**Universidad de San Carlos de Guatemala**
**Facultad de Ingeniería**
**Escuela de Ingeniería en Ciencias y Sistemas**

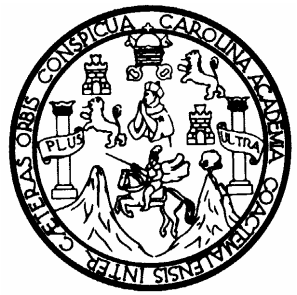
# DISEÑO DE REDES SEGURAS PARA PROTEGER SERVIDORES DE DATOS EN INTERNET PARA EMPRESA MEDIANA Y GRANDE

**Miguel Marín de León**

Asesorado por: Inga. Elizabeth Domínguez Alvarado

Guatemala, septiembre de 2006

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**




**FACULTAD DE INGENIERÍA**

# DISEÑO DE REDES SEGURAS PARA PROTEGER SERVIDORES DE DATOS EN INTERNET PARA EMPRESA MEDIANA Y GRANDE

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

**MIGUEL MARÍN DE LEÓN**
ASESORADO POR: INGA. ELIZABETH DOMÍNGUEZ ALVARADO

AL CONFERÍRSELE EL TÍTULO DE
**INGENIERO EN CIENCIAS Y SISTEMAS**

GUATEMALA, SEPTIEMBRE DE 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

**NÓMINA DE JUNTA DIRECTIVA**

| | |
|---|---|
| DECANO | Ing. Murphy Olympo Paiz Recinos |
| VOCAL I | Inga. Glenda Patricia Garcia Soria |
| VOCAL II | Ing. Amahán Sánchez Álvarez |
| VOCAL III | Ing. Julio David Galicia Celada |
| VOCAL IV | Br. Kenneth Issur Estrada Ruiz |
| VOCAL V | Br. Elisa Yazminda Vides Leiva |
| SECRETARIA | Inga. Marcia Ivonne Véliz Vargas |

**TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO**

| | |
|---|---|
| DECANO | Ing. Murphy Olympo Paiz Recinos |
| EXAMINADORA | Inga. Claudia Liceth Rojas Morales |
| EXAMINADOR | Ing. Juan Álvaro Díaz Ardavín |
| EXAMINADOR | Ing. Pedro David Tzoc Tzoc |
| SECRETARIA | Inga. Marcia Ivonne Véliz Vargas |

**HONORABLE TRIBUNAL EXAMINADOR**

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**DISEÑO DE REDES SEGURAS PARA PROTEGER SERVIDORES DE DATOS EN INTERNET PARA EMPRESA MEDIANA Y GRANDE,**

tema que me fuera asignado por la Dirección de Escuela de Ciencias y Sistemas, con fecha  febrero de 2005.

Miguel Marín de León

# AGRADECIMIENTOS A:


| | |
|---|---|
| **La Universidad de San Carlos de Guatemala** | Templo del saber y centro de sabiduría que a cada paso me ayudó a culminar la carrera con éxito. |
| **La Facultad de Ingeniería** | Gracias por brindarme la oportunidad de poder pertenecer a tan honorable y digna facultad. |
| **Mis catedráticos** | Agradeciéndoles por sus sabias enseñanzas. |
| **Ingeniera Elizabeth Domínguez** | Gracias por su apoyo y esfuerzo al asesorarme en este trabajo de graduación. |

# DEDICATORIA A:

**Dios** Quien por su poder sagrado me dio sabiduría, y derramo en mí, muchas bendiciones, para poder llegar a mis más altas metas y grandes ideales.

**Mi Patria Guatemala**

Con respeto y lealtad: Tierra que me vio nacer.
A Dios gracias de vivir en ella.

**Mis Padres** Manuel Marín Maldonado, Zoila Amparo de León Velásquez, por su amor, cariño y sacrificio que este triunfo sea una pequeña recompensa a sus esfuerzos.

**Mis hermanos** Irma Angélica, Isabel, Alba Elizabeth, Cary Estela y Josué Manuel, por su cariño y ayuda incondicional.

**Mi esposa** Sonia Yesenia Márquez, gracias por su apoyo y compañía en el lapso de mi carrera.

**Mi hija** Odalys Yesenia, a quien dedico este triunfo con todo mi corazón.

**Mi familia en general** Con mucho aprecio.

**Mis amigos(as) y compañeros (as)** Por momentos gratos y su ayuda incondicional, éxitos en el futuro.

**A usted de manera especial**

# ÍNDICE GENERAL

# ÍNDICE DE ILUSTRACIONES

## FIGURAS

## TABLAS

# LISTA DE SÍMBOLOS

| Símbolo | Descripción |
|---|---|
| **S** | Router de selección |
| **R** | Router ordinario |
| **F1** | Firewall con una sola conexión de red a la red |
| **F2** | Firewall con dos conexiones de red |
| **B1** | Host de bastión con una sola conexión de red a la red |
| **B2** | Host de bastión con dos conexiones de red |

# GLOSARIO

**Antivirus** Programa encargado de evitar que cualquier tipo de virus entre a la computadora y se ejecute. Para realizar esta labor existen muchos programas, los cuales comprueban los archivos para encontrar el código de virus en su interior.

**Backbone** Red que actúa como conductor primario del tráfico de datos de la red. Comúnmente, recibe y manda información a otras redes.

**Back Door** Puerta trasera.

**Broadcast (Difusión)** Mensaje cuya dirección de destino está codificada de forma especial para poder ser escuchado, simultáneamente, por todas las máquinas conectadas al mismo segmento de red en el que se originó.

**Bug** Un error en un programa o en un equipo. Se habla de *bug* si es un error de diseño, no cuando la falla es provocada por otra cosa.

| | |
|---|---|
| **CERT** | Es un equipo de seguridad para la coordinación de emergencias en redes telemáticas. |
| **Clave** | Es el sinónimo de *password* o contraseña en el ambiente computacional; también, puede ser el código que permite desencriptar un dato. |
| **Cookie** | Es un pequeño trozo de información enviado por un servidor de Web al buscador de un usuario. Cuando se visita un servidor que utiliza el desarrollo denominado "*Magic Cookie* (MC)", éste instruye al buscador de la PC para crear un archivo Magic Cookie al que se lo suele nombrar como cookies.txt o similar. En él, ingresa y queda una pequeña cantidad de información, dicho bloque de datos podría contener un identificador exclusivo para el usuario generado por el servidor, la fecha y hora actual, la dirección IP del proveedor del servicio de acceso a Internet mediante el cual la PC del usuario se conecta a la red, o cualquier otro grupo de datos que se desee. |

**Cortafuegos (Firewall)**

Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red de área local (LAN) de una organización Internet.

La barrera de protección impide que los crackers tengan acceso a la red interna. Por desgracia, también, impide que los usuarios de la organización obtengan un acceso directo a Internet. El acceso que proporciona la barrera de protección es indirecto y mediado por los programas llamados servidores apoderados.

**Cracker**

a) Persona que quita la protección a programas con sistemas anticopia.
b) Hacker maligno, que se dedica a destruir información.

**Criptografía**

Criptografía proviene del griego y se puede traducir como “La manera de escribir raro”, criptos de extraño y graphos de escritura. Consiste en modificar los datos de un archivo o los que se transmiten por módem, radio, etc. Para evitar así que los puedan leer personas no deseadas. Esta técnica ha tenido su principal aplicación en los ejércitos y en la diplomacia.

| | |
|---|---|
| **DMZ** | Zona desmilitarizada, red perimétrica (DMZ). |
| **Denial of Service** | Negación de servicio (DoS). |
| **Exploit** | Código que es escrito para automatizar el proceso de utilizar la vulnerabilidad conocida en un servicio o sistema en específico, para obtener, ilegalmente, acceso a recursos, los cuales, normalmente, debieran estar denegados para el individuo atacante. |
| **Firewall** | Cortafuegos. |
| **FTP** | **-**File Transfer Protocol: Protocolo de transferencias de archivos- Un conjunto de protocolos mediante el cual pueden transferirse archivos de una computadora a otra. FTP es, también, el nombre de un programa que usa los protocolos para transferir archivos de ida y vuelta entre computadoras. |

| | |
|---|---|
| **Gusanos** | Son programas que se transmiten a sí mismos de una máquina a otra a través de una red. Se fabrican de forma análoga al virus, con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos, podría decirse que un gusano es un tumor benigno, mientras el virus es un tumor maligno. Las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. |
| **Hacker** | Persona que se introduce en un sistema sin tener autorización. No confundir con cracker. |
| **Hardware** | Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación. |
| **Ingeniería social** | Arte de convencer a la gente de entregar información que no corresponde. |

| | |
|---|---|
| **Internet** | Sistema de redes de computación ligadas entre si, con alcance mundial, el cual facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias. |
| **Login, Username** | Usuario. Nombre de registro de entrada. En una red de computación, nombre único asignado por el administrador del sistema usuario, el cual se utiliza como medio de identificación inicial. El usuario debe usar el nombre, así como su contraseña -password- para tener acceso al sistema. |
| **Malware** | Software malicioso. |
| **Password** | Clave, contraseña. |
| **Privacy** | Privacidad. |

| | |
|---|---|
| **Proxy** | Un Proxy actúa de forma similar a como actúa un router con la excepción de que un router se encuentra a nivel de red y, únicamente, entiende de paquetes. Un Proxy , sin embargo, se encuentra a nivel de aplicación; por lo que, en lugar de trabajar con paquetes, trabaja con elementos de nivel de aplicación como mensajes, peticiones, respuestas, autenticaciones, etc… resumiendo, un Proxy es una entidad a nivel de APLICACION que actúa de puente entre dos extremos de una comunicación. |
| **Rabbit. En inglés, conejo** | Programa que provoca procesos inútiles y se reproduce, como los conejos, hasta que agota la capacidad de la máquina. |
| **Root** | Cuenta del administrador en UNIX. Es la más poderosa: permite el acceso a todo el sistema. |
| **Securit** | Seguridad. |
| **Snooping** | Fisgoneo. |
| **Spoofing** | Falseamiento, enmascaramiento. |

| | |
|---|---|
| **Satan** | Esta es capaz de adivinar el nivel de vulnerabilidad de un host -ordenador servidor de Internet- y de todas las máquinas conectadas a él vía Internet, -su dominio-, ya que, permite conocer su nivel de encriptación, *password*, etc. SATAN, también, se puede obtener, libremente, por FTP en la red, lo que significa que puede ser utilizado tanto por los propios servidores, para ver su nivel de vulnerabilidad, como por los hackers. Es, por tanto, un arma de doble filo. |
| **Shell** | Intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del sistema operativo las ejecute. |
| **Software** | Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de maquina. |
| **Terminal** | Puerta de acceso a una computadora. Puede tratarse de un monitor y teclado o de una computadora completa. |
| **UNIX** | Sistema operativo utilizado por la gran mayoría de máquinas de Internet. |
| **Virtual Private Network** | Red Privada Virtual (VPN). |

| | |
|---|---|
| **Virus** | Es una serie de claves en código que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Hay varios tipos de virus, desde los que no hacen mas que mostrar un mensaje, hasta los que destruyen todo lo que pueden del disco duro. |
| **Woorm** | Gusano. |

## RESUMEN

La seguridad de la información, es un tema muy importante en la actualidad, ya que, la información para las empresas es un punto medular para el éxito de sus operaciones, por lo cual abordaremos este tema, con el fin de establecer diseños de redes seguras para servidores de datos para Empresas Mediana y Grande .

Se dará a conocer conceptos de herramientas de Hardware y software, como técnicas y métodos utilizados en la seguridad de la información.

Se realizará un análisis de las herramientas de Hardware y Software que podrían utilizarse en un diseño de red Segura para Servidores de datos en Internet. Se darán a conocer precios de herramientas de Hardware, dando a conocer sus características, ventajas y desventajas.

Se realizará un análisis comparativo entre los sistemas Operativos que existen, actualmente, en lo que es en el aspecto de seguridad. Se presentará diseño de Red para una mediana Empresa y Grande.

# OBJETIVOS

## General

Proponer, diseñar y evaluar  Modelo de red segura para proteger Servidores de Datos en la Web, para empresas Mediana y Grande.

## Específicos

1. Documentar los dispositivos de Hardware a utilizar, describiendo sus características, ventajas y desventajas.
2. Documentar los recursos de Software a utilizar, describiendo sus características, ventajas y desventajas.
3. Documentar los costos de Hardware y software que se utilizaran.
4. Reunir información para el análisis y evaluación de Hardware y Software utilizados para brindar seguridad en la Web.
5. Realizar un diseño de seguridad para Servidores de datos en la Web, orientado a Mediana empresa.
6. Realizar un diseño de seguridad para Servidores de datos en la  Web, orientado a Grande Empresa.

# INTRODUCCIÓN

Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadores de propósito general. Mientras que, por una parte, Internet iba creciendo, exponencialmente, con redes importantes que se adherían a ella, por otra el auge de la informática de consumo -hasta la década de los ochenta muy poca gente se podría permitir tener un ordenador y un MODEM en casa- unido a factores menos técnicos -como la película *Juegos de Guerra***,** de 1983- iba produciendo un aumento espectacular en el número de piratas informáticos.

Sin embargo, el 22 de noviembre de 1988, Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso ***Worm*** o gusano de Internet. Miles de ordenadores conectados a la red se vieron inutilizados durante días, y las perdidas se estiman en millones de dólares para las empresas afectadas. Desde ese momento, el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos.

Teniendo en cuenta que las redes de Internet ofrecen inseguridad en transferencia de datos, se dedicará a investigar tecnologías de seguridad para poder realizar diseño de red para Mediana y Grande Empresa, analizando y estableciendo un diseño propuesto para cada una de ellas.

# 1. CONCEPTOS Y DEFINICIONES PREVIAS

## 1.1 Seguridad

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema esta libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de el) mas que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. Algunos estudios integran la seguridad dentro de una propiedad más general de los sistemas, la confiabilidad, entendida como el nivel de calidad del servicio ofrecido. Consideran la disponibilidad como un aspecto al mismo nivel que la seguridad y no como parte de ella, por lo que dividen esta ultima en solo las dos facetas restantes, confidencialidad e integridad.

¿Que implica cada uno de los tres aspectos de los que hablamos? La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos solo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

### 1.2 ¿Qué se quiere proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos 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. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorias de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, toners, cintas magnéticas, diskettes. . .), aquí no consideraremos la seguridad de estos elementos por ser externos al sistema.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el mas amenazado y seguramente el mas difícil de recuperar.

## 1.3 ¿De qué nos queremos proteger?

En la gran mayoría de publicaciones relativas a la seguridad informática en general. Con frecuencia, especialmente en las obras menos técnicas y mas orientadas a otros aspectos de la seguridad, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero en este trabajo es preferible hablar de `elementos' y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes naturales o, por qué no, Fuerzas extraterrestres; si un usuario pierde un trabajo importante a causa de un ataque, poco le importaría que haya sido un intruso, un gusano, un simple error del administrador, o un alíen que haya abducido un disco duro.

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema.

### 1.3.1 Personas mal intencionadas

La mayoría de ataques a sistema informáticos van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causar enormes perdidas.

Generalmente se trataría de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que hablaremos a continuación, especialmente agujeros del software.

Pero con demasiada frecuencia se suele olvidar que los piratas `clásicos' no son los únicos que amenazan los equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador minimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos. . . ), pocos administradores tienen en cuenta factores como la ingeniería social o el basureo a la hora de diseñar una política de seguridad.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para los sistemas; generalmente se dividen en dos grandes grupos:

Los Atacantes ***pasivos***, aquellos que fisgonean por el sistema pero no lo modifican o destruyen, y *los* ***activos***, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

### 1.3.2 Personal

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento. . . ) Puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas. . . y sus debilidades), lo normal es que mas que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el mas experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros; y en el primer caso, el *atacante* ni siquiera ha de tener acceso lógico (ni físico!) a los equipos.

### 1.3.3 Ex-empleados

Otro gran grupo de personas potencialmente interesadas en atacar el sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia).

Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo: amparados en excusas como *No me han pagado lo que me deben* o *Es una gran universidad, se lo pueden permitir* pueden insertar troyanos, bombas lógicas, virus. . . o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la universidad o empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex-compañeros o ex-jefes.

