueden ocupar la misma librería sin que ésta deba ser cargada en la memoria repetidamente sino una sola vez.*

- **Entorno**. *Otra característica de Linux es que puede trabajar sin conflicto tanto en modo texto como en entornos gráficos que emplean sistemas de ventanas estilo Windows. Ejemplos de estos entornos gráficos son FWVM, GNOME, KDE, CDE, Enlightenment, NextLevel, etc. En este caso la variedad de entornos soportados depende del tipo de tarjeta de video y del propio monitor, configurados durante la instalación.*

- **Memoria virtual**. *Linux puede utilizar una porción del disco duro como memoria virtual, lo que aumenta la eficacia del sistema, al mantener los procesos activos en el disco duro y al colocar partes inactivas, o utilizadas con menos frecuencia, en la memoria de disco. La memoria virtual también utiliza toda la memoria del sistema y no permite que se produzca segmentación.*

- **Compatibilidad con el estándar IEEE POSIX.1**. *Gracias a esta compatibilidad, Linux soporta muchos estándares establecidos para todos los sistemas Unix.*

- **Código fuente no propietario**. *El kernel de Linux no utiliza código de AT&T ni ninguna otra fuente propietaria. Otras organizaciones, como las compañías comerciales, el proyecto GNU y los programadores de todo el mundo han desarrollado software para Linux.*

- **Soporte mediante software GNU**. *Linux puede ejecutar una amplia variedad de software, disponible gracias al proyecto GNU. Este software incluye todo lo que un usuario puede necesitar, desde desarrollo de aplicaciones (GNU C y GNU C++) hasta la administración del sistema (gawk, grof, etc.) y juegos (GNU Chess, GnuGo, y NetHack).*

Algunas otras características son: soporte de servicios Web, servidores de correo, POP3, IP Masquerading e Ipv6.

Linux se distribuye bajo los términos de la GPL o Licencia Pública General de la Fundación de Software Gratuito. Esta licencia preserva los derechos de autor en el software, pero garantiza la distribución de los programas con el código fuente. Linux es un sistema operativo independiente apropiado para llevar una contabilidad, bases de datos y registros generales, para matemáticas avanzadas y otras ciencias de ingeniería, para desarrollo de aplicaciones, etc. Sin embargo, si se utiliza como sistema independiente y se realizan conexiones on-line *es necesario implantar medidas de seguridad en la red.*

De momento se describirán seis componentes de la arquitectura de seguridad de Linux.

3.2 Componentes de la Arquitectura de Seguridad de Linux

Desde un punto de vista personal, para lograr un nivel de seguridad adecuado desde el mismo sistema operativo, se deben tomar en cuenta seis aspectos principales en la configuración de Linux. Estos aspectos a considerar son independientes de las aplicaciones y servicios que ofrece un sistema Linux, es decir, no dependen de las necesidades específicas del entorno sino que sólo pretenden disminuir las vulnerabilidades que todo sistema operativo tiene.

COMPONENTE	DESCRIPCIÓN
Cuentas de usuario	Cada cuenta de usuario es una identidad independiente con derechos de acceso independientes. Cada usuario recibe un directorio principal y un espacio en el disco duro y esta ubicación es independiente de los archivos del sistema y de las áreas que ocupan los restantes usuarios
Control de acceso discrecional	Linux puede controlar el grado de acceso que tiene los usuarios a los archivos y directorios; es decir, para cada archivo, un usuario puede especificar quién puede leerlo, quién puede escribir en él o quién puede ejecutarlo
Control de acceso a la red	Es la capacidad para permitir a determinados usuarios y hosts conectarse entre sí mediante el uso de reglas de acceso estrictamente definidas
Cifrado	Los diversos mecanismos de cifrado permiten proteger las contraseñas y los datos que circulan por la red
Registro, Auditoría y control de red	La capacidad de registro fundamental para la seguridad de los sistemas porque proporciona la única evidencia real de que se ha producido un ataque y Linux graba registros a nivel de red, de host, y de usuario
Detección de intrusiones	Examinando todo el tráfico en un segmento de red, Linux tiene la capacidad para detectar intentos de intrusión en tiempo real haciendo uso de reglas de comparación y emparejamiento de patrones. De esta manera se pone en alerta al administrador del sistema ante cualquier ataque

Tabla 4.1 Componentes de la Arquitectura de Seguridad de Linux

3.2.1 Cuentas de Usuario

En Linux toda la potencia administrativa se confiere a una sola cuenta llamada root *(raíz), que es el equivalente al Administrador de Windows NT o al Supervisor de Netware; con esta cuenta se controla todo, incluyendo cuentas de usuario, archivos y directorios y recursos de red. La cuenta* root *permite realizar cambios masivos en todos los recursos, o cambios específicos solamente en unos pocos. Por ejemplo, cada cuenta es una entidad independiente con un nombre de usuario, una contraseña y unos derechos de acceso independientes, lo que permite otorgar o denegar accesos a cualquier usuario o grupos de usuarios. Linux mantiene aislados a los usuarios de esta forma, en parte por motivos de seguridad y en parte para imponer un orden en un entorno algo caótico.*

Para mantener el orden, Linux mantiene aislados los directorios de los usuarios. Cada usuario recibe un directorio principal y un espacio en el disco duro y esta ubicación es independiente de los archivos del sistema y de las áreas que ocupan los restantes usuarios. Con ello se evita que la actividad normal de los usuarios afecte al sistema de archivos y, además, proporciona a los usuarios una cierta privacidad.
Conocer bien los distintos tipos de usuarios existentes y cómo gestionarlos es fundamental para la seguridad del sistema, ya que una cuenta, en el sentido más general, consta de dos elementos: la autorización para iniciar una sesión y la autorización para acceder a los distintos servicios.

- **Usuario root**. *El usuario de más alto nivel en cualquier sistema Linux es el llamado* root *(o raíz) y es el que tiene el control absoluto sobre la totalidad de componentes de la máquina: nada está oculto para un usuario* root *y puede hacer siempre lo que quiera. Por lo tanto, para un cracker o hacker malicioso entrar como* root *en un sistema Linux le supone obtener control total sobre él. Si se observa la entrada correspondiente al usuario root en el archivo /etc/passwd se puede ver que el ID o identificador del usuario root es cero. Cualquier cuenta de usuario con un ID cero es un usuario root, incluso aunque su nombre de usuario este cambiado. El poder que tiene root sobre el sistema sólo es superado por el del propio núcleo del sistema y es éste el que establece las restricciones de root.*
- **Usuarios normales**. *Son aquellos que pueden conectarse al sistema y realizar tareas básicas como navegar por la Web, leer el correo, crear documentos, etc. Estos usuarios tienen normalmente un directorio personal y pueden crear y manipular archivos dentro de ese y de algún otro directorio del sistema. Estas son las cuentas de los usuarios estándar que la gente normal utiliza para hacer su trabajo. Los usuarios normales tienen, como norma general, restringido el acceso a archivos y directorios del sistema y, por lo tanto, no pueden realizar ninguna tarea a nivel de sistema.*
- **Usuarios de sistema**. *Los usuarios de sistema no se conectan a la máquina, son cuentas de usuario que se utilizan para propósitos específicos del sistema y que no pertenecen a una persona en particular. Ejemplos de estos usuarios los tenemos en* **ftp**, *el cual es utilizado normalmente para el acceso como FTP anónimo; el usuario* **apache** *que es el que resuelve normalmente las peticiones HTTP (algunas distribuciones de Linux llaman a este usuario* nobody *o* www-data*); y el usuario* **lp**, *el cual maneja las peticiones de impresión.*

Al crear sus cuentas, los distintos usuarios se organizan en grupos dependiendo de sus tareas respectivas y de sus necesidades de acceso. Finalmente, se definen con mayor precisión los derechos de acceso individuales de cada usuario en aquellos lugares en los que difieran de los de su grupo. El

concepto de grupo se da con el propósito de proteger un cierto conjunto de usuarios, junto con toda su información, de otro. En los sistemas sin ocultación, los datos de los grupos se almacenan en /etc/group*. Aunque todos los usuarios de los grupos tendrán los mismos derechos de acceso, se debe asignar a la parte responsable del mantenimiento o propietario de los archivos del grupo. Además, siempre que el usuario sea miembro del grupo, podrá pasar de un grupo a otro durante la misma sesión utilizando el comando* newgrp*.*

3.2.2 Control de Acceso Discrecional (DAC)

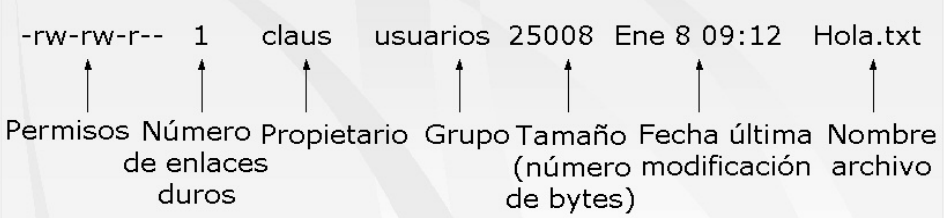
El control de acceso discrecional de Linux permite controlar el grado hasta el que pueden acceder a los archivos y directorios los distintos usuarios (permisos de lectura, escritura y ejecución). Con esto, es posible especificar con total exactitud la forma en que los usuarios acceden a los mismos archivos. Dichas limitaciones se implementa a través de los grupos.

Como Linux es un sistema operativo multiusuario, una máquina Linux puede tener más de un usuario conectado al sistema simultáneamente, y cada uno de esos usuarios puede, si así lo desea, establecer más de una sesión a la vez.

Dentro del sistema Linux todo son archivos, desde la memoria física del equipo hasta el ratón, pasando por módems, teclado, impresoras o terminales. Esta filosofía de diseño es uno de los factores que más éxito y potencia proporciona a Linux pero también uno de los que más peligros entraña. En un sistema Linux típico existen tres tipos básicos de archivos:

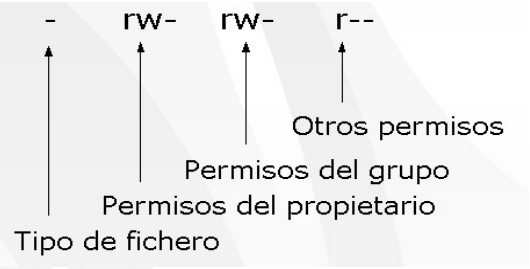
1. **Archivos planos**, *los cuales son secuencias de bytes que a priori no poseen ni estructura interna ni contenido significante para el sistema: su significado depende de las aplicaciones que interpretan su contenido*
2. **Directorios**, *son archivos cuyo contenido son otros archivos de cualquier tipo (planos, más directorios, o archivos especiales)*
3. **Archivos especiales**, *que representan dispositivos del sistema*

El sistema de permisos sobre archivos en Linux es un mecanismo que permite restringir el acceso a un usuario a un determinado archivo o directorio del sistema de archivos. Para cada archivo, un usuario puede especificar quién puede leerlo, quién puede escribir en él o quién puede ejecutarlo (en caso de que sea ejecutable). Ejemplo, ejecutamos el comando claus$ **ls -l hola.txt**, *el cual nos da la siguiente salida:*



La información de los permisos está dividida en cuatro partes; el primer caracter de la salida indica el tipo de archivo, los cinco tipos más comunes son:

- *-, Un archivo normal*
- *d, un directorio*
- *b, archivo de bloques especial*
- *c, es un archivo de caracteres especial*
- *l, un enlace simbólico*
- *s, un socket*
- *p, una canalización (pipe) FIFO*



A continuación del tipo de archivo podemos ver tres grupos de tres caracteres cada uno, y que representan los permisos que tienen sobre el archivo el propietario, el grupo y el resto de usuarios, respectivamente. Los tres caracteres indican si se tiene o no permiso para leer el archivo (r), para escribir en el archivo (w) o para ejecutar el archivo (x). Si se tiene el permiso adecuado aparecerá la letra correspondiente, de lo contrario, la posición de la letra la ocupará un guión (-).

Para definir los permisos de un usuario determinado sobre un archivo o un directorio se utiliza el comando chmod*. El método consiste en añadir letras (r, w, x) para asignar el permiso adecuado a cada archivo individual o directorio. Otra forma es utilizando el sistema octal, donde se pueden añadir valores octales para crear un conjunto de permisos final. Si se utilizan valores octales puros hay que añadirlos juntos.*
Durante la instalación, Linux gestiona los permisos de los archivos del sistema operativo, sin embargo, dichos permisos no son siempre correctos lo que puede hacer que aparezcan problemas en la seguridad.

Existen en Linux dos tipos de permisos especiales para los archivos:

1. **SGID** *(define el ID de grupo, 2000 octal o S)*
2. **SUID** *(define el ID de usuario, 4000 octal o S)*
3. **El bit de persistencia "t"**

Cuando un programa es SUID o SGID, una "s" sustituye a la "x" que corresponde al bit de ejecución del usuario o grupo. Esto es peligroso pero necesario para algunos programas. Por ejemplo, un usuario normal no puede leer o escribir en el archivo /etc/shadow*; para que ese usuario normal (sin privilegios) pueda cambiar su contraseña, el ejecutable* passwd *debe ser SUID del usuario root. El bit SGID funciona del mismo modo para los grupos. El bit de persistencia, mostrado como "t" en lugar del bit de ejecución normal para el nivel "otros usuarios" se usa normalmente en directorios tales como* /tmp*. Este atributo en concreto hace que sólo el propietario del archivo pueda eliminarlo; otros pueden leerlo, pero sólo el propietario puede eliminarlo.*
Los programas con permisos de este tipo son especiales, ya que los permisos de su propietario se respetan aún cuando los ejecuten otros usuarios. Es decir, si se

define el valor root *SUID en un programa, éste siempre se ejecutará como* root *aunque lo utilice un usuario normal. Por este motivo este tipo de archivos pueden suponer un enorme riesgo para la seguridad del sistema.*

Existen otros permisos de archivos que se deben conocer. Estos permisos son más específicos del sistema de archivos ext2 *que del archivo mismo y tienen un significado cuando se activan (ver tabla 4.2).*

Estos atributos se pueden activar y desactivar utilizando el programa chattr (cambiar atributos).

Nivel	***Permisos***
A	*Modificación de* atime *inhabilitada*
a	*Solamente agregar al final*
d	dump *inhabilitado*
i	*Inmutable (no se puede modificar ni eliminar el archivo)*
s	*Borrado seguro activado*
S	*Actualizaciones síncronas*

Tabla 4.2 Permisos especiales de archivos

Dado que las organizaciones se dividen en departamentos y que es posible que varios usuarios de dichos departamentos tengan que acceder a los mismos archivos, Linux permite agrupar a los usuarios. Dicha gestión a nivel de grupo resulta muy útil cuando hay muchos usuarios y varios subconjuntos de usuarios necesitan privilegios idénticos o muy parecidos.

3.2.3 Control de Acceso a la Red

Proteger la red es el principio para poder proteger la información, ya que Internet representa la entrada de los ataques lógicos más sofisticados, los cuales pueden causar pérdida o alteración de información, e incluso fallas y/o suspensión en el servicio que se ofrece a los diferentes usuarios que se encuentran conectados a una red. Toda la infraestructura informática que hace posible el procesamiento de datos depende de una red por la que se pueda intercambiar información y compartir recursos para que las transacciones de una empresa se lleven a cabo de forma más sencilla. Por todo esto, es importante que se cuente con un control de red que permita aislarla de manos enemigas.

Cualquier programa puede ser víctima de errores provocados por fallas en la programación. Sin embargo, un error en un servicio al que se pueda acceder desde la red puede ser explotado directamente por un atacante. Algunos de estos ataques proporcionan una shell *de* root *enganchada a un puerto TCP al que cualquiera va a poder conectarse. Por sistema de red de un equipo Linux se entiende el conjunto de software que posibilita la interconexión entre diferentes*

máquinas. Este software esta dividido en dos espacios: por un lado, tenemos el soporte de red dentro del kernel *del sistema operativo, encargado de implementar las tareas de más bajo nivel necesarias para la comunicación entre sistemas, como la pila de protocolos TCP/IP o los controladores de tarjetas de red; por otro, ya en el espacio de usuario, tenemos el conjunto de programas y archivos utilizados para configurar parámetros del sistema relacionados con la red, como la dirección IP, las tablas de ruteado, o el comportamiento de una máquina ante solicitudes de servicio desde otros equipos conectados lógicamente a ella.*

Hoy en día es muy común que las redes utilicen la dirección IP de un sistema como único mecanismo de autenticación. Sin embargo, aquellos servicios que aceptan o rechazan un intento de conexión basándose en la dirección IP del cliente son poco efectivos, ya que un atacante podría suplantar una de esas direcciones, es decir, un cracker puede engañar de muchas formas al sistema para que crea que una máquina o una dirección IP es otra distinta. Linux también proporciona control de acceso a redes o la capacidad para permitir a determinados usuarios y hosts *conectarse entre sí; es decir, es posible implantar reglas de acceso a la red extremadamente definidas, por ejemplo, un usuario que deba utilizar una máquina determinada para poder conectarse (con una IP fija) o uno que pueda conectarse libremente desde el lugar que desee. Restringir el acceso a determinadas direcciones IP o direcciones de red es una buena idea, pero como medida adicional de protección se debe considerar la idea de desactivar todos los servicios de conexión y de transferencia de archivos como telnet, FTP, etc. y sustituirlos por* Secure Shell, *el cual proporciona un proceso de cifrado y autenticación adecuado y que es más difícil de atacar. Algunos de los archivos que hay que tomar en cuenta son:*

1. **/etc/hosts**. *Este archivo se utiliza para obtener una relación entre un nombre de máquina y una dirección IP. Habitualmente se suelen incluir las direcciones, nombres y alias de todos los equipos conectados a la red local, de forma que para comunicación dentro de la red no se tenga que recurrir a DNS a la hora de resolver un nombre de máquina.*

2. **/etc/ethers**. *En este archivo se establece una correspondencia entre nombres de máquina y direcciones* ethernet, *en un formato muy similar al archivo anterior.*

3. **/etc/networks**. *Este archivo, cada vez más en desuso, permite asignar un nombre simbólico a las redes, de una forma similar a lo que* /etc/hosts *hace con las máquinas. En cada línea del archivo se especifica un nombre de red, su dirección y sus alias.*

4. **/etc/services**. *En cada línea de este archivo se especifican el nombre, número de puerto, protocolo utilizado y alias de todos los servicios de red existentes (o, si no de todos los existentes, de un subconjunto lo*

suficientemente amplio para que ciertos programas de red funcionen correctamente). El archivo /etc/services *es utilizado por los servidores y por los clientes para obtener el número de puerto en el que deben escuchar o al que deben enviar peticiones, de forma que se pueda cambiar (aunque no es lo habitual) un número de puerto sin afectar a las aplicaciones.*

5. **/etc/protocols**. *El sistema de red en Linux utiliza un número especial, denominado número de protocolo, para identificar el protocolo de transporte específico que la máquina recibe; esto permite al software de red decodificar correctamente la información recibida. En el archivo* /etc/protocols *se identifican todos los protocolos de transporte reconocidos junto a su número de protocolo y sus alias.*

Esta funcionalidad viene muy bien en los entornos de red o cuando el sistema Linux es un servidor de Internet. Posiblemente la protección mediante contraseña es una buena idea, pero si se quiere dar un paso más, quizás se desee impedir que hosts *no autorizados intenten conectarse.*

Habitualmente, cuando se transmiten datos a través de Internet atraviesan muchos gateways. En su camino, dichos datos son vulnerables a escuchas electrónicas. Linux cuenta con varias utilidades complementarias que permiten cifrar o codificar los datos para que si alguien los captura solo sea capaz de ver un tremendo desorden de letras. El servicio Secure Shell *(SSH) intenta resolver estos problemas de manera excelente.*

Programa	***Descripción***
make-ssh-known-hosts	*Un* script *de Perl que crea una base de datos de hosts (busca automáticamente todos los host en el dominio especificado a través de DNS)*
scp	*El programa* Secure Copy *de Secure Shell ofrece un medio seguro para copiar archivos de un host a otro. Funciona como* rcp*, pero utiliza* ssh *para facilitar las transferencias*
ssh	*El cliente se Secure Shell funciona de forma similar a un cliente telnet. Una vez conectado al servidor,* ssh *puede utilizarse para ejecutar comandos básicos del sistema y, en todos los sentidos, la sesión de* ssh *se parecerá a una sesión de telnet*
ssh-add	*Agrega identidades (registra nuevas claves) al agente de autenticación de* ssh-agent
ssh-agent	*Se utiliza para realizar autenticación del estilo RSA a través de redes cuando se utiliza* shh*. Permite a los host remotos acceder y almacenar claves privadas de RSA*
sshd	*El servidor de Secure Shell, que de forma predeterminada escucha el puerto 22. Cuando* sshd *recibe una solicitud de conexión de un cliente* ssh *válido, inicia una nueva sesión*
ssh-keygen	*El generador de claves para* ssh*. Con* ssh-keygen *los usuarios pueden generar una clave de RSA que posteriormente puede utilizarse para la autenticación tanto local como remota (la autenticación la lleva a cabo el* ssh-agent*)*

Tabla 4.3 Programas de la suite ssh

Este programa se incluye en la mayoría de las distribuciones de Linux y es un sustituto seguro de telnet, FTP, X11y de los r-comandos de Berkeley. SSH usa otras técnicas criptográficas para efectuar una potente autenticación de los hosts y de los clientes. Esto significa, que se puede tener un alto grado de confidencialidad en la que solo los usuarios autorizados tienen permiso para conectarse. Para reforzar la resistencia de la red a los sniffers es aconsejable ofrecer servicios SSH en todo el sistema. La distribución de ssh *se compone de varios programas (ver tabla 4.3).*

3.2.4 Cifrado

Además de la administración centralizada y del control de acceso a redes, Linux proporciona una gran variedad de mecanismos de cifrado de contraseñas y punto a punto para proteger los datos que circulan por la red, entendiendo como cifrado el proceso de mezclar los datos para que no puedan leerlos personas que no tengan autorización para ello.

En orden jerárquico en cuanto a seguridad, los ataques a contraseña son lo primero, por lo que una deficiente seguridad de las contraseñas pone en peligro a todo el sistema. Por esta razón, la seguridad de un sistema Linux (y en general de cualquier sistema) comienza por la aplicación de contraseñas que impidan el acceso de personas no autorizadas. Originalmente, todos los sistemas Linux utilizaban /etc/passwd *para almacenar la pareja de usuario y contraseña necesaria para autenticar a un usuario y permitirle el acceso al sistema. Sin embargo, las contraseñas de Linux no se almacenan como texto claro dentro del sistema. En vez de eso, la contraseña se transforma en una cadena de texto mediante un algoritmo llamado* hash criptográfico*. La cadena resultante, llamada* hash *o* valor hash*, tiene un aspecto muy diferente a la contraseña original. Existen varios tipos de algoritmos hash, pero todos son irreversibles; es decir, no hay manera de recuperar la contraseña original partiendo del hash.*

Las contraseñas de Linux se crean utilizando un avanzado algoritmo de cifrado de IBM llamado Estándar de Cifrado de Datos (DES, Data Encryption Standard). Funcionalmente, DES es un cifrado de bloque que se apoya en una clave derivada de la contraseña que se ha elegido y la cual consta de 64 dígitos binarios. Aunque DES es realmente un algoritmo de cifrado, la función crypt(3) *lo usa como algoritmo* hash *(algoritmo irreversible), lo que significa que no hay manera de recuperar la contraseña original. La función* crypt(3) *necesita dos argumentos: una clave y una sal para devolver el valor hash. Una sal no es más que una cadena de bytes (cuyo número dependerá del algoritmo que se utilice) necesaria para la generación del valor hash. El propósito de la sal es dificultar la adivinación de la contraseña. Cuando el programa* passwd *cambia la contraseña de un usuario, elegirá una sal aleatoriamente y aún en el caso de*

que dos usuarios elijan la misma contraseña, la sal asignada será distinta; por lo tanto, el valor hash obtenido será completamente diferente.

Dado que Linux almacena las contraseñas cifradas en el directorio /etc/passwd, *es conveniente actualizarlo o instalar el* shadowing *de contraseñas manualmente. Ello se debe a que, aunque los atacantes deben buscar en un mínimo de 32 cuatrillones de claves para encontrar la clave correcta, pueden concatenar* /etc/passwd *con un archivo y utilizar las claves cifradas para llevar a cabo un sencillo ataque a diccionario.*

Existen varias herramientas para realizar el shadowing, *pero la más popular es* Linux Password Shadow Suite, *que lleva años utilizándose. Sin embargo, dependiendo del tipo y antigüedad de la distribución, puede tenerla o no. La* Suite shadow *implementa dos nuevos conceptos del mantenimiento básico de las bases de datos de contraseñas:*

- **Vencimiento de la contraseña**. *Es cuando se limitan las contraseñas a un tiempo de vida finito. Cuando este tiempo se termina, Linux obliga a los usuarios a crear nuevas contraseñas. Si se utiliza el vencimiento de contraseñas junto con la comprobación proactiva de las mismas, la seguridad mejora.*
- **Bloqueo automático de cuenta**. *Simplemente se avisa a los usuarios de la necesidad de cambiar sus contraseñas. Como los usuarios suelen ser perezosos y propensos a olvidarlo, lo mejor es bloquear sus cuentas. Con la suite de shadow el bloqueo se efectúa de forma automática. (Se pueden especificar las reglas de bloqueo).*

La suite de shadow es bastante segura por sí misma, pese a ello, su seguridad depende desafortunadamente de la seguridad del sistema, ya que muchas otras aplicaciones tienen agujeros que permiten a los atacantes leer e incluso escribir en etc/shadow. *Por otro lado, el cifrado es un componente vital de la seguridad, sin embargo, fallará si los usuarios eligen contraseñas débiles.*

Un avance reciente en cuanto a autenticación son los Módulos de Autenticación Conectables (PAM), un conjunto de módulos de código que capacitan al administrador del sistema para configurar los métodos de autenticación usados por las aplicaciones de Linux. También se pueden añadir o modificar los métodos de autenticación sin tener que reconstruir la aplicación que los utiliza. Los PAM proporcionan muchas opciones de gestión de autenticación, de cuentas, de sesiones y de contraseñas pues utiliza varios archivos como ayuda para determinar si la autenticación se aprueba o se deniega. El primer conjunto de archivos que se necesita conocer es el que está en el directorio /etc/pam.d. *Cada archivo de este directorio contiene los métodos de autenticación requeridos para autenticar un servicio y la*

información que presenta contiene cuatro columnas, de las cuales la primera especifica el tipo, que puede ser uno de los siguientes:

- **auth (autenticación)**. *Este tipo se encarga de verificar que el usuario es quien pretende ser. Normalmente, esto se hace a través de una pareja nombre de usuario/contraseña, pero también se puede hacer con un dispositivo biométrico o con una tarjeta inteligente.*
- **account (cuenta)**. *Verifica los privilegios de acceso y el estado de una cuenta determinada (*active *(activa),* expired *(caducada),* inactive *(inactiva) o* disabled *(inhabilitada)).*
- **password (contraseña)**. *Se usa para actualizar los elementos de autenticación. Si una contraseña ha caducado, se obliga a una actualización.*
- **session (sesión)**. *Prepara el entorno para el usuario. Puede llevar a cabo acciones de registro y ejecutar programas al iniciar y finalizar la sesión (como montar directorios, ejecutar* chroot *y otros).*

La segunda columna es el campo de control e indica cómo se usa el valor que devuelve el módulo. Los módulos devuelven SUCCESS (éxito), FAILURE (fallo) o IGNORE (ignorar) como valores para la biblioteca PAM. IGNORE significa que el módulo no pudo determinar el éxito o el fallo. La tercera columna especifica el módulo concreto a usar. Los módulos se instalan de forma predeterminada en /lib/security*. La cuarta columna contiene cualquier opción que se le desee asignar al módulo.*
Los sistemas de archivos cifrados pueden utilizarse para disminuir muchos de los ataques que se hacen contra la información almacenada en las máquinas. Sin embargo, no las protegerá de un posible robo.

Hoy en día se ha vuelto una necesidad la encriptación de los datos que viajan a través de la red con el propósito de mantener la confidencialidad e integridad de los mismos. Cuando un intruso tiene acceso a la red interna de una organización, también tiene acceso a su información y puede hacer con ella lo que él quiera. Sin embargo, si la información viaja encriptada por la red, es muy difícil que ésta le sea útil aunque la tenga en sus manos, puesto que no podrá entender de lo que se trata. Actualmente existen diversos algoritmos de encriptación que pueden implementarse bajo Linux, ya sean de clave pública o de clave privada que ayudan a proteger la información en tránsito. Pero además de esto, lo más aconsejable es utilizar la aplicación Secure Shell *(SSH), la cual permite remplazar aplicaciones como FTP o Telnet de forma segura. Entre todas las ventajas, destaca el uso de un potente cifrado para los datos transmitidos, con lo que ni las contraseñas ni otros datos pueden ser interpretados ni siquiera por atacantes que se encuentran escuchando el tráfico de la red. El uso del cifrado impide también los ataques en los que el intruso entra en una conexión existente y cambia los datos en las dos direcciones.*

3.2.5 Registro, Auditoría y Control de Red Integrados

Desgraciadamente, aunque se apliquen rápidamente todos los controles de seguridad disponibles, a veces salen a la superficie nuevos puntos vulnerables y los intrusos de inmediato sacan partido de estas oportunidades mediante el ataque al mayor número de máquinas antes de que se arregle el agujero. Linux no puede predecir cuándo va sufrir un ataque un host, pero puede registrar los movimientos de la persona que realiza dicho ataque porque tiene exhaustivas capacidades de registro; Linux detectará, marcará la hora y grabará las conexiones de red y esa información se redirige a los registros del sistema para su posterior análisis.

La capacidad de registro es un componente vital de la arquitectura de seguridad de Linux y proporciona la única evidencia real de que se ha producido un ataque. Teniendo en cuenta que hay un gran número de metodologías de ataque distintas, Linux graba registros a nivel de red, de host, y de usuario. Por ejemplo:

- *Registra todos los mensajes del sistema y del núcleo (kernel)*
- *Registra todas las conexiones de red, la dirección IP de la que parte cada una de ellas, su longitud, y, en algunos casos, el nombre de usuario y sistema operativo de la máquina desde la cual se realiza el ataque.*
- *Registra los archivos que solicitan los usuarios remotos*
- *Puede registrar qué procesos se encuentran bajo el control de cualquier usuario*
- *Puede registrar todos y cada uno de los comandos que ha emitido un usuario determinado.*

El logging *es cualquier procedimiento por el que un sistema operativo o aplicación graba eventos mientras ocurren y los guarda para un examen posterior. El* logging *en Linux es dominante y sucede en los niveles de sistema, aplicación e, incluso, protocolo. De hecho, Linux guarda* logs *de casi todas las cosas: peticiones de conexión, fallos del equipo, negación de servicio, comandos de usuario, tráfico de paquetes, etc. Y, aunque existen excepciones, la mayoría de los servicios Linux imprimen información* log *en archivos estándar o en archivos* log *compartidos que residen en* /var/log. *El demonio* syslogd *(Syslog Daemon) se lanza automáticamente al arrancar un sistema Linux, y éste es el encargado de guardar informes sobre el funcionamiento de la máquina. Recibe mensajes de las diferentes partes del sistema (núcleo, programas, etc.) y los envía y/o almacena en diferentes localizaciones, tanto locales como remotas, siguiendo un criterio definido en el archivo de configuración* /etc/syslog.conf, *donde especificamos las reglas a seguir para gestionar el almacenamiento de mensajes del sistema. Tal es su dominio que Linux ofrece herramientas para actualizar, rotar, formatear, combinar y analizar* logs.

Algo muy interesante de los archivos log *en Linux es que la mayoría de ellos son simples archivos de texto, que se pueden visualizar con un simple* cat*. Por una parte esto es bastante cómodo para el administrador del sistema, no obstante, este hecho hace que un atacante lo tenga muy fácil para ocultar ciertos registros modificando los archivos con cualquier editor de textos; esto implica una cosa muy importante para un administrador: nunca debe confiar al 100% en lo que los informes de auditoría del sistema le digan. Para minimizar estos riesgos se pueden tomar diversas medidas como utilizar una máquina fiable que utilice un eficaz método de encriptación para registrar información del sistema o incluso enviar los registros más importantes a una impresora en tiempo real.*

Los registros son indispensables cuando se investigan las intrusiones en la red. Sin embargo, dado que Linux graba los registros en tiempo real, se podrá pensar que debe existir alguna forma en la que Linux responda a los ataques. Dicha forma existe.

3.2.6 Detección de Intrusiones

La detección de intrusiones es la práctica de utilizar herramientas inteligentes y automáticas para detectar intentos de intrusión en tiempo real. Dichas herramientas son llamadas Sistemas de Detección de Intrusos (IDS). La detección de intrusiones es una ciencia relativamente nueva que emergió a comienzos de los 80's por lo que hay muy pocos sistemas operativos que incluyen herramientas de detección de intrusos, y la mayoría no están disponibles para que los utilice el público en general. De hecho, hace muy poco tiempo que dichas herramientas se han introducido en las distribuciones estándar de Linux y con ellas, junto con los complementos que pueden descargarse de Internet, es posible establecer una avanzada capacidad de detección de intrusiones:

- *Es posible hacer que Linux registre los intentos de intrusión y que avise cuando se produzcan dichos ataques*
- *Es posible hacer que Linux lleve a cabo acciones predefinidas cuando los ataques cumplan unos criterios específicos (por ejemplo,* **si la persona que ataca hace esto, haz esto***)*
- *Es posible hacer que Linux distribuya desinformación; por ejemplo, que imite a un sistema operativo que no sea Linux. En este caso la persona que lleva a cabo el ataque pensará que está desprotegiendo a un sistema Windows NT o Solaris.*

Una forma de clasificar los sistemas de detección de intrusos es:

1. **Sistemas basados en normas**. *Basados en bibliotecas y bases de datos de ataques y firmas responsables de ataques conocidos. Cuando el tráfico entrante se encuentra con un criterio o norma particular, se etiqueta como un intento de intrusión. La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía de nuestro sistema, por lo que si fuéramos capaces de establecer un perfil del comportamiento habitual de los sistemas seríamos capaces de detectar las intrusiones por pura estadística: probablemente una intrusión sería una desviación excesiva de la media de nuestro perfil de comportamiento. La desventaja principal de estos sistemas es que dependen del paso del tiempo (la base de datos de ataques debe ser actual) y del mantenimiento oportuno. Aún más, a veces puede haber una relación inversa entre la especificación de la norma y los índices de detección asegurados. Es decir, si una regla es demasiado específica, los ataques que son similares pero no idénticos a ella, pasarán.*

2. **Sistemas adaptables**. *Éstos emplean técnicas más avanzadas, incluyendo inteligencia artificial, no sólo para reconocer firmas de ataque conocidas, sino para aprender otras nuevas. Las principales desventajas de los sistemas adaptables son su elevado costo, se desarrollan principalmente en entornos de investigación, son difíciles de mantener y requieren de conocimientos avanzados de matemáticas y estadística.*

Los sistemas de detección de intrusos basados en red son aquellos capaces de detectar ataques contra diferentes sistemas de una misma red (en concreto, de un mismo dominio de colisión), aunque generalmente se ejecuten en un solo hosts de esa red. Para lograr su objetivo, al menos uno de los interfaces de red de esta máquina sensor trabaja en modo promiscuo, capturando y analizando todas las tramas que pasan por él en busca de patrones indicativos de un ataque. Casi cualquiera de los diferentes campos de una trama de red TCP/IP puede tener un valor que, con mayor o menor probabilidad, represente un ataque real; los casos más habituales incluyen:

- Campos de fragmentación. *valores incorrectos de parámetros de fragmentación de los datagramas se han venido utilizando típicamente para causar importantes negaciones de servicio a los sistemas y, desde hace también un tiempo incluso para obtener la versión del operativo que se ejecuta en un determinado host*
- Dirección de origen y destino. *No tenemos más que pensar en el tráfico proveniente de nuestra DMZ que tenga como destino nuestra red protegida: es muy posible que esos paquetes constituyan un intento de violación de nuestra política de seguridad. Otros ejemplos clásicos son las peticiones originadas desde Internet y que tienen como destino máquinas*

de nuestra organización que no están ofreciendo servicios directos al exterior, como un servidor de bases de datos cuyo acceso esta restringido a sistemas de nuestra red.

- Puerto origen y destino. *Aparte de los intentos de acceso no autorizado a servicios de nuestros sistemas, pueden detectar actividades que también supondrán a priori violaciones a las políticas de seguridad, como la existencia de troyanos, ciertos tipos de barridos de puertos, o la presencia de servidores no autorizados dentro de nuestra red.*
- Flags TCP. *Cada uno de los campos de una cabecera TCP tiene una finalidad diferente, por lo que ciertas combinaciones de valores suelen ser bastante sospechosas, por ejemplo, una trama con los bits SYN y FIN activados simultáneamente sería indicativa de una conexión que trata de abrirse y cerrarse al mismo tiempo.*
- Campo de datos. *El campo de datos de un paquete que circula por la red es donde más probabilidades tenemos de localizar un ataque contra nuestros sistemas; esto es debido a que con toda probabilidad el firewall corporativo detendrá tramas cuya cabecera sea sospechosa (por ejemplo, aquellas cuyo origen no este autorizado a alcanzar su destino o con campos incorrectos), pero rara vez un firewall se parará a analizar el contenido de los datos transportados en la trama.*

También es posible y necesario que un detector de intrusos basado en red sea capaz de notificar otros ataques que no se pueden apreciar en una única trama; uno de estos ataques es la presencia de peticiones que, aunque por sí mismas no sean sospechosas, por su repetición en un intervalo de tiempo más o menos pequeño puedan ser indicativas de un ataque (por ejemplo, barridos de puertos horizontales o verticales). Otros ataques difíciles de detectar analizando tramas de forma independiente son las negaciones de servicio distribuidas (DDoS, Distributed Denial of Service), justamente por el gran número de orígenes que el ataque tiene por definición.