### 1.3.4 Curiosos

Junto con los crackers, los curiosos son los atacantes mas habituales de los sistemas. Recordemos que los equipos están trabajando en entornos donde se forma a futuros profesionales de la informática y las telecomunicaciones (gente que a priori tiene interés por las nuevas tecnologías), y recordemos también que las personas suelen ser curiosas por naturaleza; esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

### 1.3.5 Crackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple *exploit* los equipos que presentan vulnerabilidades; esto convierte a las redes de I+D, a las de empresas, o a las de ***ISPs*** en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los mas novatos (y a veces mas peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente mas protegidos, como los militares.

### 1.3.6 Terroristas

Por *terroristas* no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en el. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de ficheros de un servidor que alberga paginas Web de algún grupo religioso; en el caso de redes de I+D, típicos ataques son la destrucción de sistemas de prácticas o la modificación de páginas Web de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos.

### 1.3.7 Intrusos remunerados

Este es el grupo de atacantes de un sistema mas peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar mas a las grandes muy grandes empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte5 generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía. . .) o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance.

### 1.3.8 Amenazas Lógicas

Bajo la etiqueta de *amenazas lógicas* encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como ***malware***) o simplemente por error (***bugs*** o agujeros).

## 1.4 Causas de la inseguridad en las redes

Las causas mas comunes que pueden suscitarse debido a la falta de un buen sistema de seguridad en las Redes son:

- El crecimiento acelerado de las redes empresariales y particularmente el crecimiento en Internet, aunado a que el diseño de las redes se asumía en ambientes seguros controlados a través de usuarios autorizados y sin vislumbrar la futura conexión a redes externas, además de que protocolos de comunicación como el TCP/IP no fueron concebidos teniendo en cuenta aspectos de seguridad, son las principales causas de la inseguridad en las redes.
- Existen algunas ideas erróneas acerca de la seguridad, como el que se está totalmente protegidos con la asignación de contraseñas a todos los recursos, usuarios funcionales y aplicaciones, o comprar un firewall o equivalente, o suponer que los usuarios funcionales o posibles atacantes tienen bajo conocimiento.
- También es un error sentirse seguros con un Portero en la puerta de un centro de cómputo, así como también es un error pensar en que a mayor complejidad del sistema de seguridad, obtenemos mayor seguridad.

A continuación se verán explícitamente estas causas mencionadas.

### 1.4.1 El Crecimiento Acelerado de las Redes Empresariales

Las Telecomunicaciones, medio fundamental para el intercambio de información a distancia, han evolucionado para satisfacer esta necesidad, su evolución no se ha limitado a la parte tecnológica sino que ha incluido otros aspectos.

Dentro de estos nuevos conceptos se encuentran la Redes Empresariales, utilizadas hoy en día por una gran cantidad de empresas que cuentan con sucursales u oficinas en diferentes sitios de una ciudad, de un país o de varios países.

Es así como hoy en día no se concibe una transacción bancaria, de una tarjeta de crédito o una reserva aérea sin un sistema en línea, independientemente de donde se encuentre el cliente o la oficina que lo atiende. También ya es común ver medianas y pequeñas antenas para comunicaciones satelitales en los edificios y locales de los bancos, supermercados, fábricas, gasolineras y centros comerciales.

Es en tal sentido que hay un desarrollo acelerado de este tipo de redes y su tendencia hacia el uso de la banda ancha, integrando voz, datos e imágenes. Por lo tanto es importantísimo que procuremos dar a las comunicaciones la máxima seguridad, así la incrementamos también en todo el sistema.
Pero las redes crecen en magnitud y complejidad a una velocidad muy elevada, nuevos y avanzados servicios nacen continuamente sobrepasando nuestra capacidad de reacción.

También ha avanzado con rapidez la clase de información que viaja por las redes, y la más pequeña modificación en un mensaje, la revelación de la información o un retardo de unos minutos puede causar grandes pérdidas a la empresa.

La adopción de los fabricantes de los estándares nacionales e internacionales permite al usuario la compra, de acuerdo con sus necesidades y no estar ligado a un solo fabricante.

Pero por otro lado estos estándares son de conocimiento público y los pueden conocer usuarios, estudiantes, investigadores y criminales, conociendo de esta manera la mejor manera de atacar al sistema con eficacia y precisión.

### 1.4.2 El Crecimiento Acelerado de Internet

La idea de la conexión a Internet permite que las instalaciones generen un abanico extraordinario de servicios, pero a la vista de las limitaciones que se tiene que imponer en función de los condicionantes de seguridad y economía, decidimos concretarlos en unos pocos:

- Servicio de correo electrónico para todos los usuarios.
- Acceso a las Noticias de Internet, así como grupos locales, para todos los usuarios.

- Difusión a la comunidad académica y al resto de Internet de las Bases de Datos residentes en los hosts de una red interna especifica.

- Otros servicios, como Telnet a sistemas externos, y como no, el servicio principal de cualquier conexión a Internet que es el acceso a la WWW.

A la hora de utilizar el comercio electrónico por Internet cualquier usuario se cuestionará si las transacciones que realiza son realmente seguras. De hecho la posible evolución del comercio por la red está supeditada a los sistemas de seguridad que permitan al usuario comprar tranquilamente y sin riesgos.

Sin precauciones de seguridad en estas transacciones cualquier persona podría darse un paseo por los datos que estamos transmitiendo, entrar en una conversación o llegar a obtener nuestro número de tarjeta de crédito junto incluyendo nuestro número de identificación personal (NIP).

Para ser más concretos, en una comunicación podemos encontrar tres problemas claramente diferenciados:

- **ESCUCHA A ESCONDIDAS**. La información no sufre modificación pero alguien accede a ella.

- **MODIFICACIÓN**. La información es modificada, por ejemplo, alguien podría cambiar la cantidad a pagar en un pedido que se trasmite por la red.

- **IMITACIÓN**. Este problema aparece cuando alguien dice ser quien no es, siendo posible que una entidad se hiciera pasar por otra, realizara ventas que no llegaría a entregar y cobrara sus importes.

Para evitar estos riesgos son necesarias herramientas que proporcionen las siguientes propiedades a una comunicación:

- **CONFIDENCIALIDAD.** Es la propiedad por la que el destinatario de una comunicación puede conocer la información que está siendo enviada mientras que las personas que no son destinatarios no pueden determinar el contenido de lo que está siendo enviado.

- **INTEGRIDAD.** Es la propiedad de asegurar que la información sea transmitida desde su origen hasta su destino sin sufrir ninguna alteración.

- **AUTENTIFICACIÓN**. Es la propiedad de conocer que la información recibida es la misma que la información enviada y que el que dice ser que los envió realmente los envió.

La información que circula, se procesa y se almacena en una red, esta sometida a varios tipos de amenazas, tales como espionaje o acceso no autorizado a información, interrupción del flujo de información, copia de la información, alteración de la información, destrucción de información o interrupción de los servicios. Al implantar un sistema de seguridad debemos tener en mente las siguientes desventajas: degradación del desempeño, menor flexibilidad, restricción de servicios, cambio en muchos programas en las estaciones de trabajo, mayor complejidad para que los usuarios funcionales utilicen los recursos y mayores costos de personal, software y hardware.

### 1.4.3 Protocolo TCP/IP

Los cuales no fueron concebidos teniendo en cuenta aspectos de seguridad.
En tal sentido deben tenerse la optima seguridad sobre sus componentes:

- Protocolo para Transporte de Datos seguro
- Transferencia de Ficheros
- Terminal Remoto
- Correo Electrónico
- WWW (World Wide Web)

Se tiene que tener una visión sobre los protocolos más importantes de la familia TCP/IP, profundizando en su funcionamiento Interno y Especificaciones. Conocer los aspectos de Seguridad de los Protocolos TCP/IP, con la finalidad de controlarlos y hacer un uso seguro y racional de la Red.

## 1.5 Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como ***NESSUS***, ***SAINT*** o ***SATAN*** pasan de ser útiles a ser peligrosas cuando las utilizan ***crackers*** que buscan información sobre las vulnerabilidades de un host o de una red completa.

Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada *Security through obscurity*, se ha demostrado inservible en múltiples ocasiones. Si como administradores no utilizamos herramientas de seguridad que muestren las debilidades de nuestros sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por tanto, hemos de agradecer a los diseñadores de tales programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas mas seguros.

### 1.5.1 Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar `atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave `especial', con el objetivo de perder menos tiempo al depurar el sistema.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

### 1.5.2 Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores mas comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado UID o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el ***root***, o el programa que contiene la bomba esta setuidado a su nombre, los efectos obviamente pueden ser fatales.

### 1.5.3 Canales cubiertos

Los canales cubiertos son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D, ya que suele ser mucho mas fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico; sin embargo, es posible su existencia, y en este caso su detección suele ser difícil: algo tan simple como el puerto ***finger*** abierto en una máquina puede ser utilizado a modo de ***covert channel*** por un pirata con algo de experiencia.

### 1.5.4 Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a si mismo en otros programas.
Todo el mundo conoce los efectos de los virus en algunos sistemas operativos de sobremesa.

Ciertos virus, especialmente los de boot, pueden tener efectos nocivos, como dañar el sector de arranque; aunque se trata de daños menores comparados con los efectos de otras amenazas, hay que tenerlos en cuenta.

### 1.5.5 Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por si mismo a través de redes, en ocasiones portando virus o aprovechando ***bugs*** de los sistemas a los que conecta para dañarlos.

Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el ***Internet Woorm***, un gusano que en 1988 causo perdidas millonarias al infectar y detener mas de 6000 máquinas conectadas a la red.

Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo mas que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

### 1.5.6 Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de el, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

### 1.5.7 Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el numero de copias acaba con los recursos del sistema (memoria, procesador, disco. . .), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran numero de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina.

### 1.5.8 Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de quetzales se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar un quetzal de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.

Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso mas habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya ordenadores dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, comentamos esta potencial amenaza contra el software encargado de estas tareas.

## 1.6 Empresa Mediana

Características:

- Cuantitativa: Calidad del personal o facturación
- Cualitativa: El C.E.D (***comitte for economic development***) indica que una empresa es mediana si cumple con dos o más de las siguientes características:

Administraciones independientes (generalmente los gerentes son también propietarios).

- Capital suministrado por propietarios.
- Fundamentalmente área local de operaciones.
- Tamaño relativamente pequeño dentro del sector industrial que actúa.
- Entre 50 y 500 empleados

### 1.6.1 Ventajas de la mediana empresa

- Aseguran el Mercado de trabajo mediante la descentralización de la mano de la mano de obra.
- Tienen un efecto socioeconómico importante ya que permite la concentración de la renta y la capacidad productiva desde un número reducido de empresas hacia uno mayor.
- Reducen las relaciones sociales a términos personales más estrechos entre el empleador y el empleado favoreciendo las conexiones laborales ya que, en general, sus orígenes son unidades familiares.

- Presentan mayor adaptabilidad tecnológica a menor costo de infraestructura.

- Obtienen economía de escala a través de la economía interempresaria, sin tener que reunir la inversión en una sola firma.

### 1.6.2 Desventajas de la mediana empresa

- Falta de financiamiento adecuado para el capital-trabajo como consecuencia de la dificultad de acceder al Mercado financiero.
- Tamaño poco atrayente para los sectores financieros ya que su capacidad de generar excedentes importantes con relación a su capital no consigue atrapar el interés de los grandes conglomerados financieros.
- Falta del nivel de calificación en la mano de obra ocupada.
- Dificultades para desarrollar planes de investigación
- Se le dificulta a la mediana empresa hacer frente a las complicadas y cambiantes formalidades administrativas y fiscales, a las trabas aduaneras, todo lo cual le insume costo de adecuación más alto que las grandes empresas y les dificulta poder mantenerse en el Mercado.

## 1.7 La grande empresa

Se compone básicamente de la economía de escala, la cual consiste en ahorros acumulados por la compra de grandes cantidades de bienes. Estas corresponden a las grandes industrias metalúrgicas, automovilísticas, distribuidoras y generadoras de energía, compañías de aviación. En su mayoría son inyectadas por el Estado y generan una minoría de los empleos de un país. Su número de empleados oscila entre los 300 y 500.

### 1.7.1 Ventajas de la grande empresa

- Favorecen la balanza comercial con las exportaciones de los bienes generados.
- Poseen facilidad de financiamiento, por dar mayor garantía a los conglomerados financieros del pago de la deuda.
- Constan de la mayoría de profesionales de una sociedad.
- Se forman de sustanciosos montos de capital.
- Las barreras de entrada son relativamente escasas debido a la gran cantidad de mano de obra.
- Está basada en esquemas automatizados con mecanismos de control formalizados.

### 1.7.2 Desventajas de la grande empresa.

- Son víctimas del descenso de la economía lo cual genera la disminución en los salarios y sueldos.
- No satisfacen las necesidades especiales de una sociedad, por ser consideradas como una actividad no rentable.
- Se ve acechada por la burocratización.
- Los circuitos de información y las redes de comunicación son lentos y complejos.
- Desajustes entre las decisiones tomadas por los mandos medios y el empresario.

## 1.8 Router

Un router es un elemento de red, que permite cambiar de red. Debemos de darle siempre la puerta de enlaces. Y tiene por tanto una tabla de rutas.

**Tipos:**

1. **Router Adsl:** Es el router que nos proporciona el proveedor de internet (ISP).
2. **Router Software:** Es una pc que permite pasar los paquetes de una red a otra. Linux da soporte para este tipo de software, llamado reenvio (forwarding).
3. **Router Hardware:** Es un router que permite pasar de una subred a otra. Hace de enmascaramiento. Es una opción interesante si la red es nueva, y no se disponen de ordenadores antiguos para hacerlos por software.

Los router tienen dos ips, por lo que permite comunicarse con las redes de esas ips.

## 1.9 Concentradores: Hub, Switch

Un concentrador es un dispositivo que permite conectar máquinas para estar en red. Un concentrador no tiene dirección ***IP***.

Los ***hubs*** son dispositivos que retransmiten la información por todas las bocas o conexiones. A diferencia de los switch que son más inteligente, y solo mandan los datos por la boca en donde se encuentra esa IP.

Un switch, es un dispositivo de la capa 2. De hecho, el *switch* se denomina puente multipuerto, así como el ***hub*** se denomina repetidor multipuerto.

La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones *MAC* y los hubs no toman ninguna decisión.

Como los *switches* son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente. Los switches hacen esto “conmutando” datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos por medio de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

Esto hace que la **LAN** sea más lenta. A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48, o conectando 2 de 24 en serie), dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia entre un hub y un *switch* está dada por lo que sucede dentro de cada dispositivo. El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total. Básicamente un Switch es un administrador inteligente del ancho de banda.

### 1.10 Bastions Hosts

Denominaremos como Bastion Host a un sistema informático catalogado como punto peligroso en la seguridad de nuestro red informática. En base, dispone de una serie de medidas que le diferencia del resto, tales como mejores auditorias, monitorización del sistema, control de accesos al mismo (conexiones de la red interna, conexiones de la red externa…).

Este sistema debe haber sufrido un proceso de ***testing*** para catalogar posibles fallos no solo en seguridad, sino también en el propio software que utiliza.

Normalmente se suele permitir el paso del tráfico de red autorizado a través del BH debido a que este nos detallara todo en todo momento, y además conociendo correctamente su funcionamiento, podremos asegurar en un gran margen que el sistema esta preparado para evitar posibles ataques o accesos no deseados a nuestra red interna. Un Bh deberá incluir, entre otros, una serie de normas de seguridad.

### 1.11 Firewalls (Cortafuegos – FW)

Básicamente, podrías asimilar un firewall a un router al que se le añade seguridad. Esa seguridad hace que para algunas conexiones o paquetes o aplicaciones que tu le defines en lo que se llama política de seguridad, el router se niegue a mandarlo al otro lado. Esto puede valer tanto para cosas que vienen de fuera hacia dentro (lo más habitual) como de cosas que van de dentro hacía afuera.