Actualmente muchos de los sistemas de detección de intrusos más conocidos están basados en el pattern matching *(uso de reglas de comparación y emparejamiento de patrones), utilizando una base de datos de patrones que denotan ataques, estos programas se dedican a examinar todo el tráfico que ven en su segmento de red y a comparar ciertas propiedades de cada trama observada con las registradas en su base de datos como potenciales ataques.*

Todos estos mecanismos forman los componentes individuales de la compleja arquitectura de seguridad de Linux, cuando se utilizan en forma conjunta, se construye un exhaustivo método global en lo relativo a la seguridad de redes.

3.3 Particiones y Seguridad

Las particiones son áreas del disco duro que se reservan para los sistemas de archivos y, durante la instalación, Linux solicita que se haga una partición del disco duro. Las particiones se componen de un conjunto de cilindros contiguos especificados por el usuario y en Linux es recomendable tener más de una partición principalmente para mantener un estricto control sobre el lugar en que acaban los datos, es decir, todo estará más ordenado. Otro caso frecuente es cuando se instalan dos o más sistemas operativos en la misma unidad de disco, pero en distintas particiones. Aunque DOS y Windows no pueden acceder a la partición de Linux, Linux puede acceder a la partición de DOS y copiar archivos.

Número	***Tipo de partición***
2	*Root XENIX, un antiguo sistema basado en la versión 7 de Unix, posteriormente lo han comercializado Microsoft y Santa Cruz Operation (SCO)*
7	*High Performance File System o HPFS, un sistema tolerante a fallos que incorpora almacenamiento en caché avanzada, nombres de archivo largos, etc. Es la base del sistema OS/2*
8	*AIX (Unix de IBM)*
40	*Venix 80286, una versión de Unix de VentureCom compatible con System V*
63	*GNU HURD, es de la fundación Free Software Fundation y acabará siendo el sustituto del* kernel *de Unix*
64	*Novell NetWare*
81	*Minix*
82	*Partición de intercambio de Linux*
83	*Partición nativa de Linux*
93	*Amoeba, un sistema operativo distribuido que funciona en SPARCstations (Sun4c y Sun4m), así como en 386/486, 68030, Sun 3/60. Amoeba se utiliza para aglutinar la potencia de varias estaciones de trabajo en un eficaz bloque de potencia de computación*

Tabla 4.4 Tipos de particiones que admite Linux

Linux admite más particiones de las que aparecen aquí, éstas son solo unos ejemplos, pero hay pocas rutinas de instalación que resalten las relaciones entre las particiones y la seguridad y no indican que dichas configuraciones conllevan ciertos riesgos.

Al agrupar Linux en una sola partición no se deben colocar los sistemas de archivo raíz y de usuario en la misma partición, ya que si se hace aumenta la posibilidad de que las personas que deseen realizar ataques puedan explotar los programas SUID (establecer ID de usuario) para acceder a áreas restringidas. Además, agrupar todo Linux en una sola partición nativa dificulta la capacidad para actualizar o hacer copias de seguridad de los paquetes individuales o sistemas de archivos.

Por otro lado, la existencia de varias particiones ofrece ciertas ventajas:

- *Sencilla gestión de copias de seguridad y actualizaciones*
- *Arranque más rápido (en algunas ocasiones)*
- *La capacidad para controlar cómo se monta cada sistema de archivos*
- *Protección contra programas SUID renegados*
- *La capacidad de evitar la denegación de servicio accidental y proteger de desbordamientos al sistema de archivos*

Dado que las particiones tiene una gran influencia en la seguridad del sistema, es aconsejable que se ponga sumo cuidado en las opciones que se tienen antes de la instalación ya que al crear varias particiones se limita la capacidad de crecimiento de los sistemas de archivos, aunque eso sea lo que, en algunos casos, se persigue.
Para evaluar con precisión el número de particiones que se necesitan y saber qué sistemas de archivos deben dejarse aparte se puede hacer:

- *Es posible que se prefiera un menor número de particiones o dar prioridad a aquellos sistemas de archivos que hay que dejar aparte. En este caso, los sistemas de archivos que deben estar en particiones independientes son el raíz (/), /var y /tmp desde el punto de vista de la seguridad; o el raíz (/), /var y /usr desde el punto de vista administrativo. Como mínimo, es aconsejable dejar el directorio raíz en su propia partición.*
- *Si se asignan particiones a sistemas operativos diferentes de Linux, se debe planear cómo se quiere que Linux las monte; es posible que lo mejor sea que Linux las monte en modo de sólo lectura o que no las monte. De esta forma las protege de cualquier daño accidental.*
- *Si se tiene un* firewall*, un* sniffer *o cualquier otro dispositivo de monitoreo de la red, es apropiado canalizar los registros a su propia partición (preferiblemente en otro disco).*
- *Se debe tener mucho cuidado cuando se definan las opciones de montaje de las particiones, ya que a veces las políticas restrictivas pueden causar problemáticas administrativas.*

3.4 Cargadores de Arranque

Los cargadores de arranque son programas pequeños que gestionan el proceso de arranque del sistema. El proceso de arranque comienza con el registro de arranque maestro, que es el primer sector del disco. Durante la secuencia de arranque tienen lugar los siguientes pasos:

1. *El código de la rutina de carga de arranque se carga en la memoria*
2. *La rutina de carga de arranque selecciona la partición que deberá arrancar siguiendo un mecanismo independiente del cargador*
3. *Una vez seleccionada la partición, la rutina de carga de arranque cede el control al sector de arranque de la partción, que carga el sistema operativo*

En Linux, la herramienta de carga en el arranque más utilizada es LILO (LInux-LOader) y durante la instalación, Linux genera los valores de LILO que pueden ser cambiados si se tienen otras particiones y sistemas operativos. Las opciones de LILO se leen del archivo /etc/lilo.config y éste contiene los valores de las imágenes de arranque, de las unidades destino y de la partición raíz.

Si el sistema utilizado es sólo de Linux y el disco de arranque nunca se ha particionado con DOS o Windows, se debe seleccionar el registro de arranque maestro para instalar LILO, ya que no hay ninguna rutina de carga de arranque cargada actualmente. Si el sistema contiene DOS o Windows o es de arranque dual se puede seleccionar instalar LILO en el sector de arranque de la partición que contiene la partición raíz de Linux, en la que se carga un MBR (Registro de Arranque Maestro) de DOS, se busca la partición activa y el sector de arranque en ese lugar carga el kernel de Linux en la memoria y lo ejecuta. Las desventajas de este método son que el sistema debe tener instalado Windows o DOS para obtener el MBR en la unidad de disco duro y se debe activar la partición donde esta instalado LILO para que la encuentre el MBR de DOS.
Se pueden agregar una contraseña al archivo de LILO para evitar que los usuarios locales arranquen Linux sin contraseña (Ver tabla 4.5).

Es importante aclarar que a pesar de la opción de contraseña del archivo de LILO, no se puede evitar que las personas que deseen atacar al equipo arranquen con un disquete, por lo que es muy recomendable que se desactive la posibilidad de arrancar con disquete desde la BIOS-PROM y que ésta también se encuentre protegida por contraseña.

A pesar de ser el más popular para Linux, LILO no es el único gestor de arranque que existe. Hay muchas rutinas de cargas de arranque, tanto comerciales como no comerciales, capaces de cargar Linux; las más conocidas son SYSLINUX, GRUB y CHOS, éstas últimas son rutinas de carga de arranque de uso general que muestran menús interactivos y permiten arrancar el sistema operativo elegido de una manera similar al controlador de arranque de 0S/2.
GRUB (Grand Unified Boot Loader) es el administrador de arranque que supo desplazar a LILO por sus mejoradas nuevas características; por ejemplo, permite buscar imágenes de booteo en una red o puertos seriales, sistemas sin disco rígido y terminales remotos, además de ser el único capaz de arrancar el anticipadísimo GNU/Hurd.

Opción	*Propósito*
append=[hardware-params]	*Esta opción se utiliza para especificar otros parámetros del hardware. Por ejemplo, la cantidad de memoria RAM que tiene o la geometría exacta del disco duro, que no necesariamente se detecta de manera automática.*
backup=[backup-file]	*Se utiliza para indicar a LILO que copie el sector de arranque en un archivo de copia de seguridad.*
boot=[boot-device]	*Esta opción se utiliza para especificar la partición de arranque.*
delay=[time]	*Se utiliza para especificar el tiempo que debe detenerse antes de arrancar, en décimas de segundos.*
force-backup=[file]	*Se utiliza para hacer copias de seguridad del sector de arranque en un archivo y sobrescribir las copias de seguridad anteriores.*
install=[boot-sector]	*Se utiliza para instalar el archivo especificado como el nuevo sector de arranque, que no sea el predeterminado.*
message=[message-file]	*Se utiliza para especificar un archivo que contiene el mensaje de texto que aparece encima del indicativo* boot *en el momento de arranque. Normalmente es una nota del proveedor o una demanda de argumentos adicionales.*
password=[password]	*Se utiliza para definir una contraseña de arranque.*
restricted	*Se utiliza para especificar que sólo se necesita contraseña cuando los usuarios intentan pasar argumentos de arranque adicionales.*
timeout=[time]	*Se utiliza para especificar cuántas décimas de segundo debe esperar el cargador de arranque antes de arrancar sin ninguna entrada del teclado.*
verbose=[level]	*Esta opción se utiliza para controlar el detalle de los mensajes de arranque. Se recomienda el máximo, 5.*

Tabla 4.5 Opciones de /etc/lilo.conf

3.5 Actualización del Kernel

El núcleo o kernel *de Linux es el programa más importante del sistema. Los errores en otros programas pueden ser solucionados normalmente con alguna actualización poco traumática, y sin necesidad de reiniciar el sistema. Sin embargo, un error en el* kernel *del sistema supone la instalación de un nuevo núcleo, la reconfiguración del gestor de arranque para utilizar ese nuevo núcleo y reiniciar el sistema. Como el núcleo controla toda la seguridad del sistema, un error en ese código puede convertirse en un desastre.*

Cuando se descubre una nueva vulnerabilidad en el kernel*, suele aparecer algún parche para el código fuente que soluciona el problema. Secure Linux es una colección de parches para el núcleo de Linux programados por Solar Designer; este software, disponible libremente, incrementa la seguridad que el núcleo proporciona por defecto, ofreciendo cuatro importantes diferencias:*

1. **Área de pila no ejecutable**. *En un sistema con el área de la pila no ejecutable los ataques de buffer overflow (desbordamiento del búfer) son más difíciles de realizar que en los sistemas habituales, ya que muchos de estos ataques se basan en sobrescribir la dirección de retorno de una función en la pila para que apunte a código malicioso, también depositado en la pila.*
2. **Enlaces restringidos en** ***/tmp***. *Con esta característica, Secure Linux intenta que los usuarios sin privilegios puedan crear enlaces en* /tmp *sobre archivos que no les pertenecen, eliminando así ciertos problemas de seguridad que afectan a algunos sistemas Linux, relacionados principalmente con condiciones de carrera en el acceso a archivos.*
3. **Tuberías restringidas en** ***/tmp***. *Esta opción no permite a los usuarios escribir en tuberías (fifos) que no le pertenezcan a él o a root en directorios con el bit de persistencia activo, como* /tmp. *De esta forma se evitan ciertos ataques de Data Spoofing.*
4. ***/proc*** **restringido**. *Permite que los usuarios no tengan un acceso completo al directorio* /proc *(que recordemos permite un acceso a estructuras de datos del núcleo, como la tabla de procesos, desde el espacio de usuario) a no ser que se encuentren en un determinado grupo con el nivel de privilegio suficiente. De esta forma se consigue un aumento espectacular en la privacidad del sistema, ya que por ejemplo los usuarios no tendrán acceso al estado de las conexiones de red vía* netstat.

El demonio auditd *permite al administrador de un sistema Linux recibir la información de auditoría de seguridad que el núcleo genera, a través del archivo* /proc/audit, *filtrarla y almacenarla en archivos.*

Desgraciadamente, compilar un núcleo manualmente suele ser una actividad complicada las primeras veces. La mayoría de los usuarios prefieren esperar hasta que se publica una actualización oficial para su distribución de Linux; pero debido a distintos factores (pruebas de estabilidad, lanzamiento de una nueva versión del núcleo, etc.) las distribuciones de Linux no suelen publicar las actualizaciones del kernel *con la velocidad que se espera. Por esta razón, es importante saber cómo recompilar el núcleo cuando se le ha descubierto un problema de seguridad.*

Compilar un núcleo de Linux puede ser una tarea delicada porque es posible activar o desactivar cientos de opciones. Aunque migrar al núcleo más reciente que exista suponga ser inmune a la última vulnerabilidad aparecida, en ocasiones puede no ser prudente hacer esta migración ya que diferentes núcleos pueden tener diferentes características, y puede que los programas que se tienen sean más compatibles con el núcleo que esté actualmente funcionando, en cuyo caso sólo basta con parchar la vulnerabilidad que haya aparecido. Casi todas las distribuciones hacen modificaciones al código fuente del núcleo, aplican algunos parches que mejoran el rendimiento o añaden características

no disponibles en la distribución original. Por lo tanto, es importante conseguir el código fuente del núcleo que actualmente esté funcionando en el sistema. Red Hat guarda los archivos de configuración de todos los núcleos que utiliza en el directorio configs*. Independientemente de cómo se haya configurado el núcleo, se debe añadir el nuevo núcleo al gestor de arranque.*

Aunque un cracker contara con un control total del sistema que le permitiera dañar completamente la integridad de los archivos o que pudiera falsificar los resultados de las auditorías, sería posible detectar su presencia sin más que copiar de nuevo los ejecutables originales al sistema atacado. No obstante, el método más sofisticado, y uno de los más difíciles de detectar, consiste en intentar manipular el propio núcleo de Linux. Al modificar el kernel*, el atacante consigue pasar totalmente inadvertido y es totalmente invisible para cualquier herramienta de detección, ya que altera la información que proporcionan las llamadas al sistema en las que se basan todos los programas Unix. El núcleo de Linux no se puede alterar a la ligera, esto es, no es posible añadir nuevas funcionalidades al* kernel *sin tener que realizar una nueva compilación y un rearranque. Pero si alguien ha conseguido modificar el núcleo, no puede fiarse de nada de lo que ocurra en el sistema mientras el nuevo núcleo esté en ejecución: los listados de procesos y de archivos que se muestran, las conexiones de red, las estadísticas de disco y procesador, etc. La única solución efectiva en este caso es* reinstalar*. Por otro lado, a la hora de compilar el núcleo de Linux es importante configurar el sistema como un firewall (CONFIG_IP_FIREWALL), que además permitirá el IP-Masquerading. Otra opción que ayuda a incrementar la seguridad del equipo es la defragmentación de paquetes que llegan a través de la red.*

Siempre, y en todo caso, es recomendable personalizar la instalación para que se satisfagan las necesidades esenciales del (los) servidor (es) Linux específicamente para cada entorno empresarial. Para ello no existe ningún conjunto de reglas establecidas, se deben determinar las necesidades y los objetivos específicos para cada entorno, además, hay que explicar cómo se van a utilizar los servidores, quién los va a utilizar y qué datos va a servir (qué servicio va a ofrecer). Pero lo más importante es mantener siempre el sistema actualizado para evitar que existan agujeros o vulnerabilidades.

"El sistema operativo es un dispositivo complejo con tantas facetas de seguridad que disponer y configurar; es la base de la que se parte para asegurar un sistema".

CAPÍTULO 4
Herramientas Complementarias de Seguridad del Sistema Operativo

Introducción

*La configuración del sistema operativo que soporta las diferentes aplicaciones siempre es complementada con la utilización de herramientas que permiten determinar qué tan seguro es un sistema. Con este fin se presenta una recopilación de todas las herramientas que son usadas para complementar la seguridad que brinda la plataforma Linux, siguiendo con la filosofía del "*freeware*", es decir que son herramientas libres. Esta recopilación incluye las que se consideran más populares y utilizadas según una encuesta realizada en Mayo del 2003 por* Fyodor *entre casi dos mil personas y fueron ordenadas según su función específica y los tipos de ataques existentes, pues su tarea es prevenir dichos ataques.*

Es importante destacar que toda herramienta utilizada en el ámbito de la seguridad puede ser un arma de dos filos, es decir, que puede no sólo ser una herramienta de defensa sino también de ataque.

4.1 Auditores de Contraseñas

El algoritmo DES (Data Encryption Standard) que utiliza Linux para el cifrado de contraseñas; y en general cualquier algoritmo de cifrado, no es completamente infalible, sobre todo si los mismos usuarios crean contraseñas que son fáciles de descifrar o éstas son demasiado cortas. Los crackers toman

grandes listas de palabras (llamadas diccionarios) y las codifican utilizando el algoritmo DES para realizar sus ataques y conseguir las contraseñas que se encuentran almacenadas en el archivo /etc/passwd*. Durante este proceso, envían palabras corrientes, nombres propios y cualquier otro texto precisamente a través de las mismas permutaciones y transformaciones a las que se exponen las contraseñas de Linux. Utilizando herramientas de ruptura de alta velocidad los atacantes pueden codificar cada palabra del diccionario de 4096 formas diferentes. Cada vez que una herramienta de ruptura obtiene dicho texto codificado, lo compara con las contraseñas de /etc/passwd. Rápidamente encuentra una coincidencia y comunica al agresor que se ha roto una contraseña. Por todos estos motivos, es necesario el uso de herramientas que permitan una comprobación proactiva de contraseñas; con esto, se eliminan las contraseñas débiles antes de su envío a la base de datos de contraseñas. Un usuario crea una contraseña y ésta se compara con una lista de palabras y con una serie de reglas. Si la contraseña no cumple con los requisitos de este proceso, se obliga al usuario a elegir otra.*

Es muy importante señalar que, aún siendo el administrador de un sistema, se pueden presentar problemas legales si no se cuenta con la autorización adecuada para poner a prueba o romper un sistema de contraseñas, así como por llevar a cabo auditarías no autorizadas de contraseñas. Al final de los casos, las políticas en este sentido son determinadas por cada organización de manera independiente.

4.1.1 Crack

Crack *es la herramienta de auditoría de contraseñas más conocida en la comunidad Unix, desarrollada por Alec D. E. Muffet.* Crack *es un programa de estimación de contraseñas diseñado para detectar rápidamente inseguridades en los archivos de contraseñas de Unix, Linux y otros sistemas semejantes, mediante la exploración de los contenidos de los mismos, buscando aquellos usuarios que hayan elegido descuidadamente una contraseña de* login *débil. Esta diseñada para averiguar las contraseñas estándar de ocho caracteres cifradas con DES. A medida que funciona,* Crack *aplica muchas reglas a cada palabra y es flexible, configurable y rápido. Las reglas son las distintas formas posibles en que puede haberse escrito una contraseña, por ejemplo:*

- *Alternar mayúsculas con minúsculas*
- *Escribir la palabra hacia adelante y hacia atrás y concatenar ambos resultados*
- *Repetir una palabra una, dos o varias veces*
- *Añadir diferentes números al comienzo o al final de cada palabra*

Crack *es bastante rápido, pero depende en gran medida del hardware. La configuración ideal es un equipo a 400 MHz con 256 MB de RAM. Las versiones*

más recientes de Crack *también admiten las contraseñas cifradas con MD5. Para su ejecución necesita* C *y* Perl *si se lleva a cabo una ruptura en paralelo o multiprocesado y para su ejecución es indispensable ser un usuario* root*. Los archivos de configuración que se deben tomar en cuenta son:*

1. *dictgrps.conf*
2. *dictrun.conf*
3. *network.conf*

Esta herramienta se puede conseguir fácilmente de la página web siguiente: http://www.users.dircon.co.uk/~crypto/

4.1.2 John the Ripper

Una herramienta de auditoría de contraseñas de propósito general para DOS, Windows y Unix es John the Ripper*. Permite buscar las contraseñas correspondientes a un archivo de contraseñas DES o MD5 de Unix para obtenerlas en claro. Se utiliza para comprobar la calidad de las claves de los usuarios de un sistema, intentando encontrar las claves que han utilizado y así previniendo que un presunto atacante pueda obtener el archivo de claves y hacer lo mismo. Usa una cantidad de diccionarios suficiente para asegurar que si nosotros no podemos obtener las claves en un tiempo razonable tampoco podrá hacerlo un supuesto atacante. Se aconseja al administrador del sistema que haga lo mismo cada cierto tiempo y que deje un sistema preparado con el* John the Ripper *y los diccionarios para que pueda comprobar periódicamente las claves. Sin embargo, debido a que* John *maneja contraseñas estilo DES, no utiliza el enfoque* crypt(3)*. En su lugar, utiliza algoritmos propios. Aún así, esta herramienta es más rápida que Crack, admite muchas reglas y opciones y está bien documentada.*

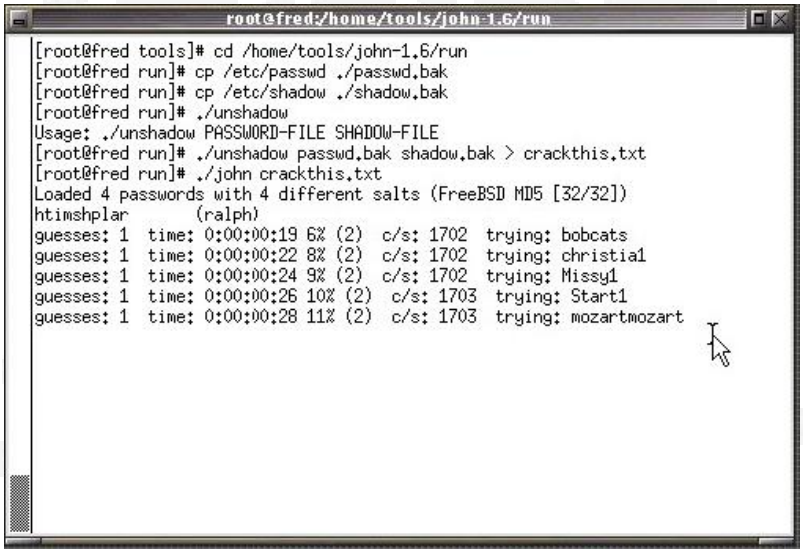


Fig. 4.1 Pantalla que muestra la salida generada por John the Ripper

Las características adicionales que tiene esta herramienta son:

- *Descifra los algoritmos estándar y de doble longitud DES, MD5 y Blowfish*
- *Es posible suspender y reiniciar una sesión*
- *Está disponible para varias plataformas*
- *Permite especificar una lista propia de palabras y de reglas a utilizar*
- *Se puede obtener el estado de una sesión interrumpida o que se esté ejecutando*
- *Es posible especificar los usuarios o grupos que se quieren atacar*

Esta herramienta se obtiene en: http://www.openwall.com/john/john-1.6.tar.gz

4.1.3 passwd+

Esta herramienta es un comprobador proactivo de contraseñas que tiene grandes capacidades de registro, entre las que se incluyen el registro de todas las sesiones, de los errores, de los usuarios que hayan cambiado sus contraseñas, de las reglas que no cumplía la contraseña y el éxito o fracaso en el cambio de una contraseña dada. Además, especifica el número de caracteres significativos de la contraseña, es decir, cuántos se utilizarán en la comprobación. Esta funcionalidad se debe utilizar para enseñar poco a poco a los usuarios los motivos por los que sus elecciones de contraseñas no siempre son acertadas. Algunas reglas que proporciona passwd+ *son:*

- *El número de oficina, el teléfono de la oficina, el nombre de* host *y el de dominio están prohibidos*
- *Las contraseñas deben tener al menos* "n" *caracteres de longitud*
- *El nombre y los apellidos (al derecho o al revés) están prohibidos*
- *Las contraseñas deben mezclar mayúsculas y minúsculas*

Esta herramienta se encuentra en la siguiente dirección electrónica: ftp://ftp.assist.mil/pub/tools/passed_utils/passwd+.tar.Z.

4.1.4 anlpasswd

Otro buen comprobador proactivo de contraseñas es anlpasswd, *del Argonne National Laboratory. Este programa, escrito principalmente en Perl, utiliza el archivo de diccionarios que se elija y permite crear reglas personalizadas. Esta herramienta es muy fácil de instalar y viene con un documento titulado "Pass or Fail: A new Test for Password Legitimacy". En él, los autores describen su motivación, su finalidad y sus resultados, con lo que ofrece una visión fuera de lo común del desarrollo de la herramienta. La dirección de Internet que ofrece esta herramienta es la siguiente: ftp://coast.cs.purdue.edu/pub/tools/unix/anlpasswd/anlpasswd-2.3.tar.Z*

4.1.5 npasswd

npasswd *es un sustituto con menos deficiencias que el comando* passwd(1) *de Unix y de todos los sistemas operativos similares a Unix implementada por Clyde Hoover, el cual somete a las contraseñas de usuario a estrictas pruebas de capacidad de adivinación para reducir la posibilidad de que los usuarios escojan contraseñas vulnerables. Esta herramienta esta diseñada para complementar o reemplazar los programas estándar de cambio de contraseñas como* passwd, chfn *y* cosh. npasswd *es una exhaustiva solución que puede reforzar considerablemente la seguridad de las contraseñas. La distribución cuenta incluso con un conjunto de herramientas de desarrollo para poder ampliar* npasswd *o incorporarlo a otras aplicaciones. Sin embargo, la configuración de esta herramienta es algo compleja porque presenta muchas opciones que no siempre se adaptan a las necesidades que se pretende resolver.*

4.1.6 Lard

Lard *es una herramienta de auditoría de contraseñas para Linux y otras versiones de Unix. Lard es lo suficientemente pequeña para caber en un disquete, lo que es útil para auditar equipos no conectados en red, de diferentes departamentos, etc.*

4.1.7 Xcrack

Xcrack *es un script en Perl para romper contraseñas de Linux. No utiliza reglas complejas, sino que ejecuta un cifrado completo del archivo de diccionarios. Es útil para entornos en los que se espera que los usuarios hayan hecho elecciones de contraseñas excepcionalmente malas.*

Herramienta / Característica	Crack	John the Ripper	passwd+	anlpasswd	npasswd	Lard	Xcrack
Sistema Operativo	Unix y sus clones	Unix y Windows	Unix y sus clones	Unix y sus clones	Unix y sus clones	Unix y sus clones	Linux
Facilidad de uso	Si	No	Si	Si	No	Si	Si
Documentación	Si	Si	Si	Si	Si	No	No
Configuración personal	Si	Si	Si	SI	Si	No	No
Capacidades de registro	No	Si	Si	No	No	No	No
Interfaz gráfica	No	No	No	No	No	No	No

Tabla 4.1 Tabla comparativa de Auditores de Contraseñas

4.2 Algoritmos de Encriptación

La encriptación es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones. En otras palabras, la criptografía es simplemente la ciencia de escribir en forma secreta cifrando la información de tal manera que quede oculta de los individuos no autorizados y permitiendo verla a las personas autorizadas, es decir, a aquellas personas que conocen la clave apropiada para descifrar la información. Entre más complicado sea un algoritmo de encriptación más difícil será para un intruso conocer el contenido de la información en tránsito o almacenada en los sistemas de cómputo. El cifrado de los datos permite desde proteger el correo personal para que ningún curioso lo pueda leer, hasta controlar el acceso a archivos de forma que sólo personas autorizadas puedan examinar, o lo que quizás es más importante, modificar su contenido, pasando por proteger nuestras claves cuando nos conectamos a un sistema remoto o los datos bancarios cuando se realiza una compra a través de Internet. Los sistemas de encriptación pueden ser atacados de tres maneras:

1. *A través de las debilidades del algoritmo*
2. *Mediante la fuerza bruta en contra de la clave*
3. *Por medio de las debilidades en el sistema de entorno*

4.2.1 Encriptación de Clave Privada

La encriptación de clave privada requiere que todas las partes que están autorizadas para leer la información tengan la misma clave. Esto reduce todo el problema de proteger la información a uno solo: proteger la clave. La encriptación de clave privada es la más utilizada porque proporciona la confidencialidad de la información y cierta garantía de que ésta no pueda ser modificada mientras se encuentra en tránsito. Este tipo de encriptación también se conoce como de clave simétrica, porque en ella se utiliza la misma clave tanto para encriptar información como para descifrarla y no proporciona autenticación por lo que cualquier persona que tenga acceso a la clave puede crear, encriptar y enviar un mensaje válido. En términos generales, la encriptación de clave privada puede ser fácil de implementar tanto en hardware como en software.

4.2.1.1 Algoritmo DES

El DES (Data Encryption Standard) es desde 1977 un algoritmo de uso obligatorio en el cifrado de informaciones gubernamentales no clasificadas creado por IBM, el cual utiliza una clave de 56 bits. El DES es un cifrado en bloque que funciona sobre un bloque de 64 bits del texto original a la vez.

Existen 16 rondas de encriptación en el DES con una subclave diferente utilizada en cada ronda. La clave pasa a través de su propio algoritmo para derivar las 16 subclaves. Existen cuatro modos de operación para el DES:

1. **Libro de código electrónico**. *Ésta es la encriptación de bloque básico, donde el texto y la clave están combinados para formar el texto cifrado. En este modo una entrada idéntica produce salida idéntica.*
2. **Encadenamiento de bloques cifrados**. *En este modo, cada bloque es encriptado como un libro de código electrónico, pero se agrega un tercer factor, derivado de la entrada anterior. En este caso, una entrada idéntica (texto original) no produce una salida idéntica.*
3. **Retroalimentación del cifrado**. *Este modo utiliza texto cifrado y previamente generado como entrada para el DES. La salida se combina entonces con el texto original para producir un nuevo texto cifrado.*
4. **Retroalimentación de salida**. *Este modo es semejante al anterior, pero utiliza la salida del DES y no texto cifrado encadenado.*

DES puede ser implementado tanto en software como en chips con tecnología VLSI (Very Large Scale Integration, Escala de Integración Muy Larga), alcanzando en hardware una velocidad de hasta 50 Mbs. Un ejemplo de implantación en hardware puede ser PC-Encryptor, de Eracom, y un ejemplo de implantación en software es DES-LOCK, de la empresa Oceanics.

En 1992, algunas investigaciones señalaron que el DES podía ser empleado múltiples veces para crear una encriptación más robusta. De esta manera nació el concepto del Triple DES (TDES). TDES puede utilizarse ya sea con tres o dos claves y es un algoritmo relativamente rápido, en la medida en que todavía pueda ser implementado en hardware. Se lleva tres veces el tiempo total de DES porque existen tres operaciones ejecutándose (ver fig. 4.2).

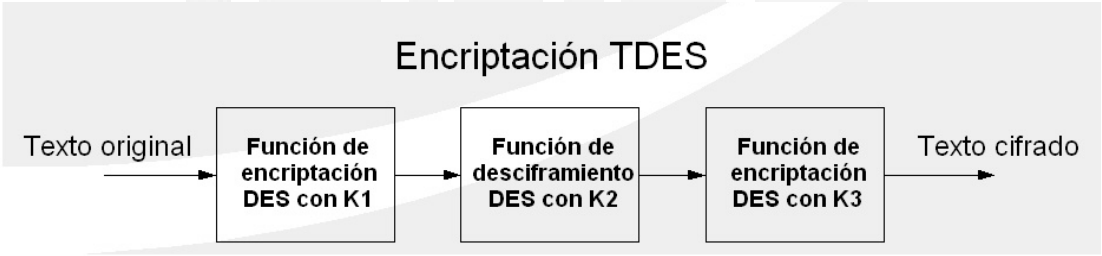


Fig. 4.2 Diagrama funcional de DES Triple

4.2.1.2 Otros Algoritmos de Clave Privada

Existen otros algoritmos de clave privada disponibles en varios sistemas de seguridad, entre los cuales se encuentran los siguientes:

1. **AES** *(Advanced Encryption Standard, Estándar de Encriptación Avanzada). Con el fin de reemplazar a DES, NIST dio a conocer una competencia para el Estándar de Encriptación Avanzada en 1997, el cual culminó con el algoritmo llamado Rijndael. Rijndael es un cifrado en bloque que utiliza claves y bloques de 128, 192 ó 256 bits. El algoritmo se compone de 10 a 14 rondas o series, dependiendo del tamaño del bloque de texto original y de las dimensiones de la clave. Es una buena alternativa del TDES por la base de su fortaleza, así como por su conveniencia para redes de alta velocidad y por su implementación en hardware.*
2. **MD5**. *MD5 es un verdadero algoritmo hash. En este caso las contraseñas pueden tener cualquier longitud y la sal (una cadena de bytes que participa en el proceso de generación del valor hash) de los valores hash de MD5 también son más largas. Las contraseñas MD5 también se pueden generar con crypt (3).*
3. **IDEA** *(Internacional Data Encryption Algorithm). El Algoritmo Internacional de Encriptación de Datos fue desarrollado en Suiza. IDEA utiliza una clave de 128 bits y también es empleado en PGP (Pretty Good Privacy).*
4. **RC5**. *RC5 fue desarrollado por Ron Rivest en el Instituto Tecnológico de Massachussets (MIT). Permite claves de longitud variable.*
5. **Skipjack**. *Fue desarrollado por el gobierno de Estados Unidos para utilizarse con el chip Clipper. Utiliza una clave de 80 bits, la cual pude ser marginal en el futuro cercano.*
6. **Blowfish**. *Blowfish, un algoritmo de hashing, toma en cuenta claves de longitud variable hasta de 448 bits y fue optimizado para su ejecución en procesadores de 32 bits. Se trata en este caso de un algoritmo rápido y seguro que puede utilizarse al estilo de DES. En concreto el algoritmo Blowfish es libre, y su código pertenece al dominio público. Además es un algoritmo que lleva ya unos años funcionando y parece ser que es de los más difíciles de romper si se genera adecuadamente el cifrado, haciendo prácticamente imposible conseguirlo por ataques de fuerza bruta y similares. Se consigue: http://www.counterpane.com/blowfish.html*
7. **Twofish**. *Twofish es un bloque cipher simétrico que puede ser utilizado como reemplazante de DES o IDEA perteneciente a Counterpane Labs. utiliza bloques de 128 bits y puede emplear claves de 128, 192 ó 256 bits. Con él no se encripta únicamente la información enviada, sino también las direcciones de red que están enviando y recibiendo esa información. Este algoritmo fue uno de los cinco finalistas del concurso (AES), no está patentado, y el código de fuente es no sujeto a Copyright y de libre licencia de uso.*
8. **CAST-128**. *Este algoritmo utiliza una clave de 128 bits y es empleado en las versiones más recientes de PGP.*
9. **GOST (Gosudarstvennyi Standard, Estándar Gubernamental)**. *Es un estándar ruso que fue desarrollado como respuesta al DES (aunque aún*

se desconoce si es más seguro), el cual hace uso de bloques de 64 bits con una clave de 256 bits.

Algoritmo / Característica	DES	TDES	AES	MD5	IDEA	RC5
Tamaño de la palabra	64 bits	64 bits	varía	-----	-----	----
Tamaño de la clave	56 bits	2 ó 3 veces la clave de 56 bits	128, 192 ó 256 bits	varía	128 bits	varía
Rondas de encriptación	16	16	de 10 a 14	----	-----	----
Adaptación en hardware	SI	SI	SI	----	-----	----

Tabla 4.2 Tabla comparativa de Algoritmos de Encriptación (clave privada)

Algoritmo / Característica	Skipjack	Blowfish	Twofish	CAST-128	GOST
Tamaño de la palabra	-----	32 bits	128 bits	-----	64 bits
Tamaño de la clave	80 bits	Varía hasta 448 bits	128, 192 ó 256 bits	128 bits	256 bits
Rondas de encriptación	-----	16	-----	-----	16
Adaptación en hardware	-----	-----	-----	-----	----

Tabla 4.2 Tabla comparativa de Algoritmos de Encriptación (clave privada)… continuación

4.2.2 Encriptación de Clave Pública

La encriptación de clave pública es una invención más reciente que la de clave privada y la diferencia radica en el número de claves utilizadas en la operación. La encriptación de clave pública utiliza dos claves, una para encriptar la información y, posteriormente, una clave diferente para descifrar dicha información. Las claves están relacionadas entre sí (par clave), pero son diferentes, por lo tanto, si se cuenta con una de las claves de un par, no se pueden calcular la otras claves.

La desventaja de los sistemas de encriptación de clave pública es que tienden a ser intensivos en términos computacionales, por lo que son mucho más lentos que los sistemas de clave privada. Sin embargo, si se combinan los dos tipos de encriptación, se obtiene un sistema mucho más robusto. El sistema de clave pública puede ser empleado para intercambiar claves y autenticar ambos extremos de la conexión. Posteriormente puede ser utilizado el sistema de clave privada para encriptar el resto del tráfico.

4.2.2.1 Algoritmo RSA

En 1978 Ron Rivest, Adi Shamir y Led Adleman, profesores del MIT, publicaron el algoritmo de clave pública RSA (por las iniciales de sus apellidos), que desde entonces se ha convertido en el prototipo de los algoritmos de clave pública. Este algoritmo puede ser utilizado tanto para encriptación como para desciframiento. La seguridad de RSA radica en la dificultad de la factorización de números grandes; es fácil saber si un número es primo, pero es extremadamente difícil obtener la factorización en números primos de un entero elevado, debido no a la dificultad de los algoritmos existentes, sino al consumo de recursos físicos (memoria, necesidades hardware, tiempo de ejecución, etc.) de tales algoritmos. El funcionamiento del algoritmo RSA es el siguiente:

Si un usuario desea enviar información cifrada, en primer lugar tiene que calcular un par de claves (pública y privada), para lo que ha de elegir aleatoriamente dos números primos grandes (del orden de cien dígitos), p y q, números que se han de mantener en secreto; si llamamos N (N se conoce como módulo) al producto p x q, el usuario ha de determinar otro entero, d, llamado exponente privado, que cumpla

mod (d; (p - 1) x (q - 1)) = 1; d < N

es decir, **d** *y el producto* **(p - 1) x (q - 1)**, *que llamaremos función de Euler y denotaremos* **φ(N)**, *han de ser primos. Con estos datos, ya tenemos la clave privada del cifrado: el par* **(N, d)**; *para obtener la clave pública, hallamos el inverso multiplicativo del número* **d** *respecto de* **φ(N)**, *de la forma* **e x d = 1 mod φ(N)**. *Calculado este entero* **e**, *llamado exponente público, la clave pública será el par* **(N, e)**.

El sistema RSA ha permanecido invulnerable hasta hoy, a pesar de los numerosos ataques de crackers; teóricamente es posible despejar **d** *para obtener la clave privada, a partir de la función de descifrado. Sin embargo, el cálculo de logaritmos discretos es un problema de una complejidad desbordante, por lo que este tipo de ataques se vuelven impracticables debido al elevado tiempo de ejecución del algoritmo.*

.

4.2.2.2 Otros Algoritmos de Clave Pública

Existen otros algoritmos de clave pública que exhiben las mismas propiedades que el RSA, mencionaremos 4 de los más populares:

1. **Intercambio de clave Diffie-Hellman**. *Whitfield Diffie y Martin Hellman desarrollaron su sistema de encriptación de clave pública en 1976 para resolver el problema de la distribución de claves de los sistemas de clave privada. La idea fue permitir un método seguro para ponerse de acuerdo en una clave privada sin el costo de enviar la clave a través de otro*

método. Por tanto, necesitaban una forma segura de decidir sobre una clave privada, utilizando un método de comunicación como el que estaban intentando proteger. Diffie-Hellman no puede utilizarse para encriptar o descifrar información. El intercambio de clave de Diffie-Hellman es utilizado por muchos sistemas de seguridad para intercambiar claves secretas que se puedan utilizar con el tráfico adicional. La única debilidad en este sistema es que es susceptible a un ataque desde una posición central. No obstante, este tipo de ataque requiere de recursos significativos y es muy poco probable que ocurra en el mundo real.

2. **Elgamal**. *Taher Elgamal desarrolló una variante del sistema Diffie-Hellman para permitir encriptación y terminó con un algoritmo que también suministraba autenticación, cuya seguridad se basaba también en la dificultad de calcular logaritmos discretos. Aunque generalmente no se utiliza de forma directa, ya que la velocidad de cifrado y autenticación es inferior a la obtenida con RSA, y además las firmas producidas son más largas, el algoritmo de Elgamal es de gran importancia en el desarrollo del DSS (Digital Signature Standard), del NIST (National Institute of Standards and Technology) estadounidense. El algoritmo Elgamal no fue patentado de modo que proporcionó una alternativa potencialmente económica.*

3. **Algoritmo de firma digital**. *El algoritmo de firma digital fue desarrollado por el gobierno de Estados Unidos como un algoritmo estándar para firmas digitales. Este algoritmo estaba basado en el Elgamal, pero solamente tiene en cuenta la autenticación; no ofrece confidencialidad.*

4. **Encriptación de curva elíptica**. *Las curvas elípticas fueron propuestas para los sistemas de encriptación en 1985. Los sistemas criptográficos de curva elíptica (ECC, Elliptic Curve Cryptosystems) están basados en un difícil problema matemático diferente al de la factorización o los logaritmos discretos. Este problema es el siguiente: dados dos puntos* **A** *y* **B** *sobre una curva elíptica, tales que* **A = kB**, *es muy difícil encontrar el entero* **k**. *Existen beneficios para utilizar ECC en lugar de RSA. El beneficio más grande es que las claves son más pequeñas (debido a la dificultad del problema de la curva elíptica) de modo que los cálculos suelen ser más rápidos para obtener el mismo nivel de seguridad. Puede tomar un tiempo antes de que las ECC sean aceptadas, en la medida que estén cubiertas por diversas patentes.*

Algoritmo / Característica	RSA	Diffie-Hellman	Elgamal	Firma digital	Curva elíptica
Encripta y descifra	SI	NO	SI	SI	SI
Permite Autenticación	SI	NO	SI	SI	-------
Ofrece Confidencialidad	SI	SI	SI	NO	-------

Tabla 4.3 Tabla comparativa de Algoritmos de Encriptación (clave pública)

4.2.3 OpenSSH

OpenSSH *es una herramienta desarrollada por OpenBSD y se considera la versión libre (licencia BSD) del protocolo SSH para redes, la cual permite la conexión remota a una máquina, para poder ejecutar comandos sobre ella, al igual que telnet o rlogin, pero con la ventaja de que la información va cifrada (incluidas las contraseñas) para eliminar de un modo efectivo las escuchas, los secuestros de las conexiones y otros ataques a nivel de red. Además, OpenSSH ofrece amplias posibilidades para la creación de túneles seguros, aparte de una variedad de métodos de autenticación. Para la autentificación, SSH puede utilizar algoritmos de cifrado como RSA o DSA. Para el envío de datos a través de la red, usa 3DES, IDEA, Blowfish, etc. Por otro lado, también con SSH se pueden establecer sesiones seguras con servidores X, SMTP, POP3, etc.*

Dentro del paquete OpenSSH vienen bastantes programas adicionales, a parte del servidor y el cliente:

- sshd*: servidor de ssh*
- sftp-server*: servidor ftp mediante ssh.*
- ssh*: el cliente, con él nos podemos conectar al servidor sshd.*
- scp*: copia archivos entre máquinas. Sustituto para rcp.*
- ssh-keygen*: para crear claves públicas y privadas RSA o DSA (host keys y user authentication keys).*
- ssh-keyscan*: utilidad para obtención de claves públicas de hosts*
- ssh-copy-id*: copia el identify.pub en una máquina remota*
- ssh-agent*: agente de autentificación. (Usado para manejar RSA keys en la autentificación.)*
- ssh-add*: para añadir nuevas claves con el agente.*
- sftp*: cliente ftp mediante ssh*

Esta herramienta es muy fácil de utilizar y se puede conseguir en la página: http://www.openssh.com

4.3 Firewalls

Actualmente, Internet es la principal vía para consultar y publicar información de una forma sencilla, económica y revolucionaria pero también ofrece la posibilidad de contaminar y destruir esta información. Por esta razón las personas necesitan instrumentar medidas de seguridad para proteger sus datos y recursos en Internet, una de ellas es la seguridad de las redes de datos. Una de las formas principales de implantar un sistema de seguridad en una red de datos es a través de un firewall*. Un* firewall *o "*cortafuego*" es un dispositivo que permite a una red, tener conexión a Internet con cierto grado de seguridad.*

Un firewall es colocado generalmente en el punto donde la red interna se conecta a Internet o red externa, tal como se muestra en la figura 4.3

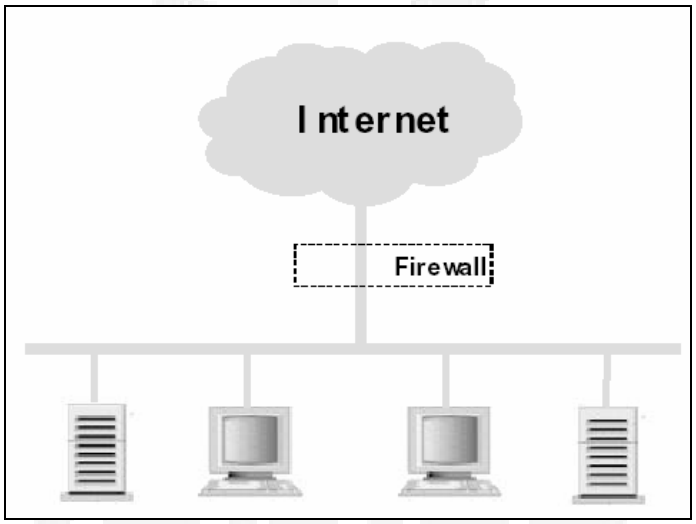


Fig. 4.3 Firewall

Al colocar el firewall de esta manera, todo el tráfico que proviene o va hacia Internet pasa a través de él y tiene la capacidad de cerciorarse de que este tráfico es conforme a las políticas de seguridad del sistema. Estas políticas definen la accesibilidad y los niveles de restricción tanto de los servicios disponibles en Internet como los que se ofrecen en la red interna y son controladas a través de un solo punto central: el punto de conexión de la red con Internet. El concepto de firewall puede ser efectuado mediante:

- **Filtrado de paquetes**, *que consiste en bloquear selectivamente el tráfico de red. Estos firewalls son diseñados para controlar el flujo de paquetes basándose en la dirección IP de origen y destino, los puertos de origen y destino e información del tipo del paquete. El filtrado de información puede ser por dirección IP o por servicio ofrecido.*

- **Servidores Proxy**, *que realizan la comunicación de red en lugar del cliente. Los servicios Proxy son aplicaciones especializadas que corren en una máquina firewall (ya sea en el enrutador de la red o en una máquina bastión), estas aplicaciones toman los requerimientos de los clientes y los reenvían a los servidores verdaderos, basándose en las políticas de seguridad del sistema. En un sistema como éste, el servidor Proxy evalúa la solicitud de los clientes y decide si debe ser aprobada o denegada.*

4.3.1 ipfwadm/ipchains/iptables

Desde la series 1.1, el kernel de Linux posee en mayor o menor medida capacidad para filtrar tramas. Originalmente (1994), ipfwadm *era la herramienta proporcionada con Linux para la implementación de políticas de filtrado de paquetes y debido a sus limitaciones (por ejemplo, sólo puede manejar los protocolos TCP, UDP o ICMP)* ipfwadm *fue reescrito para convertirse en* ipchains *a partir del núcleo 2.1.102 en 1998. Esta nueva herramienta (realmente, todo el subsistema de filtrado de los núcleos 2.2) introdujo bastantes mejoras con respecto a la anterior, pero seguía careciendo de algo fundamental: era difícil ver a un sistema tan potente como Linux sin una herramienta de filtrado decente, libre, y de serie con el sistema. De esta forma, a partir del núcleo 2.3.15 (por tanto, en todos los kernels estables, de la serie 2.4, desde mediados de 1999)* ipchains *fuera sustituido por* iptables*, que de nuevo introducía importantes mejoras con respecto a su predecesor. Sin duda la más importante era que ya incorporaba un sistema de NAT (Network Address Translation) mucho más avanzado, incorpora mejoras en el filtrado (llegando incluso a filtrar en base a la dirección física de las tramas) e inspección de paquetes, y presenta un subsistema de* log *mucho más depurado que* ipchains*.*

Históricamente, todos los sistemas de firewall nativos de Linux han sido orientados a comando, esto significa, que no leen su configuración de un determinado archivo, por ejemplo durante el arranque de la máquina, sino que ese archivo de arranque ha de ser un script *donde, línea a línea, se definan los comandos a ejecutar para implantar la política de seguridad deseada. La sintaxis de* iptables *(o la de* ipchains*, bastante similar) puede llegar a resultar muy compleja si se invoca al sistema de filtrado desde la línea de comandos; por fortuna, existen diferentes interfaces para el administrador, algunos tan cómodos e intuitivos como el de Firewall-1, capaces de presentar las políticas de una forma gráfica basada en objetos y de transformar después esas políticas en* scripts *con las órdenes de* iptables *o* ipchains *equivalentes. Un ejemplo de estos interfaces es* fwbuilder*. Quizás lo más importante de estas herramientas es que son herramientas flexibles, potentes y gratuitas, que funcionan sobre un sistema operativo también gratuito.*

Iptables *es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Este comando lo que realmente hace es aplicar reglas con las que se añade, se borra o se crean nuevas reglas de filtrado. Un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall. El kernel lo que hace es, dependiendo si el paquete es para la propia máquina o para otra máquina, consultar las reglas del firewall y decidir qué hacer con el paquete.*

Características de iptables:

- *Filtrado por puerto, dirección, protocolo, flags tcp, mac*

- *Estado temporal de las conexiones: limit*
- *Filtrado por UID y GID del generador de paquetes: owner*
- *Filtrado por estado de las conexiones: state*
- *Filtrado por TOS y TTL*
- *NAT en Origen y Destino*
- *Muy modular y extensible*

Evidentemente, iptables *está preparado para generar logs en el sistema; permite registrar mediante* syslogd *los paquetes que cumplan cierta regla, por lo que lo habitual es almacenar solamente los paquetes que no sean rutinarios (por ejemplo, intentos de conexión desde direcciones no autorizadas, ciertos paquetes ICMP no habituales, etc).*

4.3.2 Netfilter

En las versiones 2.4 del kernel Linux el viejo mecanismo de reglas de filtrado y NAT basadas en ipchains fueron sustituidas por un paradigma mucho más potente llamado NetFilter. Netfilter es un poderoso filtro/firewall de paquetes el cual es implementado en el kernel Linux estándar. Permite crear reglas iptables *de una forma sencilla basándose en archivos de configuración muy sencillos que permiten crear en un tiempo mínimo un firewall completo compuesto por miles de reglas. También permite especificar el tratamiento de todo el tráfico TCP, UDP, todos los tipos de mensajes ICMP, todos los tipos de protocolos así como el tratamiento del tráfico fragmentado o anormal. Tiene un sistema de logs basado en* syslog *o* ulogd*, permitiendo fácilmente loggear a bases de datos o a archivos de texto plano. También tiene un sistema de estadísticas gráficas que crea gráficas del tráfico de los servicios que deseemos con solo especificarlo en las reglas del archivo de configuración. Actualmente Netfilter soporta filtrado de paquetes* stateless *o* statefull *y todos los diferentes tipos de NAT (Network Address Translation) y modificación de paquetes.*

4.3.3 FireStarter

FireStarter *es una herramienta gratuita para configuración de firewalls destinada a usuarios y administradores de sistemas Linux, la cual permite proteger una estación de trabajo o una red completa ya que constituye una línea de defensa contar ataques basados en sistemas de red. Las características más sobresalientes de esta herramienta son:*

- *Cuenta con una interfaz amigable optimizada para GNOME 2*
- *Es fácil de configurar para las necesidades de seguridad específicas, a través de un asistente de configuración*
- *Muestra en tiempo real los ataques*

- *Abre y cierra puertos, configurando su defensa fácilmente*
- *Está diseñado para GNOME pero también funciona con KDE*
- *Contiene funciones avanzadas para afinar el Kernel*
- *Soporta versiones del Kernel de Linux 2.5, 2.4 y 2.2*

FireStarter *incluye asistentes, monitores, listas negras, y función para compartir Internet con servicio DHCP, entre muchas otras cosas más. Esta herramienta permite realizar un NAT mediante wizard, y después solo copiar los directorios* /etc/firestarter *y* /etc/init.d/firestarter *a cualquier otro servidor incluso si estos últimos no tienen instalado interfaz X; además los scripts que genera son estructurados cuando se quiere tener un firewall restrictivo tanto con las conexiones entrantes y las salientes (NAT) así como configurar las políticas para bloquear todo y solo permitir lo que se quiera. Esta es en definitiva una buena herramienta para ir jugando con Iptables, la única cosa mala que tiene es que debe utilizarse como un usuario* root*. La página donde se puede encontrar u descargar es: http://firestarter.sourceforge.net*

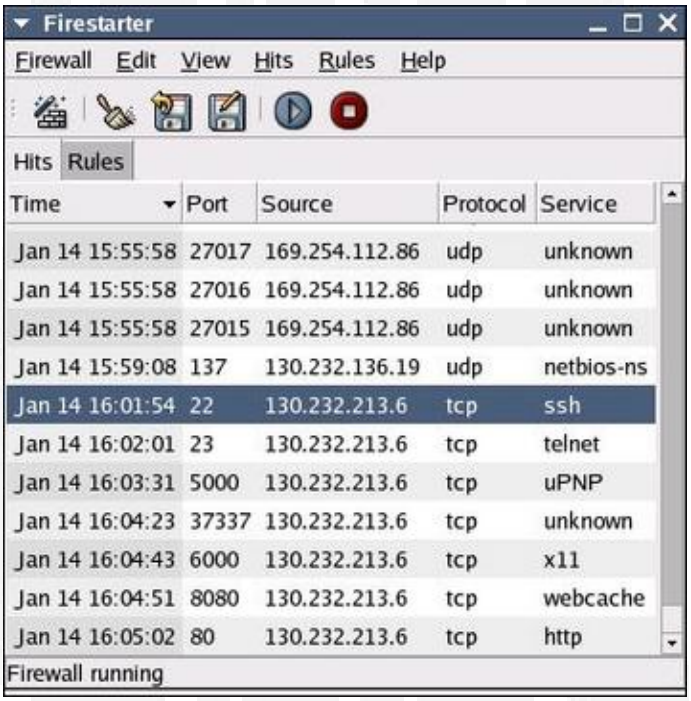


Fig. 4.4 Pantalla del Firewall Firestarter

4.3.4 Firewalk

Firewalk *es un programa desarrollado por MDS y DHG que utiliza un estilo similar al traceroute para escanear un firewall e intentar deducir las reglas impuestas en ese firewall. Al enviar paquetes con diferentes tiempos de vida y*

ver dónde mueren o si son rechazados, se puede engañar al cortafuegos para que revele sus reglas. No existe una defensa real contra esto, aparte de denegar silenciosamente los paquetes en lugar de enviar un mensaje de rechazo, lo cual con suerte revelará menos cosas. Esta herramienta aporta muchas funcionalidades como una serie de normas aplicadas a las IP de usuarios o reglas de protocolos para TCP, UDP y ICMP, así como una optimización de la actividad de escaneo con un sistema de alarmas en tiempo real, a fin de prevenir todo tipo de intrusiones. Firewalk *escanea sistemáticamente todos los puertos y funciona a través de la formación de paquetes con una IP TTL, calculada de tal forma que caduque en un segmento situado después del firewall. Además de tener acceso a un fichero log detallado, con todos los eventos ocurridos,* Firewalk *adapta automáticamente su configuración en función del entorno de conexión. Es recomendable utilizar esta herramienta para escanear los sistemas, pues los resultados pueden ayudar a reforzar su seguridad. Sin embargo, su interfaz de configuración es un poco confusa. La página de descarga del Firewalk es: http://www.packetfactory.net/firewalk/*

Firewall / Característica	Netfilter	Firestarter	Firewalk
Sistema Operativo	Unix y sus clones	Unix y sus clones	Unix y sus clones y Windows
Interfaz gráfica	SI	SI	SI
Documentación suficiente	SI	SI	SI
Fácil configuración	SI	SI	NO
Realiza estadísticas	SI	NO	NO

Tabla 4.4 Tabla comparativa de Firewalls

4.4 Sistemas de Detección de Intrusos (IDS)

Un Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema. Las técnicas de detección de intrusos consisten en analizar y determinar las actividades anómalas, incorrectas e ilegales a las que puede estar sometido un sistema o una red. Este análisis de la actividad de una red no sólo se produce en la zona externa o en la DMZ (zona desmilitarizada), sino también en las redes internas. Con todo esto se puede deducir que el control de actividades anormales se debe realizar desde cada una de las zonas en las que se puede dividir una red de comunicaciones, y que los objetivos del control son, por ejemplo, el uso de protocolos o aplicaciones no autorizadas,

actividad ICMP no autorizada, estímulos-respuesta, suplantaciones de usuarios, reconocimiento DNS, etc.

Para poder descubrir todo este tipo de acciones se pueden utilizar técnicas diferentes como:

- **Análisis del tráfico de paquetes**. *Se monitorean los paquetes que atraviesan el IDS desde y hacia redes de éstas. Este tipo de monitoreo comprueba el empaquetado de los datos que proviene de Internet, las direcciones físicas y lógicas de origen y destino, servicios y puertos por los que se comunican los sistemas a través de diferentes aplicaciones, sistemas de nombres de dominio (DNS) y el enrutamiento de los datos desde el sistema origen hasta el destino.*

- **Análisis de firma de paquetes**. *Los IDS disponen de plantillas de ataques conocidos. Por ejemplo, cuando se emplea la fragmentación para realizar ataques de denegación de servicio, ésta es complicada de analizar, concluyendo si la misma es normal o maliciosa. Cuando un IDS puede volver a ensamblar los fragmentos y analizarlos mediante una plantilla o firma de ataque y coincide con ésta, el sistema puede alertar sobre el tipo de ataque del que es víctima la red o el sistema.*

- **Análisis estadístico**. *Al monitorear la red durante un tiempo determinado se pueden establecer umbrales y modelos de funcionamiento habitual, por ejemplo, cantidad de tráfico de red, protocolos más utilizados, sistemas que lo utilizan, cómo se utilizan y volumen de datos que atraviesa la red. Con todo esto se pueden advertir desviaciones o discrepancias con el funcionamiento habitual.*

- **Comprobación de integridad de archivos**. *Se puede comprobar qué archivos han sido modificados y el usuario que lo ha llevado a cabo.*

Por otro lado, existen tres tipos de sistemas de detección de intrusiones:

1. **HIDS (IDS basado en Host)**. *Protege contra un único Servidor, PC o host. Monitorean gran cantidad de eventos, analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción. Recaban información del sistema como ficheros, logs, recursos, etc., para su posterior análisis en busca de posibles incidencias. Todo ello en modo local, dentro del propio sistema. Fueron los primeros IDS en desarrollar por la industria de la seguridad informática.*
2. **NIDS (IDS basado en Red)**. *Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados,*

buscando patrones que supongan algún tipo de ataque. Bien ubicados, pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan, "ven" todos los paquetes que circulan por un segmento de red aunque estos no vayan dirigidos a un determinado equipo). Analizan el tráfico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.

3. **IDS Híbridos**. *Este tipo de IDS es una combinación de los dos anteriores.*

La decisión de dónde colocar el IDS esta determinada por las necesidades que se tengan, por ejemplo: Si se coloca el IDS antes del firewall se capturará todo el tráfico de entrada y salida de la red. La posibilidad de falsas alarmas es grande. Sin embargo, la colocación detrás del firewall monitorizará todo el tráfico que no sea detectado y parado por el firewall, por lo que será considerado como malicioso en un alto porcentaje de los casos. La posibilidad de falsas alarmas muy inferior. Los problemas con los IDS se dan cuando queremos implementarlos en redes conmutadas, ya que no hay segmento de red por donde pase todo el tráfico o en las redes con velocidades de tráfico muy altas en las cuales es difícil procesar todos los paquetes.

4.4.1 Snort

Snort *es un sistema de detección de intrusiones basado en red (NIDS), relacionada con* tcpdump *o* ipchains*. Esta herramienta es una aplicación de seguridad la cual implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida, como intentos para aprovechar alguna vulnerabilidad, análisis de protocolos, sistema operativo, información sobre el equipo, etc. Además, permite detectar todos los intentos de acceso no autorizados a una máquina conectada en red, controlando incluso el contenido de cada paquete de datos en tiempo real.* Snort *es una herramienta basada en el uso de reglas de comparación y emparejamiento de patrones (*pattern matching*). Utilizando una base de datos de patrones que denotan ataques, éste programa se dedica a examinar todo el tráfico que ve en un segmento de red y a comparar ciertas propiedades de cada trama observada con las registradas en su base de datos como potenciales ataques; si alguna de las tramas empareja con un patrón sospechoso, automáticamente se genera una alarma en el registro del sistema. Además,* Snort *implementa un lenguaje de creación de reglas flexibles, potentes y sencillas. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, ddos, finger, ftp, ataques web, CGI, escaneos Nmap, etc.*

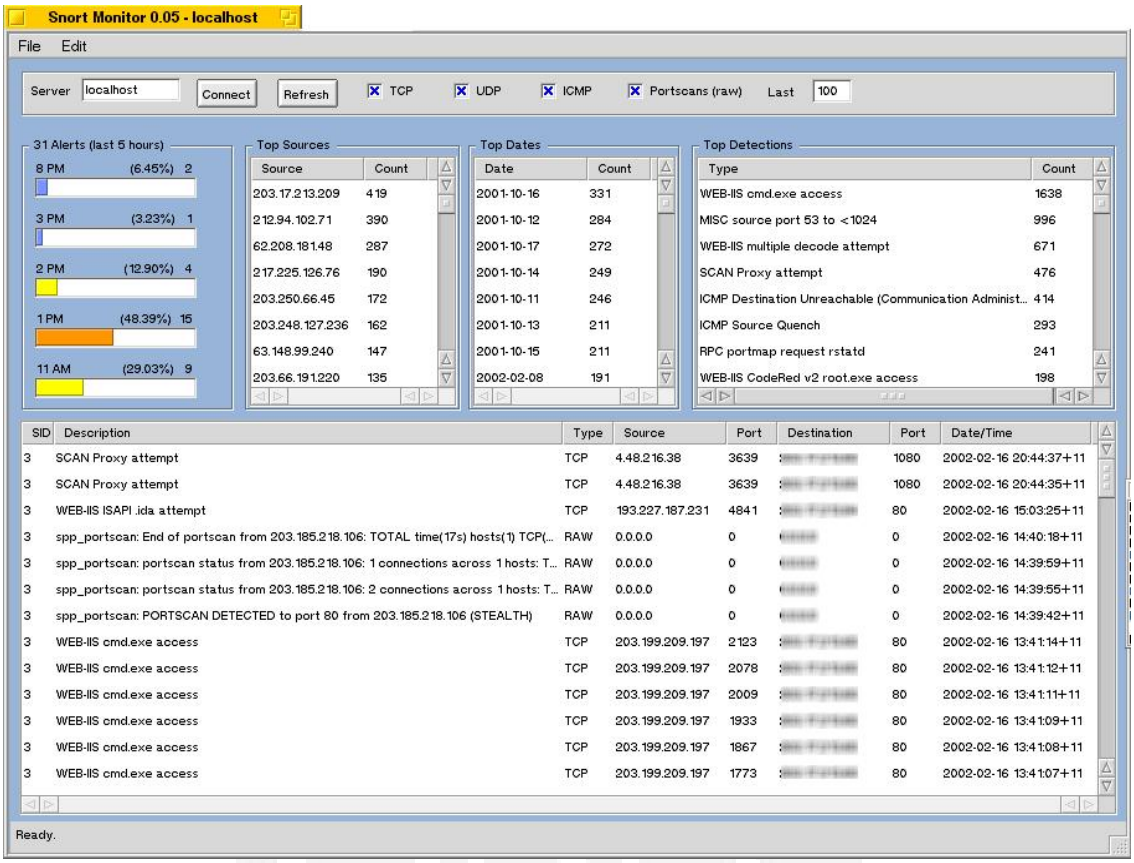


Fig. 4.5 Pantalla de monitorización de Snort

*Las características más sobresalientes de esta herramienta son su facilidad de configuración, su adaptabilidad a las necesidades específicas de cada sistema, sus requerimientos mínimos (funciona en diferentes clones de Unix), pero sobre todo, que es totalmente gratuita y se puede descargar fácilmente de su página oficial (*http://www.snort.org*). Asimismo,* Snort *puede funcionar como un sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico, registro de paquetes, permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS híbrido.*

4.4.2 LIDS (Linux Intrusion Detection System)

El Sistema de Detección de Intrusos Linux, basado en host, es un sistema de detección/defensa de intrusión en Linux, cuyo objetivo es proteger los sistemas Linux para prevenir intrusiones a nivel de root, deshabilitando algunas llamadas al sistema en el kernel mismo y asignar reglas las cuales se van a ir comprobando. LIDS, escrito por Xie Huagang y Philippe Biondi, es un parche del kernel y una herramienta de administración que también puede controlar la modificación de archivos a través de las listas de control de acceso (ACL) y proteger procesos, archivos y recursos de red, hasta del súper usuario o root.

Esta herramienta se encuentra en su sitio oficial: http://www.lids.org/

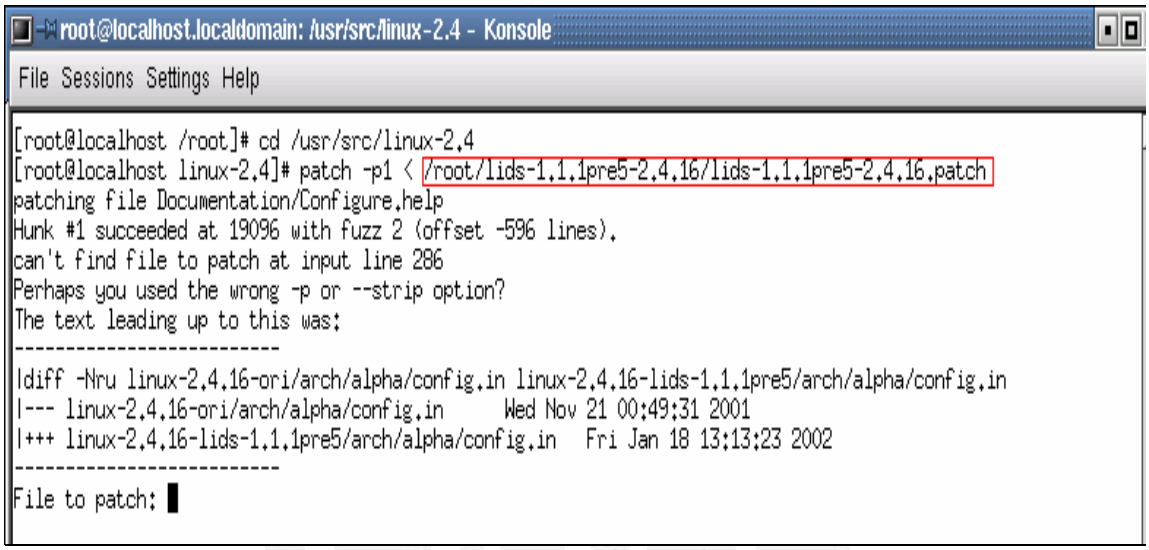


Fig. 4.6 Pantalla de compilación de LIDS

4.4.3 LogCheck

Logcheck *es parte del Proyecto Abacus de herramientas de seguridad. Es un programa creado para ayudar en el procesamiento de los archivos de registro de UNIX generados por varias herramientas del Proyecto Abacus, TCP Wrapper y el Firewall Toolkit de Trusted Information Systems (TIS).*

Logcheck *es una herramienta basada en archivos logs, la cual revisa periódicamente las bitácoras del sistema, analizando cada una de las líneas y clasificándola según diferentes niveles de alerta, reportándolo al administrador del sistema en un formato fácil de leer, descartando las líneas que no tengan relevancia, y enviándolo por correo. Logcheck checará cada línea contra cuatro niveles de seguridad: ignorar, actividad inusual, violación de seguridad y ataque. Esta herramienta mantiene en su configuración la caracterización de eventos normales y de eventos que indican un probable ataque y se basa en patrones definidos por el usuario. Además, ayuda a localizar problemas y violaciones de seguridad en los archivos de registro automáticamente y envía los resultados por e-mail al administrador del sistema. Este programa es de uso gratuito en cualquier sitio y se puede obtener descargándolo de la página: http://www.gwolf.cx/seguridad/logcheck/*

4.4.4 AIDE (Advanced Intrusion Detection Environment)

AIDE es un sistema de detección de intrusos de distribución libre, el cual reemplaza a TripWire, basado en el sistema de archivos (host), el cual detecta cambios en los archivos del sistema local. Para su funcionamiento se crea una base de datos a partir de reglas y expresiones regulares definidas; una vez que la base de datos es inicializada, ésta se utiliza para verificar la integridad de los archivos del sistema mediante diversos algoritmos como MD5, sha1, RMD160, tiger, haval, etc., además de los que se le agreguen. Este IDS se puede obtener de la página: http://www.sourceforge.net

IDS / Característica	Snort	LIDS	LogCheck	AIDE
Tipo	Basado en red	Basado en host	Basado en host	Basado en host
Modo de operación	Uso de reglas de comparación y emparejamiento de patrones	Deshabilita llamadas al sistema en el kernel de Linux	Revisa periódicamente las bitácoras del sistema	Detecta cambios en los archivos del sistema
Fácil configuración	SI	SI	SI	NO
Esta bien documentado	SI	SI	SI	SI
Interfaz gráfica	SI	NO	SI	NO
Configuración personal	SI	NO	SI	SI

Tabla 4.5 Tabla comparativa entre los Sistemas de Detección de Intrusos

4.5 Monitoreo de redes (Sniffers)

Cualquier ataque que pueda presentar una red de datos puede ser dramático, sin embargo, los intrusos reales no suelen anunciar su presencia ni hacen alarde de lo que consiguen, sino que instalan dispositivos de monitoreo ocultos que recogen la información de la red. Estos dispositivos reciben el nombre de analizadores de protocolos *o* sniffers*.*

De forma predeterminada, las estaciones de trabajo (incluso aquellas que se encuentran en la misma red) escuchan y responden solamente a los paquetes que van dirigidos a ellas. Sin embargo, es posible modelar el software que lanza la interfaz de red de una estación de trabajo en algo llamado modo promiscuo*. Teniendo en cuenta esto, la estación de trabajo puede monitorear y capturar todo el tráfico de red y los paquetes que pasen por ella, independientemente del destino que tengan. Los sniffers se suelen escribir en C, aunque también se puede utilizar Perl, y salvo en raras excepciones, abren su fuente con directivas* include*; cada una de las cuales gestiona un aspecto distinto de la escucha, grabación y generación de informes sobre el tráfico TCP/IP.*

Los distintos sniffers *realizan tareas que van desde capturar nombres de usuarios y contraseñas hasta grabar todo el tráfico de la interfaz de red.*

4.5.1 Sniffers de Linux

Linux cuenta con herramientas propias, diseñadas con los archivos de cabecera, que le permiten realizar monitoreo de sus redes, éstas son algunas de ellas:

1. **linsniffer**. *Esta herramienta es sencilla y directa. Su propósito general es capturar nombres de usuarios y contraseñas.* linsniffer *es una herramienta creada por Mike Edulla, la cual necesita los archivos de cabecera C e IP para su ejecución. La salida que proporciona es sencilla, excelente para robar contraseñas y registrar la actividad general, pero no es muy útil para un análisis más detallado. Este sniffer se compila perfectamente en Red Hat 5.1, sin embargo, en las últimas distribuciones de Red Hat pueden surgir problemas.*

2. **linux_sniffer**. *Esta herramienta ofrece una vista algo más detallada que la anterior puesto que graba datos adicionales de la dirección, la conexión, el inicio de sesión, todos los comandos emitidos durante la misma y todas las pulsaciones emitidas. Este sniffer también proporciona mucha información cuando se realiza una autenticación básica en sesiones HTTP, telnet o ftp.*

3. **hunt**. *Es otra opción útil cuando se necesita una salida menos compleja y más fácil de leer, un seguimiento de comandos más sencillo y* snooping *(indagación) de sesiones, ya que* hunt *utiliza Curses. El creador de ésta herramienta ha proporcionado archivos binarios enlazados dinámica y estáticamente a aquellos usuarios que no tengan tiempo de compilar el paquete. Además cuenta con las siguientes utilidades que la hacen una buena opción para los principiantes en Linux y una magnífica herramienta de aprendizaje:*
   - *Permite especificar las conexiones determinadas en las que se esté interesado, en lugar de registrar todo*
   - *Detecta conexiones ya establecidas, no solamente las iniciadas en SYN o las que se acaban de iniciar*
   - *Cuenta con herramientas de* spoofing *(engaño)*
   - *Ofrece control activo de las sesiones (secuestro de sesiones), es decir, detectar una conexión TCP entre dos máquinas y tomar el control de esa conexión, haciéndola inutilizable para el usuario que la inició.*

   Esta herramienta se encuentra disponible en la siguiente página:
   http://lin.fsid.cvut.cz/~kra/index.html#HUNT

4. **sniffit**. *Es una herramienta realmente potente, ya que su capacidad de configuración es enorme. Por lo tanto, si se desea información más detallada se debe crear un archivo de configuración que especifique algunos parámetros como las direcciones de origen y destino, el formato de salida, datos de diagnóstico sobre los paquetes (por ejemplo en STDOUT), etc. (Tabla 4.6). Esta herramienta se encuentra disponible en: http://reptile.rug.ac.be/~coder/sniffit/sniffit.html*

Aplicación	*Necesita*	*Archivos de configuración*	*Historial de seguridad*	*Notas*
linsniffer	*Archivos de cabecera C e IP*	*ninguno*	*ninguno*	*Necesita todo el complemento de los archivos de cabecera de IP*
linuxsniffer	*Archivos de cabecera C e IP*	*ninguno*	*ninguno*	*Necesita todo el complemento de los archivos de cabecera de IP*
hunt	*Archivos de cabecera C e IP, Linux 2.0.35+, GlibC 2.0.7 con Linux Threads*	*ninguno*	*ninguno*	*Se han proporcionado archivos binarios enlazados dinámica y estáticamente para no compilar el paquete*
sniffit	*Archivos de cabecera C e IP*	*Hay que definir de forma explícita varias opciones*	*ninguno*	*Su capacidad de configuración es enorme, pero su proceso de aprendizaje es laborioso*