# 2. SEGURIDAD DE LA INFORMACIÓN

La seguridad tiene su nacimiento con la aparición de los ataques a la información por parte de intrusos interesados en el contenido de ésta.
El objetivo de la seguridad de la información es:

- Mantener el secreto, evitando los accesos no autorizados.
- Mantener la autenticidad, evitando modificaciones no autorizadas.
- Dentro del concepto de seguridad debemos distinguir la Seguridad Física de la Seguridad
- Lógica, y para tener un concepto mas claro, detallaremos a continuación cada una de ellas.

## 2.1 Seguridad Física

La Seguridad física comprende el aspecto del hardware, la manipulación del mismo, así como también el ambiente en el cual se van a instalar los equipos. Para garantizar la seguridad de los mismos podríamos considerar los siguientes criterios:

- . Uso del equipo por personal autorizado.
- Solo podrá tener acceso al equipo aquella personal que cuente con conocimientos mínimos sobre computación.
- Tener más de un servidor de *base de datos,* lo cual asegurará la integridad total de la información.
- Ubicación de las instalaciones, la cual debe cumplir las normas internacionales de calidad (ISO 9000).

- Control de alarma la cual notifique en todo momento sobre la integridad física del sistema.

## 2.2 Seguridad Lógica

La seguridad lógica comprende el aspecto de los sistemas, tanto operativos como de información. Dentro de las medidas a tomar para garantizar la seguridad de los mismos se recomienda las siguientes:

- Construcción de contraseñas en diversos niveles del sistema, donde permita solo el acceso en base a niveles de seguridad de usuarios con permiso.
- En base al sistema operativo que use como plataforma, utilizar algoritmos que generen claves para poder encriptar los archivos de contraseñas dentro del sistema, me permita mayor seguridad en un entorno de red.

- Generar un módulo del sistema para la emisión de reportes para el administrador del sistema, en donde se muestre tablas de uso del sistema, usuarios y los niveles de acceso por parte de los tales para poder determinar el uso y acceso al sistema.

- Es necesario contar con el diseño de módulos que ejecuten un Control de alarma la cual notifique en todo momento sobre la integridad de la información del sistema.

## 2.3 Respuesta frente a violaciones de los Sistemas

Hay un gran número de respuestas, eficaces y menos eficaces, que una Empresa o Institución puede elegir tras la comprobación de una violación de la seguridad Informática.

Siempre que una empresa sufra un incidente que pueda poner en compromiso la seguridad informática, las estrategias de reacción pueden recibir la influencia de dos presiones opuestas.

- Si la Empresa o Institución teme ser lo suficientemente vulnerable, puede elegir una estrategia del tipo *"*Proteger y Proceder*"*. Este planteamiento tendrá como objetivo principal, la protección y preservación de las instalaciones de la empresa, y la vuelta a la normalidad para sus usuarios tan pronto como sea posible.

  Prevenir futuros accesos, y empezar de inmediato la valoración de daños y la recuperación. El mayor inconveniente es que a menos que el intruso sea identificado, puede volver a través de una ruta diferente, o bien atacar a otro.

  Esta acción se tomará:

  - Si los activos no están bien protegidos.
  - Si una intrusión continuada puede provocar un riego financiero.
  - Si no se quiere proceder judicialmente.
  - Si el trabajo de los usuarios es vulnerable.

- El otro planteamiento, “Perseguir y Procesar”, es la filosofía opuesta. La meta principal es la de permitir que los intrusos continúen con sus actividades en la empresa, hasta que se pueda identificar a las personas responsables.

Esto solo es aplicable si se cumple con los siguientes requisitos.

- Si los sistemas están bien protegidos.
- Si existen buenas copias de seguridad.
- Si se trata de un ataque que se produce con frecuencia.
- Si puede controlarse el acceso del intruso.
- Si se quieren llevar a cabo acciones judiciales

## 2.4 La Seguridad Informática

El concepto exacto de Seguridad Informática es difícil de proporcionar, debido a la gran cantidad de factores que intervienen. Sin embargo es posible enunciar que Seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

### 2.4.1 Propiedades de la Seguridad Informática

La Seguridad Informática debe vigilar principalmente las siguientes propiedades:

- **Privacidad** – La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial.

- **Integridad** – La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

- **Disponibilidad** – La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio ( *Denial of Service o DOS*) o **tirar** el servidor.

### 2.4.2 Áreas de Administración de la Seguridad

Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes rubros. Estos son:

- **Autenticación.**- Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

- **Autorización.**- Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

- **Auditoria.**- Se refiere a la continua vigilancia de los servicios en producción.

Entra dentro de este rubro el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Para ejemplificar lo anterior, tomemos el ejemplo de una compañía ficticia a la que llamaremos “Servicios de Cómputo”. Esta compañía dispone de un servidor donde corre el software a través del cual se lleva a cabo el procesamiento de las nóminas y el control de recursos humanos. (Ambos muy relacionados).

Autenticación se refiere a que sólo las personas de esos departamento tengan cuentas de acceso a dichos equipos, puesto que sería peligroso que algún otro departamento lo tuviera. El responsable de los equipos de cómputo llevaría a cabo la labor de Autorización, al no permitir que todas las personas responsables de recursos humanos tuvieran acceso a las Bases de Datos de Nóminas, si no lo necesitan.

La Auditoria se lleva a cabo al establecer políticas de uso y acceso a los recursos, así como reglamentos que rijan la no-divulgación de información confidencial. También aquí se debe llevar un registro de los recursos utilizados para prevenir, por ejemplo, que un uso del 100% en un disco provoque que el sistema deje de funcionar. Debe vigilarse también los intentos de acceso legal e ilegal al mismo.

### 2.4.3 Clasificación de los Factores que Intervienen en Seguridad

**La seguridad en un sistema está determinada por**

#### 2.4.3.1 El factor Organizacional

##### 2.4.3.1.1 Usuarios

Tipo de usuarios que se tienen Reglamentos y políticas que rigen su comportamiento Vigilar que esos reglamentos y políticas se cumplan, y no queden sólo en papel.

##### 2.4.3.1.2 La alta dirección

- Inversión en capacitación de los administradores
- Apoyo económico orientado a la adquisición de tecnología de seguridad.
- Negociar acuerdos de soporte técnico con los proveedores de equipo.

#### 2.4.3.2 El factor software

##### 2.4.3.2.1 La Aplicación

- Vigilar que tenga mecanismos para control de acceso integrados
- Observar las facilidades de respaldo de información que se tienen
- Establecer qué tan crítica es la aplicación y desprender su disponibilidad.

#### 2.4.3.2.2 El Sistema Operativo

- Mostrar preferencias por los sistemas abiertos (UNIX)
- Vigilar que soporte estándares de seguridad como C2
- Observar las recomendaciones del fabricante y aplicar los parches que libere.
- Vigilar siempre las bitácoras
- Mantenerse informado sobre las alertas de seguridad

#### 2.4.3.2.3 Software de red

- Vigilar de cerca las estadísticas de acceso y tráficos de la red.
- Procurar implementar cortafuegos (firewalls), pero no confiar en ellos
- En la medida de lo posible, apoyar las conexiones cifradas.

### 2.4.3.3 El Factor Hardware

#### *2.4.3.3.1 Hardware de Red*

- Elegir adecuadamente el tipo de tecnología de transporte (*Ethernet*, FDDI, etc.).
- Proteger muy bien el cableado, las antenas y cualquier dispositivo de red.
- Proporcionar periódicamente mantenimiento a las instalaciones

#### 2.4.3.3.2 Servidores

- Mantenerlos en condiciones de humedad y temperatura adecuadas.
- Establecer políticas de acceso físico al servidor.
- El mantenimiento también es importante aquí.

### 2.4.4 Principales Métodos de Protección

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda (pro actividad).

#### 2.4.4.1 Sistemas de detección de intrusos

Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, en base a la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

#### 2.4.4.2 Sistemas orientados a conexión de red

Aquí están considerados los cortafuegos (*Firewall*) y los *Wrappers*, los cuales monitorean las conexiones de red que se intentan establecer con una red o un equipo en particular, siendo capaces de efectuar una acción en base a datos como: origen de la conexión, destino de la conexión, servicio solicitado, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador vía correo electrónico.

#### 2.4.4.3 Sistemas de análisis de vulnerabilidades

Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que busquen acceso no autorizado al sistema.

#### 2.4.4.4 Sistemas de protección a la privacidad de la información

Herramientas que utilizan criptografía para asegurar que la información sólo es visible a quien tiene autorización de verla. Su aplicación es principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas podemos situar a *Pretty Good Privacy* (**PGP**), *Secure Sockets Layer* (**SSL**) y los certificados digitales tipo X.509.

#### 2.4.4.5 Sistemas de protección a la integridad de información

Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como *Message Digest* 5 (**MD5**) o *Secure Hash Algorithm* 1 (**SHA-1**), o bien sistemas que utilizan varios de ellos como *Tripwire*.

### 2.4.5 Medidas aplicables en cualquier ambiente

#### 2.4.5.1 Informar al usuario/administrador

El administrador, debe notificar a sus usuarios de los mecanismos de seguridad que se han implementado, y animar a los usuarios a utilizar estos mecanismos de seguridad, dando conocer las posibles consecuencias de no cumplir con ellos. Hacerles saber a los usuarios que si prestan su *password* están cometiendo una falta, y que igualmente serán responsables por los actos, de buena o mala fe, que alguien más realice con su *cuenta* o sistema, si logra adivinar dicho *password*.

El usuario por otra parte, debe considerar todas las disposiciones y recomendaciones que brinda el Administrador de los sistemas de la institución, además el usuario debe hacer conocer al administrador, cualquier sospecha de violación de cualquier recurso al que el usuario tiene acceso legítimo.

#### 2.4.5.2 Respaldar siempre

Sin embargo no basta con efectuar respaldos. Una buena política de respaldos contempla, entre otras cosas: tiempos óptimos de respaldo y recuperación, periodicidad del respaldo y verificación de integridad (de nada sirve un respaldo no íntegro), necesidad de duplicidad y expiración de los respaldos.

El usuario, debe además hacer su propio respaldo adicional, al que hace el administrador siempre que le sea posible, dependiendo también de la importancia de su información.

#### 2.4.5.3 Realizar verificaciones no predecibles

Por ejemplo, si un ladrón conoce las horas a las que la guardia de un banco hace su ronda de vigilancia, seguramente decidirá no robarlo a esas horas. Lo mismo sucede con los sistemas; si se hacen verificaciones periódicas, y alguien más conoce cómo y cuándo se realizan estas verificaciones, entonces será necesario además hacer verificaciones de periodicidad no predecible, a fin de obtener una estadística más real del comportamiento del sistema.

#### 2.4.5.4 Leer las bitácoras

Las bitácoras del sistema reflejan lo que ocurre en el mismo. De nada sirve tenerlas si no son leídas. Ahí es donde pueden descubrirse ataques no exitosos perpetrados contra su sistema.

#### 2.4.5.5 Aplicar “parches” o tener las últimas versiones del software

Las vulnerabilidades sobre algún producto o plataforma, pueden dar la vuelta al mundo rápidamente gracias a Internet. Es recomendable por ello contar siempre con la versión más actualizada del software, o bien aplicar los *“parches”* respectivos cuando son liberados. En este rubro, el *software* libre (*Linux/Apache*) cuenta con una ventaja sobre software comercial, pues el tiempo de respuesta es dramáticamente más rápido para el *software* libre.

#### 2.4.5.6 Leer noticias sobre seguridad

Si su proveedor mantiene una lista de seguridad, únase a ella. Así mismo suscríbase a listas que le informen sobre seguridad en general de modo que obtenga un panorama amplio pero conciso sobre el tema.

### 2.4.5.7 Cancelación de cuentas de accesos

Todo lo anterior no sirve si personas que han trabajado para la institución poseen sus cuentas de acceso después de haber dejado de colaborar con ella. Las estadísticas demuestran que un 85% de los ataques de seguridad son realizados desde dentro de la institución, o bien a través de cuentas de personal que estuvo dentro de ella.

Este interés por la seguridad de las redes se ha extendido tanto que ha nacido una palabra nueva que se utiliza en el mundo de la seguridad de las comunicaciones. La palabra es **COMSEC** (***Comunications Security***) e incluye todo lo que hace referencia a la seguridad en todas sus formas de comunicación, fax, telex, telefonía móvil, vía satélite, etc.

Los principales puntos a tratar sobre la seguridad de las redes de comunicación son:

- Autenticidad de usuarios y sistemas.
- Integridad de los mensajes.
- Privacidad de la información.
- Disponibilidad y rendimiento.
- . **La autenticidad**. Comprende la identificación y su validación.

Cada sistema debe poder demostrar al otro que es quien dice ser, que no lo engaña. De esta manera evitaremos una falsa respuesta del mensaje que hemos enviado. El problema se complica en sistemas distribuidos o en redes *multihost*, donde el usuario entra en un sistema y la autenticidad se necesita en el otro extremo de la red.

Este debe fiarse que la información que le envía el primer sistema es auténtica, y necesita estar seguro de que la información no ha sido cambiada. La Autentificación se realiza en cascada, lo que se llama una red ***trusted***. Un mecanismo que soluciona el problema recibe el nombre de *Pasaporte*. Otro mecanismo es el del *Paso fiable*. En todos los servicios de autentificación se usa la criptografía.

- Para asegurar la *integridad* podemos usar mecanismos tan sencillos como registrar la hora de emisión o la numeración secuencial de los mensajes, o utilizando la criptografía ***end-to-end*** o ***point-to-point***.
- Para el tratamiento de la *confidencialidad*, la solución es la criptografía. Cuando sólo parte del mensaje se debe cifrar, se utiliza el cifrado selectivo.
- . La disponibilidad de la red se ve afectada por defectos de diseño, fallos del sistema, etc. Emisor y receptor pueden perder la comunicación sin darse cuenta, para evitarlo se usa la técnica de intercambio de mensajes especiales.

Cuanto mas a menudo son enviados estos mensajes, más seguro se estará de la continuidad del servicio. Pero esto produce una sobrecarga del servicio y hace bajar el rendimiento. Por lo tanto, es necesario llegar a un equilibrio entre seguridad y rendimiento.

### 2.4.6 Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los **RR.HH**.

# 3. TÉCNICAS Y TECNOLOGÍAS DE SEGURIDAD A NIVEL DE RED

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Por sí mismas, las aplicaciones de software y los productos de hardware que componen la red informática de una empresa no constan de política de seguridad, y, sin embargo, son elementos esenciales en el establecimiento de la seguridad de las empresas.

Las herramientas que tienen como fin la protección de las redes informáticas han sufrido una continua evolución durante las dos últimas décadas, prácticamente el mismo tiempo que se lleva intentando “piratearlas” y violar las redes informáticas En la actualidad se cuenta con diversos métodos que garanticen la seguridad de nuestra información, dentro de los mas difundidos tenemos a los siguientes:

## 3.1 Criptología

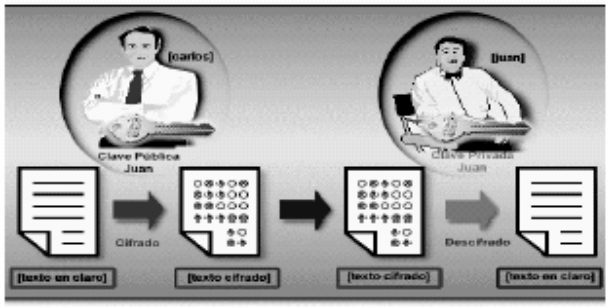
Las amenazas que sufre la información durante su proceso, almacenamiento y transmisión son crecientes y complejas. Para contrarrestarlas se han desarrollado numerosas medidas de protección, que se implementan en el equipo físico o lógico mediante los denominados mecanismos de seguridad.

La lista de estos mecanismos es muy numerosa y en ella encontramos, entre otros muchos: Identificación y autenticación de usuarios, control de accesos, control de flujo de información, registros de auditoria, cifrado de información, etc. De éstos, el mecanismo por excelencia es el de cifrado de la información.

La Criptología se divide en dos ciencias importantes: **la Criptografía** *y el* **Criptoanálisis**. La Criptografía se puede traducir como *La manera de escribir raro* (Criptos, extraño; Graphos, escritura).

Es una ciencia que se ocupa principalmente de conseguir que nuestros mensajes sean comprensibles exclusivamente para aquellos que nosotros deseemos e inteligibles para el resto de la Humanidad, aplicando para ello procedimientos matemáticos o claves. El texto inicial, el de partida, recibe el nombre de texto claro. El que resulta de aplicarle el algoritmo criptográfico, es el texto cifrado.