Tabla 4.6 Tabla comparativa entre los distintos Sniffers de Linux

4.5.2 Ethereal

Esta herramienta es un sniffer para Linux (y Unix en general) libre que utiliza GUI y que ofrece servicios interesantes como examinar fácilmente los datos del sniffer, bien desde una captura en tiempo real o desde archivos de captura tcpdump *previamente generados en algún disco. Ethereal es un analizador de protocolos de red que permite examinar la información capturada, viendo detalles y sumarios por cada paquete. Todo ello, unido al continuo filtro para obtener una mejor exploración de lo que se quiere ver, así como la compatibilidad con SNMP (Protocolo Simple de Administración de Red) y la capacidad para realizar capturas sobre Ethernet, FDDI (Interfaz de Datos Distribuidos por Fibra), PPP (Protocolo Punto a Punto), Token Ring estándar, IEEE 802.11 (redes inalámbricas), Classical IP over ATM y loopback*

interfaces y la habilidad de mostrar el flujo reconstruido de una sesión de TCP, hace que Ethereal *sea una muy buena herramienta.*

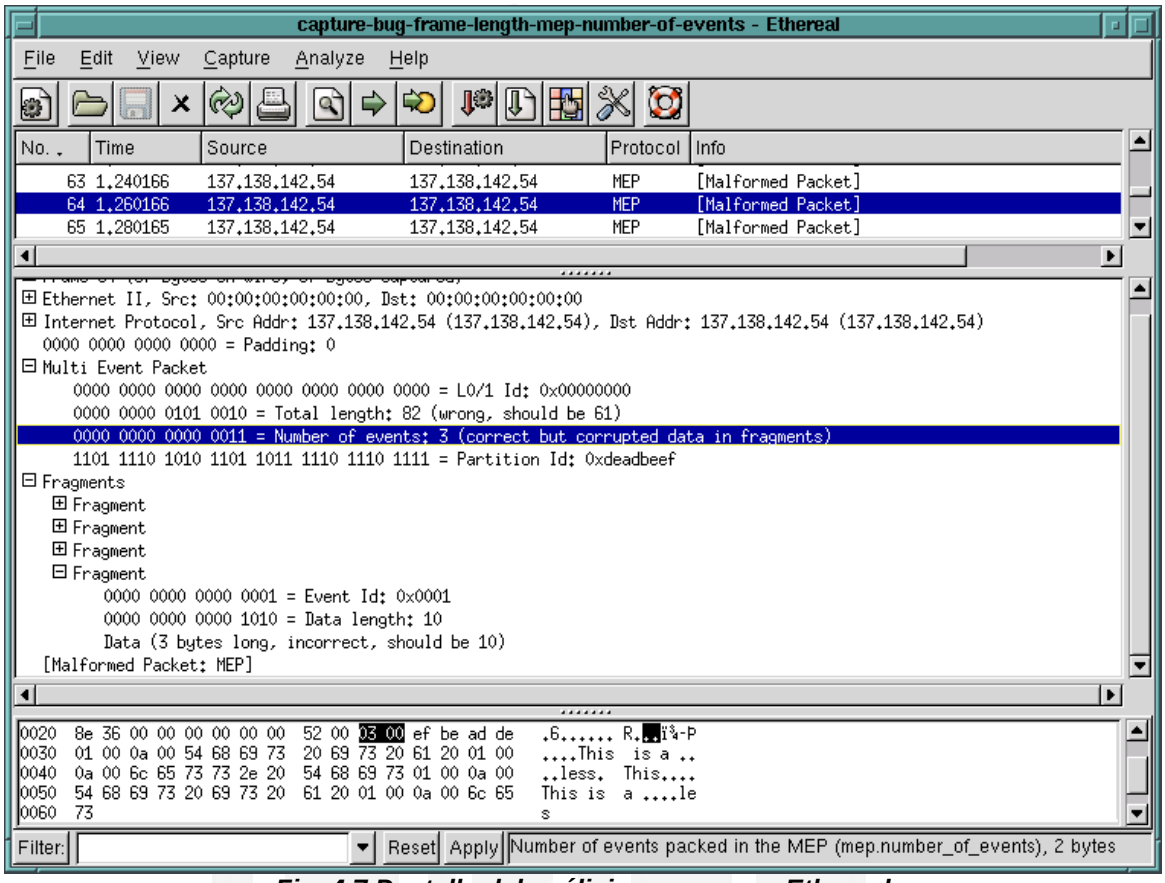


Fig. 4.7 Pantalla del análisis que genera Ethereal

Esta herramienta incluye una versión basada en texto llamada tethereal *y para su funcionamiento hay que tener en cuenta que es necesario instalar tanto GTK+ como* libcap, *una biblioteca que facilita la captura y el filtrado de paquetes. Sin duda Ethereal es un potente analizador de protocolos de red que permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco (puede leer más de 20 tipos de formato distintos). Destaca también por su impresionante soporte de más de 300 protocolos, gracias sin duda a la licencia GPL y sus más de 200 colaboradores de todo el mundo. Se encuentra en: http://www.ethereal.com/*

4.5.3 Otros Sniffers Comunes

1. **TCPDump**. *Es un conocido analizador de paquetes de red basado en texto para Linux, escrito originalmente por Van Jacobsen para analizar problemas de funcionamiento del TCP. Puede ser utilizado para mostrar*

los encabezados de los paquetes en una interfaz de red que concuerden con cierta expresión de búsqueda. Esta herramienta se puede utilizar para rastrear problemas en la red o para monitorear actividades de la misma. TCPDump *es también la fuente de las bibliotecas de captura de paquetes* Libpcap *y* WinPcap *que son utilizadas por* Nmap *y muchas otras utilidades. Los sistemas actualmente apoyados incluyen SunOS, Ultrix, y la mayoría de los Linux. Esta herramienta se consigue de la página: http://www.tcpdump.org/*

2. **Ettercap**. Ettercap *es un interceptor/sniffer/registrador para LAN's con Ethernet basado en terminales. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados como SSH, POP y HTTPS), es decir, se puede usar su interfaz para interactuar con el programa modificando su comportamiento en tiempo real y obteniendo de esta manera los resultados en pantalla o ponerlo en background colectando datos que serán almacenados en archivos de logs. También es posible la inyección de datos en una conexión establecida y "filtrado al vuelo", aun manteniendo la conexión sincronizada. También soporta plug-ins y tiene la habilidad de comprobar si se encuentra en una LAN conectada mediante switches o un hub, y de identificar huellas de sistemas operativos que permite conocer la geometría de la LAN. En síntesis usada éticamente es una poderosa herramienta para la seguridad y se encuentra bien documentada.*

3. **NGrep**. *Esta herramienta se esfuerza por proveer de la mayoría de características comunes del "*grep*" de GNU, aplicándolas a la capa de red del modelo OSI.* NGrep *es consciente de la presencia de* pcap *y permite usar expresiones regulares que concuerden con el "*payload*" (o sea la carga, el cuerpo y no los encabezados) de los paquetes. Usando sus capacidades avanzadas de comparación de cadenas Ngrep puede buscar los paquetes en puertos específicos y asistir en la búsqueda de cadenas con los usernames y los passwords que transitan por la red. Actualmente reconoce TCP, UDP, ICMP sobre ethernet, PPP, SLIP e interfaces nulas, y comprende la lógica de un filtro "*bpf*" de la misma manera que las herramientas más comunes de sniffing. Esta herramienta se encuentra en: http://www.packetfactory.net/Projects/ngrep/*

4. **NTop**. *Esta herramienta muestra el uso de la red de forma similar a lo que hace top por los procesos. En modo interactivo, muestra el estado de la red en una terminal de usuario. En modo Web, actúa como un servidor de Web (protegido por contraseña), mostrando en HTML el estado de la red de forma remota y en tiempo real. Los protocolos que es capaz de monitorizar son TCP, UDP, ICMP, ARP, IPX, DLC, Decnet, AppleTalk y Netbios; y dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP,*

DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11, etc. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico. Sin embargo, algunos informes señalan que bajo determinadas circunstancias, NTop puede permitir ejecutar código arbitrario con los privilegios de root por diversos problemas de "buffer overflow". La recomendación es eliminar el SETUID (bandera "+s") de NTop, de forma que sólo sea ejecutable por root, y no emplear nunca la opción de microservidor web. La página donde se encuentra esta herramienta es: http://www.ntop.org/

Sniffer / Característica	Ethereal	TCDump	Ettercap	NGrep	Ntop
Sistema Operativo	Unix y sus clones	SunOS, Ultrix y Unix	Unix y sus clones	Unix y sus clones	Unix y sus clones
Protocolos que analiza	Más de 300	TCP	Varios, incluyendo TCP, SSH y HTTPS	TCP, UDP e ICMP	TCP, UDP, ICMP, ARP, IPX, DLC, Decnet, AppleTalk y Netbios
Tecnologías sobre las que realiza el análisis	Ethernet, FDDI, PPP, Token Ring, PPP, 802.11, Classical IP over ATM y loopback	-------	------	Ethernet, PPP, SLIP e interfaces nulas	------
Interfaz gráfica	SI	NO	NO	NO	NO
Presenta un informe detallado y fácil de comprender	SI	SI	SI	SI	SI

Tabla 4.7 Tabla comparativa entre los distintos Sniffers

4.6 Auditores de Sistema (Scanners)

Un scanner *es una herramienta de seguridad que detecta los puntos vulnerables del sistema. Existen diferentes tipos de scanners que rastrean el sistema en busca de distintos puntos débiles, pero todos ellos se basan en una de dos categorías: scanners del sistema o scanners de red. Los scanners de sistema rastrean host locales en busca de los puntos vulnerables obvios (y no tan obvios) de la seguridad que aparecen a causa de descuidos o negligencias, y los problemas de configuración que se llegan a olvidar, por ejemplo:*

- *Permisos débiles o erróneos para los archivos*

- *Cuentas predeterminadas*
- *Entradas de UID erróneas o duplicadas*

Por el contrario, un scanner de red prueba hosts sobre conexiones de red, de forma similar a como lo haría un intruso. Examina los servicios y puertos disponibles en busca de debilidades conocidas que pueden explotar los atacantes remotos (Fig. 4.8).

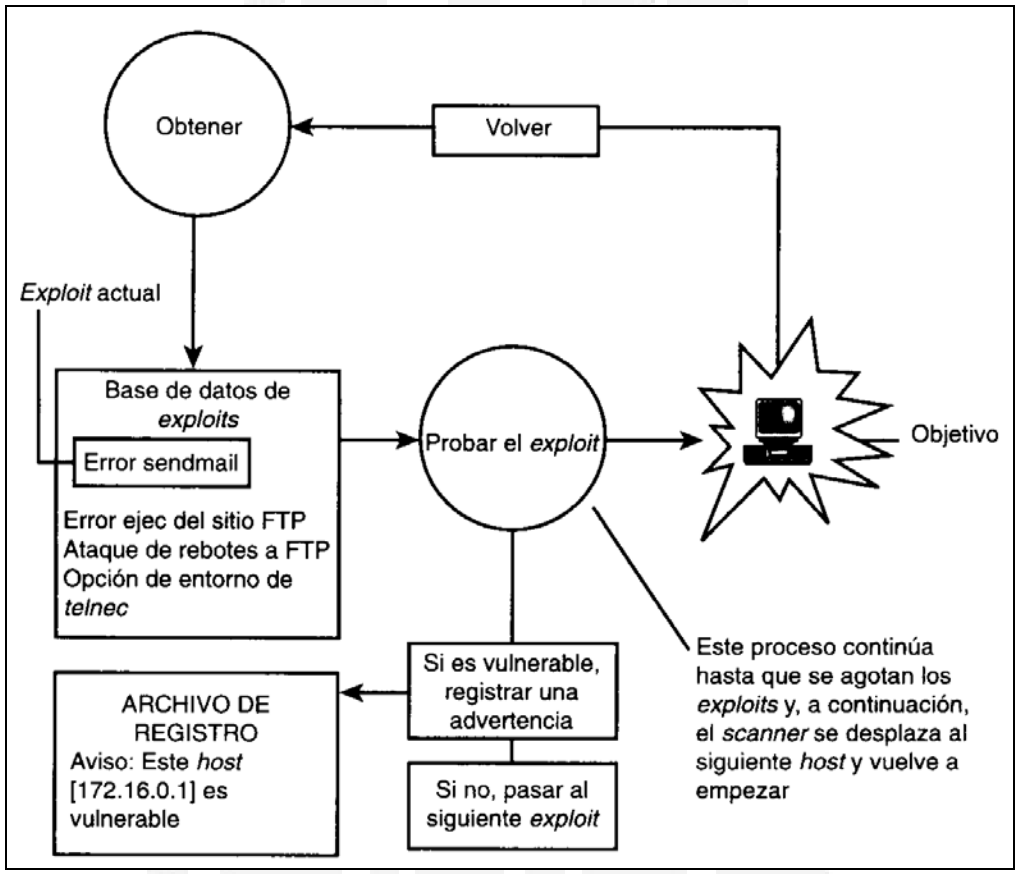


Fig. 4.8 Proceso típico de los scanners de red

Aunque desde un punto de vista técnico los scanners de sistema y de red difieren, también comparten algunas características comunes; de éstas, la más importante es su proceso lógico. La mayoría siguen este patrón:

- *Cargan un conjunto de reglas o una serie de ataques*
- *Prueban el objetivo con éstos parámetros*
- *Informan de los resultados*

Las reglas o los exploits *pueden ser de cualquier tipo. Algunos ejemplos incluyen pruebas de permisos válidos, la estructura de los archivos de contraseñas, programas que se sabe que tiene varios errores, servicios abiertos, conexiones predeterminadas, etc.*

Dado que los puntos vulnerables del sistema y de la red no son los mismos, y a que a cada usuario le preocupa un aspecto distinto de la seguridad, existen muchos tipos diferentes de scanners. Algunos de ellos están especializados y prueban solamente determinados servicios, mientras que otros, prueban servicios conocidos pero añaden funciones de generación de informes. En los últimos años, los patrones de desarrollo de scanners han seguido las tendencias de uso y del mercado; los actuales pueden evaluar entornos heterogéneos (distintos sistemas operativos).

4.6.1 Nessus

Sin duda una de las herramientas de seguridad más utilizadas durante años en todo tipo de entornos Unix ha sido SATAN (Security Analysis Tool for Auditing Networks), cuya tarea era detectar vulnerabilidades de seguridad en sistemas Unix y redes, desde fallos conocidos en el software hasta políticas incorrectas y el resultado de su ejecución se mostraba en formato HTML. Sin embargo, todo esto sucedía en abril de 1995, y SATAN no se ha actualizado mucho desde entonces, por lo que en 1998 surgió Nessus *(como un proyecto de Renaud Deraison), un analizador de vulnerabilidades gratuito, de código fuente libre, y lo más importante, igual de fácil o más de utilizar que su predecesor por su interfaz bastante eficaz.*

Nessus *es la herramienta de evaluación de seguridad de mayor renombre dentro del movimiento "Open Source".* Nessus *es un escáner de seguridad remoto para Linux y otros clones de Unix, el cual está basado en plug-ins (módulos externos de código), tiene una interfaz basada en GTK y realiza más de 1200 pruebas de seguridad remotas (como bugs en su software, backdoors, etc.), generando no sólo extensivos reportes en HTML, XML, LaTeX y texto ASCII, sino también sugiriendo posibles soluciones para los problemas de seguridad. Además proporciona tutoriales y explicaciones de todos los puntos vulnerables que encuentra. La distribución de* Nessus *consta de cuatro archivos básicos: las librerías del programa, las librerías NASL (Nessus Attack Scripting Language), el núcleo de la aplicación y sus plug-ins; es necesario compilar en este orden cada una de esas partes. Además, el programa requiere para funcionar correctamente pequeñas aplicaciones adicionales, como la librería GMP, necesaria para las operaciones de cifrado. Por otro lado, la arquitectura de esta herramienta consiste en un servidor que provee de los ataques y un cliente que es la interfaz con el usuario.*

Este scanner tiene la posibilidad de utilizarse con una interfaz gráfica o desde un shell de usuario, generando reportes en formato de texto.
Nessus se obtiene de su página oficial: http://www.nessus.org/

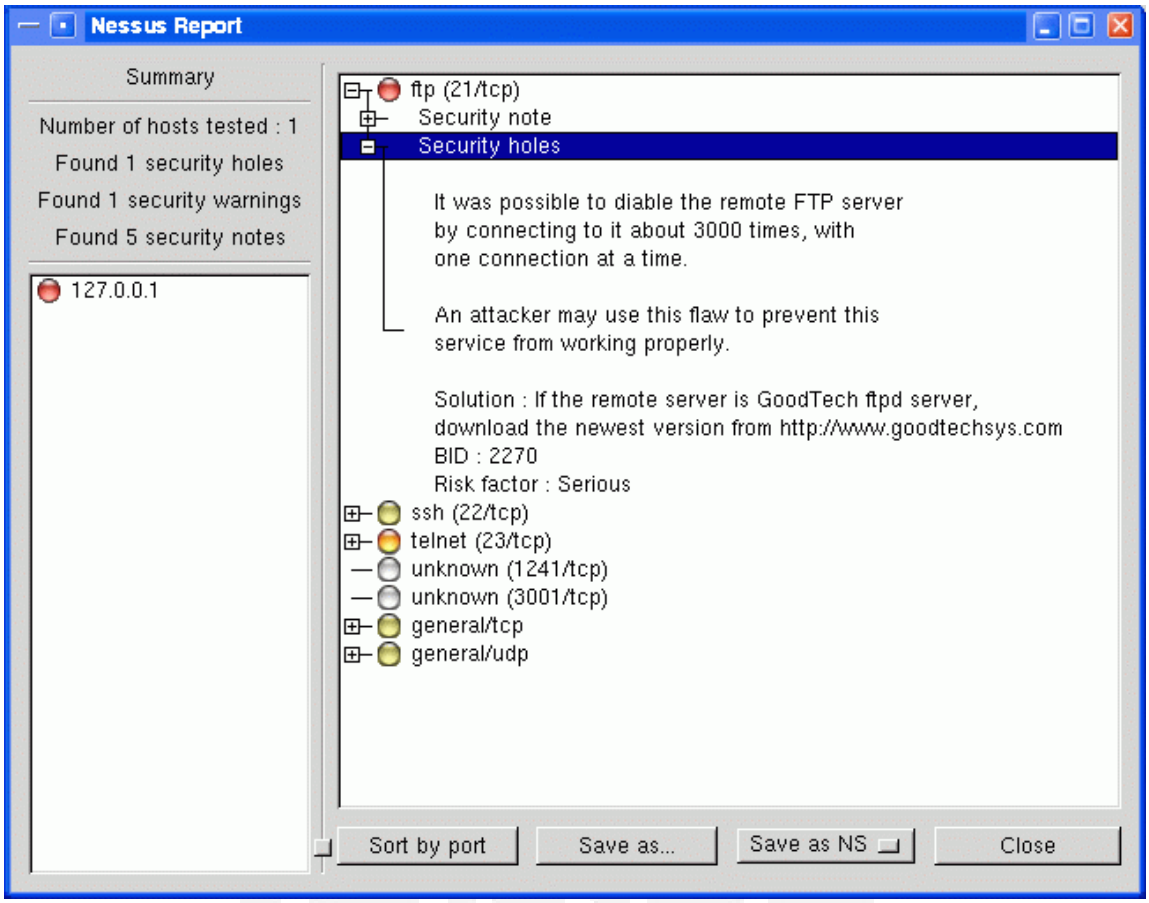


Fig. 4.9 Pantalla del reporte que genera el Scanner Nessus

4.6.2 Nmap (The Network Mapper)

Nmap *es una herramienta libre diseñada para explorar y para realizar auditorias de seguridad en una red extensa o en solo host, ya que pone al descubierto puertos abiertos en los sistemas y permite conocer como se encuentra organizada la red y de cuántas computadoras consta.* Nmap *tiene muchas características entre las que se incluyen la predicción del número de secuencias, la identificación del sistema operativo del host remoto, rastreo oculto, etc. Sus múltiples modos de funcionamiento son perfectos para probar firewalls, IDS, IPS y todo tipo de sistemas de red. Además, explora diferentes protocolos, como UDP, TCP, ICMP, etc. Es una herramienta fundamental, pues permite ver si se tienen programas escuchando en puertos que no deberían estar abiertos o se puede fabricar tráfico para probar los sistemas de seguridad y de detección. Esta herramienta incluye un documento fácil de entender que describe con lujo de detalle las distintas técnicas de rastreo de puertos y se rige por la filosofía TMTOWTDI (There's More Than One Way To Do It, Hay más de una forma de hacerlo).*

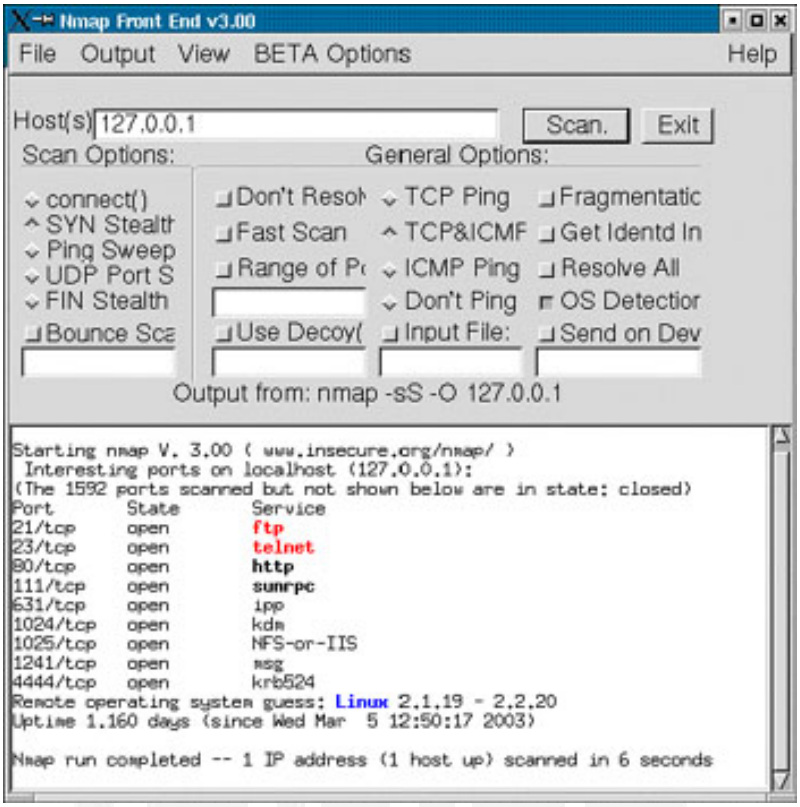


Fig. 4.10 Pantalla del reporte que genera el Scanner Nmap

Nmap soporta:

- *Exploración SYN/FIN usando fragmentos IP*
- *Exploración TCP SYN*
- *Exploración TCP con pings*
- *Exploración RPC*
- *Identificación remota de SO, etc.*

La última versión de Nmap ofrece gran cantidad de mejoras incluyendo exploración de protocolos, exploraciones anónimas en reposo, más de 700 versiones de sistemas operativos y dispositivos reconocidos, soporte nativo para Windows y Mac OS X, salida XML, soporte para máscara de red ICMP, análisis predecibles de secuencias IPID, varios tests de detección de sistemas operativos, listados de exploraciones y más. Esta se puede obtener fácilmente en la siguiente dirección: http://www.insecure.org/nmap/

4.6.3 DSniff

Los protocolos de red son, en su mayoría, inseguros, haciendo las redes muy vulnerables frente a todo tipo de embestidas contra SSH, HTTPS, intercepciones de llaves SSH y PGP, escuchas y explotaciones de las DNS. DSniff

es un set de poderosas herramientas (sniffer) que permiten auditar redes y encontrar passwords y otra información, ya que demuestra lo inseguras que son las redes cuando se envían contraseñas en formato de texto plano. Esta herramienta permite explotar algunas de las fallas fundamentales de los protocolos de encriptación SSH y SSL, utilizados para proteger un alto número de tráfico de paquetes en la red, desde transacciones financieras con bancos en línea, hasta servidores que contienen información extremadamente valiosa.

El objetivo de esta herramienta consiste en introducirse por cualquier medio en una red, con un analizador de contraseñas, utilidades de escucha pasiva de una red (como filesnarf, mailsnarf, urlsnarf, y webspy), y por otra parte, herramientas de intercepción de paquetes (como arpspoof, dnsspoof, y macoff) o métodos de ataques activos como sshmitm y webmitm. En definitiva, es una herramienta muy potente que, además, incluye técnicas sofisticadas para vencer la supuesta protección que ofrecen los switches con respecto a los hubs y que permite probar problemas de spoofing*. Se puede conseguir de la página: http://naughty.monkey.org/~dugsong/dsniff/*

Scanner / Característica	Nessus	Nmap	DSniff
Sistema Operativo	Linux y clones de Unix	Unix y Linux	Unix y sus clones y Windows
Permite configuración personalizada	SI	SI	SI
Interfaz gráfica	SI	SI	NO
Formato del reporte fácil de entender	SI	SI	------
Sugiere soluciones	SI	NO	NO

Tabla 4.8 Tabla comparativa entre los distintos Scanners

4.7 Antivirus

Un virus es una secuencia de código que se inserta en un archivo ejecutable denominado host, de forma que al ejecutar el programa también se ejecuta el virus; generalmente esta ejecución implica la copia del código viral, o una modificación del mismo, en otros programas. El virus necesita obligatoriamente un programa donde insertarse para poderse ejecutar, por lo que no se puede considerar un programa o proceso independiente. Un antivirus por consiguiente, es un programa desarrollado para la detección y eliminación de virus. Existen en el mercado una gran variedad de ellos, puesto que son las únicas herramientas no libres y su efectividad radica en que se mantenga actualizado de forma permanente; la mayoría permite que esta actualización se realice por

Internet. A la hora de adquirir un programa antivirus se deben considerar las siguientes características:

- *Que detecte virus del sector de arranque en tiempo real desde el programa residente*
- *Que elimine virus de la memoria*
- *Que permita la opción de desinstalar*
- *Que recupere el sector de arranque de disquetes dañados por un virus*
- *Soporte técnico especializado a nivel nacional*
- *Conexión/actualización desde Internet*
- *Chequeo del sistema en el momento de la instalación*
- *Que bloquee completamente acciones de macrovirus evitando infecciones*
- *Que permita realizar un disco de arranque flexible para DOS.*

4.7.1 ServerProtect

ServerProtect para servidores Linux proporciona un escaneo en tiempo real detectando y eliminando virus de todo tipo de archivos (hasta comprimidos) antes que estos lleguen al usuario final. ServerProtect puede ser configurado para descargar automáticamente las últimas descripciones de virus y actualizaciones del motor de búsqueda. La administración remota vía consola-web permite al administrador realizar tareas de mantenimiento y configuración, búsqueda de virus, actualizaciones de patrones de virus, notificaciones, visualizar reportes de estado del servidor, estado de infecciones etc. Las principales características de este antivirus son:

- **Actualizaciones automáticas de patrones de virus.** *ServerProtect puede ser configurado para descargar el patrón de virus y actualizaciones de motores de búsqueda que ayudan a asegurar que se cuenta con la última actualización.*
- **Administración y configuración flexibles.** *Permite la administración remota desde una consola basada en Web. La consola otorga a los administradores la posibilidad configurar las tareas de mantenimiento incluyendo actualizaciones de patrones de archivos y de motores de búsqueda. Esto además provee datos del estatus del servidor, incluyendo patrón de archivos, versión del programa y estatus de infección.*
- **Bitácoras robustas y notificaciones.** *Despliega la historia de antivirus del servidor en un archivo central de registros, que puede también ser exportado a otras aplicaciones para análisis posterior. Notifica a receptores predefinidos del surgimiento de virus y eventos del programa, los administradores pueden enviar notificaciones vía pager y correo electrónico de Internet.*

- **Escaneo de alto desempeño.** *Realiza un escaneo a nivel de kernel para virus y código malicioso dentro del sistema operativo Linux para minimizar la degradación del performance. Este usa un motor de búsqueda multi-proceso para mejorar la velocidad de escaneo de archivos y minimiza el impacto para el servidor.*
- **Protección antivirus confiable.** *Combina tecnologías de reconocimiento de patrones basados en reglas para una detección eficiente de virus. Las tecnologías patentadas de Trend Micro proveen protección adicional removiendo virus basados en macro y script. El motor de búsqueda de ServerProtect ha sido certificado por La asociación de Seguridad internacional de Computadoras "International Computer Security Association" (ICSA) por un escaneo confiable.*
- **Soporte antivirus 7x24.** *TrendLabs, el centro de investigación y soporte mundial antivirus de Trend Micro, respalda sus productos de con tiempo y servicio de alta calidad. Un grupo de ingenieros trabaja a contratiempo para monitorear la actividad de virus, desarrollar información de nuevas amenazas y entregar soluciones efectivas.*

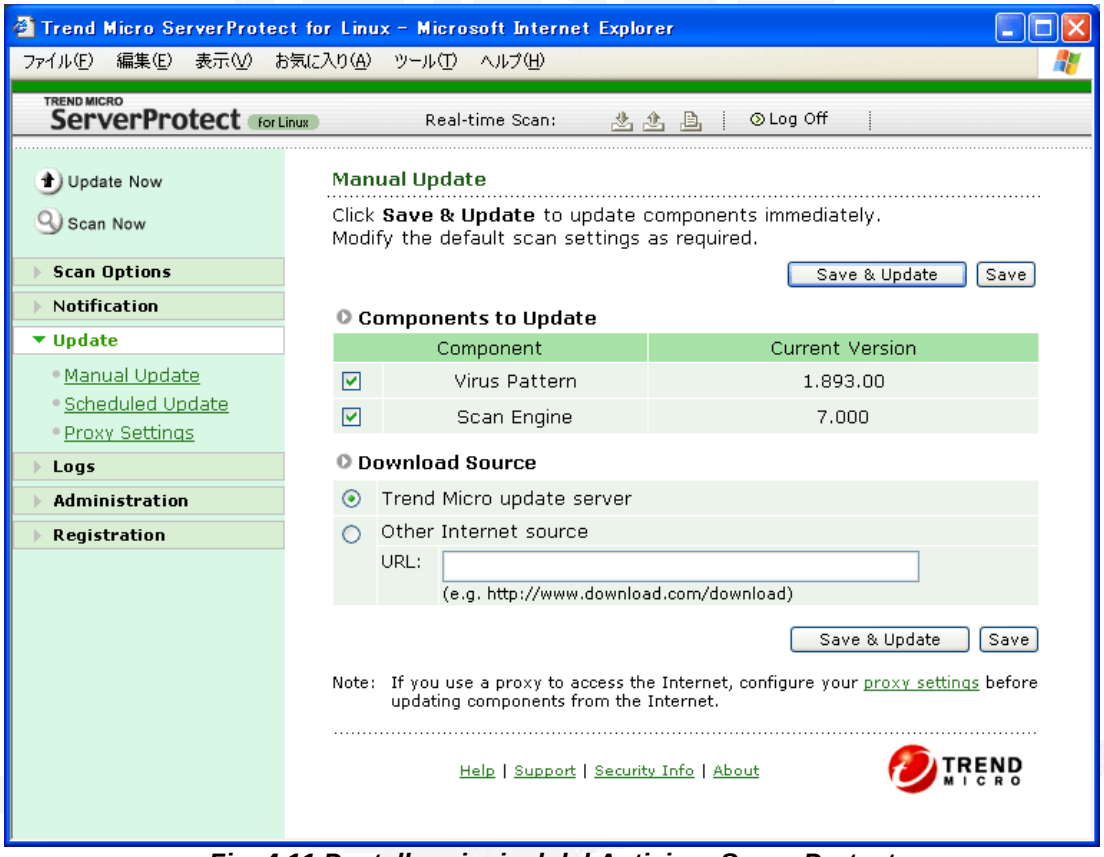


Fig. 4.11 Pantalla principal del Antivirus ServerProtect

4.7.2 eTrust Antivirus

La herramienta eTrust Antivirus v7, proporciona a la empresa completa protección desde la PDA hasta el Gateway, protegiendo puestos, servidores, servidores de correo etc. eTrust Antivirus 7, compatible con plataforma Linux, dispone de un doble motor de escaneo de alto rendimiento certificados por ICSA Labs. Actualizaciones automáticas incrementales, esto hace que se descargue únicamente las nuevas descripciones de virus que no posea ya el motor, disminuyendo así el tiempo de descarga y el trafico de información. Herramientas de administración centralizada y creación de informes de incidencias de virus, acciones tomadas etc. mediante consola web tanto en local como en remoto. Actualizaciones gratuitas de firmas de virus de por vida.

Fig. 4.12 Pantalla principal del Antivirus eTrust

4.7.3 InterScan VirusWall

Solución de alto rendimiento para gateway de Internet sobre Linux, proporciona protección contra virus y código malicioso a través de comunicaciones HTTP, FTP y SMTP. Incorpora reglas de escaneo inteligente para detectar tanto virus conocidos como desconocidos. Su ponente herramienta de administración centralizada permite configuración de actualizaciones automáticas o manuales, completos reportes de infección que incluyen origen y destino del archivo infectado, fecha, acción tomada etc., todo ello desde un

puesto local o remoto. Integrable con módulos opcionales para eliminar spam, filtrado de contenidos etc. Compatible con Microsoft ISA Sever, Check Point FireWall-1, Cisco PIX y otros firewalls.

4.7.4 Kaspersky

Kaspersky dispone de dos versiones de antivirus para plataforma Linux, una versión personal dirigida a sistemas monousuario y otra versión para proteger servidores también sobre plataforma Linux. En ambas versiones es compatible con las más famosas distribuciones de Linux, y ofrece total protección contra virus y otros códigos malignos como applets Java y ActiveX. Incluye módulo Anti-Virus Daemon, una variante del scanner de virus con optimización de carga de memoria que se encarga de chequear los archivos en tiempo real. El módulo Integrity Checker se encarga de supervisar constantemente la integridad del sistema detectando cualquier signo de intento de modificación sospechosa. El empleo de análisis heurístico permite la detección de virus todavía desconocidos.

"La seguridad no solo depende de herramientas, sino también es un comportamiento".

CAPÍTULO 5
Implementación de la Estrategia de Seguridad

Introducción

La parte práctica de este trabajo comprende el desarrollo de una estrategia de seguridad informática que parte del sistema operativo Linux, la cual se propone implantar en los servidores de la Gerencia de Tecnología Informática del Instituto Mexicano del Petróleo. El objetivo de dicha gerencia esta enfocado a establecer nuevos controles que permitan disminuir los riesgos y las vulnerabilidades a las que esta expuesta su información y las aplicaciones que dan servicio a sus distintos usuarios por medio de herramientas que no representen un gasto muy significativo. La estrategia que se propone comprende diversas etapas como son: el proceso de migración de la plataforma Microsoft a Linux, configuración de los servidores, uso de herramientas complementarias para la seguridad del sistema operativo Linux y el desarrollo de políticas y procedimientos.

5.1 Generalidades de la Problemática

Hoy en día se ha vuelto indispensable que las diversas organizaciones tengan una conectividad que les permita tener cierta comunicación y hacer transacciones entre ellas, intercambiando información, sobre todo en las instituciones gubernamentales donde se implementan proyectos o programas de asistencia social en las que deben intervenir varios sectores y organizaciones. Es por ello, que el intercambio de información a través de Internet se ha vuelto una

necesidad básica de todas las dependencias gubernamentales. Pero, al servirse de la conectividad, las empresas también aumentan el número de intrusiones externas a sus redes internas, pues se intercambia información confidencial en un entorno que por naturaleza no es seguro. Internet representa el punto principal de entrada para cualquier intruso que desee hurtar, modificar o borrar información confidencial de una institución, pues a través de Internet puede tener acceso a la red interna y, a su vez, a la información privada, almacenada en los servidores de dicha organización. Es por ello que lo primero que se debe proteger es la salida de la red interna hacia Internet por medio de firewalls o servidores Proxy que filtren el acceso de personas no permitidas. Generalmente ninguna persona externa y ajena al propio Instituto debe tener acceso a la Intranet, sin embargo, cualquier persona esta autorizada para consultar la página web del Instituto sin ninguna restricción, consultando la información que el mismo Instituto publica para conocimiento de todos.

Ahora bien, el Instituto Mexicano del Petróleo (IMP) y muy en particular la Gerencia de Tecnología Informática han sido víctimas en diversas ocasiones de intrusiones y ataques de todo tipo de virus que han interrumpido el servicio por periodos de tiempo considerables, lo que hace tener más cuidado en el nivel de seguridad que se implementa en sus sistemas, sobretodo sabiendo que una de las funciones de dicha gerencia es la investigación sobre los avances tecnológicos en el campo de la informática y la computación. Vamos a representar los riesgos que presenta la gerencia con la tabla 5.1 siguiente.