**Figura 1. La criptografía**



Ej. Proceso de cifrado de mensajes

El Criptoanálisis es la ciencia que se dedica a quebrantar el cifrado obtenido de la Criptografía.

Una de las propiedades necesarias que debe tener un algoritmo criptográfico, es que cada texto , al aplicarle el algoritmo de descifrado con la misma clave de cifrado o la clave de descifrado relacionada, debe convertirse en el mismo texto claro del que procede.

Históricamente dos los militares y los cuerpos diplomáticos han utilizado y han contribuido, de una manera importante, en el arte de la Criptología.

Sin embargo, hoy en día su interés merece una atención especial para todos los sectores públicos o privados para los que la información es algo muy valioso.

Con la introducción de las computadoras, la necesidad de herramientas automatizadas para proteger archivos y otro tipo de información almacenada en las computadoras es evidente.

La implementación de sistemas distribuidos y la utilización de redes entre un usuario Terminal y una computadora o entre computadoras afecta a la seguridad. Las medidas de seguridad en una red de datos son necesarias para proteger los datos durante la transmisión.

### 3.1.1 Los sistemas de cifrado modernos se clasifican en

#### 3.1.1.1 **Simétricos o de clave secreta**:

La clave utilizada es la misma tanto para cifrar como para descifrar. El algoritmo debe ser público, pero la clave debe ser siempre secreta.

#### 3.1.1.2 Asimétricos o de clave pública

La clave para cifrar es pública y la de descifrar secreta, y están relacionadas entre sí. El algoritmo puede ser público o secreto. Cualquier persona que disponga de la clave pública puede cifrar el mensaje, pero solo el que ha generado las claves y tiene la clave secreta puede descifrar el mensaje.

No hay ningún algoritmo irrompible. El algoritmo puede ser más o menos duro. La dureza de un algoritmo se mide teniendo en cuenta su factor de trabajo, que es la cantidad necesaria de trabajo para descubrir las claves.

Dentro de la criptografía moderna, es decir, aquella en que los algoritmos operan en bits, dos son los algoritmos más conocidos y utilizados, el DES y el RSA.

### 3.1.2 Algoritmos más utilizados

#### 3.1.2.1 DES

Las siglas DES corresponden a las iniciales de Data ***Encryption Standard***. Este algoritmo se convirtió en un estándar y se utiliza en gran parte de los sistemas informáticos que precisan de un cierto grado de protección, a pesar de las restricciones que el gobierno de los Estados Unidos impuso para su comercialización fuera del país. El algoritmo consiste en un complejo sistema de operaciones matemáticas basado en sustituciones y permutaciones de bits en función de una clave. El conocimiento del algoritmo no permite descifrar la información cifrada; de hecho éste es de dominio público.

El proceso de cifrado trabaja con bloques de 64 bits y una clave de otros 64 bits, siendo 56 de la clave en sí y los restantes 8 de paridad impar para detección de errores. Tras la aplicación de un algoritmo, que efectúa una serie de complejas permutaciones, sustituciones y operaciones lógicas, los 64 bits de información se transforman en otros tantos cifrados. Dividiendo la información en bloques de este tamaño y realizando la misma operación para cada bloque, se consigue cifrar un texto completo.

**Seguridad del algoritmo**

Cuando el algoritmo DES se presentó existían numerosas dudas sobre si contendría "puertas traseras" que permitiesen al gobierno de los Estados Unidos descifrar todo tipo de comunicaciones. Más tarde se demostró que estas dudas no tenían fundamento; sin embargo, el tamaño de la clave utilizada hace que el algoritmo sea vulnerable y esta situación se agrave más según vaya incrementándose la potencia de los ordenadores y disminuyendo su precio.

La única forma conocida de violar el algoritmo es probar a descifrar la información con todas las posibles claves. Puesto que constan de 56 bits habría que probar con 2E56, es decir, 72.057.594.037.927.936 claves distintas. Suponiendo que se dispone de un ordenador de gran potencia capaz de generar y probar un millón de claves por segundo, se requerirían unos 72.000 millones de segundos lo que, traducido a años, serían 2.285.

Sin embargo, utilizando un superordenador con multitud de procesadores en paralelo se podrían generar todas las claves en tan sólo unas horas, aunque este tipo de ordenadores no está al alcance de cualquiera.

#### 3.1.2.2 RSA

El algoritmo RSA fue desarrollado en los años setenta por ***Rivest, Shamir*** y ***Adleman***, de cuyas iniciales toma su nombre, y está basado en el problema de hallar los factores primos de grandes números.

Frente a sus diversas ventajas sobre los sistemas de clave privada presenta el inconveniente de la carga que supone al sistema, puesto que se basa en operaciones que consumen mucho tiempo de proceso. Además, cada vez el tamaño de los números a emplear debe ser mayor para garantizar la inviolabilidad del sistema debido al incremento en la potencia de cálculo de los ordenadores.

La encriptación ***RSA*** es un sistema de encriptación de clave pública, y se trata de una tecnología patentada en los Estados Unidos, por lo que no puede utilizarse sin licencia.

Sin embargo, el algoritmo se hizo público antes de ser adjudicada la patente, lo que dio lugar a que la encriptación ***RSA*** pudiera utilizarse en Europa y Asia sin necesidad de pagar royalties. La encriptación ***RSA*** está creciendo en popularidad, y se considera bastante segura frente a ataques de fuerza bruta.

**Seguridad del algoritmo**

La seguridad del algoritmo radica en el tamaño de un número n, que es el producto de los números primos. No es aconsejable trabajar con valores inferiores a 154 dígitos o lo que es lo mismo 512 bits y para aplicaciones que requieran un alto grado de seguridad 1024 bits (308 dígitos) ó incluso 2048.

El algoritmo más rápido conocido para factorizar un número se debe a ***R***. ***Shroeppel***, que permite hacerlo con un número de operaciones definido por la expresión:

**ev(ln (ln n))ln n**

Por ejemplo con un número de 300 dígitos. Suponiendo que se dispone de un ordenador de gran potencia capaz de realizar un millón de operaciones por segundo, se requerirían 4800 billones de años para factorizar el número. Aun dividiendo el problema en partes y utilizando múltiples sistemas o un superordenador con multitud de procesadores en paralelo, con 300 dígitos la seguridad está garantizada.

- **Aplicaciones**

La Criptología se utiliza también para la autentificación de mensajes y para firmas digitales.

El método de la autentificación consiste en incorporar al mensaje un código llamado MAC (***Modification Autentification Code***), que se calcula aplicando un algoritmo de cifrado al texto entero. El receptor hace lo mismo y compara el valor que le da con el que lleva el mensaje, si es igual, el mensaje se considera autentico.

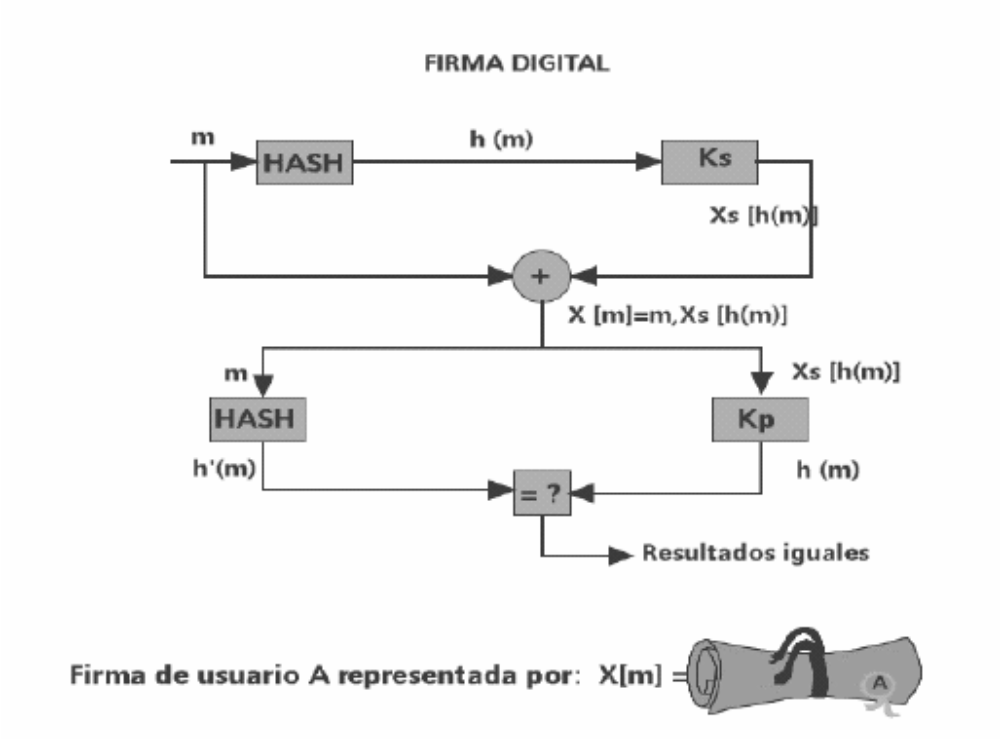
## 3.2 Firmas digitales

Una firma digital es un bloque de caracteres que acompaña a un documento, acreditando quién es su autor ("autentificación") y que no ha existido manipulación posterior de los datos (integridad).

El proceso de la firma digital lo realiza un software (por ejemplo PGP, Eudora, Outlook,...) que aplica un algoritmo sobre el texto a firmar, obteniendo un extracto (número) de longitud fija, y único para ese mensaje. Este extracto cuya longitud oscila entre 176 y 160 bits se somete a continuación al cifrado (RSA o DSS) mediante la clave secreta del autor, previa petición de contraseña.

Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función *hash* al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

**Figura 2. Esquema Firma Digital**




El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

### 3.2.1 Control de acceso

Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el emisor está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos.

Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

El mecanismo de control de acceso soporta el servicio de control de acceso.

### 3.2.2 Integridad de datos

Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

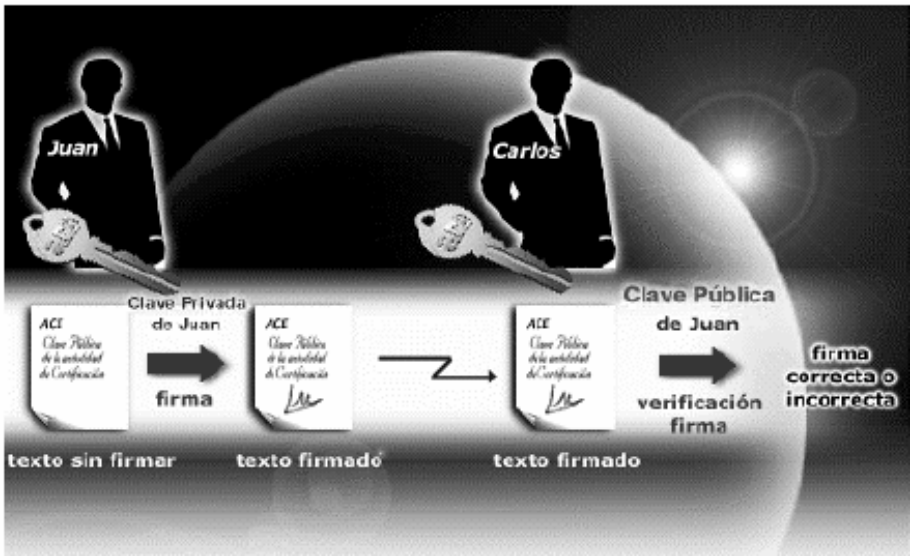
El mecanismo de integridad de datos soporta el servicio de integridad de datos.

Intercambio de autenticación. Existen dos grados en el mecanismo de autenticación:

- **Autenticación simple**. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.
- **Autenticación fuerte.** Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta.

Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

**Figura 3. Firma digital**




## 3.3 Firewalls

Si tu política de seguridad es ninguna, un firewall y un router es lo mismo. Si tienes algunas reglas que te interesa que cumpla tu router y que signifiquen que bajo ciertas circunstancias a algún tipo de tráfico debe impedírsele atravesarlo, tienes un firewall.

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con dos(2) o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Esa sería la definición genérica, hoy en día un firewall es un hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP / UDP / ICMP /... / IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall:

Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización conciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por módem (*dial-in módem calling*).

Ello no quiere decir que la instalación de un sistema de firewall permita la relajación de la seguridad interna de las máquinas, sino que se podrá distinguir fácilmente entre el interior y el exterior, pudiendo determinar qué comportamiento general se quiere para cada servicio.

Otra característica importante de estos sistemas es que permiten llegar donde los mecanismos de seguridad de los sistemas operativos a veces no pueden.

### 3.3.1 Beneficios de un firewall

Los firewalls manejan el acceso entre dos redes, si no existiera todos los hosts de la intranet estarían expuestos a ataques desde hosts remotos en Internet. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador de la red escogerá la decisión si revisar estas alarmas o no, la decisión tomada por este no cambiaría la manera de operar del firewall.

Otra causa que ha hecho que el uso de firewalls se halla convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el numero disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones CIRD (o direcciones sin clase), las cuales salen a Internet por medio de un NAT (***Network address traslator***), y efectivamente el lugar ideal y seguro para alojar el NAT ha sido el firewall.

Los firewalls también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido mas en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor ancho de banda.

Finalmente, los firewalls también son usados para albergar los servicios WWW y FTP de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

### 3.3.2 Tipos de Firewalls

#### 3.3.2.1 *Packet filter*, filtro de paquetes

Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones.

Normalmente se implementa mediante un router con dos interfaces de red, uno de cara al exterior y otro al interior, aunque podría utilizarse cualquier máquina con dos placas de red y un software adecuado para filtrado de los paquetes IP.

Al tratar paquetes IP, los filtros que podremos establecer serán a nivel de direcciones IP, tanto fuente como destino. Normalmente, se establece una lista de filtros por interfaz que se aplicarán a cada paquete independiente de los anteriores, o de si forma parte de una determinada comunicación para un cierto servicio.

Algunos filtros de paquetes permiten establecer filtros también a nivel de puertos TCP o UDP , con lo que se podrá filtrar qué servicios se dejan pasar o no.

- **Cortafuegos - filtro de paquetes ejemplarizado en un router**

La lista de filtros se aplican secuencialmente, de forma que la primera regla que el paquete cumpla marcará la acción a realizar (descartarlo o dejarlo pasar). La aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos.

Aunque no puede parecer importante lo es, pues tiene que ver con el tratamiento del '*address-spoofing'* uno de los ataques utilizados con más frecuencia para saltarse la protección establecida por un cortafuegos, que como hemos descrito antes, consiste en generar paquetes IP con direcciones falsas.

Los filtros de paquetes son una buena solución, pero tienen sus limitaciones a la hora de tratar los servicios como tales, pues para ellos cada paquete es independiente y no forma parte de ningún todo, por los tanto, de ningún servicio.

Además, existen servicios como DNS o FTP, que dificultan realizar una configuración segura de un filtro de paquetes.

Son muy pocos los sistemas de filtrado de paquetes que se basan en la propia información para aceptar o denegar un paquete. Esta posibilidad, aunque tiene un elevado coste, puede utilizarse por ejemplo, para evitar la entrada de archivos infectados con virus en una red interna.

- **Ventajas del filtrado de paquetes**

La protección centralizada es la ventaja más importante del filtrado de paquetes. Con un único enrutador con filtrado de paquetes situado estratégicamente puede protegerse toda una red. Si sólo existe un enrutador con salida a una red insegura, independientemente del tamaño de nuestra red interna, podrá controlarse todo el tráfico en dicho enrutador.

#### 3.3.2.2 Firewalls a nivel de aplicación

Es el extremo opuesto a los filtros de paquetes. En lugar de basarse en el filtrado del flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado para cada uno.

Es probablemente el sistema más seguro, ya que no necesita tratar complicadas listas de acceso y centraliza en un solo punto de gestión los servicios.

Y además permitir controlar y recoger información de cada uno de los servicios por separado.

Las pasarelas a nivel de aplicación son prácticamente la única solución efectiva para el tratamiento seguro de aquellos servicios que requieren permitir conexiones iniciadas desde el exterior (servicios como FTP, Telnet, Correo Electrónico).