Elemento en riesgo	***Probabilidad***	***Pérdida***	***Riesgo exposición***
Intrusión externa por no actualizar la tecnología de perímetro (firewalls, IDS, etc.)	*50%*	*10*	*5*
La información y los recursos son expuestos si no se mantienen los passwords en secreto	*80%*	*5*	*4*
Posibilidad de robo o daño físico a los equipos por no tener una política de seguridad física en el Site	*90%*	*10*	*9*
Pérdidas de información y modificaciones no autorizadas por un inadecuado aseguramiento y control en la compartición de archivos	*70%*	*5*	*3.5*
Pérdida de información, posibles ataques con software malicioso y uso inadecuado de los recursos del IMP (como el uso de Internet) por un mal proceso de administración de políticas sobre aquellos equipos que sean ajenos a la organización	*80%*	*8*	*6.4*
Infección en la red y degradación en los servicios por no contar con un sistema de antivirus funcionando y actualizado	*60%*	*3*	*1.8*
La información confidencial puede ser vista por cualquier persona externa si no se encuentra encriptada	*80%*	*8*	*6.4*

Tabla 5.1 Evaluación de riesgos de la GTI

Esta evaluación de riesgos se realizó en Octubre de 2003 y fue proporcionada por la gerencia como un antecedente de la situación que enfrenta la misma en cuestión de seguridad informática.

La Gerencia de Tecnología Informática del IMP cuenta con un inventario de aproximadamente 1500 computadoras personales (entre servidores y clientes) en sus diferentes áreas, de las cuales cerca de 200 pertenecen al área de Soporte Informático y unas 80 al área de Seguridad de la Información. Todos estos sistemas de cómputo son soportados por la plataforma de Microsoft en sus diferentes versiones, es decir, que existen equipos con Windows 95, 98, Me y, en su gran mayoría, con Windows XP. Todas las máquinas tienen integrada una tarjeta de red con tecnología Ethernet y se encuentran conectadas a la Intranet del Instituto para la compartición de recursos.

Como se mencionó en el entorno del problema, la Intranet sigue las normas del cableado estructurado. La topología física es tipo estrella con 5 switches enlazados en forma redundante. La conexión del Backbone está conformada con fibra óptica, la cual tiene una velocidad de transmisión de 622 Mbps empleando la tecnología ATM. El cableado vertical también está conformado por fibra óptica y tecnología ATM, en tanto que el cableado horizontal lo constituye el cable de par trenzado categoría 5 con tecnología Ethernet y Fast-Ethernet, que puede alcanzar una velocidad de transmisión de 100 Mbps.

5.2 Estructura Organizacional del IMP

De acuerdo a la metodología de seguridad informática Scitum planteada en el capítulo 2, es indispensable identificar las necesidades y los objetivos que persigue la Gerencia de Tecnología Informática mediante las actividades que realiza, cuáles son sus procesos y de qué forma los lleva a cabo. En este contexto, el campo de estudio de la tesis se centra en el área de Seguridad de la Información de la Gerencia de Tecnología Informática (GTI), la cual tiene como función evaluar técnicamente los bienes y servicios informáticos para asegurar la correcta operación de los mismos, considerando las necesidades de la Institución y los productos existentes en el mercado. Además, la GTI esta encargada de dar soporte a los usuarios ante cualquier problema o eventualidad que se presente con los equipos de cómputo durante el desarrollo de su trabajo. (Ver figura 5.1)

Así mismo, la GTI tiene a su resguardo el software que emplea la parte administrativa del Instituto. Por tanto los servicios de instalación de software, configuración de cuentas de correo electrónico, antivirus institucional, depuración de los equipos, instalación de sistema operativo, solución de problemas con el software, etc. son atendidos por el área de Soporte Informático de la misma gerencia.

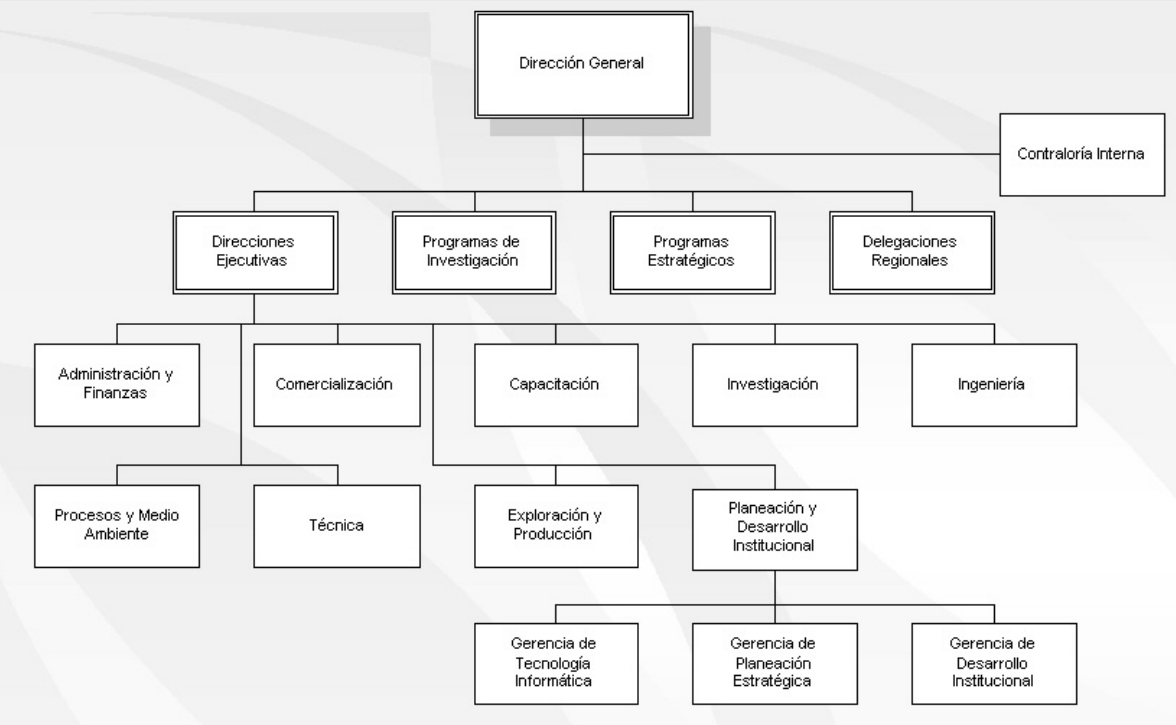


Fig. 5.1 Estructura organizacional del IMP

La Gerencia de Tecnología Informática, con sus distintas áreas, cumple con diferentes funciones dentro del IMP las cuales son:

1. *Evaluar los bienes y servicios informáticos existentes en el mercado para su utilización dentro del Instituto, de acuerdo a sus necesidades.*
2. *Asegurar el buen funcionamiento de todos los recursos informáticos con los que cuenta el IMP para el desarrollo de sus actividades.*
3. *Asegurar el adecuado funcionamiento de los recursos que hacen posible la conectividad de la red interna del Instituto, así como la conectividad externa y/o hacia Internet.*
4. *Impulsar la investigación en cuestión de tecnología informática para el mejor aprovechamiento de los recursos informáticos.*
5. *Atender las solicitudes de los usuarios ante cualquier evento que se presente durante el desarrollo de sus actividades cuando estén haciendo uso de recursos informáticos.*
6. *Asegurar la confidencialidad, integridad y la disponibilidad de la información que maneja el Instituto y que es almacenada en los recursos informáticos con los que cuenta el Instituto, así como la que viaja a través de la red interna del mismo.*
7. *Garantizar que la información confidencial del Instituto no sea expuesta a personas ajenas al propio Instituto o que se haga mal uso de ella.*
8. *Responder ante cualquier contingencia o evento imprevisto que pueda dañar la operabilidad de la gerencia.*

Para poder realizar sus actividades, la GTI cuenta con diversas áreas y brinda también diferentes servicios entre los que se encuentran:

- **Servidores de Correo**. *Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros con independencia de la red que dichos usuarios estén utilizando. El IMP cuenta con servidores de correo para todos sus empleados como un medio de comunicación y transferencia de archivos de manera inmediata.*

- **Servidores de Bases de Datos**. *El servidor de la base de datos almacena los programas y los datos de uso de la SAP en el concepto cliente/servidor R/3. También maneja el programa de actualización de la SAP y los tratamientos por lotes. La SAP R/3 es el nombre del software principal de ERP producido por la compañía de la SAP. Su nuevo nombre es el mySAP.*

- **Servidores de Web Hosting**. *El Web Hosting permite a un sitio web estar conectado a Internet a alta velocidad a través de un servidor web para que la información pueda ser por vista en todo el mundo a través de un navegador (browser). En otras palabras, el web hosting provee el lugar en Internet donde reside un sitio Web. Dentro de este tipo de servidores la gerencia administra el que aloja el portal de la página web del Instituto, el de la Intranet y el de la Extranet.*

- **Servidores ERP (Enterprise Resource Planning)**. *La Planeación de Recursos Empresariales es una herramienta de software administrativo que ayuda a las empresas en la gestión de sus procesos (como contabilidad, compras, inventarios, finanzas, logística, producción y recursos humanos) mediante procesos transparentes y en tiempo real en bases de datos relacionales y centralizadas. Entre las características de un ERP están la optimización de los procesos empresariales, el acceso a información confiable, precisa y oportuna, la posibilidad de compartir información entre todos los componentes de la organización, la eliminación de datos y operaciones innecesarias y la reducción de tiempos y de los costos de los procesos.*

- **Servidores de Aplicaciones o Administración**. *Son una serie de componentes y/o programas que puedan ser accedidos por otros. Dentro de este tipo de servidores la GTI tiene a su cargo un servidor que permite la actualización del antivirus institucional, uno más de respaldos para la información de mayor importancia que la misma gerencia genera y otros dos que alojan sistemas multi-agentes para la configuración de hardware y la instalación de software vía remota.*

Existen diversos servidores que alojan diferentes aplicaciones, las cuales dan soporte a los usuarios de la gerencia y con los que se cumplen las funciones de cliente. Estos servidores forman parte de la red interna o Intranet del Instituto Mexicano del Petróleo por lo que también interactúan con otros servidores que dan soporte a otras gerencias y áreas del mismo Instituto. Ahora bien, las características actuales de hardware de los distintos servidores de aplicaciones que componen la Gerencia de Tecnología Informática son las siguientes:

- *Equipo Compaq DeskPro EN*
- *Procesador Pentium III a 866 MHz*
- *512 MB de memoria RAM*
- *Disco duro de 30 GB*
- *Tarjeta de red y sonido integradas*
- *Monitor genérico de 15 pulgadas*
- *Floppy de 3½ pulgadas*
- *CD-ROM 12x*
- *Puerto SVGA y puerto serial*
- *2 puertos USB*
- *Slots PCI e ISA*

En tanto a software se refiere, todos los servidores de aplicaciones trabajan bajo la plataforma Microsoft Windows 2000 Advanced Server y cuentan con la protección del antivirus institucional Norton 2005 de Symantec.

Todos los servidores de aplicaciones tienen las características de hardware anteriores y se encuentran ubicados en un solo cubículo cerrado con llave, pero las condiciones de ventilación no son las más adecuadas puesto que el cubículo se encuentra cerrado la mayor parte del tiempo y únicamente tiene ventilación por una ventana. El funcionamiento de los diferentes servidores se considera bueno a pesar de los distintos ataques de virus que han recibido, sin embargo, se encuentra un tanto limitado por el hardware en el que se soporta por la razón de que ya se encuentra atrasado de la nueva tecnología. De manera personal, sería aconsejable que estos equipos contaran por lo menos con un disco duro configurado en espejo para evitar pérdidas de información cuando se dañe uno, es decir, tener un respaldo. Toda la atmósfera bajo la que funcionan estos servidores representa un gran número de riesgos que han motivado a que los servicios que ofrecen sean soportados por un sistema operativo que pueda brindar un nivel de seguridad más alto del que tienen actualmente. Como parte de un proyecto para la mejora en la calidad de los servicios y con la necesidad de asegurar la información confidencial que genera, la GTI evaluó la situación y decidió implementar ciertas medidas de seguridad para todos sus servidores que permitan reducir al mínimo los riesgos de intrusiones no deseadas, pérdidas de información y, sobre todo, la interrupción de su operabilidad; para este nuevo proyecto se propuso una migración a Linux como la plataforma de los diversos servicios que ofrece dicha gerencia.

5.3 Justificación para la Migración a Linux

Debido a los recientes ataques de los que han sido víctimas los distintos servidores de la Gerencia de Tecnología Informática, y los cuales han afectado seriamente su operación y han puesto en riesgo la integridad de su información, los directivos de la misma gerencia tomaron la decisión de implantar nuevos controles de seguridad con el fin de proteger al máximo su red de datos de personas con malas intenciones. La propuesta inicial de dicha gerencia se basó en implementar una estrategia que fuera efectiva pero que al mismo tiempo le permitiera no consumir demasiados recursos económicos, por lo tanto, se pensó en el uso de herramientas gratuitas que reforzarán la seguridad de los servidores bajo la plataforma Microsoft Windows 2000 Avanced Server; sin embargo, esta solución traería, desde una perspectiva personal, ciertas limitantes y no se considera la solución más adecuada por varias razones:

1. *El sistema operativo Windows 2000 Advanced Server se considera un tanto obsoleto para los fines de seguridad que debe cumplir; en su lugar se recomendaría la implementación de la plataforma de Windows 2003 para servidores porque no presenta las vulnerabilidades de la versión anterior y cuenta con nuevas funcionalidades que lo hacen más "seguro". Sin embargo, esto traería consigo un desembolso bastante grande por el pago de las licencias del nuevo software.*

2. *Los principales ataques que sufrieron los servidores de la GTI fueron causados por virus, gusanos y programas semejantes. Los sistemas operativos de la plataforma Microsoft son demasiado vulnerables a los ataques de todo tipo de virus, aún contando con un buen antivirus actualizado, debido a la forma de administración de los usuarios y sus archivos (los usuarios no son propietarios de sus propios archivos).*

3. *Las diversas herramientas gratuitas que son afines con el sistema operativo Windows 2000 Advanced Server son limitadas y la mayoría de ellas son herramientas nativas del sistema operativo Unix, por lo que su implementación sería más adecuada bajo Linux. Por otro lado, no todas las herramientas son lo suficientemente prácticas para los objetivos que se persiguen, por ejemplo:*

   - **Analizadores del tráfico de red**. Ethereal *y* Sam Spade *son dos excelentes analizadores de red y cuentan con un gran potencial, además de mostrar sus resultados de una manera fácil de entender y contar con una interfaz gráfica que las hace unas herramientas bastante amigables. Sin embargo, la red del Instituto es monitoreada diariamente y en todo momento con el fin de tener un control sobre lo que consultan los usuarios en Internet, además de que se considera una norma básica de seguridad que permite*

detectar anomalías en el tráfico de la red interna por lo que no se considera que haya necesidad de implementar otro analizador de red, ya que únicamente se aumentaría el tráfico interno.

- **Sistemas de detección de intrusiones**. Snort *y* Fragroute *se consideran los mejores detectores de intrusos dentro de las herramientas consideradas como freeware, pero se descartó su uso por el hecho de que la Intranet del Instituto esta protegida con su propio detector de intrusiones y, además,* Fragroute *se encuentra implementado en otro punto de la red del Instituto, por lo que se considera redundante utilizar otro IDS más en la subred de la GTI.*

- **Escáneres para servidores HTTP**. *Los auditores de sistemas como* Whisker *y* Tripwire *son herramientas muy útiles para medir los riesgos que presentan los sistemas, sin embargo, éstas dos no se consideran lo suficientemente funcionales porque presentan muchos agujeros de seguridad y su poder de análisis no es muy completo; además, sus resultados son mostrados en una forma compleja de entender, lo cual hace perder mucho tiempo en su lectura.*

- **Cracker de passwords**. John the Ripper *es un buen comprobador proactivo de passwords para la plataforma Microsoft, el cual permite configurar las reglas que se consideren convenientes y presenta sus resultados de forma clara; sin embargo, no se considera una herramienta absolutamente necesaria puesto que el IMP tiene dentro de sus políticas que los usuarios creen sus passwords de acuerdo a cierto criterio establecido.*

- **SSH, Secure Shell**. *Esta herramienta es absolutamente necesaria en un entorno de red por el que viajan datos confidenciales porque es un medio seguro que encripta los datos. Es un excelente reemplazo de aplicaciones como Telnet y ftp; pero también funciona en Linux.*

4. *La implementación de seguridad bajo la plataforma de Microsoft depende únicamente del fabricante y se encuentra limitada por las soluciones que el mismo haya implementado en un tiempo no definido; es decir, no se cuenta con el código del sistema operativo para poder implementar la seguridad ajustada a las necesidades de los diferentes sistemas. Linux en cambio, tiene la ventaja de ofrecer abiertamente el código fuente del sistema operativo para que puede ser modificado y ajustado a lo que se necesite y con esto desarrollar un adecuado nivel de seguridad.*

Mi propuesta personal, después de analizar las limitaciones anteriores, fue hacer una migración hacia un sistema implementado bajo la plataforma Linux

por su estabilidad en funciones críticas. Y de todas las distribuciones que existen de este sistema operativo me inclino por la distribución de Red Hat principalmente por su fácil configuración y manejo, además por su interfaz gráfica muy útil y funcional gracias a su semejanza con el ambiente de Windows.

Las principales características que ofrece Linux son:

- *Debido a su naturaleza, Linux es un sistema operativo gratuito que se puede conseguir fácilmente en Internet o en algunas revistas de carácter informático.*
- *Linux se distribuye junto con las fuentes de los programas, lo que permite hacer cambios en los mismos para mejorarlos o adaptarlos a nuestras necesidades. Eso hace que tanto el desarrollo del Linux como la depuración de errores, adaptación de nuevo hardware, etc. Se realice de una manera más rápida.*
- *Tiene un amplísimo soporte de comunicaciones y redes, que es muy importante en estos tiempos en los que las empresas necesitan de una buena conectividad.*
- *Casi todo lo que sirve para Unix, sirve también para Linux (GCC, Bash, Emacs, X windows, Perl, Python, etc) y todo es gratis.*
- *Tiene un amplio soporte de hardware (tarjetas, periféricos, etc.) de todos los sistemas operativos. Linux es un sistema operativo realmente de 32/64 bits multipuesto y multitarea, o sea, que aprovecha mucho mejor la potencia real de los PCs de hoy en día y soporta múltiples procesadores.*
- *Es un sistema operativo multiplataforma. Es decir, existen versiones de Linux para PC, Macintosh, Apple, Amiga, SUN, Alpha, PowerPC, etc.*
- *Linux provee con todas las herramientas necesarias para montar su propio servidor Web, HTTP, FTP, de correo, news y lo más importante con soporte CGI de todo tipo (Perl, C, PHP). Incluso se pueden instalar las extensiones FrontPage y soporte ASP con ChiliASP.*
- *Un núcleo estable y seguro, puede configurar los drivers como módulos separados o compilarlos dentro del núcleo para mejorar el rendimiento incluso después de haber instalado el sistema operativo.*
- *Posee una gran cantidad de utilidades para Internet*, finger, whois, ping, *varios shells (*ash, bash*),* telnet, ftp, *todo desde su línea de comandos donde también puede usar los mismos comandos de interpretes que haya instalado, incluso puede desarrollar sus scripts junto con sus bases de datos SQL instaladas.*

5.3.1 Linux contra Windows

Ahora bien, las ventajas que presenta la plataforma Linux frente a la plataforma Microsoft Windows son:

1. **Confiabilidad**. *Probablemente una de las características de los sistemas operativos a la que mayor importancia le dan los administradores de sistemas es la confiabilidad. Linux tiene tras de sí 30 años de desarrollo en Unix, el cual tiene la reputación de ser el más confiable de todos. Muchos servidores han estado en operación durante años sin tener que ser arrancados de nuevo por alguna falla. En este sentido, a Microsoft le falta mucho camino por recorrer para lograr la estabilidad y confiabilidad de Unix.*

2. **Seguridad**. *Dado el avance tecnológico en las telecomunicaciones, hoy día los sistemas de cómputo trabajan en un ambiente de intercomunicación global, por lo tanto la seguridad en los sistemas operativos es un aspecto de máxima importancia. Así, se puede afirmar categóricamente que Linux es uno de los sistemas operativos más seguros que existen. La seguridad en Linux puede ser configurada de acuerdo a necesidades particulares, debido a que viene implementada desde el kernel, de modo que es posible configurarla a nivel de sistema de archivos, de servicios de red, de facilidades en el host y de capacidades de usuario. Utilizar mecanismos de seguridad propietarios tampoco es garantía de una operación a prueba de manipulaciones. Al menos los esquemas de seguridad de dominio público están abiertos a una comprobación meticulosa y a la revelación de los resultados de esos análisis. Por otra parte, Linux se ha mantenido de cierta forma inmune al ataque de los virus que constantemente asedian a Microsoft Windows porque cada usuario es propietario de sus archivos, y otro usuario no puede acceder a estos archivos y los avances tecnológicos en el campo de la autenticación y la encriptación se dan en el ambiente Linux donde son adoptados en primera instancia y luego implementados por otros sistemas operativos.*

3. **Funcionalidad**. *Frecuentemente se malentiende que Windows NT es un sistema operativo multiusuario, cuando lo cierto es que solamente un usuario puede entrar al sistema a la vez y no puede ejecutar programas en el servidor para aprovechar el poder de procesamiento del mismo, solamente puede tomar ventaja de este poder a través de aplicaciones cliente/servidor. Un usuario de Linux puede hacer* login *al servidor de manera segura y ejecutar aplicaciones, aprovechando así el poder de procesamiento del servidor, balanceando la carga de trabajo entre éste y su estación de trabajo. En Linux es posible acceder a un equipo remoto y trabajar en el, utilizando su teclado y su ratón como si fueran los que están conectados en la otra máquina, todo esto sin comprar software adicional.*
   Para muchas compañías el correo electrónico es una herramienta indispensable de comunicación, sin embargo con Windows usted tiene que comprar otra suite de aplicaciones para tener este servicio habilitado

(más dinero a la cuenta del costo de la licencia). En Linux este servicio es manejado con programas como: sendmail, fetchmail, pop3, qmail, *etc. los cuales son muy poderosos, flexibles y además gratuitos.*
Otra falta en el diseño de los sistemas operativos de Microsoft tiene que ver con el uso anticuado de letras en el manejo de discos. Esta metodología está limitada al número de letras del alfabeto, además de que tampoco es posible crear jerarquías con los directorios compartidos por otras máquinas de la red. En Linux es posible montar los recursos compartidos en cualquier lugar de la estructura de directorios. Un directorio compartido puede abarcar varios discos o aún diferentes máquinas, permitiendo así a los administradores mantener las estructuras de directorios existentes, las cuales ya son bien conocidas por los usuarios, esto permite expandir el espacio en disco del servidor de manera transparente. Esto pone de manifiesto el hecho de que Linux fue concebido desde sus orígenes como un sistema operativo cliente/servidor para uso profesional, mientras que Windows proviene del DOS, un sistema operativo que no fue concebido para trabajar en un ambiente cliente/servidor y mucho menos para funcionar como un servidor.
Facilidad de configuración y la posibilidad de hacerlo sin tener que reiniciar el servidor es otra característica de funcionalidad importante, la cual posee Linux, por ejemplo se pueden cargar y descargar módulos de software mientras el sistema esta operando sin tener que reiniciar el equipo. Al efectuar algún cambio significativo en la configuración de Windows se tendrán que interrumpir los servicios del equipo y desconectar a los usuarios mientras la máquina se reinicia.

4. **Administración**. *Para muchos resulta sorprendente el hecho de que los parámetros de configuración de Linux se almacenan en archivos de texto. Los archivos de configuración de Linux son poderosos y flexibles en su sencillez, por ejemplo, se puede manejar su configuración con un sistema de control de versiones, permitiendo analizar los cambios que se han efectuado y con la posibilidad de revertirlos y dejar el sistema con una configuración anterior, cosa que no posee Windows. Ahora bien, a medida que los equipos se van dispersando a otras localidades aún es posible configurarlos remotamente, ya sea mediante una sesión telnet, o a través de sesiones X Windows, o por medio de aplicaciones Java. Existen decenas de aplicaciones para la administración Linux, las cuales tienen la capacidad de operar sobre equipos remotos. En contraste con la plataforma de Windows, la mayoría de los sistemas Linux vienen equipados con lenguajes de script (BASH Shell, Korn Shell, C Shell, Perl, Python, TCL, etc.) y con los comandos "cron" y "at" los cuales permiten programar y ejecutar tareas complejas en cualquier intervalo de tiempo deseado. Gran parte de la administración de Linux se maneja en forma automática y personalizada a través del uso de estas herramientas, lo cual redunda en el aprovechamiento óptimo de los recursos (tiempo, personal, etc.) y La utilización de recursos de Linux es mucho menor que*

en las distintas versiones de Windows. Además, en el mundo Linux existen, desde hace algún tiempo, entornos gráficos muy poderosos que proporcionan una interfaz gráfica de alto nivel.

5. **Desempeño**. *Tal vez uno de los aspectos más polémicos de los sistemas operativos es el del desempeño. Respecto a esto es muy importante resaltar el hecho de que el hardware es responsable en gran medida del desempeño del sistema. El asunto radica en la capacidad del sistema operativo para correr sobre plataformas de hardware poderosas y escalables. Tradicionalmente Linux ha sido el campeón en este campo, es por eso que las empresas con grandes necesidades de procesamiento ejecutan sus sistemas en alguna versión de éste. Linux corre en diversas plataformas de hardware como Intel, Alpha, SPARC, MIPS, PowerPC, etc. La mayoría de los expertos concuerdan en que Linux se desempeña mejor que Windows en máquinas con escasos recursos de hardware y sus excelentes prestaciones como servidor Web mediante el servidor Apache no son objeto de ninguna discusión, lo cual no resulta extraño si recordamos el hecho de que el kernel de Linux es compacto, estable y configurable, de modo que éste puede ser manipulado para efectuar de manera más ágil las tareas que se le encomiende. En cuanto a posibilidades de configuración Linux brilla por su calidad al poder configurar casi cualquier aspecto del sistema operativo para adaptarse a las necesidades específicas del usuario.*

6. **Costo**. *Tal vez este sea el factor más determinante en la adopción de Linux como plataforma de trabajo, porque si Linux fuera igual de inestable, inseguro, disfuncional y con la misma interfaz de Windows, solo por ser de libre distribución todo mundo lo usaría. Así es que, siendo realistas Linux vale por lo menos lo mismo que cualquiera de los otros sistemas operativos comerciales. Ahora bien, el costo no sólo se compone por lo que se paga al adquirir su sistema, si no por el software adicional que se requiera, el soporte técnico necesario, la instalación y configuración del mismo, así como por las subsecuentes actualizaciones de versión y en el caso del software comercial, por las licencias adicionales que más tarde se necesiten.*

5.4 Aplicación de la Estrategia de Seguridad

Para la aplicación de la estrategia de seguridad se tomará como base uno de los servidores con los que cuenta la gerencia. El propósito fundamental es sentar las bases para que la misma estrategia sea implantada posteriormente en todos los demás servidores de la GTI. Es imposible seguir una receta o procedimiento que permita determinar una estrategia de seguridad universal, es decir, que pueda aplicarse por completo a cualquier servidor, puesto que

depende del tipo de servicio que este ofrezca y del perfil de cada usuario que solicita el servicio, el nivel de seguridad y las políticas que serán aplicadas. Sin embargo, con este trabajo se pretende aplicar una estrategia de seguridad a un determinado servicio, la cual permita un ajuste para su implementación en otro tipo de servicios dependiendo de las necesidades individuales de cada uno de ellos. El servidor sobre el que se trabajó para implementar la estrategia de seguridad es un servidor de aplicaciones que contiene un sistema multi-agente para instalación remota de software.

La implementación de la estrategia de seguridad se compone de varias etapas (ver fig. 5.2), las cuales son:

1. **Detección de las necesidades de la Institución**. *En esta etapa se define detalladamente la forma en que esta constituido el Instituto Mexicano del Petróleo, su estructura organizacional, sus diferentes áreas y las actividades que realiza la Gerencia de Tecnología Informática.*

2. **Definición de la problemática encontrada**. *Una vez definidos los servicios que presta la Gerencia de Tecnología Informática, se plantean los riesgos que presentan sus aplicaciones.*

3. **Análisis de Riesgos**. *De la definición del problema, se realiza un análisis de los riesgos y las vulnerabilidades que ponen en peligro la operación.*

4. **Análisis de las distintas plataformas de distribución libre**. *Se analizan las ventajas y desventajas de la seguridad y la funcionalidad que brinda una plataforma u otra.*

5. **Implementación de la plataforma Linux**. *Una vez elegido la plataforma que brindará soporte a las distintas aplicaciones, se realiza la implementación de la misma en el servidor mediante dos fases:*
   - Migración de la base de datos. *Dado que la aplicación estaba originalmente programada para funcionar bajo la plataforma de Microsoft, se tuvo que hacer una migración de toda la base de datos a MySQL Server con la finalidad de que fuera compatible con la plataforma Linux.*
   - Configuración del servidor. *Se configuraron todos los aspectos necesarios para que el servidor funcionara adecuadamente bajo la plataforma Linux.*

6. **Análisis de las distintas herramientas de seguridad libres**. *Se revisaron detalladamente todas las herramientas de seguridad libres existentes con el fin de elegir las que fueran más adecuadas para las necesidades del servidor.*

7. **Implementación de las herramientas libres en el servidor**. *De las herramientas que se revisaron, se eligieron solo algunas para que sirvieran de complemento a la configuración del servidor.*

8. **Pruebas de seguridad a la nueva configuración**. *Una vez configurado en su totalidad el servidor con su aplicación, se realizaron algunas pruebas de penetración, etc. para comprobar que la configuración realizada cumplía con los criterios de seguridad esperados.*

9. **Desarrollo de políticas y procedimientos**. *Las políticas y los procedimientos constituyen una parte de la documentación que debe entregarse a la Gerencia de Tecnología Informática, en la cual se define la manera en la que operará el servidor, la participación que tiene el administrador del sistema en dicha operación, la participación de los usuarios, etc.*

10. **Concientización del personal**. *La última parte de la estrategia comprende el crear consciencia en el personal de la importancia que tiene la seguridad informática dentro de las organizaciones, con la cual se pueden evitar muchísimos riesgos provenientes, por ejemplo, de la ingeniería social.*

Durante la realización de cada una de estas etapas se pudo aprovechar mucha de la información que la misma Gerencia de Tecnología Informática pudo brindar para facilitar el trabajo, es decir, que existía trabajo previo del cual se aprovechó alguna información; por ejemplo, existía un pequeño análisis de los riesgos que sufren las aplicaciones, había reportes que describían de manera sencilla la problemática que traviesan dichas aplicaciones, se contaba con un manual de políticas y procedimientos internos de la propia gerencia, etc. Con todo esto se pudo recabar información más rápidamente y se pudieron definir de forma más adecuada las características de servicio que se presentan a continuación.

Fig. 5.2 Gráfica de Gantt con las distintas etapas de la Estrategia Implementada

5.4.1 Características del Servicio

Como se mencionó anteriormente, uno de los principales servicios que se ofrecen dentro de la Gerencia de Tecnología Informática del IMP hacia los usuarios es la instalación remota de software, la cual se realiza a través de una aplicación compuesta de un sistema Multi-Agente (MAS) que se encuentra alojado en uno de los servidores con las características de hardware antes descritas. Alterno a este servidor se encuentra otro similar en el que se aloja también un MAS para configuración remota de hardware. Anteriormente este servicio se realizaba manualmente por personal del área de Soporte Informático, encargada de resolver cualquier problema técnico y dar mantenimiento a los equipos de cómputo de la gerencia en cuestión. La forma en que este servicio era ofrecido se muestra en las figuras 5.4. Sin embargo, desde hace ya casi un año este servicio se automatizó por medio de sistemas multi-agente con el propósito de dar una respuesta oportuna a las necesidades de software y hardware que los distintos usuarios presentan para llevar a cabo sus actividades cotidianas dentro del IMP.

El enfoque de agentes permite una mayor flexibilidad en comparación con otros enfoques de programación para este tipo de aplicaciones por su comportamiento autónomo y la evolución del comportamiento dinámico, además de poder enfrentarse con situaciones no previstas o inesperadas. Toda esta funcionalidad del sistema permite que el personal de la GTI dedique su tiempo a otras actividades que requieran mayor atención.
Ahora bien, el software bajo el que trabaja el sistema multi-agente para la instalación remota de software es:

- *Sistema Operativo Microsoft Windows 2000 Advanced Server con todas las actualizaciones vigentes (Service Pack)*
- *Servidor Apache como contenedor de Aplicaciones Web TOMCAT*
- *Servidor FTP como mecanismo de autenticación*
- *MySQL para*
- *Antivirus institucional Norton 2005 de Symantec*
- *Firewall de Microsoft ISA Server 2000 Enterprise Edition con todas las actualizaciones vigentes (Service Pack)*

El sistema para la instalación remota de software se enfoca a proporcionar el servicio de instalación, configuración y restauración de software, por lo que los agentes involucrados para dar el servicio son:

- **Asistente**. *Este agente será la interfaz con el usuario que captura los requerimientos de éste y los problemas que pueda presentar con su máquina con alguna aplicación previamente instalada.*
- **Secretario**. *Desempaña el papel de administrador de documentos. Este agente será la interfaz con la secretaria y se encarga de elaborar*

reportes globales así como tener comunicación con otros agentes y permitir administrar los reportes para un antecedente.