En realidad, lo que se utiliza es una puerta de acceso para cualquier servicio. Al ser esta puerta de uso obligatorio, podemos establecer en ella los criterios de control que queramos.

Atravesada la puerta, puede ocurrir que la propia pasarela de nivel de aplicación ofrezca el servicio de forma segura o que establezca una conexión con el ordenador interno que realmente ofrece el servicio, teniendo en cuenta que éste último deber estar configurado para aceptar conexiones tan solo desde nuestra pasarela de nivel de aplicación para este servicio.

#### 3.3.2.3 Firewalls a nivel de circuito

Se basan en el control de las conexiones TCP y actúan como si fuesen un cable de red:

por un lado reciben las peticiones de conexión a un puerto TCP; y por otro, establecen la conexión con el destinatario deseado, si se han cumplido las restricciones establecidas, copiando los bytes de un puesto al otro.

Este tipo de cortafuegos suelen trabajar conjuntamente con los servidores 'proxi', utilizados para la acreditación, es decir, comprobaciones sobre máquina fuente, máquina destino, puerto a utilizar. Una acreditación positiva, significa establecer la conexión.

Son el tipo de cortafuego más adecuado para el tratamiento de las conexiones salientes.

#### 3.3.2.4 Cortafuegos basados en certificados digitales

Este tipo de cortafuegos basados en certificados digitales son extremadamente seguros y con una gran funcionalidad. Su popularidad no ha sido muy grande porque hasta hace poco tiempo no existían distribuidores de certificados digitales universales. Actualmente este defecto está cambiando a nivel mundial.

### 3.3.3 Decisiones de diseño básicas de un firewall

Hay varias consideraciones a tener en cuenta al momento de implementar un firewall entre Internet y una intranet (red LAN) Algunas de estas consideraciones son:

#### 3.3.3.1 Postura del firewall

Todo lo que no es específicamente permitido se niega. Aunque es una postura radical es la más segura y la mas fácil de implementar relativamente ya que no hay necesidad de crear accesos especiales a los servicios.

Todo lo que no es específicamente negado se permite. Esta no es la postura ideal, por eso es mas que todo usado para subdividir la intranet. No es recomendable para implementar entre una LAN e Internet, ya que es muy vulnerable.

#### 3.3.3.2 Política de seguridad de la organización

Depende mas que todo de los servicios que esta presta y del contexto en el cual esta.

No es lo mismo diseñar un firewall para una ISP o una universidad que para proteger subdivisiones dentro de una empresa.

#### 3.3.3.3 Costo del firewall

El costo del firewall depende del numero de servicios que se quieran filtrar y de la tecnología electrónica del mismo, además se necesita que continuamente se le preste soporte administrativo, mantenimiento general, actualizaciones de software y parches de seguridad.

### 3.3.4 Componentes de un firewall

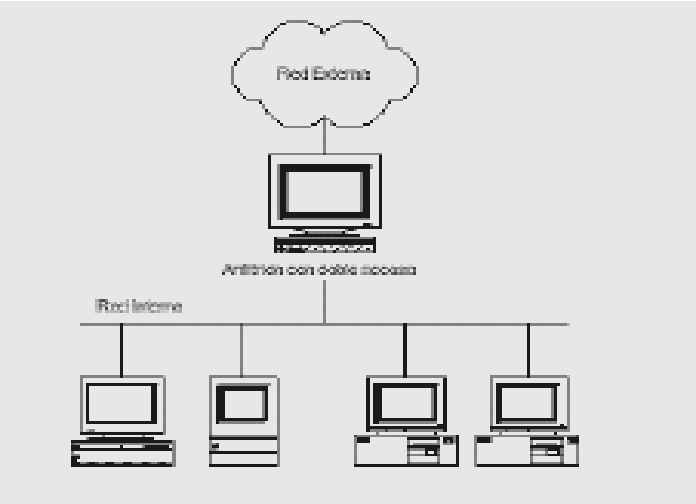
Los componentes típicos de un firewall son:

- Un enrutador que sirva única y exclusivamente de filtro de paquetes.
- Un servidor Proxy o gateway a nivel de aplicación (debido al costo, implementado comúnmente en una maquina Linux).
- El gateway a nivel de circuito.

### 3.3.5 Configuraciones de cortafuegos

Los tipos de cortafuegos que existen se han tratado de forma independiente, no como sistema. Cuando se realiza un sistema de cortafuegos, suelen emplearse varios o todos los tipo. Se hace así porque, cada uno de ellos trata la protección a un nivel distinto, desde los paquetes de red, pasando por los puertos de conexión, hasta el servicio propiamente dicho.

**Figura 4. Composición de una pasarela de aplicaciones con filtro de paquetes**




Existen múltiples variaciones sobre los esquemas de configuración. Algunos de ellos aportan un nivel mayor de seguridad, pero requieren la dedicación de un número mayor de recursos del sistema, con el consiguiente coste, mientras que otras reducen gastos a costa de la seguridad, pero siendo aún plenamente funcionales.

Se ha de encontrar la configuración adecuada a cada sistema, en función del nivel de seguridad que requiera la política de seguridad del sistema y el trabajo y los recursos que se quieran invertir en dicha seguridad. Esta configuración se conseguirá equilibrando esos dos factores de forma coherente.

#### 3.3.5.1 Host de Base Dual

En las redes de TCP/IP, el término host de base múltiple (*multi -homed host*) describe a un host que tiene varias tarjetas de interfaz de red (vea la figura 8).

Por lo general, cada tarjeta de interfaz de red se conecta a una red. Históricamente, este host de base múltiple también puede enrutar el tráfico entre los segmentos de la red. El término gateway se utilizó para describir la función de enrutamiento desarrollada por estos host de base múltiple.

Hoy en día, el término router se utiliza para describir esta función de enrutamiento, mientras que el término gateway se reserva para aquellas funciones que corresponden a las capas superiores del modelo OSI.

Si la función de enrutamiento en el host de base múltiple está inhabilitada, el host puede proporcionar aislamiento del tráfico de red entre las redes a las que está conectado, y cada red todavía podrá procesar aplicaciones en los hosts de base múltiple. Es más, si las aplicaciones lo permiten, las redes también pueden compartir datos.

Un host de base dual (*dual-homed host*) es un ejemplo, especial de host de base múltiple que cuenta con dos interfaces de red y tiene inhabilitadas las funciones de enrutamiento.

En la figura **9** se muestra un ejemplo de un host de base dual con las funciones de enrutamiento inhabilitadas.

El host A de la Red 1 puede tener acceso a la Aplicación A del host de base dual. De igual manera, el Host B puede tener acceso a la Aplicación B del host de base dual. Incluso, las dos aplicaciones de los hosts de base dual pueden compartir datos.

Es posible que los hosts A y B intercambien información a través de los datos compartidos en los hosts de base dual, y aún así no hay intercambio de tronco de red entre los dos segmentos de red conectados al host de base dual.

**Figura 5. Un host clásico de base múltiple**

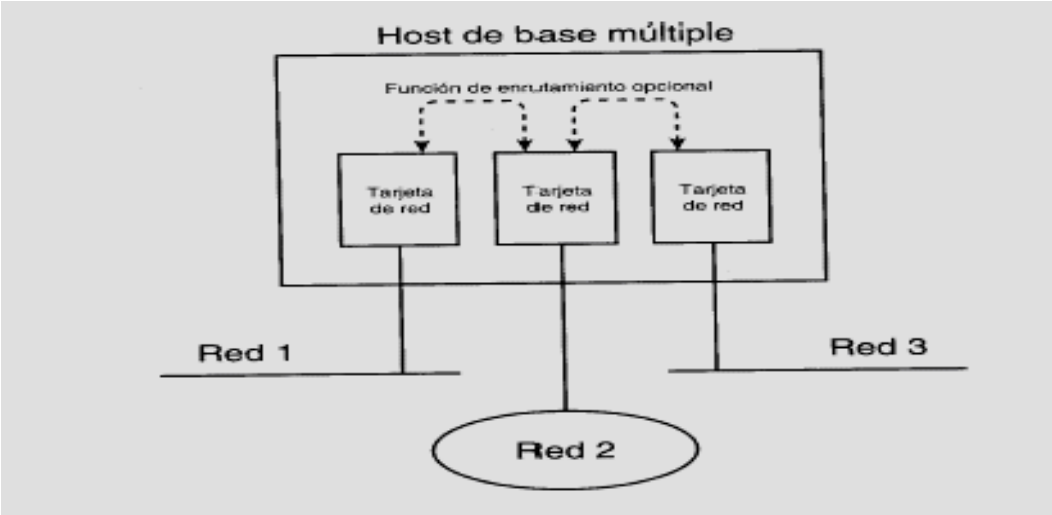
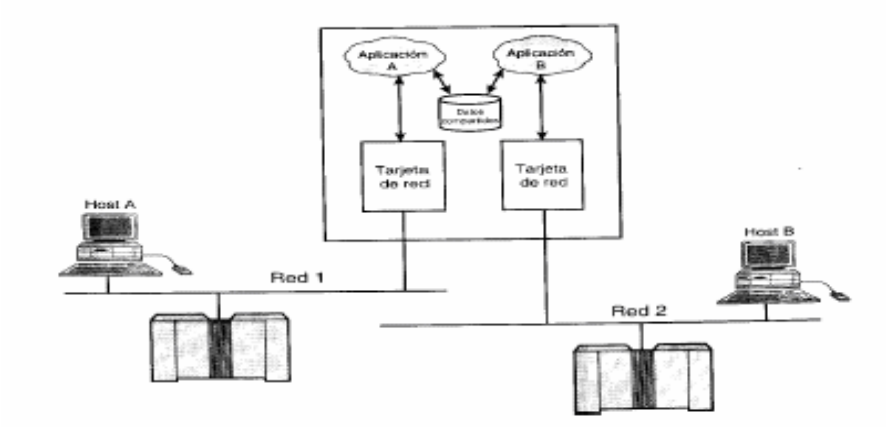


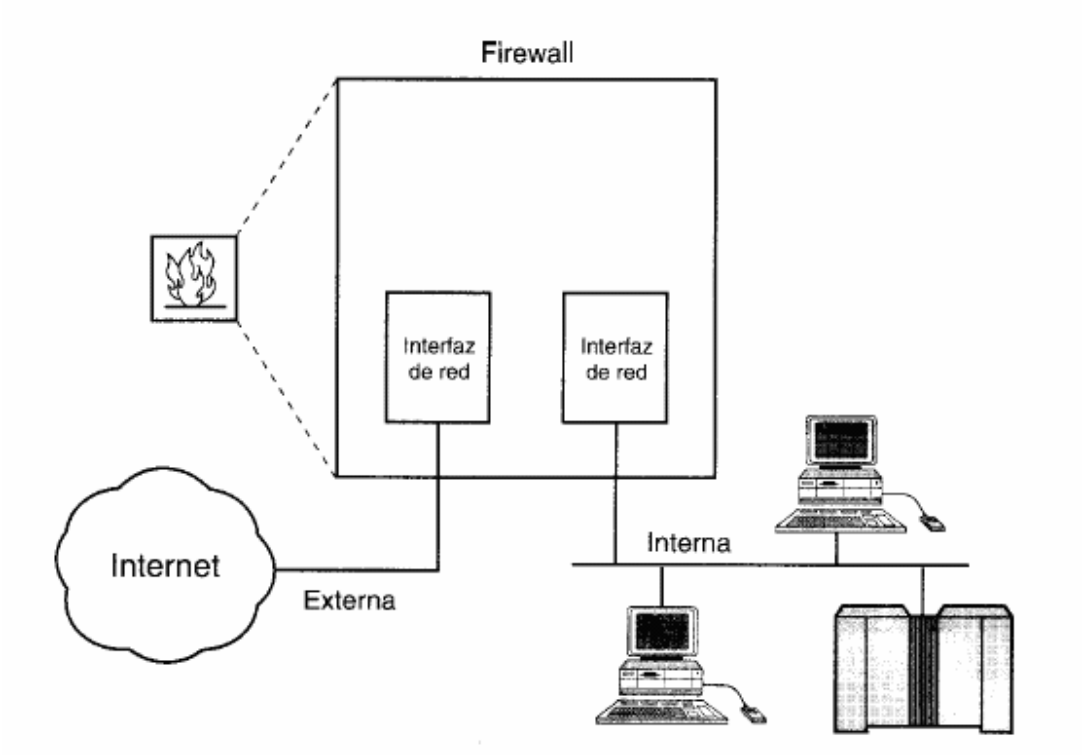
**Figura 6. Host de base Dual**




### 3.3.5.2 Host de Base Dual Como Firewall

El host de base dual puede utilizarse para aislar una red interna de una red externa no confiable (vea la figura 10). Debido a que el host de base dual no envía ningún tráfico de TCP/IP, bloquea completamente cualquier tráfico de IP entre la red interna y la red externa no confiable.

**Figura 7. Un host de base Dual como firewall.**




Los servicios de Internet, como correo y noticias, son esencialmente servicios de almacenamiento y envío. World Wide Web también puede considerarse como de almacenamiento y envío, pero los términos *cacheo* y *Proxy* se utilizan de manera más común en el vocabulario de Web. Si estos servicios se ejecutan en un host de base dual, pueden configurarse para transmitir servicios de aplicación de una red a otra. Si los datos de la aplicación deben cruzar la firewall, pueden configurarse los agentes emisores de aplicación para ejecutarse en el host de base dual (vea la figura **11**). Los agentes emisores de aplicación son un software especial utilizado para enviar las solicitudes de la aplicación entre dos redes conectadas. Otro método consiste en permitir que los usuarios se conecten al host de base dual, y luego acceder a los servicios externos desde la interfaz de red externa del host de base dual (vea la figura **12**).

Si se utilizan emisores de aplicación, el tráfico de la aplicación no puede cruzar la firewall de base dual a menos que el emisor de aplicación esté ejecutándose y que se haya configurado en la máquina de la firewall.

Se trata de una implementación de la política *Lo que no está permitido expresamente, está prohibido*. Si se le permite a los usuarios conectarse directamente con la firewall (vea la figura **12**), puede comprometerse la seguridad de la firewall. Esto se debe a que la firewall de base dual es un punto central de conexión entre la red externa y la red interna. Por definición, la firewall de base dual es la zona de riesgo.

Si el usuario selecciona una contraseña débil, o permite que su cuenta de usuario se comprometa, la zona de riesgo puede extenderse a la red interna, frustrando así el propósito de la firewall de base dual.

El administrador de seguridad inteligente prohibirá la creación de cuentas de usuario para tener acceso a la firewall. La firewall sólo debe utilizarse para autentificar usuarios para permitir que sus sesiones pasen a través de la firewall.

Si se conserva un registro apropiado de las conexiones de usuarios, es posible rastrear conexiones no autorizadas a la firewall cuando se ha descubierto una brecha de seguridad.

Sin embargo, si los usuarios no tienen permitido conectarse directamente a la firewall de base dual, cualquier intento de conexión directa de usuario se registrará como un evento digno de atención y una potencial brecha de seguridad.

Ejemplos de servicios de almacenamiento y envío son SMTP (Correo) y NNTP (Noticias). En la figura **13** se muestra una situación donde el host de base dual está configurado para proporcionar envío discrecional de mensajes de correo entre una red externa no confiable y una red interna. En la figura **14** se muestra una situación donde el host de base dual está configurado para proporcionar envío discrecional de mensajes de noticias entre servidores de una red externa no confiable y una red interna.