- **Supervisor**. *Desempeña el papel de monitor de los servicios solicitados. Es una interfaz en donde el supervisor permite revisar los reportes, elaborar las estadísticas de servicio, enviar mensajes de confirmación de servicios prestados y visualizar las respuestas de confirmación de servicios.*
- **Administrador**. *Agente que captura las solicitudes y elige al agente que puede proporcionar el servicio y que administra el software con el cual puede proporcionar sus servicios. Sirve como motor de comunicación y coordinación con otros agentes que realizan propiamente las tareas del sistema.*
- **Instalador**. *Agente encargado de realizar la instalación del software en un equipo, lo cual involucra desde trasladarse a la máquina del solicitante hasta enviar un reporte de las acciones realizadas y los resultados obtenidos.*
- **Configurador**. *Está encargado de efectuar la configuración del software después de que haya sido instalado en un equipo trasladándose e introduciendo parámetros necesarios para personalizar las aplicaciones.*
- **Ejecutor**. *Encargado de ejecutar las aplicaciones que sirven para dar mantenimiento al sistema operativo.*
- **Restaurador**. *Encomendado a efectuar la restauración de los archivos de configuración de aplicaciones instaladas en el sistema operativo.*

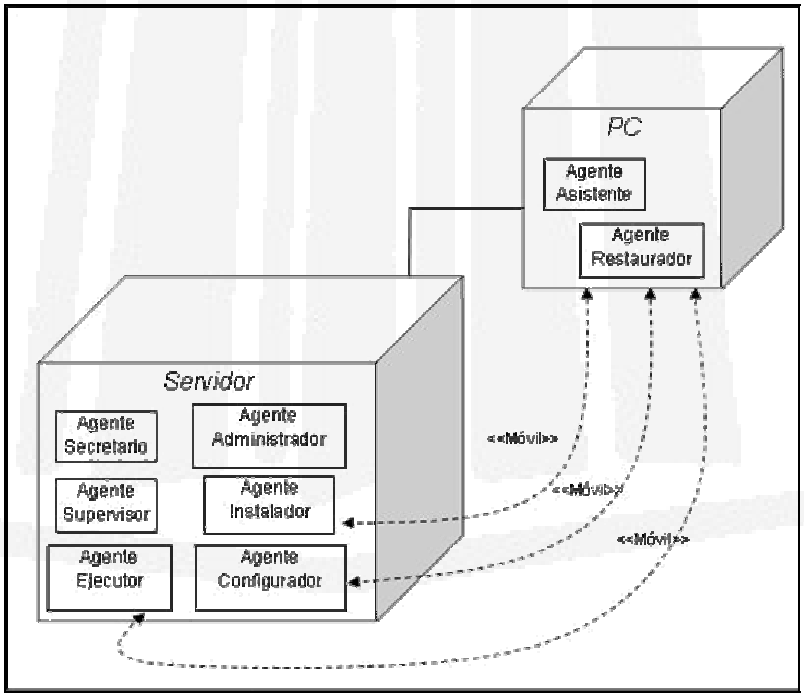


Fig. 5.3 Diagrama de distribución del MAS para instalación remota de software

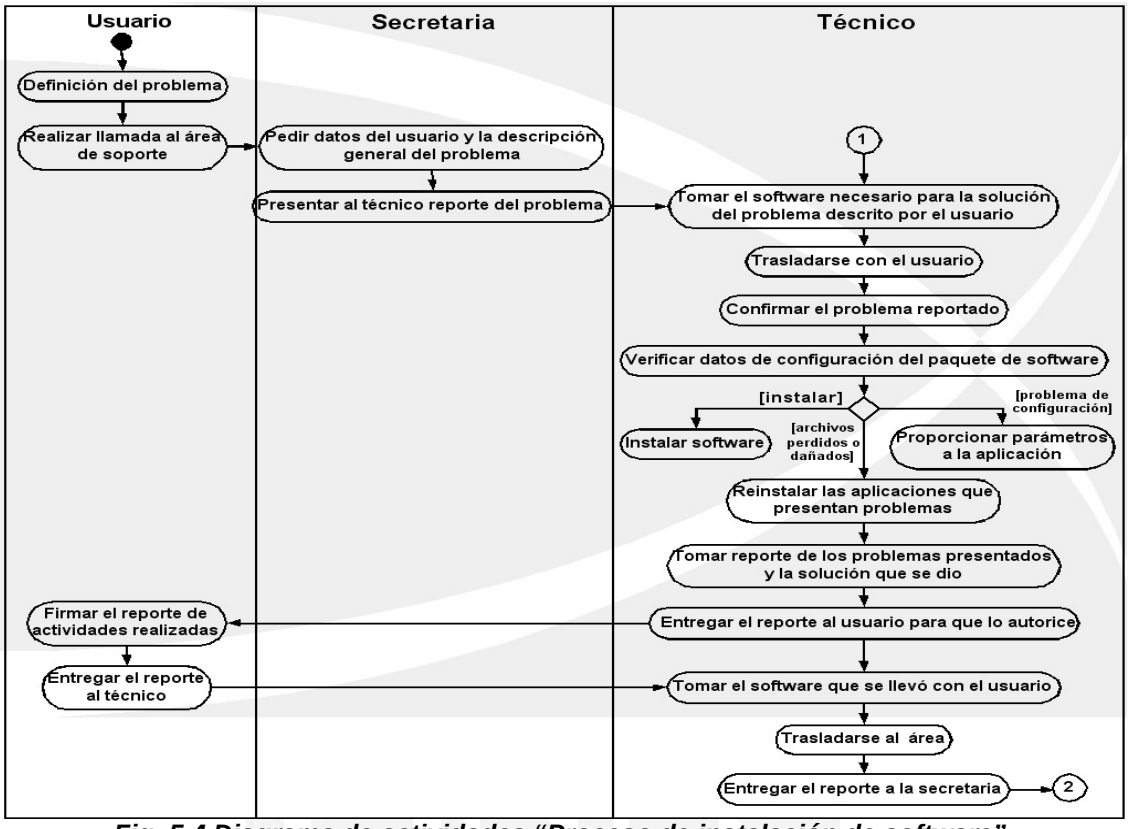


Fig. 5.4 Diagrama de actividades "Proceso de instalación de software"

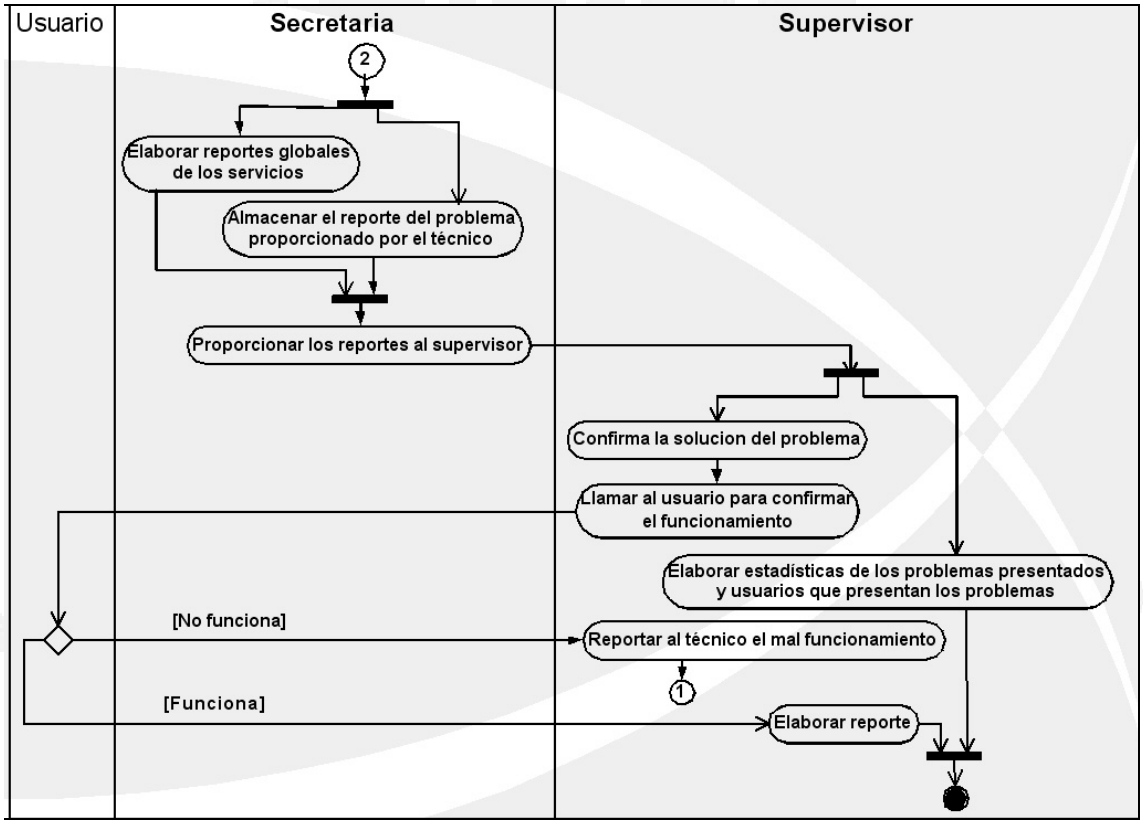


Fig. 5.4 Diagrama de actividades "Proceso de instalación de software" (continuación)

A continuación se muestra la tabla 5.2 en la cual se denota cómo se encuentran distribuidas las tareas que se han identificado con respecto a los agentes que se enlistaron en la sección anterior:

Tareas / Agentes	Obtener Datos del Equipo	Obtener Datos del Usuario	Obtener Archivos de Configuración del Equipo	Elaborar Cadena de Servicio
Asistente	X	X		X
Secretario				
Supervisor				
Administrador				
Instalador				X
Configurador				X
Ejecutor				X
Restaurador			X	X

Tabla 5.2 Tareas Vs Agentes

Tareas / Agentes	Obtener Información del Reporte	Guardar Archivo de Reporte	Elaborar Cadena Solicitud de Servicio	Elaborar Estadísticas
Asistente				
Secretario	X	X		
Supervisor			X	X
Administrador				
Instalador				
Configurador				
Ejecutor				
Restaurador				

Tabla 5.2 Tareas Vs Agentes (continuación)

Tareas / Agentes	Coordinar Acción de Agentes	Instalar Software	Introducir Parámetros de Instalación	Evaluar Datos de la PC
Asistente	X			
Secretario				
Supervisor				
Administrador	X			
Instalador		X	X	X
Configurador				
Ejecutor				
Restaurador				

Tabla 5.2 Tareas Vs Agentes (continuación)

Tareas / Agentes	Configurar	Ejecutar Aplicación	Crear Accesos Directos	Restaurar Archivos de Configuración del Equipo
Asistente				
Secretario				
Supervisor				
Administrador				
Instalador				
Configurador	X			
Ejecutor		X		
Restaurador			X	X

Tabla 5.2 Tareas Vs Agentes (continuación)

Tareas / Agentes	Ingresar Datos de DB	Obtener Datos de DB
Asistente		
Secretario		
Supervisor		
Administrador	X	X
Instalador		X
Configurador		X
Ejecutor		
Restaurador		X

Tabla 5.2 Tareas Vs Agentes (continuación)

Ahora bien, los servicios son tareas que un agente ofrece a otro agente, derivándose de las conversaciones, por tanto de las tareas de cada agente se han identificado los siguientes servicios que pueden ser demandados por los agentes:

- **Restaurar aplicaciones**. *Restaurar los archivos de registros que contiene la configuración de aplicaciones con anomalías.*
- **Crear reportes**. *Conformar unas cadenas en un documento con formato específico del tipo de cadena entrante.*
- **Obtener datos de reportes**. *Extraer de un documento con formato específico, los datos demandados.*
- **Instalar**. *Trasladarse a la máquina que necesite el software e instalarlo.*
- **Configurar**. *Obtener datos necesarios de la DB y trasladarse a la máquina del usuario e introducir los parámetros necesarios.*
- **Ejecutar aplicaciones**. *Trasladarse a la máquina y ejecutar una aplicación específica.*

El funcionamiento de este sistema se puede explicar de manera breve de la siguiente forma: el servidor contiene a los agentes secretaria, administrador, instalador, configurador *y* ejecutor, *de los cuales únicamente los tres últimos*

son móviles porque son los que se desplazan hasta la máquina del usuario que solicita un servicio. El agente asistente*, alojado en la máquina del usuario, captura los datos del servicio solicitado por el usuario y los envía a los* agentes secretaria *y* administrador*. El* agente secretaria *levanta el reporte del servicio solicitado y el* agente administrador *decide qué agente se desplazará a la máquina del usuario dependiendo del servicio solicitado. El* agente supervisor *se encuentra alojado en otra PC que le sirve de interfaz al administrador del sistema para consultar los reportes de todos los servicios que ha brindado el MAS, por lo cual éste agente se comunica directamente con el* agente secretaria*. Por último, el* agente restaurador*, alojado el la PC del usuario, monitorea el estado del software instalado en su máquina para que cuando se presente un problema sea reparado.*

Cuando un usuario tiene la necesidad de instalar o reparar software en su máquina, éste debe levantar en su máquina la interfaz del agente asistente *donde captura la información del servicio que solicita, la cual se manda directamente al servidor que tiene alojado el MAS, específicamente a los* agentes administrador *y* secretaria*. Una vez que el* agente administrador *decide qué agente realizará el servicio, éste se traslada hasta la máquina del usuario para interactuar con él cuando sea necesario que éste introduzca datos requeridos para la instalación. Una vez realizado el servicio, el* agente secretaria *muestra al usuario las acciones que se llevaron a cabo y levanta el reporte. Existen 3 tipos de reportes: el de la petición del servicio, el del servicio ya realizado y el que el administrador programa para su estudio cada cierto tiempo. Este último sirve como bitácora de todas las acciones realizadas por los usuarios, la cual permite llevar un control general del sistema y da la pauta del nivel de seguridad que tiene el servicio ofrecido, ya que debe estar ajeno a personas externas a la gerencia y sobre todo a personal externo.*

El MAS que realiza la instalación remota de software esta elaborado con la herramienta JADE (Java Agent Development Framework), un software de ambiente de trabajo implementado totalmente en lenguaje Java. Esta herramienta simplifica la implementación de MAS a través de un middle-ware (software que se coloca entre una computadora cliente y un servidor para garantizar que se transmita la información aunque corran sobre plataformas distintas) que demanda para cumplir con las especificaciones de FIPA (Foundation for Intelligent Physical Agents, Fundación para Agentes Físicos Inteligentes).

Las principales características del sistema multi-agente que realiza la instalación remota de software son:

- *No instala sistemas operativos, únicamente herramientas y utilerías de Microsoft y algunas aplicaciones que genera el mismo Instituto.*

- *Valida al usuario que solicita el servicio para corroborar que esté autorizado para instalar cierto software en su máquina, dependiendo del área y perfil del usuario.*
- *Tiene una salida a Internet por medio de la cual actualiza el software que tiene en su base de datos y/o baja los parches correspondientes.*
- *No instala ni actualiza antivirus. El antivirus institucional se encuentra alojado en otro servidor y es actualizado automáticamente desde éste.*
- *Cuando se ha llevado a cabo una tarea, el MAS presenta al usuario una interfaz con el resumen de lo que se realizó; sin embargo, los reportes que se generan no se almacenan en archivos y permanecen ocultos a los usuarios.*
- *Tiene la posibilidad de ser programado para que cada cierto tiempo presente un reporte global con todos los movimientos que ha realizado, cuando el administrador del sistema lo solicite.*
- *Puede interactuar con el sistema multi-agente que realiza la configuración de hardware, el cual se encuentra en otro servidor.*

Descritas las características primordiales del sistema multi-agente, se describen ahora los requerimientos necesarios para su implementación en el servidor:

- *Un servidor Apache donde se encuentra el repositorio de todos los programas que puede instalar el MAS*
- *Una base de datos en SQLServer con toda la información que el MAS requiere para llevar a cabo sus tareas*
- *La plataforma JADE versión 3.0b1y FIPA-ACL (Lenguaje de Comunicación de Agentes)*
- *Lenguaje de programación Java j2sdk 1.4.0*

La funcionalidad práctica que tiene este sistema de agentes se entiende por el hecho de que al área de Soporte Informático presentó diferentes problemas al ofrecer este servicio de manera manual, es decir, con la intervención directa de un técnico, pues son muchas las solicitudes de servicio que se tienen que atender diariamente. De esta manera, al automatizar este proceso repetitivo por medio de un sistema multi-agentes se consigue cumplir con los siguientes puntos; ya que esta aplicación permite de manera autónoma darle solución a problemáticas que se presenten interactuando con su entorno:

- *Instalación de software de forma oportuna.*
- *Configuración del software eficazmente.*
- *Personalización del equipo del usuario oportunamente.*
- *Solución de problemas detectados por el usuario en su computadora.*
- *Automatización de los procesos de administración de la información recabada durante el proceso de servicio.*
- *Se elimina la necesidad de que el responsable se encuentre disponible para realizar el servicio, ya sea que se trate del personal del área de soporte o del usuario.*

5.4.2 Configuración del Servidor

Anteriormente se mencionó que la primera línea de seguridad comienza con una adecuada configuración del sistema operativo que soporta las distintas aplicaciones por lo que en esta parte se definirán de manera simple los aspectos más importantes que se tomaron en cuenta para la configuración del servidor que contiene el sistema multi-agente antes descrito. Por otro lado, cabe mencionar que la aplicación en sí cuenta ya con un nivel de seguridad aceptable debido a los métodos de autenticación que utiliza para brindar el servicio a los distintos usuarios de la GTI. Sin embargo, que la aplicación por sí misma sea segura no la hace inmune a los ataques de personas malintencionadas que diariamente se conectan a Internet. Para evitar todo tipo de riesgos, es importante definir una configuración adecuada que permita darle un nivel más alto de seguridad a la información que maneja el servidor del sistema multi-agente para la instalación remota de software.

El proceso de asegurar un host o servidor comienza incluso antes de la instalación cuando se decide qué tipo de servidor se construye, debido a que existen diferentes tipos y cada uno de ellos requiere una configuración diferente para un nivel de seguridad adecuado. Además, la instalación de Linux incluye por defecto muchos servicios innecesarios para los propósitos del servidor como el FTP, el NFS, los servicios RPC, los servicios R, etc.

Vamos a comenzar la configuración del servidor instalando Linux en su distribución Red Hat versión 9.0 con la versión compilada del kernel 2.6.11.11 en el equipo con las características antes mencionadas (para una referencia de la instalación ver el apéndice A). Los puntos que se toman en cuenta para la instalación son:

1. **Partición del disco duro**. *Será necesario crear varias particiones que contengan los archivos de la instalación de Linux. El disco duro tiene una capacidad de 30 GB, de los cuales 1 GB serán para la partición de intercambio (*/swap*), 200 MB para el núcleo del sistema (*/boot*), 10 GB para una partición que contendrá el repositorio con el software del sistema multi-agente (*/repositorio*), 5 GB para una partición que contendrá los reportes que se generan de las diferentes actividades que realiza el MAS (*/reportes*) y el resto del espacio será ocupado por la raíz.*

2. **Gestión de arranque**. *Debido a que el servidor sólo contendrá un sistema operativo (Linux), no es necesario modificar el gestor de arranque que por defecto arrancará Linux, pero se asegurará por medio de una contraseña.*

3. **Configuración de la red**. *Debido a las políticas del Instituto, las direcciones IP se asignan de forma estática, por lo cual al servidor se le*

debe especificar la dirección IP, el servidor DNS, el router (puerta de enlace) y el servidor Proxy.

4. **Configuración del firewall**. *Para tener un buen nivel de seguridad a través del mismo sistema operativo se debe configurar el firewall con su nivel de protección más alto, permitiendo sólo los servicios de HTTP (Web) y Secure Shell (SSH).*

5. **Grupos de paquetes**. *En vista de que debemos solo dejar los servicios que son necesarios, sólo se instalarán los paquetes siguientes:*
   - *El sistema X Window*
   - *El entorno de escritorio gráfico GNOME*
   - *Herramientas de configuración del servidor*
   - *El servidor Web*
   - *El servidor de archivos Windows (Samba)*
   - *Servidor de la base de datos SQL*
   - *Herramientas de administración*
   - *Herramientas del sistema*
   - *Soporte para la impresión*

6. **Disco de arranque**. *La creación de un disco de arranque es indispensable en el momento en el que se tenga que arrancar el sistema cuando éste presenta alguna falla. Con este modo de arranque se pueden resolver ciertos problemas, sin embargo, es necesario no dejar este disco de arranque a la mano porque puede ser utilizado por personas ajenas al sistema.*

5.4.2.1 Configuración de Apache

La aplicación del sistema multi-agente para la instalación remota de software contiene un repositorio en el cual se encuentra almacenado todo el software que el MAS puede instalar. El servidor Apache será el que funcionará como el repositorio que contiene todo el software necesario para las funciones de la GTI. Cuando un usuario ha solicitado la instalación de algún programa, el MAS busca en el servidor Apache el software solicitado y lo trasporta hasta la máquina del usuario para que el agente instalador *realice la instalación. Una vez realizada la instalación, el software se regresa nuevamente al servidor Apache.*

*Un servidor web responde a las peticiones que se le hacen utilizando el protocolo HTTP (Protocolo de Transferencia de Hipertexto), el cual permite, principalmente, que los clientes soliciten documentos al servidor. El protocolo HTTP también permite que los clientes envíen información de vuelta al servidor para operaciones interactivas. Apache es el servidor web (*httpd*) en la mayoría*

de las distribuciones de Linux, el cual se inicia automáticamente cuando se arranca la máquina y el demonio init *ejecuta un script* rc*, y ofrece muchos mecanismos de seguridad internos, incluyendo:*

- *Control de acceso de red basado en host vía* access.conf
- *Control sobre si los usuarios pueden y dónde pueden ejecutar* scripts *CGI (Common Gateway Interface o Interfaz de Pasarela Común)*
- *Control sobre si los usuarios locales pueden y cuándo pueden sobrescribir sus configuraciones*

Los principales aspectos de la configuración del servidor Apache que se tomaron en cuenta para el sistema multi-agente antes descrito están basados en una técnica que permite disminuir los cinco ataques básicos de todo sitio web:

- *Ataques XSS (Cross-site Scripting)*
- *Abusos de JavaScript y Java*
- *Manipulación de cookies*
- *Descubrimiento de contraseñas*
- *HTTP en texto plano y claro*

A continuación hablaremos de los aspectos para configurar de forma segura el servidor Apache:

1. *Se modificó la información de la cabecera con el fin de evitar que los usuarios, y más aún los intrusos maliciosos, consigan información útil sobre el sistema que ejecuta el servicio.*
2. *Para proteger los datos se utilizó la restricción mediante IP de los usuarios que realizan la petición.*
3. *Se utilizó la autenticación HTTP en el servidor mediante una ventana de diálogo para que el usuario introduzca su nombre de usuario y su contraseña.*
4. *Se cambió la ruta del directorio que contiene los documentos web y los enlaces simbólicos.*
5. *Se eliminó la opción de que se muestren los manuales de Apache desde la consola.*
6. *Se eliminó la página de bienvenida de Apache donde se muestra información de la distribución de Linux utilizada.*
7. *Se desactivaron todos los archivos SSI (Server Side Includes, Inclusiones en la parte del Servidor).*
8. *Se cambió el número de puerto por el trabajará Apache.*
9. *Se renombraron los archivos que almacenan las contraseñas y se modificó su ruta dentro del sistema de archivos.*

5.4.2.2 Configuración de MySQL Server

Debido a la función que desempeña la aplicación que se encuentra alojada en el servidor, el MAS que realiza la instalación remota de software, se hace indispensable el aseguramiento de la base de datos que permite la autenticación

de los usuarios. Originalmente la base de datos de dicha aplicación estaba implementada en Postgres, por lo que se tuvo que hacer una migración de la misma a MySQL Server con el fin de que fuera lo más compatible posible con Linux.

MySQL es un servidor SQL (Structured Query Language, Lenguaje de Consulta Estructurado) libre, robusto, completo y rápido que puede utilizarse para gestionar bases de datos pequeñas y grandes, ejecutar algunas consultas, y ver los resultados; el cual consiste de un demonio servidor llamado mysqld *y de diferentes librerías y programas cliente. MySQL permite almacenar y actualizar información fácilmente; por ejemplo, puede utilizarse para manipular información de los clientes de un sitio web o para almacenar archivos log, imágenes, etc. Además, MySQL cuenta con un sistema de autenticación basado en host muy flexible y seguro; asimismo, los passwords que verifican la identidad de los usuarios que se conectan al servidor MySQL son encriptados mediante un algoritmo.*

El servidor MySQL proporciona una interfaz que requiere que los usuarios se autentiquen para propósitos administrativos.

Los diferentes aspectos que se tomaron en cuenta para la segura configuración del servidor MySQL, donde se encuentra almacenada toda la información de los distintos perfiles de usuario de la GTI, son:

1. *Se protegió con contraseña la conexión hacia el servidor MySQL de cada usuario permitido, es decir, únicamente los administradores del sistema. Las contraseñas utilizadas para la conexión a MySQL son todas distintas entre sí; y al mismo tiempo, siempre serán diferentes a la de root, al del usuario de Linux y a la del servidor Apache.*
2. *Se restringió el acceso al servidor MySQL únicamente al administrador del sistema. Ningún otro usuario está permitido para acceder al servidor y hacer modificaciones a la base de datos.*
3. *Se configuró MySQL de forma que sólo se otorgaron los privilegios necesarios y limitados al administrador del sistema.*
4. *Los accesos a la base de datos serán tanto locales como remotos. Por esto, se configuró la conexión remota del host desde el cuál el administrador del sistema podrá analizar los reportes generados por el sistema multi-agente.*
5. *Se cambió el número de puerto por que funcionará MySQL.*
6. *Se renombraron los archivos que almacenan las contraseñas y se modificó su ruta dentro del sistema de archivos.*

5.4.2.3 Configuración de Internet

Como se mencionó anteriormente en la descripción del servicio, el servidor que contiene la aplicación para la instalación remota de software tiene una salida hacia Internet, la cual le permite realizar las actualizaciones automáticas del software que contiene el servidor Apache.

La implementación de la seguridad para la conexión a Internet del servidor incluye un dispositivo de control de acceso (firewall) entre Internet y la red interna del Instituto. Específicamente los puntos que se tomaron en cuenta para la configuración de Internet son:

1. *Se configuró el firewall de Linux (reglas de iptables) con el fin de restringir el acceso externo al servidor, únicamente a los host que pertenecen a la subred de la GTI.*
2. *Se cerraron todos los puertos de las aplicaciones que no se consideran necesarias y únicamente se dejaron abiertos los que utiliza el MAS.*
3. *Igualmente, se desactivaron todos los demonios de las aplicaciones innecesarias.*
4. *Se implementó el uso del programa Open Secure Shell (OpenSSH) con el fin de que la información que viaja desde y hacia Internet se mantenga encriptada.*
5. *Se configuraron todas las utilidades de Linux que permiten un registro completo de las actividades que realizan los usuarios (archivos log).*
6. *Se compiló el parche del kernel de Linux para implementar el detector de intrusiones LIDS.*

Servicio	***Descripción***
Servicios NetBIOS (puertos 135, 137, 138 y 139)	*Utilizado por los sistemas Windows para compartir archivos y comandos remotos*
RPC de Unix (puerto 111)	*Utilizado por los sistemas Unix para llamadas de procedimiento remoto*
NFS (puerto 2049)	*Utilizado para los servicios de archivos de red*
X (puertos 6000 hasta el 6100)	*Utilizados para sesiones remotas del sistema X Window*
Servicios "r" (rlogin puerto 513, rsh puerto 514, rexec puerto 512)	*Permite la interacción remota con un sistema sin una contraseña*
Telnet (puerto 23)	*No recomendado porque la contraseña y la identificación de usuario viajan sin protección en Internet y pueden ser capturadas. En su lugar se recomienda SSH.*
FTP (puertos 21 y 20)	*No recomendado por la misma razón que Telnet. En su lugar se recomienda SSH.*
TFTP (puerto 69)	*Semejante a FTP pero no requiere de identificaciones o contraseñas de usuario para tener acceso a los archivos*
NetMeeting	*Potencialmente peligroso pues requiere que se abran varios puertos altos a fin de funcionar apropiadamente. En lugar de abrir esos puertos, se debe utilizar un Proxy H.323*
Protocolos de Control Remoto	*Incluyen programas como PC Anywhere y VNC. Si estos protocolos son requeridos para permitir a usuarios remotos controlar sistemas internos, deben ser utilizados sobre una VPN*
SNMP (puerto 169)	*Puede utilizarse para la administración de la red interna, pero no debe emplearse desde un sitio remoto hacia los sistemas internos*

Tabla 5.2 Servicios que representan riesgos a la seguridad

La tabla anterior muestra los servicios más significativos que deben cerrarse porque representan una puerta abierta a intrusos, además, se consideran innecesarios para el buen funcionamiento de la aplicación de agentes. Sin embargo, únicamente se dejarán abiertos los puertos que realmente necesita la aplicación; uno para el sistema-multi-agente, otro para MySQL (la base de datos) y otro para el servidor Apache. Además, a todos los archivos que almacenan las contraseñas del sistema se les cambiaron el nombre y se les asignó otra ruta dentro del sistema de archivos.

5.5 Uso de Herramientas Complementarias

Una vez hecha la configuración correspondiente para cerrar todo agujero que el sistema operativo pueda tener, se sugiere el uso de diversas herramientas de distribución libre que complementan la seguridad de Linux, con el fin de garantizar que el servidor de aplicación estará protegido de amenazas externas. El uso de herramientas complementarias es importante para el control de riesgos en el servidor; sin embargo, dadas las características de hardware del servidor que lleva a cabo la tarea de instalar software vía remota, se considera que la implementación de herramientas adicionales provocaría un déficit en el rendimiento del sistema puesto que dichas herramientas también hacen uso de una buena parte de la memoria, necesaria para que la aplicación lleve a cabo su función. Desde mi punto de vista, es aconsejable que el uso de herramientas alternas se lleve a cabo por medio de una PC externa al sistema, con el fin de que no sean compartidos los recursos del servidor. Por otro lado, como el la red interna del Instituto se encuentra ya asegurada con diferentes herramientas (como firewalls, un detector de intrusos, etc.), no es razonable saturar más el tráfico de la misma red con demasiadas herramientas; por lo que las únicas herramientas que se considera implementar como complemento a la seguridad del servidor de aplicación que se ha descrito son:

1. *El auditor de contraseñas* **John the Ripper**, *el cual permitirá conocer la debilidad de las contraseñas que utilizará el o los administradores al acceder al servidor. Se recomienda que su ejecución se practique periódicamente (cada vez que se cambien las contraseñas) en una máquina distinta para evitar que interfiera con el sistema multi-agente.*

2. *El sniffer* **Ethereal**, *el cual permitirá contar con un análisis detallado del tráfico que genera el servidor. También es recomendable su utilización periódicamente (por lo menos una vez a la semana) en una máquina distinta con el fin de formar un patrón del tráfico que se genera y poder responder debidamente cuando ese patrón se altere.*

3. *El auditor de sistemas (scanner)* **Nessus**, *con el cuál se podrá hacer un análisis de las vulnerabilidades del sistema cada cierto tiempo (al menos una vez por semana), evitando con esto que se abran puertos que no deban estar abiertos, se corran aplicaciones que no deban hacer uso del servidor, etc.*

4. *El antivirus* **ServerProtect**, *cuya utilización es recomendable debido a que el principal problema que presenta el servidor es el ataque por diversos tipos de código malicioso o virus, a pesar de que esto representaría una inversión por el pago de la licencia correspondiente para su uso.*

5.6 Políticas y Procedimientos

Toda organización puede tener una arquitectura de seguridad y, sin embargo, no tener un marco formal ni documentos para implementarla. Esta carencia acarrea enormes consecuencias, tanto para la mitigación de los riesgos como para la percepción del mercado. Es por eso, que las organizaciones deben definir políticas y procedimientos específicos relacionados con la estrategia de seguridad, prestando atención a ciertos riesgos.

En esta parte, se dan a conocer las políticas y procedimientos planteados para implementar la estrategia de seguridad dentro de la Gerencia de Tecnología informática del IMP, como parte de la documentación que requiere la solución de seguridad propuesta. Las políticas definen cómo implantar la seguridad; esto incluye las configuraciones apropiadas en los sistemas de cómputo y redes, las medidas de seguridad física, los mecanismos adecuados para proteger la información y los sistemas, la forma en que los empleados deben realizar ciertas labores relacionadas con la seguridad (como la administración de los usuarios) y cómo se espera que se comporten cuando utilicen los sistemas de cómputo que pertenezcan a una organización. Pero lo más importante es, quizá, que las políticas también definen como deberían reaccionar las organizaciones cuando las cosas no marchan como se espera, es decir, que cuando ocurre un incidente de seguridad o falla en los sistemas, las políticas y los procedimientos de la organización definen lo que debe hacerse y cuáles son sus objetivos durante el incidente.

Una política de seguridad de servidores debe comprender lo siguiente:

- *Configuración del servicio*
- *Permisos y control de acceso a datos compartidos*
- *Permisos y control de acceso a datos privados*
- *Respaldos y procedimientos de restauración*
- *Respuesta a incidentes*

5.6.1 Políticas de Información

Las políticas de información definen qué información confidencial se encuentra dentro de la organización y cómo debe ser protegida.

1. **Identificación de la información confidencial**. *La información que se encuentra alojada en los servidores de la GTI se considera fundamental porque corresponde a datos que alimentan cada uno de los servicios que dicha gerencia ofrece a sus distintos usuarios.*
   - *La información que está almacenada en el servidor que realiza la instalación remota de software, de la Gerencia de Tecnología Informática, se considera absolutamente confidencial debido a que contiene todo el software que los empleados utilizan para realizar su trabajo y mucho de éste software no es de fuente libre, es decir, que el Instituto compra las licencias correspondientes para poder hacer uso de él. Por lo tanto, dicho software debe protegerse para que no sea utilizado deliberadamente por personas con intenciones que no sean afines a sus propósitos de trabajo.*
   - *Todo el personal de la Gerencia de Tecnología Informática tiene la libertad y el derecho de solicitar el servicio de instalación remota por medio del* agente asistente *que se encuentra instalado en su máquina de escritorio personal, pero únicamente puede instalar el software que requieran sus propias actividades de trabajo.*
   - *Es obligación del personal de la GTI no hacer uso indebido del software que el Instituto les proporciona para desarrollar sus actividades laborales.*

2. **Almacenamiento.** *Se define cómo debe ser marcada y almacenada la información para que no pueda ser alterada o destruida.*
   - *La información almacenada en el servidor que realiza la instalación remota de software se encontrará protegida mediante controles de acceso en los archivos (contraseñas) y selección de direcciones IP.*
   - *Los dispositivos de almacenamiento (disquetes, CD's, etc.) que contengan el software original que utiliza el servidor, junto con los contratos de licencia y los números de serie de cada uno deberán ser guardados bajo llave y controlados por el administrador del sistema.*

3. **Transmisión de información.** *La aplicación almacenada dentro del servidor utiliza un sistema de agentes que deben trasladarse hasta los sistemas cliente a los que da servicio. Así mismo, dicho servidor tendrá una salida hacia Internet con el fin de realizar las actualizaciones automáticas de software. Por lo tanto se utilizarán mecanismos de*

encriptación para la información que viaja por la red interna a fin de evitar intrusiones malintencionadas.

4. **Destrucción de la información.** *Cuando sea necesario que la información que se encuentra en el servidor sea modificada o se elimine parte de ella, es indispensable que se realicen los respaldos correspondientes. Si con el paso del tiempo dicha información requiere que se remplace por otra o se vuelve inservible, entonces se volverá indispensable que se elimine completamente de forma adecuada y que se destruyan también todos sus respaldos y copias con el fin de eliminar las evidencias que puedan comprometer las actividades que desarrolla el Instituto.*

5.6.2 Políticas de Seguridad

Las políticas de seguridad definen los requerimientos técnicos que los administradores de redes deben tomar en cuenta para configurar un sistema en el nivel de seguridad que se espera obtener del mismo. Este tipo de política debe definir los requerimientos a implantarse en cada sistema, sin embargo, no define configuraciones específicas para diferentes sistemas operativos. Esto más bien aparece en los procedimientos de configuración para cada sistema.

1. **Identificación y validación (validación)**. *Aquí se define como serán identificados los usuarios, es decir, se deberá adoptar un estándar para los ID de usuario, o bien señalar un procedimiento de administración del sistema que defina ese estándar. Algo más importante, debe definirse un mecanismo de autenticación para los administradores y para los usuarios del sistema.*
    - *Las contraseñas deberán crearse con un mínimo de 8 caracteres y un máximo de 15 y su contenido mezclará todo tipo de caracteres (números, mayúsculas, minúsculas y caracteres especiales). Así mismo, las contraseñas de los administradores tendrán una duración mínima de 15 días y máxima de un mes; por otro lado, las contraseñas de los usuarios del sistema tendrán una duración mínima de 6 meses y máxima de un año.*
    - *Los identificadores de usuario (userID) tendrán un estándar para todos los empleados del Instituto, los cuales serán dados de alta en el servidor de correo interno (Active Directory). El administrador del servidor de aplicación siempre accederá a él como usuario root para hacer las configuraciones y/o cambios correspondientes, pero también contará con su nombre de usuario común, antes mencionado.*
    - *Mientras que no se cuente con los mecanismos de autenticación antes mencionados, ningún usuario de la Gerencia de Tecnología*

Informática podrá conectarse al servidor de instalación remota de software.

2. **Control de acceso**. *Define los requerimientos estándar para el control de acceso a los archivos.*
   - » *El acceso directo al servidor de aplicación (instalación remota de software) queda restringido únicamente al administrador del mismo para que pueda realizar las modificaciones necesarias en su configuración y/o a los usuarios que él mismo designe en caso de que no se encuentre. Solamente un máximo de 3 personas podrán conocer la contraseña de acceso al servidor y ésta contraseña será cambiada por lo menos una vez al mes con el fin de evitar que personas hagan mal uso de ella.*
   - » *El acceso al servidor por parte de los clientes se realizará también por medio de un nombre de usuario/contraseña que identifique al usuario que quiere acceder al servicio en el momento que dicho usuario levante el* agente asistente *que se encuentra instalado en su máquina de escritorio.*
   - » *Cuando un usuario solicite instalar un software en su máquina, el sistema multi-agente verificará en su base de datos el perfil de dicho usuario para otorgarle los derechos de instalación. Cada empleado de la GTI tendrá su propio perfil de usuario y podrá instalar el software adecuado, basándose en las actividades que realiza.*
   - » *El administrador del sistema tendrá control absoluto sobre el sistema, haciendo uso del usuario* root *para crear nuevas cuentas de usuario y otorgar los permisos necesarios a los archivos para los diferentes usuarios de la GTI.*

3. **Auditoría**. *En este sección se definen los tipos de eventos que van a ser auditados en el servidor que realiza la instalación remota de software.*
   - » *Todas las conexiones o entradas al sistema (logins), las desconexiones o salidas del sistema (logouts) y los accesos remotos con éxito o sin éxito*
   - » *Accesos fallidos a los archivos u objetos del sistema*
   - » *Acciones privilegiadas (realizadas por los administradores, tanto con éxito como sin éxito)*
   - » *Eventos del sistema (como cuando se apaga y se reinicia). Cada evento deberá capturar también el ID del usuario, fecha y hora, acción realizada y el éxito o fracaso del evento*

4. **Conectividad de redes**. *Para cada tipo de conexión dentro de la red de la organización, se especifican las reglas para la conectividad de la red y los mecanismos de protección que serán empleados en la misma.*

- *El servidor que realiza la instalación remota de software de la Gerencia de Tecnología Informática se encuentra conectado a la red interna del Instituto y a su vez se encuentra conectado hacia Internet para realizar las actualizaciones automáticas de software.*
- *El servidor se encuentra protegido por medio de mecanismos de autenticación para el acceso a su información, pero esta protegido también por medio de firewalls conectados a la red del Instituto.*

5. **Excepciones**. *A pesar de las buenas intenciones del personal y de los administradores del sistema, habrá ocasiones en que los sistemas que deben ser utilizados en la producción no satisfagan los requerimientos de seguridad definidos en la política de seguridad, dependiendo de los objetivos específicos que se persigan. En este caso, los sistemas en cuestión estarán obligados a cumplir algunas necesidades del negocio, y éstas son más importantes que lograr que los sistemas cumplan con la política de seguridad establecida. Cuando esto ocurra, se deberá hacer un análisis de los riesgos que esto conlleva, midiendo el impacto en la organización, y un plan de contingencias detallado. Para cada situación específica, el administrador del proyecto deberá llenar una forma de excepción con la información siguiente:*
   - *El servidor que se exceptuará de la seguridad*
   - *La sección de la política de seguridad que no se cumplirá*
   - *Las ramificaciones hacia la organización (el riesgo incrementado)*
   - *Los pasos que se están tomando para reducir o manejar el riesgo*
   - *El plan para que el sistema cumpla con la política de seguridad*

5.6.3 Políticas de Uso de las Computadoras

Las políticas de uso de las computadoras son aquellas que definen quién puede utilizar los sistemas de cómputo y cómo deben ser utilizados.

1. **Propiedad de las computadoras**. *Todas las computadoras y/o equipo de cómputo, incluyendo los equipos que funcionan como servidores son propiedad del Instituto Mexicano del Petróleo y son asignadas a los diferentes empleados del mismo de acuerdo con sus labores dentro de la organización y por ningún motivo deben salir de las instalaciones del Instituto sin el permiso escrito de una autoridad asignada.*
2. **Propiedad de la información**. *Toda la información almacenada, utilizada o procesada en los equipos de cómputo pertenecientes al Instituto, es propiedad del mismo; sin embargo, por ningún motivo el administrador puede utilizar las computadoras que fungen como servidores para guardar información personal, ya que esto repercutiría en el rendimiento del servidor al dar servicio a sus clientes.*

3. **Uso de las computadoras.** *Dado que el administrador es la única persona que tiene control absoluto de los servidores, su uso queda bajo su responsabilidad y es obligatorio que su uso quede en términos del trabajo que esté desarrollando, es decir, para los propósitos del Instituto, ya que de no ser así, dicho administrador será el responsable de los daños que le ocurran al equipo y al mal uso de éste. Queda prohibido utilizar los servidores como un medio de diversión o distracción haciendo uso de juegos, chats, servicios de mensajería instantánea, etc., así como que se instale software no autorizado en el servidor que no sea para los fines del servicio que presta. Por otro lado,*
4. **Expectativas de privacidad.** *El empleado debe tener conocimiento pleno de que no puede esperar una plena privacidad respecto a cualquier información almacenada, enviada o recibida en o desde cualquier equipo del Instituto, ya que toda la información, incluyendo el correo electrónico, puede ser examinada y analizada por los administradores con el propósito de dar seguimiento a las actividades realizadas por cada usuario, incluyendo los sitios Web que visitan.*

5.6.4 Políticas del Uso de Internet

Se plantea una política aparte del uso de las computadoras debida a la naturaleza específica del uso de Internet.

1. *El servidor que presta el servicio de instalación remota de software debe tener una conexión hacia Internet que le permita realizar las actualizaciones automáticas del software que contiene en su base de datos. Por esto, la conectividad a Internet queda limitada únicamente para que dicho servidor pueda hacer las actualizaciones de los diferentes programas que instala vía remota, en virtud de que todo software tiene errores que ponen en riesgo la seguridad del sistema y día con día aparecen las correcciones a esos errores, las cuales son publicadas en Internet.*

2. *El uso del Internet queda restringido en los siguientes casos:*
   - *Visitas a sitios Web que no estén relacionados con el servicio que se presta*
   - *Programas para intercambio de mensajes instantáneos*
   - *Descarga de archivos o software protegido por derecho de autor*
   - *Comercio o intercambio de archivos de música*

5.6.5 Política de Respaldos

Aquí se define de qué forma se realizarán los respaldos del sistema y con qué frecuencia.

1. **Frecuencia de los respaldos**. *Por conveniencia, se realizarán respaldos completos de los servidores de la GTI un día a la semana (específicamente los viernes), con respaldos incrementales diarios que permitan respaldar los archivos que han cambiado desde el último respaldo. El respaldo incremental permite que los respaldos semanales se efectúen más rápido y ocupen una cantidad menor de espacio en cinta.*

2. **Almacenamiento de los respaldos**. *Debido a la importancia que implica guardar los medios utilizados para los respaldos en un lugar seguro, pero que al mismo tiempo sea accesible cuando sea necesario restaurar la información, los respaldos se almacenarán de la siguiente manera:*
   - *Las cintas de los respaldos serán almacenadas en estantes o archivos bajo llave, la cual tendrá únicamente el administrador, sin ninguna etiqueta que las identifique.*
   - *Se llevará un control escrito de los respaldos que se realicen con los datos de la fecha que se realizó el respaldo, el nombre de la persona que lo hizo y los datos que fueron respaldados; dicho control se guardará en un lugar diferente de donde se encuentren las cintas de respaldos, igualmente bajo llave y bajo control del administrador.*
   - *Se realizará una rotación de cintas cada determinado tiempo (mínimo de una semana y máximo de un mes) con el fin de que las cintas con respaldos más recientes permanezcan un tiempo y las más antiguas sean reutilizadas para los siguientes respaldos.*

3. **Información que será respaldada**. *No toda la información ni todos los archivos de un sistema de cómputo requieren de un respaldo diario; como por ejemplo los archivos binarios y los archivos del sistema, ya que no cambian. Por lo tanto, únicamente los archivos de datos, especialmente los que se modifican a diario (los reportes que emite el sistema multi-agente de las acciones que realizó), son los que serán respaldados tal y como se mencionó en el punto anterior.*

5.6.6 Procedimiento de Administración del Sistema

Este procedimiento define la manera en la que los departamentos de seguridad y administración de sistemas trabajarán en conjunto para asegurar los sistemas de cómputo del Instituto. Se advierte que este procedimiento forma

parte de la política del uso de computadoras y debería ser un reflejo de la forma en que el Instituto espera que se administren los sistemas.

1. **Actualizaciones de software**. *El administrador informático tiene la obligación y la responsabilidad de verificar la existencia de nuevas correcciones (parches) o actualizaciones de los diferentes programas de software que se encuentren instalados en los servidores de la GTI, en especial del sistema operativo que soporta cada uno de los servicios que se ofrecen en dicha gerencia, con una frecuencia mínima de una semana y máxima de un mes. Asimismo, estará encargado de hacer las pruebas correspondientes a dichas correcciones antes de ser instaladas con el fin de evitar fallas.*

2. **Rastreos de vulnerabilidad**. *Las exploraciones en busca de sistemas vulnerables realizadas por el personal de seguridad, serán enviadas al administrador para que éste realice los ajustes correspondientes haciendo uso de herramientas comerciales y/o gratuitas de escaneo. La frecuencia de dichas exploraciones será de una semana como mínimo y de un mes como máximo, debido a que esto va muy de la mano con las actualizaciones del sistema.*

3. **Revisiones de la política**. *Las políticas de seguridad del Instituto especificarán los requerimientos de seguridad para cada sistema dentro de la Gerencia de Tecnología Informática.*
   - *La revisión del contenido y del cumplimiento de las políticas de seguridad se llevará a cabo cada fin de año (por parte del personal encargado de la seguridad informática dentro de la gerencia), con el objetivo de comparar los resultados con los objetivos planteados al inicio del mismo. Dicha revisión deberá incluir un análisis detallado de los procesos y de sus fallas, si las hubiere.*
   - *El incumplimiento de las políticas por parte del administrador o del personal encargado de los distintos servidores de la GTI, será sancionado de distintas formas según sea la gravedad del incumplimiento, conforme lo establecido con las leyes internas del Instituto.*
   - *Dentro del Instituto se realizará una auditoría informática cada determinado tiempo, el cual será designado por las autoridades del Instituto dependiendo de los resultados obtenidos en los informes anuales que presenta el personal de seguridad informática de cada gerencia del Instituto.*

4. **Revisiones de las bitácoras**. *Las bitácoras de diversos servidores de la GTI deberán ser revisadas de manera regular por parte de la gerencia con el fin de conocer si se cumplió con las actividades programadas.*

- *Algunas de las aplicaciones que tienen los servidores de la GTI deben realizar ciertas actividades de forma periódica, es decir cada cierto tiempo, por lo que se deberá llevar un registro de las actividades que se lleven a cabo, únicamente por llevar un control.*
- *Ciertas actividades que se llevan a cabo dentro de los servidores también se consideran como tareas programadas y deben documentarse; por ejemplo, el hacer respaldos, dar mantenimiento a las bases de datos, la revisión de los archivos log, etc. Este tipo de actividades deben llevar un registro completo que contenga el nombre de la persona que lo realizó, la fecha, el estado en que se encuentra el servidor, etc., como parte de las medidas preventivas.*

5. **Monitoreo regular**. *Como en toda organización, la Gerencia de Tecnología Informática del IMP tendrá un procedimiento que documente cuando se presente un monitoreo o seguimiento de tráfico de la red.*
   - *El monitoreo de la red será constante durante los periodos activos del Instituto, es decir que se realizará un monitoreo diario de todo el tráfico de red que se genere.*
   - *De igual forma, dicho monitoreo deberá ser impreso diariamente con el fin de evitar que sea alterado. El informe generado será revisado cuidadosamente por el administrador en el caso de que existiera algún indicio de mal comportamiento en el tráfico de la red (como lentitud, solicitudes de accesos desconocidos, etc).*

5.6.7 Procedimiento de Administración de Usuarios

El procedimiento de administración de usuarios es el que más se pasan por alto las organizaciones a pesar del gran riesgo que éstos suponen. Los mecanismos de seguridad usados para proteger los sistemas de los individuos no autorizados son muy útiles, pero pueden convertirse en algo completamente inútil si los usuarios de los sistemas de cómputo no son administrados de manera apropiada.

1. **Nuevos empleados.** *El departamento de seguridad deberá trabajar conjuntamente con el departamento de recursos humanos y con los administradores del sistema.*
   - *Se elaborará un perfil de usuario a cada nuevo empleado de la GTI con el fin de evaluar qué recursos le son necesarios para realizar su trabajo y los privilegios de acceso a los distintos sistemas que se le otorgarán.*
   - *La solicitud de recursos de cómputo será generada por el supervisor y/o jefe inmediato del nuevo empleado y será también firmada por él.*

2. **Empleados transferidos**. *Se debe revisar el acceso a las computadoras de los empleados que sean trasferidos por alguna razón a alguna parte del Instituto.*
   - » *Tanto el antiguo como el nuevo supervisor (jefe) del empleado transferido deben identificar cuáles serán los nuevos recursos que el empleado necesitará para desempeñar su trabajo, para que éstos les sean asignados. Se creará un nuevo perfil de usuario.*
   - » *El administrador de los servidores hará los cambios pertinentes para que el empleado transferido sólo tenga acceso a los servicios y recursos que necesite para desempeñar sus labores.*
3. **Revocación de empleados**. *En el procedimiento de eliminación de los usuarios que ya no trabajan para la gerencia deben participar conjuntamente el departamento de recursos humanos y la administración de sistemas.*
   - » *Una vez que el departamento de recursos humanos identifica que un empleado dejará de trabajar en el Instituto, el administrador de los servidores deberá ser avisado de manera anticipada, de modo que las cuentas del empleado queden deshabilitadas el último día de empleo del trabajador.*
   - » *Cuando existan empleados temporales y consultores que tengan cuentas en los sistemas se mantendrá un control estricto de las actividades que desempeñan estas personas dentro de la gerencia y se tomarán las mismas medidas mencionadas en el punto anterior.*
   - » *En el caso de la revocación de los administradores de los servidores, todas las contraseñas ocupadas por ellos dentro de la gerencia deberán ser cambiadas y todas sus cuentas de usuario serán eliminadas el mismo día que éstos abandonen la organización.*

5.6.8 Procedimiento de Respuesta a Incidentes

El siguiente procedimiento define la manera en la que el Instituto reaccionará cuando se presente un incidente que afecte la seguridad de la información. Dado que existen diversos tipos de incidentes y todos ellos afectan en diferentes grados, se definirá quién tiene la autoridad y cómo debe proceder, pero no necesariamente qué debe hacerse.

1. **Objetivos del manejo de los incidentes.** *Se deben especificar los objetivos de la gerencia cuando se maneje un incidente. Algunos objetivos incluyen:*
   - » *La GTI es responsable de los equipos de cómputo a su cargo, por lo cualquier extravío, robo, o daño a alguno de sus equipos queda bajo la total responsabilidad del personal de la gerencia.*

- *La información almacenada en los distintos servidores de la GTI es responsabilidad de los administradores de los mismos por lo que serán dichos administradores los que deben garantizar que no exista robo, falsificación, extravío, pérdidas o alteraciones de la misma; ya que dicha información no solo le concierne a dicha gerencia, sino que es parte también de las operaciones mismas del Instituto.*
- *Cuando ocurra un incidente no grave con algún servidor de la GTI, el administrador de dicho servidor tendrá la responsabilidad de solucionar el incidente y elaborar un reporte de lo ocurrido, mismo que presentará al gerente.*
- *Cuando ocurra un incidente grave con algún servidor de la GTI, éste deberá ser reportado inmediatamente al gerente para que conjuntamente se elabore un plan que permita reanudar las operaciones lo antes posible.*
- *La misma Gerencia de Tecnología Informática y el administrador de los servidores deberán investigar qué provocó el incidente para poder corregirlo de forma automática, y en caso de encontrar un culpable éste será sancionado por la misma gerencia, de acuerdo con los lineamientos del propio Instituto.*
- *El administrador de los diversos servidores de la GTI tiene la responsabilidad de implantar los controles necesarios para prevenir cualquier tipo de incidente que pueda afectar la seguridad de los servicios que se prestan.*
- *Una vez ocurrido un incidente grave la GTI implantará los controles necesarios para reducir su impacto y no perjudicar la imagen de la gerencia hacia otras áreas o personas externas.*

2. **Identificación de eventos.** *La identificación de un incidente es una parte muy importante, algunos eventos son obvios, mientras que otros pueden ser un poco difíciles de detectar, como las intrusiones o errores de usuario. Es por eso que, antes de que se declare un incidente, el departamento de seguridad deberá encargarse de hacer una investigación a fondo de lo que suceda, mientras que los administradores del sistema, determinarán si en verdad ocurrió un incidente.*

3. **Control de la información.** *A medida que se desarrolla un incidente, la GTI deberá controlar la información que se difunda de éste para evitar que sea alterada o mal interpretada. Además, la información que se revele depende del efecto que tendrá el incidente sobre el Instituto y su base de clientes.*

4. **Respuesta.** *La forma en que se responde a un incidente tiene que ver directamente con los objetivos planteados para el manejo de los*

incidentes (punto número 1). Por ejemplo, si el objetivo es la protección de los sistemas, puede ser apropiado eliminar los sistemas de la red y hacer las reparaciones necesarias. En otros casos, puede ser más importante conservar la conexión a la red para mantener el servicio o para dejar que el intruso regrese de manera que puede obtenerse más información y éste pueda ser identificado. De cualquier forma, la respuesta que se de al incidente será determinada por la GTI.

5. **Autoridad.** *Las personas con autoridad para emprender alguna acción de respuesta a incidentes serán determinadas por el gerente de la GTI después de analizar con detenimiento el incidente causado.*

6. **Documentación.** *Se debe definir de qué manera se van a documentar las acciones para la respuesta a incidentes.*
   - *El equipo de respuesta a incidentes debe llevar un control escrito de todas las acciones realizadas en el seguimiento de un incidente dado: qué equipo falló, a qué se debió la falla, cómo afectó dicha falla a la operación y/o al rendimiento, qué medidas se tomaron para solucionar la falla, quién las llevo a cabo, etc.*
   - *En caso de tomar acción judicial contra algún responsable debido al incidente cometido, se hará uso de la documentación elaborada en el punto anterior como parte de las evidencias.*

7. **Prueba del procedimiento.** *La respuesta a los incidentes requiere de práctica, por lo que una vez que se establezca una respuesta a un incidente dado, se deberán realizar varios ensayos.*
   - *Se identificará alguna situación y el equipo de respuesta platicará para determinar las acciones que se llevarán a cabo.*
   - *Todos los miembros del equipo y los empleados, sin distinción, deberán seguir el procedimiento en tiempo y forma.*
   - *Cada vez que sea posible se simularán ataques en contra de los sistemas de la gerencia y se dará respuesta a ellos, con el fin de descubrir las deficiencias obvias en el procedimiento que deban ser corregidas. Tales pruebas se harán sin previo aviso a los usuarios.*

5.6.9 Administración de la Configuración

La administración de la configuración define los pasos que se llevarán a cabo para modificar el estado de los sistemas de cómputo, dispositivos de red y sistemas de software del Instituto. El propósito de ésta administración es identificar los cambios apropiados de modo que no se vean como incidentes y, de este modo, la nueva configuración pueda ser examinada desde una perspectiva de la seguridad.

1. **Estado inicial del sistema**. *Cuando un nuevo sistema entra en operación, su estado debe quedar bien documentado. Dicha documentación debe incluir como mínimo:*
   - *El sistema operativo y su versión*
   - *Nivel de actualizaciones y/o correcciones*
   - *Aplicaciones que se ejecutan y sus versiones*
   - *Configuraciones iniciales para dispositivos, sistemas de software y aplicaciones*

2. **Control de cambios**. *Cuando se efectúe un cambio a un sistema, debe ejecutarse un control de cambios que permita mantener el respaldo de la antigua configuración y la prueba del cambio propuesto antes de su implementación.*
   - *Los cambios que se realicen en los equipos de cómputo deberán ser solicitados al administrador mediante un oficio que explique las razones que justifiquen dichos cambios. El oficio deberá ir firmado por el jefe inmediato del empleado que lo solicitó.*
   - *Cualquier cambio en la configuración que se efectúe a un sistema de cómputo deberá hacerse siempre con un respaldo previo de la configuración actual, con el fin de evitar pérdidas de información.*
   - *Una vez hechos los cambios en la configuración de los sistemas, deberán hacerse las actualizaciones correspondientes al sistema.*

Como parte de las políticas internas del propio Instituto y de la misma estrategia de seguridad, es imposible mostrar el código de la configuración del servidor, ya que, de lo contrario, se pondría al descubierto el panorama sobre el que funciona y con esto se estaría incurriendo en una falta en contra de la seguridad informática.

"Ninguna solución de seguridad por sí sola ha demostrado ser absolutamente segura. Y por muchas razones, ninguna lo será. Todas las soluciones son relativas."

"La seguridad no es nunca más fuerte que el eslabón más débil".

Conclusiones

Cuando se pretende implementar una estrategia de seguridad sobre algunas aplicaciones que son críticas dentro de una organización siempre se encuentran ciertas limitantes que hacen que esta tarea sea algo complicada, ya que se debe comenzar con un análisis exhaustivo de los riesgos que presentan dichas aplicaciones así como de la conveniencia de implantar ciertos controles de seguridad o no. A pesar de que la aplicación sobre la que se trabajó para el desarrollo de este trabajo no se considera crítica por el tipo de servicio que presta, si es importante tomar en cuenta su seguridad porque representa un punto de entrada hacia la red interna del IMP y una fuente de contagio por los diversos virus que suelen introducirse a través de Internet. Además, si se hiciera mal uso del software comercial que contiene la aplicación, se estaría incurriendo en un delito que atenta contra los derechos de autor.

Por otro lado, es evidente que cuando se decide implementar un nivel de seguridad informática adecuado, se tenga la confianza de que haciendo una gran inversión se puede estar totalmente tranquilo únicamente porque la inversión lo respalda; pero, en general esto no es completamente cierto. Aunque parezca que el software y las herramientas libres y de código abierto no son lo suficientemente buenas para lograr un nivel de seguridad óptimo, la realidad es que éste no depende directamente de que el software sea libre o no. Un nivel de seguridad adecuado comienza evaluando las diversas plataformas de sistemas operativos que existen para determinar cuál es la que más se adapta a las necesidades que se requieren cubrir y realizando una adecuada configuración del propio sistema operativo que dará soporte a las diversas aplicaciones.

La finalidad de este trabajo se centra en el propósito de implementar la estrategia de seguridad desarrollada en cada uno de los servidores que conforman la Gerencia de Tecnología Informática del Instituto Mexicano del Petróleo para que su principal plataforma de trabajo sea Linux en un futuro no muy lejano. Las razones para esto son muchas; la primera es, que siendo Linux un sistema operativo de distribución libre, se reducirían considerablemente los gastos por el pago de licencias que permiten su utilización; la segunda es, que

Linux es considerado un sistema operativo con un alto nivel de seguridad con lo cual se puede tener la certeza de que el propio sistema operativo protegerá de manera más eficaz las aplicaciones que se tengan bajo su soporte de forma personalizada; y la tercera es, que Linux cuenta con una estabilidad muy superior a la que tiene la plataforma Microsoft, por lo que se evitan muchas de las problemáticas que obligan el reinicio del sistema de manera frecuente. Además, el desarrollo de Linux es constante por lo que diariamente aparecen mejoras para esta plataforma, las cuales le brindan un gran soporte a nivel mundial.

Por el momento, Red Hat Linux fue implementado únicamente en el servidor de aplicación para instalación remota de software y al menos se han registrado resultados significativos en contra de los ataques por virus y todo tipo de códigos maliciosos, además de un rendimiento óptimo. Sin embargo, se pretende realizar, cada cierto tiempo, pequeñas auditorías que permitan conocer el estado del servidor y la funcionalidad de la estrategia implementada. Por otro lado, una estrategia de seguridad no sería suficientemente funcional si no se capacita al personal para respetar las políticas establecidas y se crea consciencia de los riesgos que implica no hacerlo. Por esta razón, la última fase de la estrategia corresponde a la concientización del personal y en éste ámbito, la Gerencia de Tecnología Informática y el mismo Instituto Mexicano del Petróleo tienen un largo camino por comenzar a recorrer, ya que educar a los usuarios para que se enfrenten a situaciones de riesgo para la seguridad informática no es una tarea fácil, por el contrario, lleva mucho tiempo.

APÉNDICE A
Instalación de Linux

Existen varias razones por las que es necesario un procedimiento de instalación de Linux: porque la mayoría de los manuales de instalación no se centra en la seguridad, pero sobre todo porque precisamente la seguridad que brinda cualquier sistema operativo, y especialmente Linux, comienza en la instalación, o incluso antes.

Todo sistema operativo requiere un conjunto de utilerías y herramientas para llevar a cabo las tareas de instalación y configuración; a este conjunto se le llama distribución *la cual facilita al usuario el trabajo con el sistema. Actualmente son cuatro las distribuciones de Linux más difundidas en el mundo: Slackware, Debian, Suse y Red Hat. La distribución a la que haremos referencia en esta tesis es Red Hat debido principalmente a la popularidad que se le ha dado en entornos de trabajo.*
La ventaja que presenta Red Hat frente a las otras distribuciones de Linux radica en su sistema de instalación, ya que permite utilizar una interfaz completamente gráfica o una en modo texto, lo que facilita demasiado la tarea de instalación y configuración a los usuarios.
Como Linux es un software completamente gratuito y libre, la mayoría de los usuarios emplea Internet para conseguir una versión de Linux, lo cual no es muy recomendable porque el tiempo que se necesita para su descarga es muy grande y se corre el riesgo de contraer un virus por este medio. La mejor opción, desde un punto de vista personal, para adquirir Linux es la compra de revistas especializadas en el tema, las cuales son acompañadas en muchas ocasiones de uno o varios CDs con software catalogado como freeware, *y que pueden incluso contener más de una distribución de Linux.*

Los requerimientos básicos de hardware para la instalación de Linux son:

1. *Procesador 386 o superior, o uno de los clones de éstos como Cyrix, AMD, TI o IBM; con una velocidad de procesamiento de 66 hasta más allá de los 500 MHz.*

2. *Linux acepta discos duros IDE y SCSI de forma indistinta y el espacio en disco debe ser como mínimo de 900 MB, dependiendo del tipo de instalación que se desee realizar.*

3. *La memoria RAM puede ser mínimo de 32 Mbytes aunque lo recomendable son 64 MB, incluso para un entorno gráfico. La cantidad de memoria dependerá del entorno bajo el cual se desee operar Linux (texto o gráfico) así como del desarrollo de programas que vaya a realizar una vez instalado.*

4. *Es necesario que se cuente con una unidad de disquete de 3½ y de 1.44 Mbytes.*

5. *Para poder instalar Linux desde un CD es necesario que la computadora cuente con una unidad lectora de CDs de tipo IDE o SCSI o con una norma propia, pues Linux reconoce casi todos los modelos de unidades de CD-ROM. La velocidad mínima de la unidad debe ser 2X y la ideal de 4X.*

6. *Linux soporta la mayoría de tarjetas gráficas existentes en el mercado, aunque es recomendable usar una tarjeta de video VGA para un adecuado funcionamiento en modo gráfico.*

Proceso de Instalación

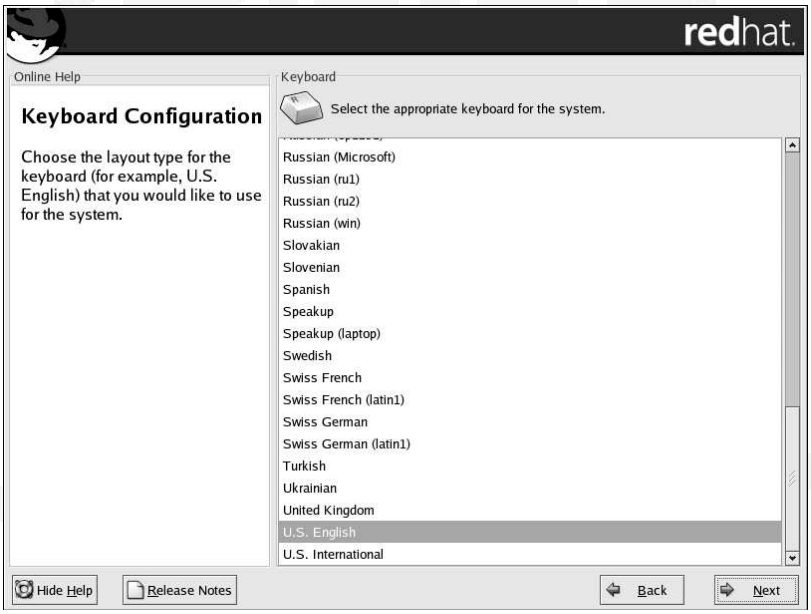
El proceso de instalación que se mostrará constituye una parte fundamental para la implementación de la estrategia que se desarrollará a lo largo de la tesis. Se pretende configurar un servidor Linux con la distribución Red Hat 9.0 y la versión 2.4.2 del kernel.
Una instalación para un servidor requiere 850 MB para una instalación mínima sin X (el entorno grafico), por lo menos 1.5 GB de espacio libre en disco si se quiere instalar todo el grupo de paquetes de X, y por lo menos 5 GB para una instalación completa incluyendo los entornos GNOME Y KDE. Es importante que antes de comenzar la instalación se conozcan las características de los componentes de la máquina, es decir todo el hardware con que cuenta la máquina.

1. *Insertar el primer CD-ROM de Linux Red Hat 9.0, con el cual bootea la máquina. Cuando se arranca desde este dispositivo se muestra una*

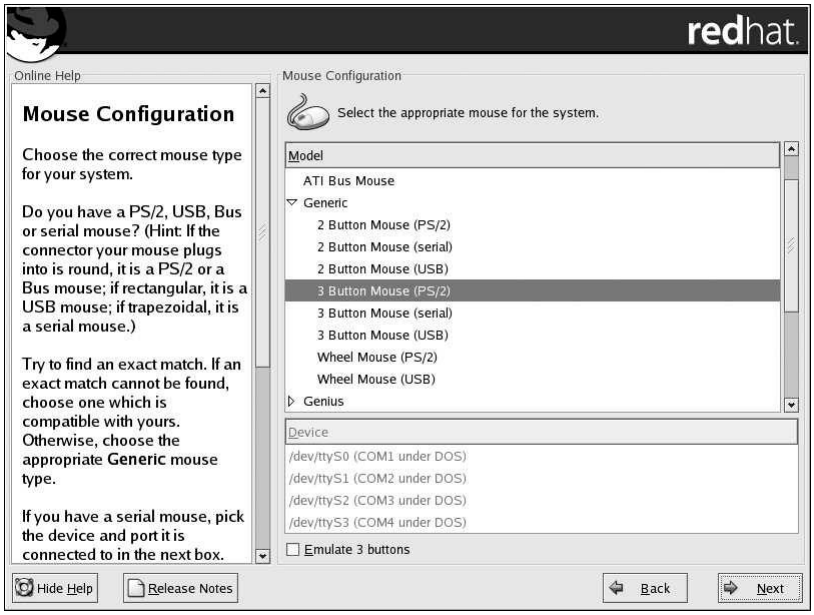
ventana para elegir si la instalación será en modo texto o basándose en ventanas (gráfico).

2. *En seguida se mostrará la pantalla de bienvenida y luego se pide una verificación del CD para comprobar que no tiene ninguna falla.*
3. *Aparece la pantalla para* **seleccionar el idioma** *con el cual se realizará la instalación.*

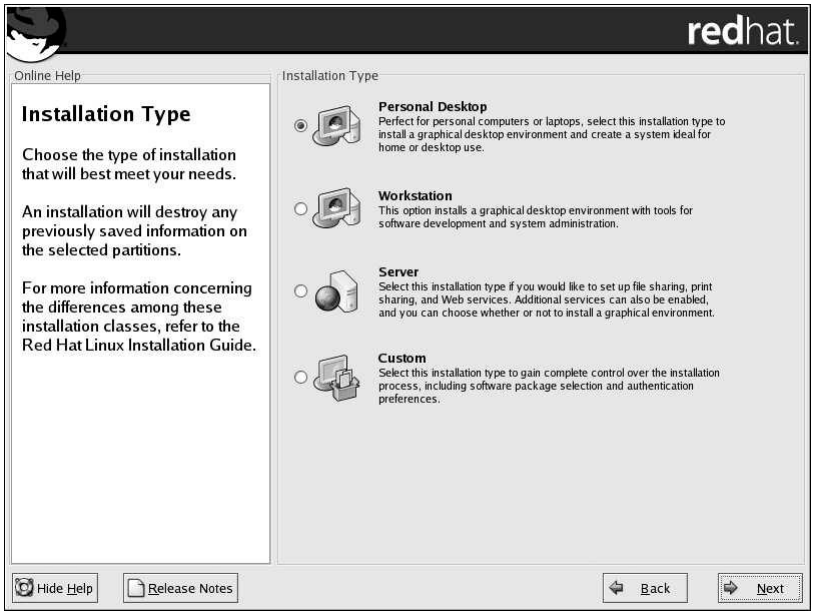
4. **Configuración del teclado**, *se debe elegir el idioma que utilizará el teclado, y que se adapte mejor al sistema.*



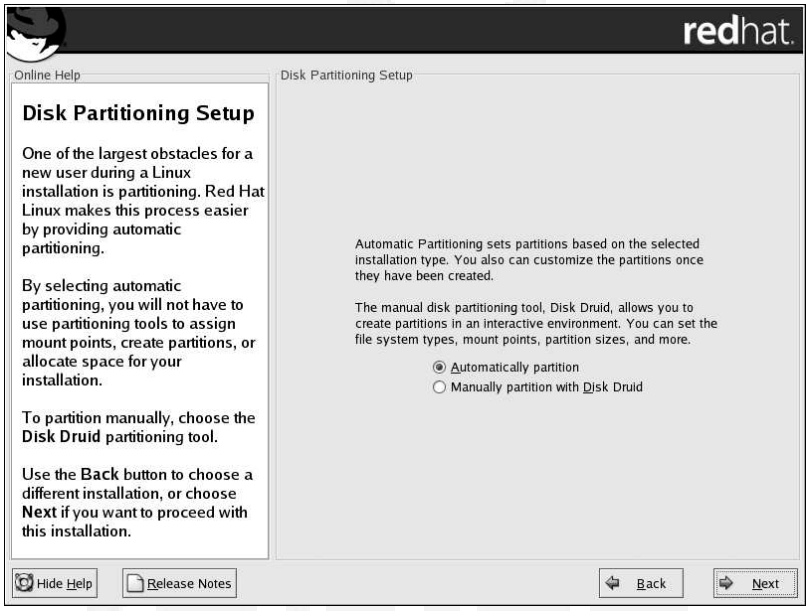
5. **Configuración del ratón** *(Mouse), elegir el que coincida con las características del dispositivo con el que se cuenta, dependiendo de la entrada que tenga, ya sea serial, PS/2, USB o AT; y del número de botones con los que cuenta.*



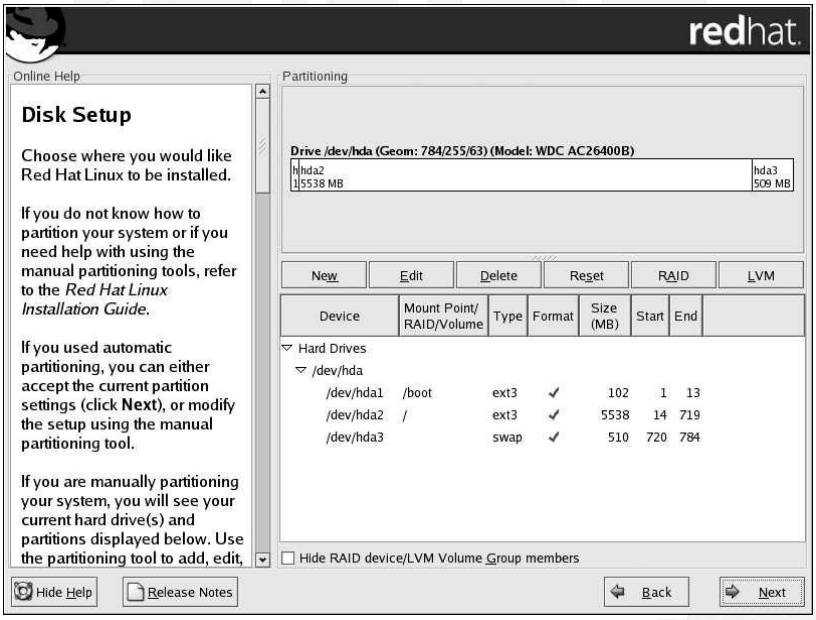
6. *A continuación se elige el* **tipo de instalación** *que se llevará a cabo en la máquina, el cual puede ser para un escritorio personal, para una estación de trabajo, para un servidor o personalizada. En nuestro caso en particular, elegimos la de tipo Servidor.*



7. *En seguida se configura la* **partición del disco duro**, *la cual realizaremos manualmente con Disk Druid para personalizar y optimizar el espacio del disco duro.*

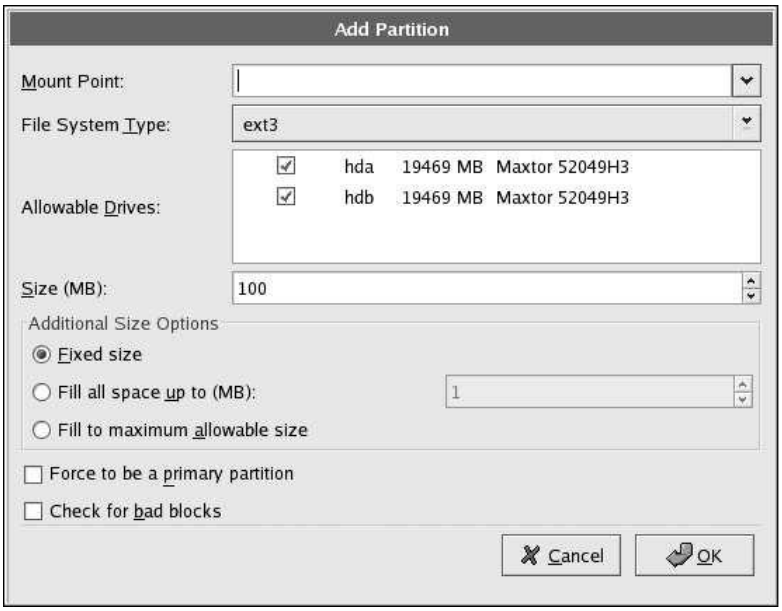


7.1 Al hacer las particiones con **Disk Druid**, *aparece la siguiente ventana, donde se muestran las particiones existentes.*



7.2 Cuando se tiene un disco duro que ya se encuentra particionado, lo primero que debe hacerse es eliminar todas las particiones eligiendo una por una y dando clic en eliminar. Después se procede a crear las nuevas particiones, pulsando en nueva, con lo cual se muestra la siguiente

ventana donde se debe especificar el punto de montaje y el tamaño de la partición que se desea crear.



7.3 La primera partición que se realiza es la **swap**, *la cual funciona como una memoria virtual cuando hay una carga muy grande de procesos. Este espacio del disco duro guarda por tiempo limitado los procesos que están compartiendo el tiempo del procesador. No hay punto de montaje para esta partición, sólo se especifica que el tipo de sistema de archivos es* **swap** *y su tamaño en MB, el cual debe ser como mínimo el doble de la memoria RAM con que cuenta el equipo. Particularmente será de 1024 MB, es decir, 1 GB.*

7.4 La siguiente partición que se realiza es la que almacena el kernel (núcleo) de Linux, llamada comúnmente **boot**. *Por lo tanto, su punto de montaje será /***boot**, *el tipo de sistema de archivos que utiliza es* **ext3** *y su tamaño será de 200 MB.*

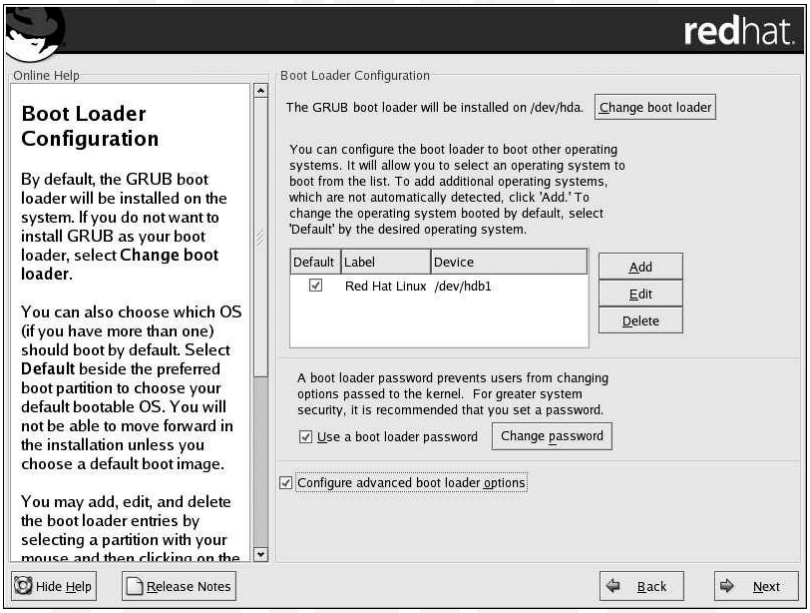
*7.5 Realizaremos una partición llamada /***repositorio** *que contendrá el software que el sistema multi-agente puede instalar en los diversos equipos. Su tamaño es de 10 GB y su sistema de archivos* **ext3**.