**Figura 8. Host de base dual con emisores de aplicación**

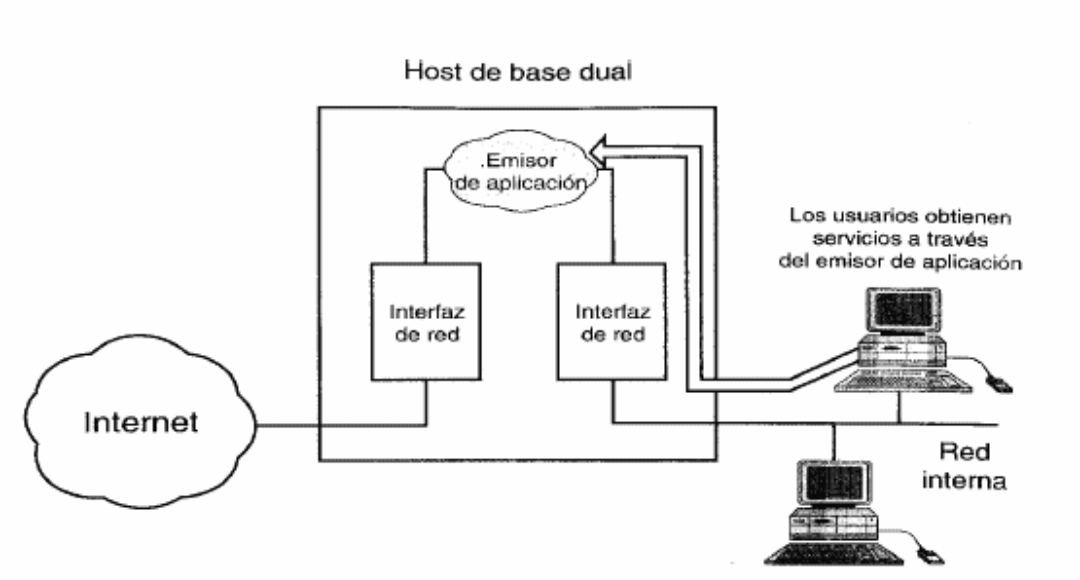


**Figura 9. Inseguridad introducida con la conexión de usuario estándar a un host de base dual.**

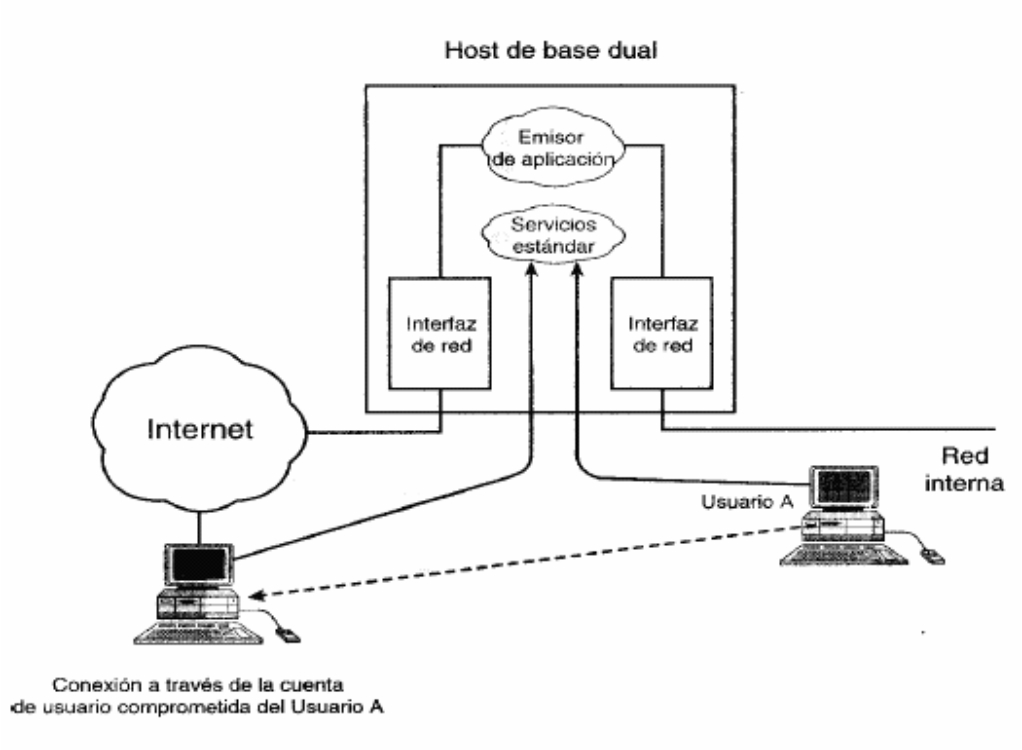
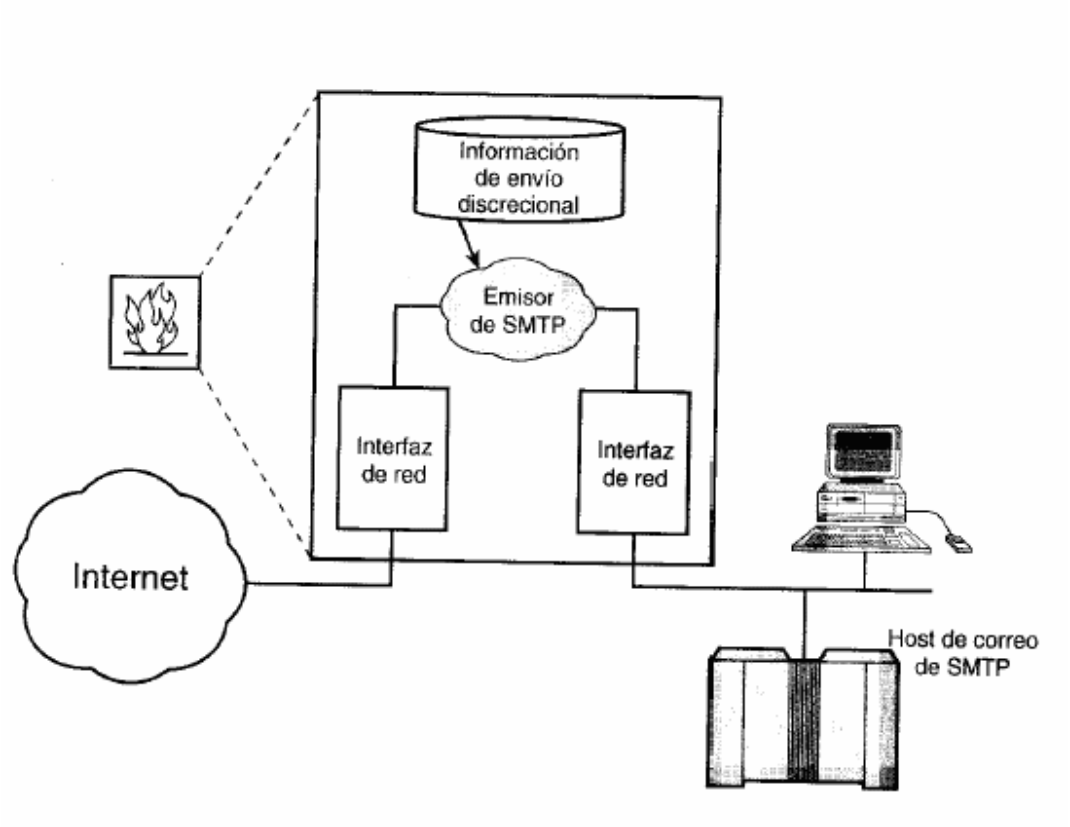


**Figura 10. Un host de base dual como emisor de correo.**




El host de base dual es la configuración básica utilizada en *firewalls*. El aspecto importante de los hosts de firewall de base dual es que se inhabilita el enrutamiento y que la única ruta entre los segmentos de red es a través de una función de capa de aplicación.

Si el enrutamiento se configura mal por accidente (o por diseño) de modo que se habilite el envío IP, es posible que se ignoren las funciones de la capa de aplicación de las firewalls de base dual (vea la figura 15).

La mayoría de las firewalls se construyen con base en máquinas Uníx. En algunas implementaciones de Unix, las funciones de enrutamiento están permitidas de manera predeterminada. Por lo tanto, es importante verificar que las funciones de enrutamiento de la firewall de base dual estén inhabilitadas o, si no lo están, usted debe saber cómo inhabilitarlas.

**Figura 11. Hot de base dual como emisor de Noticias**

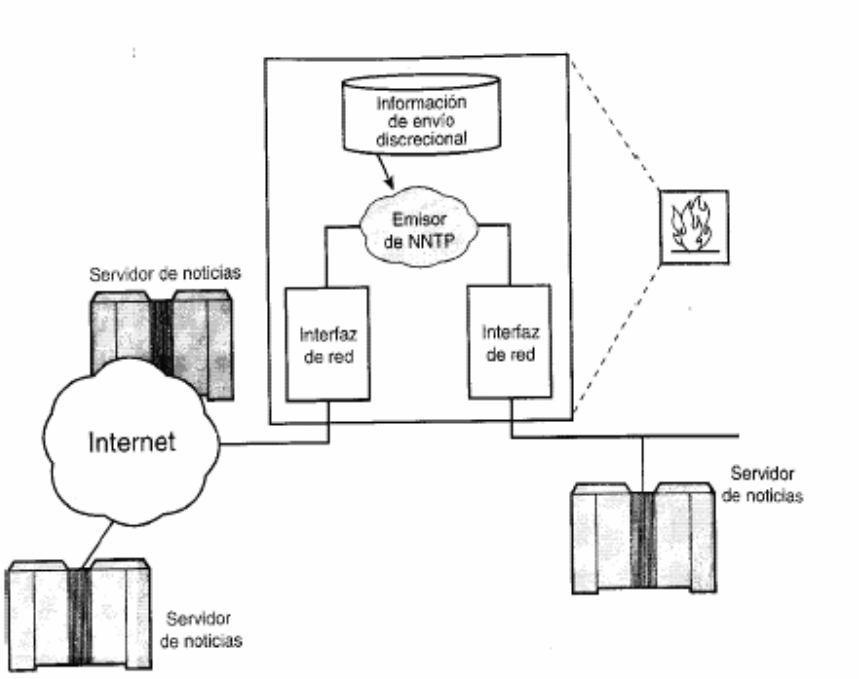
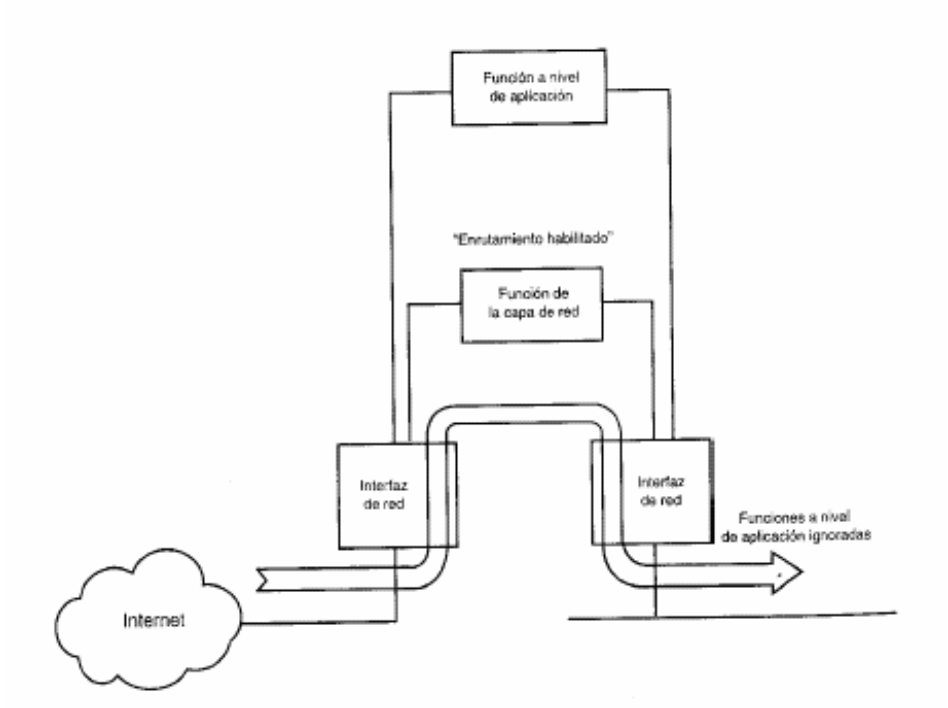


**Figura 12. Firewall de base dual mal configurada**




### 3.3.5.3 Cómo Comprometer la Seguridad de una Firewall de Base Dual

Se deben conocer las acciones que pueden comprometer la integridad de un firewall de base dual. Con este conocimiento se pueden tomar las medidas para evitar que esto ocurra.

La amenaza más grande es que un intruso obtenga acceso directo al host de base dual. La conexión siempre debe establecerse a través de un Proxy de aplicación en el host de base dual. Las conexiones desde redes externas no contables deben sujetarse a una autentificación estricta.

El único acceso a la firewall misma debe ser a través de la consola o del acceso remoto seguro. Para evitar que se esquive el firewall, no deben permitirse cuentas de usuario en el sistema.

Si el usuario obtiene acceso directo al host de base dual, la red interna estará sujeta a intrusiones.

Estas intrusiones pueden provenir de cualquiera de las siguientes fuentes:

- Permisos débiles en el sistema de archivos.
- Red interna con volúmenes montados en NFS.
- Permisos otorgados a utilerías r* de Berkeley a través de archivos equivalentes de host, como *rhosts*, en directorios base de usuarios para cuentas de usuarios que han sido comprometidos.
- Programas de respaldo de red que pueden restaurar permisos excesivos.
- Uso de scripts de *shell* administrativos que no han sido asegurados apropiadamente.
- Aprendizaje sobre el sistema a partir de niveles de revisión antiguos de |software y notas liberadas que no han sido debidamente aseguradas.
- Instalación de kernels antiguos de sistema operativo que tienen habilitado el envío IP, o instalación de versiones de kernels antiguos de sistemas operativos con problemas de seguridad conocidos.
- El uso de programas de rastreo como tcpdump o etherfind para "rastrear" la red interna que busca la información del nombre de usuario y de la contraseña. Si falla el host de base dual, la red interna está abierta de par en par para intrusos futuros, a menos que se detecte el problema y se corrija rápidamente.

#### 3.3.5.4 Servicios en una Firewall de Base Dual

Además de inhabilitar el envío IP, se debe eliminar todos los programas, utilerías y servicios de la firewall de base dual que puedan resultar peligrosos en manos de un intruso. La siguiente es una lista parcial de algunos puntos de verificación útiles para firewalls de base dual de Unix:

Elimine las herramientas de programación: compiladores, enlazadores, etcétera.

Elimine los programas con permisos SUID y SGID que no necesite o no comprenda. Si las cosas no funcionan, siempre es factible restaurar los programas esenciales. Si tiene experiencia, construya un monitor de espacio de disco que apague el host de base dual en caso de que se llene una partición crítica del disco.

Utilice particiones de disco para que una intrusión para llenar todo el espacio de disco de la partición sea confinada a esa partición. Elimine las cuentas especiales y de sistema innecesarias.

Elimine servicios de red que no sean necesarios. Utilice el comando netstat para verificar que sólo tenga los servicios de red que necesita. Edite los archivos /etc/inetd.conf y /etc/services y elimine definiciones innecesarias de servicios.

Modifique los scripts de inicio del sistema para evitar la inicialización de programas innecesarios como routed/gated y cualquier programa de soporte de enrutamiento.

### 3.3.4 Hosts de Bastión

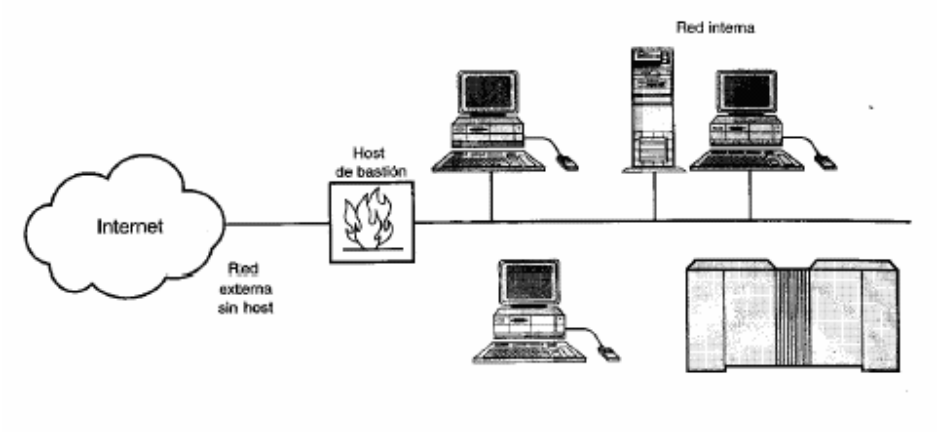
Un host de bastión es cualquier host de firewall que resulta determinante para la seguridad de la red. El host de bastión es el host central en la seguridad de red de una organización.