*7.6 Una partición más llamada /***reportes** *es utilizada para almacenar los reportes que genera el sistema multi-agente cada vez que realiza un servicio. Su tamaño será de 5 GB y el tipo de sistema de archivos que utiliza es* **ext3**.

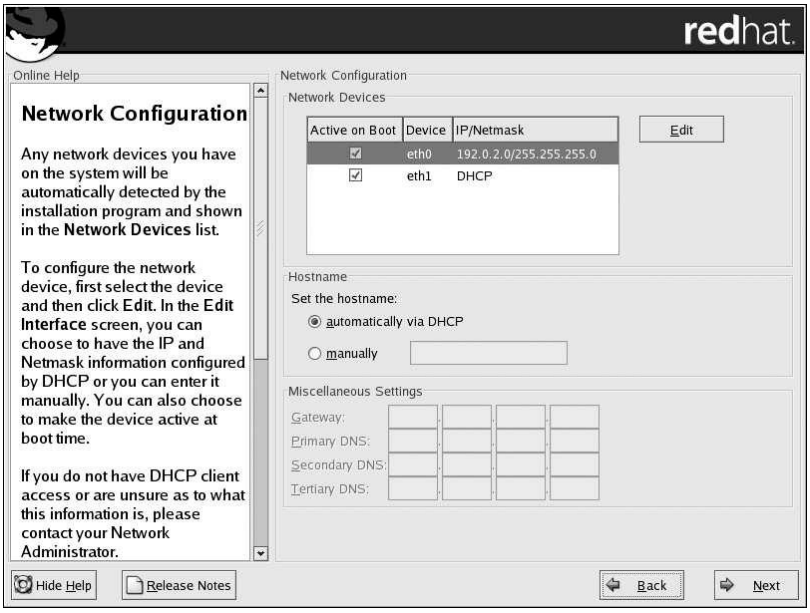
7.7 Finalmente dejamos el espacio restante del disco duro para la partición que contendrá la **raíz** *de Linux, es decir, todos los archivos del*

sistema. Su punto de montaje es / y su tipo de sistema de archivos es **ext3**.

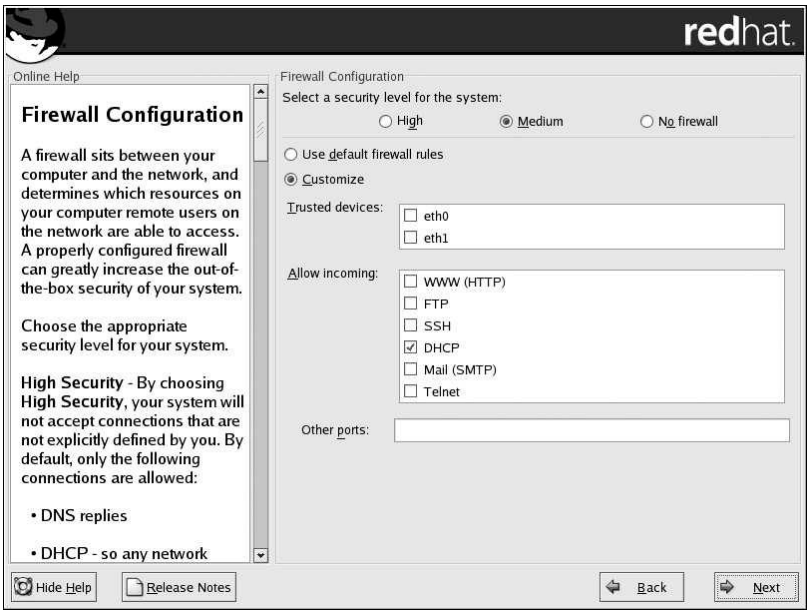
8. *En la siguiente pantalla se* **configura el gestor de arranque**, *el cual es un programa que se instala en el MBR (Registro de Arranque Maestro) del disco duro; es el primer programa que se carga y que determina cuál va a ser el sistema operativo que va a arrancar al ordenador, desde qué disco e incluso qué partición. Por default aparece marcada la opción de Linux que se esta instalando. Únicamente es necesario protegerlo con una contraseña, para evitar que personas ajenas arranquen el sistema.*



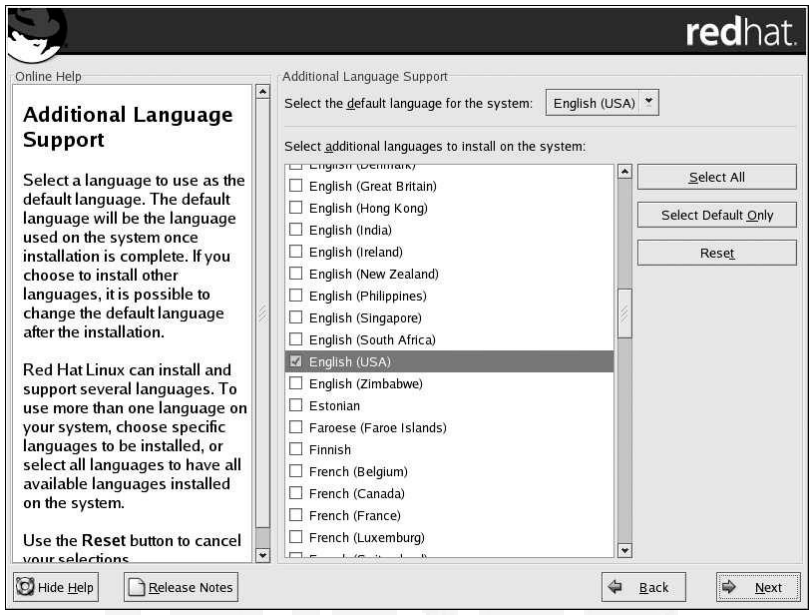
9. *Después, es necesario* **configurar la red** *(los dispositivos de red se detectan automáticamente), en esta parte se deben introducir los datos que se tiene en el mapa de servidores con sus nombres de host, la dirección IP aleatoria por medio de un servidor de DHCP (Protocolo de Configuración Dinámica de Host) o fija (se recomienda que sea fija), la máscara de subred, la puerta de enlace, los DNS (Servidor de Nombres por Dominio) y el nombre del host.*



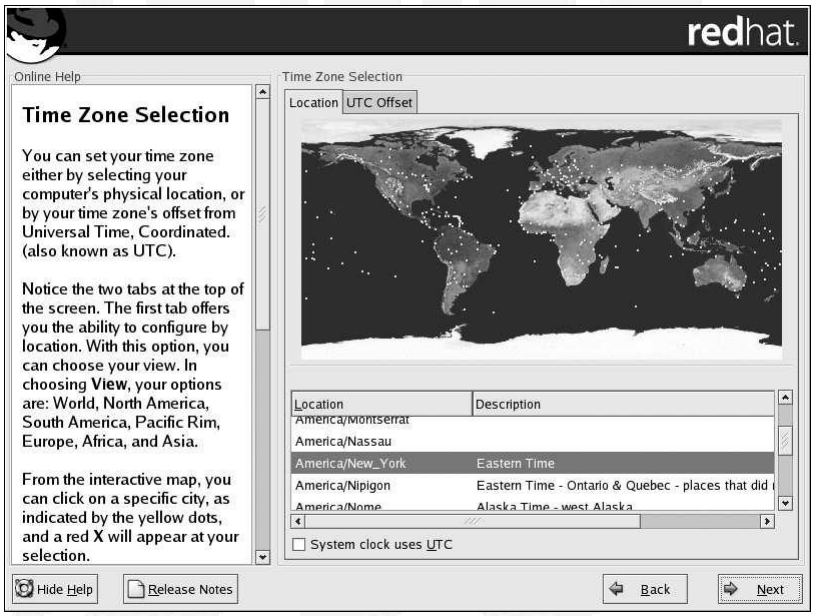
10. *Ahora, es necesario* **configurar un firewall**, *Linux ofrece protección vía firewall para una seguridad mejorada del sistema; este mecanismo se coloca entre el ordenador y la red y determina qué recursos del equipo están accesibles para los usuarios remotos de la red. Seleccionamos el nivel más alto con las únicas entradas permitidas a* **WWW** *(HTTP) y* **SSH**.



11. **Selección del soporte del idioma**, *aquí se elegirá uno o más idiomas que el sistema utilizará por defecto. Linux puede instalar y soportar varios idiomas para usar en el sistema, pero si sólo se usa uno se ahorra espacio en disco. En nuestro caso sólo se utilizará el español.*

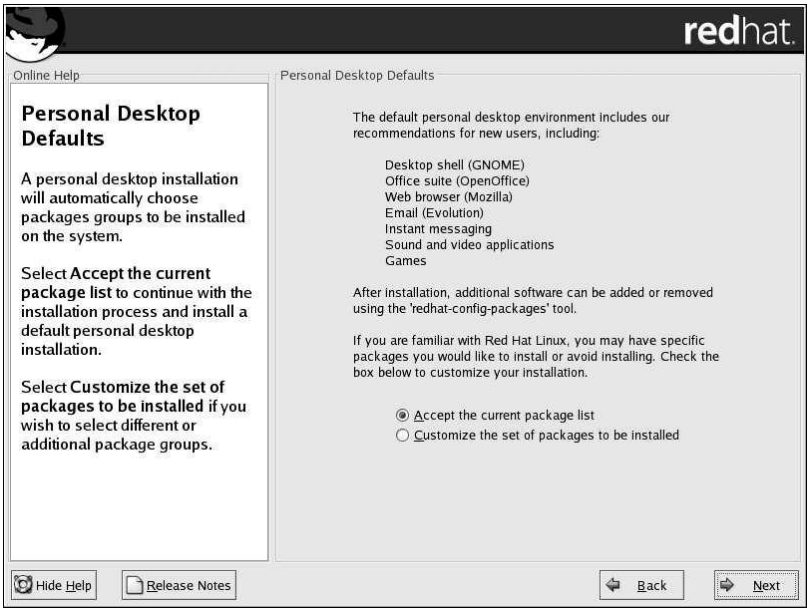


12. **Configuración del huso horario**, *aquí se elige la hora local a través de la localización física de la máquina o bien especificando el huso horario en función del UTC (Coordinated Universal Time). Particularmente se eligió el que corresponde a la ciudad de México.*

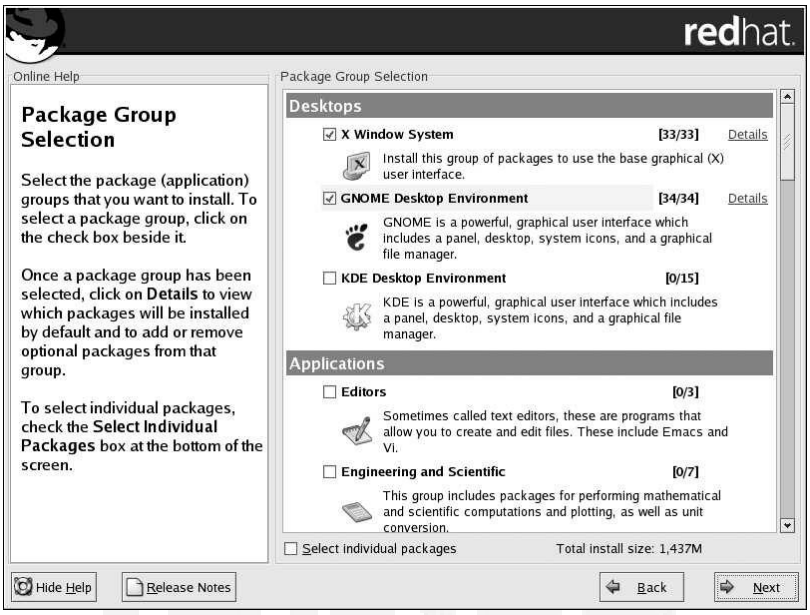


13. **Configuración de la cuenta de root**, *la cual administra el sistema. Esta es la cuenta más importante porque con ella se administran usuarios, grupos, archivos y todo el sistema en general;* **root** *es la única cuenta que tiene el poder absoluto sobre todo el sistema.*

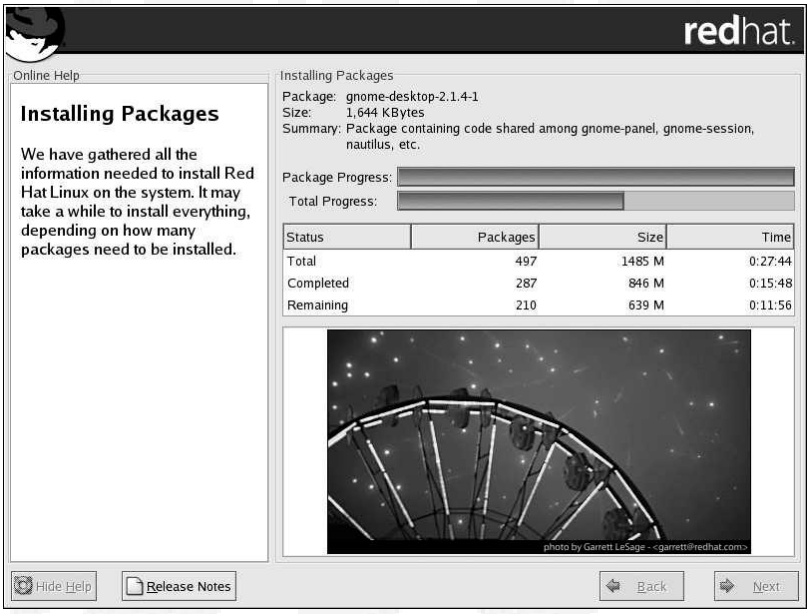
14. En seguida se seleccionan los **grupos de paquetes** *que desea que se instalen en la máquina. A no ser que se elija una instalación de tipo personalizada, el programa de instalación elegirá la mayoría de los paquetes por usted.*



14.1 Para personalizar la instalación de paquetes, se deberán elegir uno por uno de una lista con el fin de no instalar paquetes que no sean necesarios o que dejen puertas abiertas en el sistema operativo. Los paquetes que se eligieron son únicamente los esenciales para el buen funcionamiento del servidor y no ocupan demasiado espacio en disco.

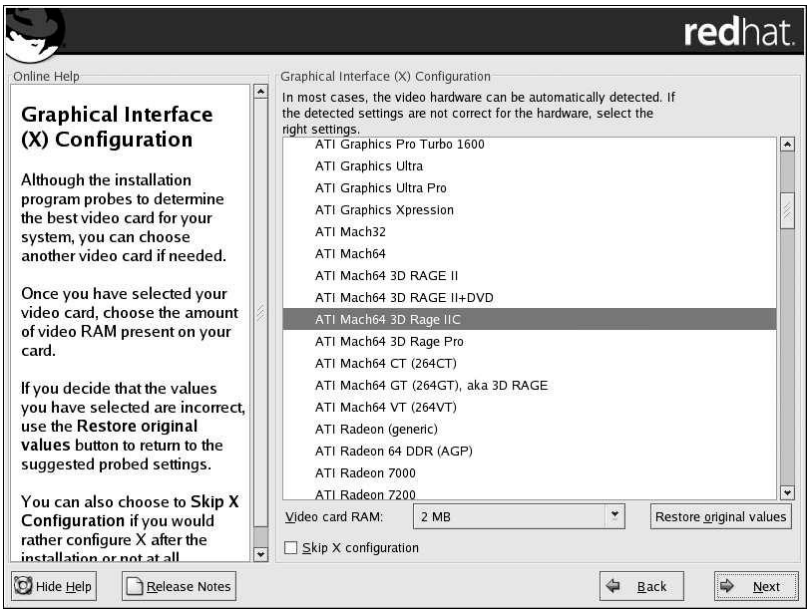


15. *Ahora ya está todo listo para* **comenzar la instalación**, *solo basta esperar a que las aplicaciones se carguen en la máquina. La rapidez de este proceso dependerá del número de paquetes que se hayan elegido y de la velocidad del procesador.*



16. *Durante la instalación se pedirá* **crear un disco de arranque** *que es útil cuando el sistema no pueda arrancar adecuadamente usando GRUB, LILO u otro factor de arranque externo. La creación de este disco permite arrancar de forma adecuada Red Hat Linux y resolver diversos problemas.*

17. *Finalmente, se deberá* **configurar la interfaz gráfica** *y el monitor; también se deben personalizar las X.*



18. *Una vez terminada la instalación es muy importante* **crear una cuenta de usuario** *para poder entrar al sistema de forma fácil y segura sin tener que acceder con la cuenta de root. Se podrán modificar o cancelar las cuentas de usuario posteriormente cuando ya no se necesiten.*

Glosario de Términos

Amenaza. *Las amenazas son los sucesos o las acciones que podrían tener un impacto negativo en la disponibilidad, integridad o confidencialidad de la información. Una amenaza es una acción o evento que puede violar la seguridad de un entorno de sistemas de información.*

ASP, Application Service Provider *(Proveedor de Servicios de Aplicación). Compañía que hospeda, en las instalaciones de sus propios servidores, aplicaciones de software para otras compañías.*

Backbone (Columna Vertebral). *Mecanismo de conectividad primario en un sistema distribuido. El backbone es una línea de transmisión de información de alta velocidad o una serie de conexiones que juntas forman una vía con gran ancho de banda. Todos los sistemas que tengan conexión al backbone pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas.*

CERT, Computer Emergency Response Team *(Equipo de Respuesta a Emergencias Informáticas). Centro de investigación federal dirigido por la Universidad de Carnegie Mellon, creado en diciembre de 1988 por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), la cual formaba parte del Departamento de Defensa de Estados Unidos.*

CGI, Common Gateway Interface *(Interfaz de Pasarela Común). CGI es un estándar que especifica cómo los servidores web utilizan aplicaciones externas para pasar información dinámica a los clientes web. CGI es neutral a la plataforma y al lenguaje, mientras se tenga el compilador o intérprete necesario, así que se pueden escribir programas pasarela en cualquier lenguaje como BASIC, C/C++, Perl, Pitón, REXX, TCL, los lenguajes shell, etc.*

Clúster. *Un clúster (o unidad de asignación según la terminología de Microsoft) es un conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento de un disco. Los archivos se almacenan en uno o varios clústeres, dependiendo de su tamaño. Sin embargo, si el archivo es más pequeño que un clúster, éste ocupa el clúster completo.*
Código abierto. *Es una parte o la totalidad de un programa fuente, el cual se distribuye libremente con el software ejecutable del que forma parte, con la finalidad de que pueda ser modificado como se necesite.*
Concurrencia. "*N" procesos son concurrentes cuando se ejecutan (acción por acción) en el mismo intervalo de tiempo; es decir, para ejecutarlos concurrentemente se requiere tan solo "repartir" el procesador entre ellos a una velocidad tal que, por unidad o intervalo de tiempo, todos reciban su atención (aunque sea sólo parcial).*
Consola. *Configuración usuario-pantalla donde se pueden teclear comandos para administrar el sistema.*
Contraseña. *Palabra o código utilizado como medida de seguridad contra el acceso no autorizado a los datos residentes en equipos de cómputo.*
Cracker. *Usuario y programador informático que tiene amplios conocimientos y crea código malicioso capaz de romper los sistemas de seguridad, para acceder a otros ordenadores o computadoras y así poder recabar o destruir información. En ocasiones se utiliza como sinónimo de hacker, aunque este último tiene como finalidad su propia satisfacción o vencer retos tecnológicos, sin ánimo de realizar daño u obtener información de forma ilegal.*
Criptografía. *Ciencia que se encarga del cifrado de las comunicaciones; hace referencia a la creación y descifrado de los algoritmos utilizados para ocultar, o cifrar de cualquier otro modo, una cierta información.*
Demonio*. Es un proceso de segundo plano relacionado con el sistema que suele ejecutarse con los permisos de root y las peticiones de servicio de otros procesos*
Depurador. *Un depurador (debugger), es una herramienta para limpiar de errores algún programa informático. Habitualmente, entre las opciones de compilación, deben añadirse instrucciones para generar información para el depurador.*
Distribución. *En el contexto GNU/Linux, es una colección de programas informáticos que contienen el núcleo (kernel) del sistema operativo y aplicaciones que permiten el uso completo de un ordenador como herramienta productiva. Un sistema operativo (en general Linux), que se ha empaquetado para facilitar su instalación.*
DMZ (Zona Desmilitarizada). *Subred que contiene un firewall y un servidor proxy, que sirve como línea divisoria entre la intranet de una organización y la Web.*
DNS, Domain Name Server *(Servidor de Nombres de Dominio). Servicio de Internet que traduce los nombres de dominio a direcciones IP.*
DoS, Denial of Service *(Denegación de Servicio). Estado en el que un sistema ya no puede responder a solicitudes normales. Ataque contra una red que consiste*

en inundarla con tantas solicitudes adicionales que se ralentiza el tráfico normal o se interrumpe el servicio por completo.

E-mail (Correo Electrónico). *Los mensajes enviados a través de un medio electrónico en lugar de un servicio postal local.*

Estrategia. *En el proceso de resolver un problema, la estrategia es el curso de acciones que se elige para resolverlo. La estrategia es en sí una opción, entre varias que pudieran elegirse (o construirse) a fin de resolver el problema. Las acciones forman un plan, que incluye actividades, responsables, recursos, tiempos y metas.*

Ethernet. *Es una especificación de red de área local (LAN) desarrollada en 1976 por Xerox, en cooperación con DEC e Intel. Se trata de una red muy difundida, de la cual se derivó la norma (o estándar) IEEE 802.3 para redes de conexión.*

Exploit. *Un exploit es, como su nombre lo indica, un programa que explota las vulnerabilidades del sistema operativo y aprovecha sus fallas para poder ser atacado por un intruso malicioso.*

FTP, File Transfer Protocol *(Protocolo de Transferencia de Archivos). Protocolo de comunicaciones utilizado para transferir archivos sin pérdidas de datos, a través de redes TCP/IP.*

GNU. *GNU significa "GNU no es UNIX" y es el nombre de los paquetes de software gratuitos que se suelen encontrar en entornos de Unix y que los distribuye el proyecto GNU en el MIT (instituto Tecnológico de Massachussets).*

GPL. *Licencia Pública General de GNU.*

Hacker. *Término utilizado para referirse a un aficionado a los ordenadores o computadoras, totalmente cautivado por la programación y la tecnología informática. Los hackers son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección sin intención maliciosa.*

Hardware. *El hardware es el equipo físico utilizado para el funcionamiento de las computadoras, es decir, son todos los componentes materiales que componen un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento, los cuales están conectados a través de un conjunto de cables o circuitos llamados bus con la Unidad Central de Proceso (CPU).*

HTTP, Hyper Text Transport Protocol *(Protocolo de Transferencia de Hipertexto). Sistema para solicitar documentos HTML a través de la Web.*

ICMP, Internet Control Message Protocol *(Protocolo de Mensajes de Control de Internet). Ampliación del protocolo IP. Se trata del protocolo de mensajes de control y error utilizado de forma estándar en los sistemas Internet.*

IEEE, Institute of Electrical and Electronic Engineers *(Instituto de Ingenieros Eléctricos y Electrónicos). Sociedad situada en Estados Unidos responsable de la publicación de normas, que incluye los estándares que definen los protocolos conocidos comúnmente como Ethernet y Token Ring, así como muchos otros.*

Interfaz. *Una interfaz es la parte de un programa informático que permite a éste comunicarse con el usuario o con otras aplicaciones permitiendo el flujo de información.*

Internet. *Es un conjunto de distintas redes que proporcionan la posibilidad de mover datos entre ellas. Esta integrado en el protocolo de comunicaciones TCP/IP.*
Intranet. *El término Intranet se define como una red basada en TCP/IP con acceso restringido a un determinado grupo de usuarios; en muchos casos se refiere a un sitio Web que funciona en una red privada.*
IP, Internet Protocol *(Protocolo de Internet). Hace referencia a todos los estándares que permiten el funcionamiento de Internet. El protocolo fundamental es el TCP/IP, el cual proporciona el mecanismo básico de comunicaciones, así como las formas de copiar archivos y enviar mensajes de correo electrónico.*
Kernel. *El núcleo del sistema operativo que maneja tareas como la asignación de memoria, la entrada y salida de dispositivos, la seguridad y el acceso de los usuarios.*
LAN, Local Area Network *(Red de Área Local). Un conjunto de hardware, software, computadoras de escritorio, servidores y hosts todos conectados entre sí en un área local definida, como el campus de una universidad.*
Memoria RAM (Memoria de Acceso Aleatorio). *Memoria de semiconductor en la que se puede tanto leer como escribir. Es un tipo de memoria temporal que contiene los programas y datos con los que el ordenador está trabajando en un momento concreto. Aunque se denomine memoria de acceso aleatoria, en realidad es una memoria de acceso directo y temporal puesto que si se apaga el ordenador se pierde el contenido.*
Messenger. *Programa de mensajería instantánea, el cual funciona a través de una conexión a Internet. Sirve también para intercambio de archivos.*
Norma. *Documento establecido por consenso y aprobado por un organismo reconocido, que proporciona, para un uso común y repetido, reglas, directrices o características para actividades o sus resultados, con el fin de conseguir un grado óptimo de orden en un contexto dado.*
Página Web. *Una página web es un documento de la World Wide Web, normalmente en formato HTML/XHTML, publicada a través de un servidor de Internet, que proporciona información o servicios, a determinada comunidad en el mundo y se vincula a otros documentos mediante ligas de hipertexto.*
Password. *(Contraseña) Es una cadena de caracteres seguidos que un usuario introduce en un sistema como código de identificación para tener acceso a una aplicación o programa. En informática, una contraseña es una medida de seguridad utilizada para limitar el acceso a sistemas informáticos y archivos confidenciales.*
PGP. *Sistema de encriptación Pretty Good Privacy.*
PHP, Hypertext Preprocessor *(Preprocesador de Hipertexto). Es un lenguaje de programación de scripts. Se utiliza principalmente para la programación de CGIs para páginas web, destaca por su capacidad de ser embebido en el código HTML.*
Plataforma. *La arquitectura del hardware de un modelo particular o familia de computadoras. La plataforma es el estándar con el que los diseñadores de*

software escriben sus programas. El término plataforma a menudo se utiliza para referirse al sistema operativo incluido con el hardware.

Política. *Una política proporciona las reglas que gobiernan cómo deberían ser configurados los sistemas y cómo deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales.*

Procedimiento. *Una serie secuencial de pasos que son seguidos por los miembros de la organización para cumplir un propósito específico. Secuencia de actividades relacionadas entre si que especifican sus formas de ejecución para llevarlas a la práctica.*

Puerto. *Un puerto es una forma genérica de denominar a una interfaz por la cual diferentes tipos de datos pueden ser enviados y recibidos. Dicha interfaz puede ser física, o puede ser a nivel software.*

Rastreador (Sniffer). *Programa y/o servicio que supervisa el movimiento de los datos a través de la red. Los sniffers se pueden utilizar tanto para funciones de administración de red como para robar información de la misma porque son prácticamente imposibles de detectar y se pueden insertar en casi cualquier lugar o punto de la red.*

Recurso. *Elemento de un ordenador, ya sea espacio de almacenamiento o periférico conectado a él. Un recurso puede ser cualquier parte de un sistema de información. También se denomina así a la actividad de un programa que puede ser utilizada por varios programas de modo concurrente o simultáneo.*

Rendimiento. *Es el desempeño de un ordenador o de uno de cada uno de sus componentes. Proceso continuo y estructurado para identificar los puntos fuertes y oportunidades de un sistema.*

Riesgo. *El riesgo es el potencial de lo que puede ser perdido y necesita protección.*

Script. *Un programa escrito para una utilidad Unix, que incluye los shells* awk, Perl, sed *y otros.*

Servidor Proxy. *Se utiliza para los servidores host que residen detrás de los firewalls. El servidor Proxy intercepta y retransmite todas las solicitudes al servidor real.*

Servidor. *Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos.*

Shell. *Elemento de software, que puede ser un programa independiente o constituir un elemento básico de un sistema operativo. Proporciona una comunicación directa entre el usuario y el propio sistema operativo, y así facilita la ejecución de órdenes o comandos del sistema y de los programas que se ejecutan en él. Se trata definitivamente de la parte del sistema que se muestra al usuario final, para que interactúe con él.*

SMTP, Simple Mail Transfer Protocol *(Protocolo Simple de Transferencia de Correo). Protocolo empleado para enviar mensajes de correo electrónico entre servidores.*

Software. *El software compone todos los programas de computadora, es decir, son todas aquellas instrucciones responsables de que el hardware funcione como es debido.*

SSL, Secure Sockets Layer *(Capa de Conectores Seguros). Desarrollado por Netscape, se trata del mecanismo de seguridad más importante en Internet. Cuando se inicia una sesión SSL, el servidor envía su clave pública al explorador y éste la utiliza para enviar de vuelta al servidor una clave secreta generada aleatoriamente, con el fin de realizar un intercambio de claves secretas para esa sesión.*

Switch. *Un switch es un dispositivo de interconexión de redes de ordenadores/computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), o sea pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los frames en la red.*

TCP/IP, Transmission Control Protocol/Internet Protocol *(Protocolo de Control de Transmisión/Protocolo de Internet). Protocolo de comunicaciones desarrollado bajo contrato para el Departamento de Defensa de Estados Unidos y que sirve para interconectar en red diferentes sistemas.*

Telnet. *Protocolo para el acceso de terminal interactivo (interfaz de usuario de caracteres) a sistemas remotos.*

Terminal. *Un terminal es un aparato capaz de realizar operaciones de diálogo con un servidor. También se le llama cliente. Cualquier dispositivo con capacidad de enviar y recibir datos en un canal de comunicaciones.*

Topología. *Es la forma en la que las redes LAN conectan computadoras en varios tipos de configuraciones, que dependen del tipo de cable usado y de los protocolos utilizados por los equipos.*

UDP, User Datagram Protocol *(Protocolo de Datagrama de Usuario). Parte del TCP/IP que se utiliza para los mensajes de control y para la transmisión de datos, donde no se necesita el reconocimiento del envío. La aplicación debe garantizar la transmisión de datos en este caso.*

Unix. *Unix es un sistema operativo multiusuario y multitarea desarrollado originalmente por Ken Thompson y Dennis Ritchie en los Laboratorios Bell en 1969.*

Username. *Es un nombre que identifica a un usuario particular y le permite acceder a un sistema informático que a menudo es utilizado por varias personas. Suele emplearse en conjunción con un password o contraseña para mayor seguridad.*

VPN, Virtual Private Network *(Red Privada Virtual). Red privada configurada dentro de una red pública. Las VPN ofrecen la seguridad de una red privada, en cuanto al control de acceso y el cifrado, al mismo tiempo que permiten disfrutar de las ventajas de las grandes redes públicas.*

Vulnerabilidad. *La vulnerabilidad es la ausencia, inadecuación o incoherencia de las utilidades y los procesos implementados para proteger el valor del activo frente a las amenazas identificadas.*

Fuentes Consultadas

1. Fuentes Bibliográficas

- *Arroyo, José;* **"Linux, Máxima seguridad"**, *Prentice Hall, Madrid 2000.*
- *Bandel, David y Napier, Robert;* **"Linux, Edición Especial",** *Prentice Hall, Madrid 2001, sexta edición.*
- *Campderrich, Benet;* **"Técnicas de Bases de Datos"**, *Editores Técnicos Asociados, Barcelona 1988, segunda edición.*
- *González Sánchez, José Luis;* **"Red Hat Linux 8, Manual avanzado"**, *ediciones Anaya Multimedia, Madrid.*
- *Gratton, Pierre;* **"Protección Informática"**, *editorial Trillas, México 1998.*
- *Hansen Gary W. y Hansen, James V.;* **"Diseño y Administración de Bases de Datos"**, *Prentice Hall, Madrid 1997, segunda edición.*
- *Hatch, Brian y Lee, James;* **"Hackers en Linux",** *McGraw-Hill, segunda edición.*

- *LeBlanc, Dee-Ann;* **"La Biblia de administración de sistemas Linux"**, *editorial Anaya.*

- *Long, Larry;* **"Introducción a las Computadoras y a los Sistemas de Información",** *editoral Prentice Hall.*

- *Maiwald, Erick;* ***"*****Fundamentos de Seguridad de Redes***", McGraw-Hill, México 2005.*

- *Márquez Vite, Juan Manuel;* **"Sistemas de Información por computadora, Metodología de desarrollo"**, *editorial Trillas.*

- *McCarthy, Mary Pat;* **"Seguridad Digital***", McGraw-Hill, España 2002.*

- *Mediavilla, Manuel;* **"Seguridad en Unix"**, *editorial RA-MA.*

- *Míguez Pérez, Carlos;* **"Hacker, la Biblia"**, *ediciones Anaya Multimedia, Madrid 2003.*

- *Milenkovic, Milan;* **"Sistemas Operativos",** *editorial McGraw-Hill.*

- *Rodao, Jesús de Marcelo;* **"Piratas cibernéticos"**, *editorial RA-MA.*

- *Rodríguez, Luis Angel;* **"Seguridad de la Información en Sistemas de Cómputo"**, *ediciones Ventura, México 1995.*

- *Schenk, Thomas;* **"Administración de Red Hat Linux, Al descubierto",** *Prentice Hall, Madrid 2001.*

- *Senn, James A.;* **"Análisis y Diseño de Sistemas de Información"**, *editorial McGraw-Hill, segunda edición.*

- *Senn, James A.;* **"Sistemas de Información para la Administración"**, *Grupo Editorial Iberoamérica, EUA 1987.*

- *Stallings, William;* **"Sistemas Operativos",** *Noriega Editores.*

- *Streib, M. Drew;* **"Linux, Serie práctica"**, *Prentice Hall, Madrid 2000.*

- *Tanenbaum, Andrew S.;* **"Modern Operating Systems",** *Prentice Hall, segunda edición.*

- *Theriault, Marlene;* ***"*****Oracle, Manual de seguridad***", MacGraw-Hill, España 2002.*

» *Zacker, Craig; "***Redes, Manual de Referencia"***, editorial McGraw-Hill, España 2002.*

2. Fuentes Hemerográficas

» **"Revista RED, La comunidad de expertos en redes",** *Número 150, Junio de 2003, año XIV. Presidente: Pablo Payró. Suplemento especial guía de redes.*

» **"Revista RED, La comunidad de expertos en redes",** *Número 153, Septiembre de 2003, año XIV. Presidente: Pablo Payró.*

» **"Revista RED, La comunidad de expertos en redes",** *Número 159, Abril de 2004, año XIV. Pablo Payró. Suplemento especial guía de seguridad 2004.*

3. Páginas Web

» *http://www.astalavista.com*
» *http://www.bgsec.com/seguridad.html*
» *http://www.cantv.net/seguridadeninternet*
» *http://www.delitosinformaticos.com*
» *http://www.elhacker.net*
» *http://www.insecure.org*
» *http://www.linux.cu/manual/avanzado-html/node1.html*
» *http://www.mandrakeLinux.com/es/security.php3*
» *http://www.noticias3d.com/articulo.asp?idarticulo=375*
» *http://www.psionic.com*
» *http://www.recursosgratis.com/noticias/seguridad.html*
» *http://www.redhat.com/solutions/security*
» *http://www.securemac.com*
» *http://www.securityfocus.com*
» *http://www.securityfocus.com/archive/1*
» *http://www.securityportal.com.ar*
» *http://www.venezolano.web.ve/archives/95_Que_es_Linux_y_que_puede_hacer_por_usted.html*

4. Documentos PDF

- *Aguilar, Luis;* **"Recursos de Seguridad en Ambientes de Redes de Datos y Acceso a Internet",** *2000.* http://www.itrainonline.org/itrainonline/spanish/networking.pdf

- *Bremer, Steve;* **"LIDS FAQ",** *2001.* http://www.lids.org

- *Fernández-Sanguino Peña, Javier;* **"Administración de la seguridad en un sistema GNU/Linux",** *2005.* http://www.fdi.ucm.es/libre/formativas/transpa05-04-22.pdf

- *Mellado Gatica, Alejandro Mauricio;* **"Apuntes de Sistemas Operativos",** *Abril 2003.* http://www.inf.uach.cl/apuntes/apuntes_so.pdf

- *Morales Vázquez, José María;* **"Internet Firewalls",** *2002.* http://www.interhack.net/pubs/fwfaq/firewalls-faq.pdf

- *Villalón Huerta, Antonio;* **"Seguridad en Unix y Redes",** *Julio 2002.* http://andercheran.aiind.upv.es/toni/personal/unixsec.pdf

- **"Linux Security Howto",** *Mayo 1998.* http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/pdf/Security-HOWTO.pdf

- **"Red Hat Linux Security Guide",** *Red Hat 9.0, 2002.* http://www.redhat.com

- **"Red Hat Linux x86 Installation Guide",** *Red Hat 9.0, 2003.* http://www.redhat.com