Debido a que el host de bastión es determinante para la seguridad de la red, debe estar bien fortificado. Esto significa que los administradores de red deben monitorear de cerca el host de bastión. El software de host de bastión y la seguridad del sistema deben auditarse con regularidad. Los registros de acceso deben examinarse en busca de cualquier brecha potencial de seguridad y cualquier intento de asalto al host de bastión.

El host de base dual analizado antes es un ejemplo de un host de bastión, ya que resulta crítico para la seguridad de la red.

El Despliegue mas Simple de un Host de Bastión debido a que los hosts de bastión actúan como punto de interfaz a una red externa no confiable, a menudo son sujetos de intrusión. El despliegue más simple de un host de bastión es como el primero y único punto de entrada para el tráfico de la red externa (vea la figura 16).

**Figura 13. El despliegue mas simple de un host de bastion(configuración B2)**




Por lo tanto la red de la Figura **13** es una configuración **B2**.

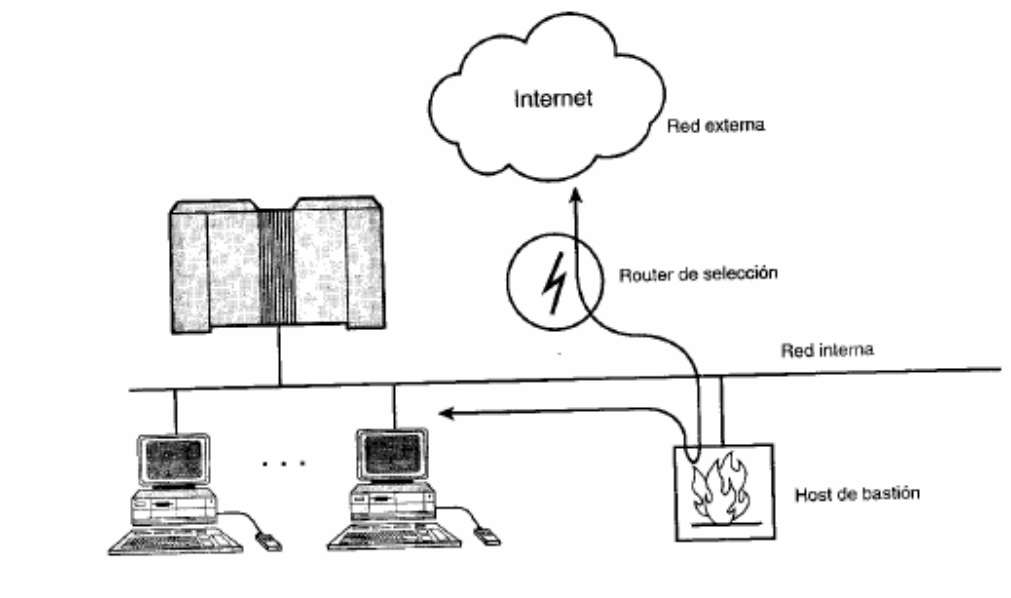
#### 3.3.4.1 *Gateway* de *Host* Seleccionado

Debido a que el host de bastión es crucial para la seguridad de la red interna, a menudo se introduce otra primera línea de defensa entre la red externa no confiable y la red interna. La primera línea de defensa es proporcionada generalmente por un router de selección.

En la figura **13** se muestra el uso de un host de bastión con un router de selección como primera línea de defensa. En este ejemplo sólo está configurada la interfaz de red el host de bastión, la cual se encuentra conectada a la red interna. Uno de los puertos del router de selección está conectado a la red interna y el otro a Internet. A este tipo de configuración se le llama gateway de host seleccionado.

Utilizando la notación definida en este capítulo, la configuración del gateway de host seleccionado, mostrada en el figura 14, puede describirse como configuración S-B 1 o sólo "SB1".

**Figura 14. Un host bastion con una sola interfaz de red y un router de selección como primera línea de defensa(configuración SB1)**




Debe configurar el router de selección para que éste le envíe primero al host de bastión todo el tráfico que la red interna recibe de las redes externas. Antes de enviarle el tráfico al host de bastión, el router de selección aplicará sus reglas de filtración al tráfico de paquetes. Sólo, tráfico de red que pasa las reglas de filtración se desvía al host de bastión; todo el demás tráfico de red es rechazado. Esta arquitectura da un nivel de confianza a la seguridad de la red que no se ve en la figura 16. Un intruso debe entrar primero al router de selección y después, si consigue, debe enfrentarse con el host de bastión.

El host de bastión utiliza funciones a nivel de aplicación para determinar si se permiten o niegan las solicitudes que van y vienen de la red externa. Si la solicitud pasa el escrutinio del host de bastión, se envía a la red interna para el tráfico entrante. Para el tráfico saliente, (tráfico a la red externa), las solicitudes se envían al router de selección.

### 3.3.5 Limitaciones del firewall

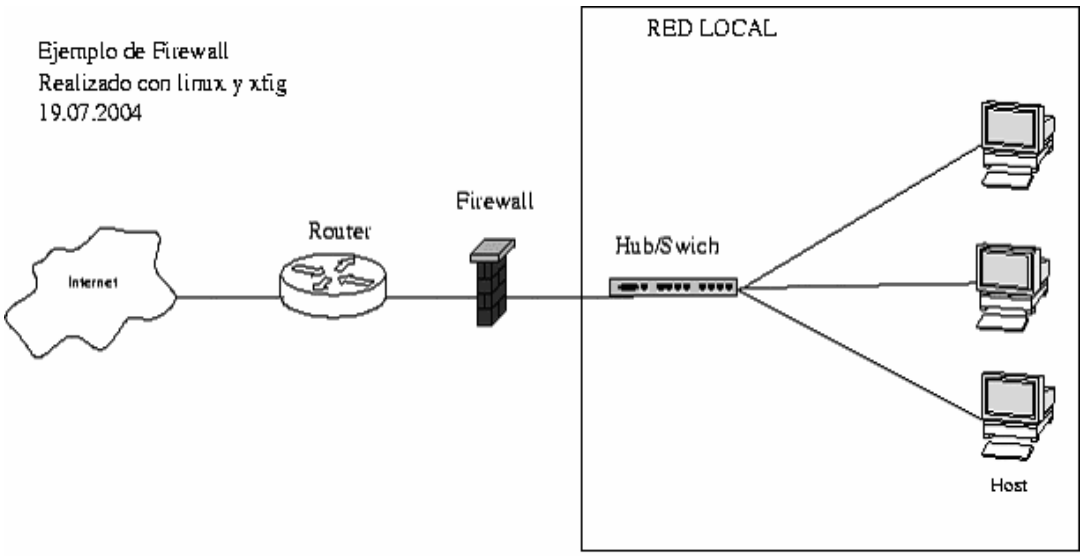
La limitación mas grande que tiene un firewall sencillamente es el hueco que no se tapa y que coincidencialmente o no, es descubierto por un *hacker*. Los *firewalls* no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo dejara pasar. Pero este no es lo más peligroso, lo verdaderamente peligroso es que ese hacker deje "*back doors*" es decir abra un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el firewall *no* **es contra humano**, es decir que si un hacker logra entrar a la organización y descubrir *passwords* o se entera de los huecos del firewall y difunde la información, el *firewall* no se dará cuenta.
Es claro que el firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus.

### 3.3.6 Modelos de configuración usando firewall en una red Lan con acceso a Internet

En el figura de la página siguiente, muestra un ejemplo de firewall entre Internet y una red local.

**Figura 15. Firewall entre Internet y una red local**



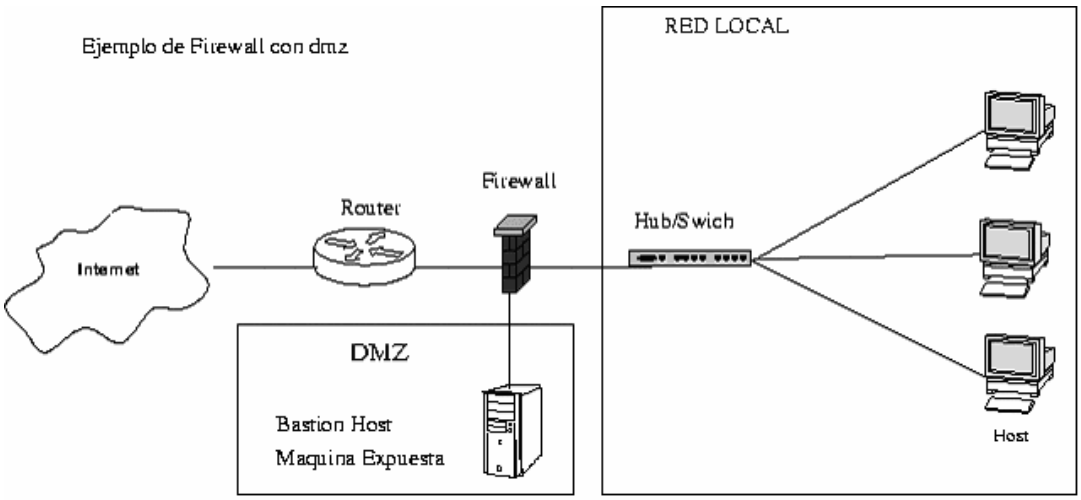

Fuente: http://es.tldp.org/COMO-INSFLUG/COMOs/Cortafuegos-Como/Cortafuegos-Como.html

Esquema típico de firewall para proteger una red local conectada a internet a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN)

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a Internet (como es el caso de un servidor Web, un servidor de correo, etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El firewall tiene entonces tres entradas:

En el figura de la página, muestra un ejemplo de ***firewall*** entre Internet y una red local, con zona ***dmz.***

**Figura 16. Firewall entre Internet y una red local, con zona *dmz***




Fuente: http://es.tldp.org/COMO-INSFLUG/COMOs/Cortafuegos-Como/Cortafuegos-Como.html

### 3.3.6.1 ¿Por qué es necesaria la seguridad en las redes?

Actualmente, Internet se compone de decenas de miles de redes conectadas entre sí. La seguridad en las redes resulta esencial en este entorno, ya que toda red organizada es accesible desde cualquier computadora de la red y potencialmente es vulnerable a las amenazas de personas que no necesitan acceso físico a ella. En un sondeo reciente dirigido por el ***Computer Security Institute*** (CSI), el 70% de las organizaciones encuestadas declararon que las defensas de sus redes habían sido atacadas y el 60% afirmaba que los incidentes procedían desde dentro de las propias empresas.

Aunque sea difícil calcular el número de empresas que tiene problemas de seguridad relacionados con Internet y las pérdidas financieras debidas a tales problemas, queda claro que los problemas existen. Definición del diseño de redes seguras Una internetwork se compone de muchas redes que están conectadas entre sí. Cuando se accede a información en un entorno de internetwork, hay que crear áreas seguras. El dispositivo que separa cada una de estas áreas se denomina firewall. Aunque un firewall suele separar una red privada de una red pública, esto no siempre es así. Lo normal es usar un firewall para separar los segmentos de una red privada.

Un router firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada . Un firewall suele tener un mínimo de tres interfaces, aunque las primeras implementaciones sólo incluían dos.

Todavía resulta habitual instalar firewalls de dos interfaces.

Cuando se usa un firewall con tres interfaces, se crea un mínimo de tres redes. Las tres redes que crea el firewall se describen de este modo:

#### 3.3.6.2 Interior

El interior es el área de confianza de la internetwork. Los dispositivos que están en el interior forman la red privada de la organización. Estos dispositivos comparten unas directivas de seguridad comunes con respecto a la red exterior (Internet). Sin embargo, resulta muy habitual que un firewall segmente el entorno de confianza. Si un departamento, como Recursos Humanos, tiene que ser protegido del resto de usuarios de confianza, se puede utilizar un firewall.

#### 3.3.6.3 Exterior

El exterior es el área de no confianza de la internetwork. El firewall protege los dispositivos del interior y de la DMZ (Zona desmilitarizada) de los dispositivos del exterior. Para ofrecer servicios, ya sean Web, FTP publico u otros, las empresas suelen permitir el acceso a la DMZ desde el exterior. En ocasiones, es necesario configurar un firewall para el acceso selectivo desde el 2 exterior hasta los hosts y servicios de la DMZ. Si es inevitable, es posible configurar un firewall para permitir el acceso desde un dispositivo del exterior hasta un dispositivo de confianza del interior, siendo la razón principal para esto, el que no todas las empresas quieren invertir en tener varios servidores. Esto es mucho más arriesgado que permitir el acceso, desde el exterior hasta la DMZ aislada.

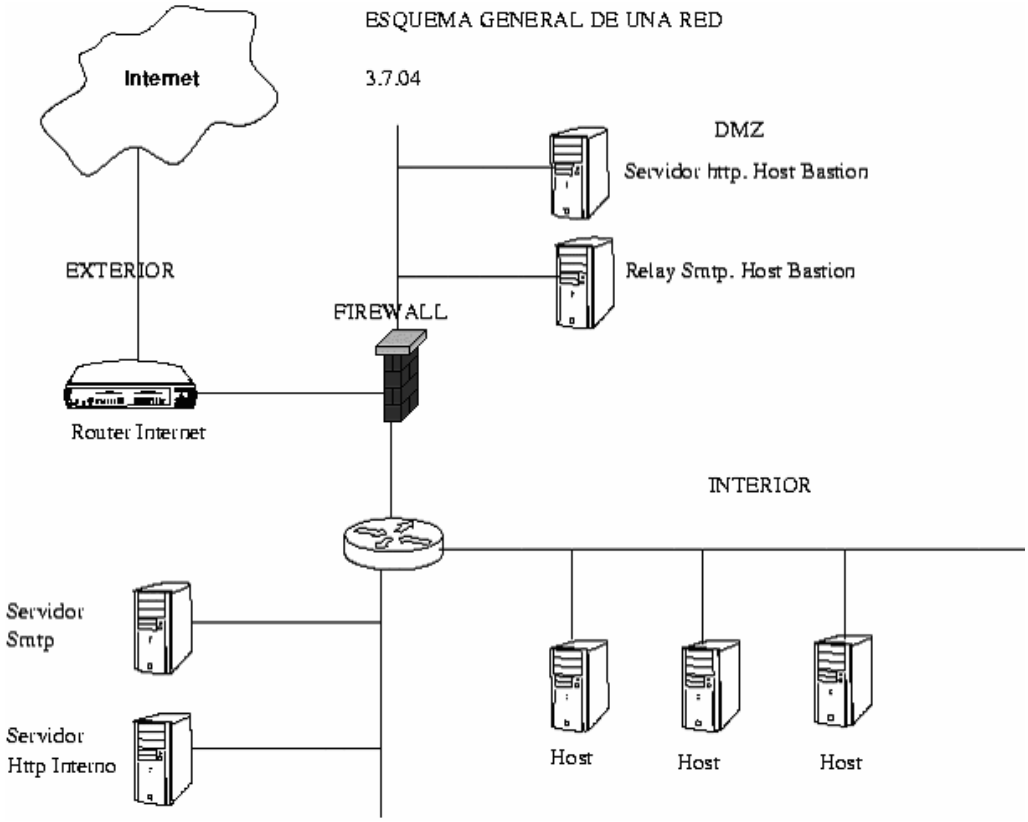
#### 3.3.6.4 DMZ (Zona desmilitarizada)

La DMZ es una red aislada, a la que pueden acceder los usuarios del exterior. Es necesario configurar el firewall para permitir el acceso desde el exterior o el interior hasta la DMZ. La creación de una DMZ posibilita que una empresa ponga la información y los servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado. Esto permite el acceso a los usuarios del exterior, sin permitir el acceso al interior.

Los hosts o servidores que residen en la DMZ suelen denominarse hosts bastión. En este caso, un host bastión es un host que está actualizado con respecto a su sistema operativo y las modificaciones experimentadas por este último. El hecho de que esté actualizado generalmente lo hará menos vulnerable a los ataques, ya que el fabricante habrá establecido o "parcheado" todos los defectos conocidos. El host bastión es un host que sólo ejecuta los servicios necesarios para realizar sus tareas de aplicación. Los servicios innecesarios (y a veces más vulnerables) son desactivados o eliminados.

En el figura de la página, muestra una red general.

**Figura 17. Red General**




Fuente: http://es.tldp.org/COMO-INSFLUG/COMOs/Cortafuegos-Como/Cortafuegos-Como.html

El cometido básico de un firewall consiste en llevar a cabo las siguientes funciones:

- No permitir acceso desde el exterior hasta el interior
- Permitir un acceso limitado desde el exterior hasta la DMZ
- Permitir todo el acceso desde el interior hasta el exterior
- Permitir un acceso limitado desde el interior hasta la DMZ

En muchos diseños de red existen excepciones a algunas de estas reglas (o a todas ellas). Por ejemplo, podría ser necesario permitir los mensajes SMTP desde el exterior hasta el interior. Si un entorno no tiene un servidor SMTP en la DMZ o carece de un host de relay de correo SMTP en la DMZ, sería necesario permitir acceder al servidor SMTP que resida físicamente en el interior. El hecho de permitir este tráfico incrementa considerablemente el riesgo en la red interna. Otra excepción podría ser que no se permitiera a la totalidad del tráfico pasar del interior al exterior. Potencialmente, una dirección IP, una subred, o la totalidad de la red del interior, podrían estar limitadas a la hora de usar una determinada aplicación (puerto). Otra restricción podría ser el filtrado de los URL.

#### 3.3.6.5 Proxies

Con los "*Packet Filtering Firewalls*" sólo es posible realizar filtrajes cuando los criterios están limitados a las direcciones y a los puertos. Una de las técnicas más usadas para resolver este problema son los proxies.
Introducción a los servidores Proxy:

Los servidores Proxy proporcionan el acceso a una red insegura para determinados protocolos de aplicación a través de un host con doble acceso.

El programa del cliente se comunica con el servidor Proxy en lugar de hacerlo directamente con el servidor real situado en la red insegura. El servidor Proxy es el encargado de evaluar las solicitudes del cliente y decide cuáles deja pasar y cuáles no. Si una petición es aceptada, el Proxy se comunica con el servidor real en nombre del cliente (el término Proxy significa representante) y lleva a cabo las peticiones de servicio del cliente al verdadero servidor y transmite las respuestas de éste de nuevo al cliente.

Es importante realizar las conexiones a través de un Proxy junto con algún método de restricción de tráfico IP entre los clientes y los servidores en la red insegura, como un router con filtrado de paquetes o un host con doble acceso que no enrute paquetes. Si hay conectividad a nivel IP entre clientes y servidores de la red insegura, los clientes pueden saltarse el servidor Proxy y producirse ataques desde el exterior.

#### 3.3.6.5.1 Ventajas y desventajas de los servidores Proxies

- **Ventajas de los servidores Proxy**

**Acceso directo a la red externa**

Si se utiliza la arquitectura de host con doble acceso, un usuario debe iniciar una sesión con el host antes de utilizar cualquier servicio de la red exterior, algo que resulta molesto para la mayoría de usuarios.

Al utilizar un servidor Proxy, los usuarios pueden conectarse de una forma más o menos transparente a un servidor de la red externa de forma directa sin que se den cuenta que están pasando por una máquina intermedia, el servidor Proxy. No obstante, esto requiere re-configuraciones en los programas cliente (navegador HTTP, cliente FTP, etc.).

***Logging* del sistema**

Gracias a que los servidores Proxy trabajan a nivel de aplicación resulta fácil generar *logs* o monitorizar las conexiones de los usuarios a cada tipo de servicio de forma cómoda sin tener que profundizar a nivel IP.

- **Desventajas de los servidores Proxy**

Disponibilidad de servidores para nuevos servicios:

Debido a que es necesario un servidor Proxy específico para cada tipo de servicio esto resulta bastante problemático a la hora de utilizar servicios de reciente aparición. Aunque existen servidores Proxy para la gran mayoría de servicios (HTTP, Telnet, FTP, SMTP, etc.) el administrador de red puede encontrarse en la necesidad de utilizar un nuevo servicio para el cual todavía no se ha creado ningún Proxy.

#### 3.3.6.5.2 Dependencia del servicio

Puede ser necesario utilizar un servidor Proxy exclusivo para cada protocolo. La instalación, configuración y administración de varios servidores puede requerir mucho trabajo.

También existen servicios para los cuales difícilmente existirá alguna vez un servidor *Proxy.*

Son servicios como *talk* con interacciones complicadas y desordenadas entre cliente y servidor.

**Modificaciones en los clientes**

La utilización de un servidor Proxy requiere la modificación o configuración de los clientes.

Esto requiere tiempo y trabajo. Los navegadores HTTP de última generación incluyen la opción centralizada de configuraciones para Proxy.
Desde un puesto de trabajo, el administrador pueda cambiar la configuración en lo que respecta a servidores Proxy de todos los clientes de forma automatizada

#### 3.3.6.5.2.1 Tipos de servidores proxies

- **Servidores Proxy a nivel de aplicación y a nivel de circuito**

Un Proxy a nivel de aplicación conoce la aplicación o servicio específico para el cual está proporcionando los servicios de Proxy, es decir, comprende e interpreta los comandos en el protocolo de aplicación.

Un Proxy a nivel de circuito crea un circuito entre el cliente y el servidor sin interpretar el protocolo de aplicación. Normalmente se utiliza con aplicaciones como SMTP, que implementa un protocolo de guardar y enviar. La versión más avanzada de un Proxy a nivel de circuito actúan como Proxy para el exterior pero como enrutador con filtrado para el interior.

En general, los Proxy a nivel de aplicación emplean procedimientos modificados y los Proxy a nivel de circuito clientes modificados. Esto se relaciona con los aspectos prácticos del Proxy.

Un Proxy a nivel de aplicación obtiene la información necesaria para conectarse al servidor exterior del protocolo de aplicación.

Un Proxy a nivel de circuito no puede interpretar el protocolo de aplicación y necesita que le proporcione la información a través de otros medios (por ejemplo, mediante un cliente modificado que le dé al servidor la dirección de destino).

La ventaja de un Proxy a nivel de circuito es que proporciona servicios para una amplia gama de protocolos. La mayoría de los servidores Proxy a nivel circuito también son servidores Proxy genéricos; pueden adaptarse para servir casi a cualquier protocolo.

No todos los protocolos pueden manejarse fácilmente por un Proxy a nivel de circuito. Los protocolos como FTP, que comunican datos del puerto cliente al servidor, necesitan cierta intervención a nivel de protocolo y, por lo tanto, ciertos conocimientos a nivel de aplicación.

La desventaja de un servidor Proxy a nivel circuito es que proporciona muy poco control sobre lo que circula a través del Proxy.

Al igual que un filtro de paquetes, controla las conexiones con base en su fuente y destino y no puede determinar fácilmente si los comandos que están pasando a través de él son seguros o están en el protocolo esperado. Un Proxy a nivel de circuito es fácilmente engañable por servidores instalados en los números de puerto asignados a otros servidores.

- **Servidores Proxy genéricos y dedicados**

Un servidor Proxy dedicado funciona para un único protocolo, mientras que uno genérico sirve para varios protocolos. En la práctica los servidores Proxy dedicados son a nivel de aplicación y los genéricos son a nivel de circuito.

Servidores *Proxy* inteligentes: Se denomina servidor Proxy inteligente a aquellos que son capaces de hacer algo más que transmitir peticiones como por ejemplo funciones de cache de datos (páginas *web*, ficheros de **FTP**,...). A medida que se consoliden los servidores Proxy sus habilidades se irán incrementando de forma rápida.
Generalmente los servidores *Proxy* inteligentes son dedicados a aplicación. Un servidor *Proxy* a nivel de circuito tiene habilidades limitadas.
Esquema del funcionamiento de un Proxy

### 3.4 Redes Privadas Virtuales (VPN)

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. Las firewalls o ambos sitios permiten una conexión segura a través de Internet. Las VPNs son una alternativa de coste útil, para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegiendo la información y el *password*. La tecnología de VPN proporciona un medio para usar el canal público de Internet como una canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privada a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de un red local.

### 3.4.1 Modo de trabajo de las VPN

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos. La tecnología de túneles - *Tunneling*- es un modo de transferir datos entre 7 redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado - encapsulación, ya que los paquetes están encriptados de forma de los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.
Los proveedores de varias firewall incluyen redes privadas virtuales como una característica segura en sus productos.

### 3.4.2 Redes privadas virtuales dinámicas - *Dynamic Virtual Private Networks* (DVPN)

Basadas en la tecnología de Internet, las intranets, han llegado a ser una parte esencial de los sistema de información corporativos de hoy en día. Sin embargo, Internet no fue diseñada, originalmente, para el ámbito de los negocios.

Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios.

Se presenta, un tema peliagudo en los negocios: ¿Cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo, para permitir un acceso libre a la información? Para decirlo de otro modo: ¿Cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperatividad y facilidad de uso?. A diferencia de una VPN tradicional que ofrece seguridad limitada e inflexible, una VPN dinámica proporciona ambos extremos, con altos niveles de seguridad, e igualmente importante es que proporciona la flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs dinámicas, pueden ofrecer esta flexibilidad porque están basadas en una misma arquitectura así como pueden proporcionar otras ventajas.

Una VPN dinámica es una habilitadora de intranet. Habilita que una intranet ofrezca más recursos y servicios que de otra forma imposibilitaría al mundo de los negocios a hacer mayor uso de los recursos de información.

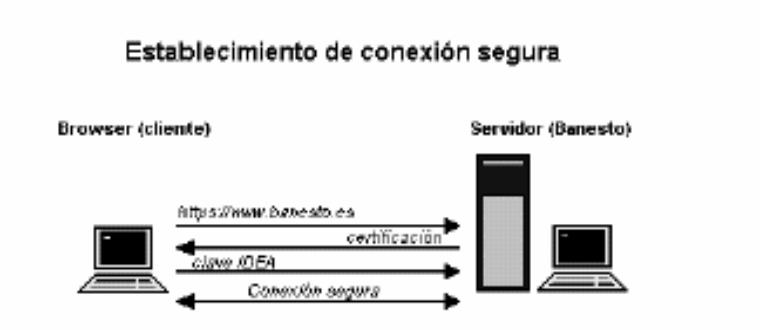
### 3.4.3 Potencial de una Red Privada Virtual Dinámica

Una VPN dinámica, permite que los negocios extiendan sus comunicaciones, y que el acceso a la información se produzca en un entorno agradable, versátil y controlado. En vez de estar diseñando engorrosas pantallas de usuario con las conocidas limitaciones y con esquemas de seguridad inflexibles, una VPN dinámica ha sido diseñada para proporciona el más alto nivel de libertad dentro de un entorno seguro, consiguiendo que el mayor número de usuarios pueda realizar su trabajo con la mayor cantidad de información posible.

### 3.5 El Protocolo SSL

Cuando transmitimos datos mediante HTTP se establece una comunicación entre un cliente y un servidor. Para realizar transacciones seguras el protocolo más utilizado hoy día es el SSL (Secure Sockets Layer) que impone la certificación del servidor, conociéndose como servidor seguro. este protocolo encripta los datos transferidos mediante HTTP. Un servidor seguro funciona de la siguiente forma:

**Figura 18. Establecimiento de Conexión Segura**




Un cliente accede a la dirección del web seguro a través de la URL correspondiente. Una vez establecida la conexión, el visualizador solicita una conexión segura. Si el servidor a que se accede es un servidor seguro, responderá afirmativamente a la solicitud, enviándole un certificado electrónico de tipo RSA. Tras recibir este certificado, el visualizador lo desempaquetará con la clave de la autoridad de certificación, ya integrada en el software, obteniendo de este modo la clave según el algoritmo RSA.

Por último, el cliente genera una clave de encriptación simétrica según el algoritmo RC4 y se la envía encriptada al servidor (con su clave pública). A partir de este momento, tanto el cliente como el servidor pueden establecer una comunicación segura basada en esta clave simétrica, que ambos, y sólo ellos conocen.

Las claves simétricas son generadas aleatoriamente en cada sesión, por lo cual no hay posibilidad de que éstas sean conocidas por eventuales hackers.

Un factor importante en la seguridad es quién tiene acceso a nuestros datos de cuentas bancarias, ya que si la tienda *on-line* se quedara con los números de la tarjeta de crédito podrían darse fraudes. Para evitar este fenómeno la mayoría de las tiendas dejan que la entidad bancaria realice toda la transacción, desde la captación de datos hasta la transacción en sí. Esto se consigue mediante una redirección https hacia la entidad bancaria. El proceso de compra on-line suele dividirse en dos etapas:

- Introducción de datos personales no bancarios y comprobación del importe de la compra.
- Introducción de datos bancarios (nº tarjeta de crédito)

La primera parte se realiza en la Web de la tienda, al principio no supone ninguna transacción crítica (aunque sería deseable que también fuera encriptada mediante SSL) y la segunda se realiza directamente en una página del banco.

## 3.6 Transacciones seguras Set

Los servicios financieros electrónicos: servicios de compras, de crédito, debito o prepago (monedero electrónico), gestión de activos o banca electrónica exigen transacciones seguras a través de Internet. Actualmente está en fase de pruebas el sistema SET (*Secure Electronic Transaction*) que regirá las transacciones a través de Internet en un futuro no muy lejano.

### 3.6.1 Set - Solucionando los problemas de SSL

Aparece una figura muy importante en el contexto de la autentificación: la autoridad certificadora, que expide certificados electrónicos que autentifican que el propietario de la tienda *on-line* (en general, cualquier web site segura) es quien dice ser y esta dentro del contexto legal del comercio electrónico.
Además, el protocolo SSL utiliza un sistema de encriptación asimétrica y simétrica, encriptando tanto la comunicación tienda-cliente como cliente - tienda. El protocolo SSL ofrece un alto nivel de seguridad pero puede mejorarse.

El protocolo **SET** (*Secure Electronic Transaction*) ofrece mecanismos de seguridad para las transacciones con tarjetas de pago en redes abiertas, ofreciendo un nivel de seguridad superior a SSL solucionando todos sus problemas. Este protocolo ha sido desarrollado por VISA y Mastercard, con la ayuda de otras importantes compañías como **IBM**, **Microsoft, Netscape**, **RSA**, **Terisa y Verisign**, entre otros.

El protocolo SET usa técnicas criptográficas a fin de ofrecer confidencialidad de la información, asegurar la integridad de los mensajes de pagos y autentificar tanto a los titulares de las tarjetas como a los vendedores. Estas son las características de SET:

- . Ofrece confidencialidad de la información de los medios de pago así como de la información de los pedidos mediante el cifrado de todos los mensajes intercambiados usando algoritmos de clave simétrica y asimétrica.
- Garantiza la integridad de todos los datos transmitidos gracias al uso de firmas digitales.
- Ofrece autentificación de que el poseedor de la tarjeta es un usuario legítimo de una cuenta asociada a dicha tarjeta de pago, usando firmas digitales y el certificado del titular de la tarjeta.
- Ofrece autentificación de que un vendedor puede aceptar transacciones con tarjetas de pago gracias a su relación con una institución financiera, usando para ello firmas digitales y el certificado del vendedor.
- Utiliza un protocolo que no depende de otros mecanismos de seguridad de transporte, así como tampoco evita su utilización.

Actualmente parece complicado predecir cuando funcionará SET debido que las previsiones no se cumplen, fundamentalmente por problemas técnicos, logísticos y de universalidad. Son tantos los agentes que intervienen en el proceso SET que dificulta la integración de todos ellos y por encima de todo, existe un problema fundamental: la cultura informática y de seguridad. Posiblemente para comercio electrónico empresa-empresa, SET tenga un éxito indiscutible.

# 4. HERRAMIENTAS DE HARDWARE UTILIZADOS PARA SEGURIDAD INFORMÁTICA

En la actualidad existen muchas tecnologías para brindar seguridad en redes de empresas mediana y grande, pero nos basaremos en las marcas Firewalls mas conocidas en Guatemala, y que según su marca tienen un lugar privilegiado en el mercado de Seguridad de redes. En la cual las clasificaremos en tecnologías para Pequeña y Mediana empresa y empresas grandes(empresariales. Entre ellas tenemos 3com y Cisco System).

Los diferentes modelos que mencionaremos a continuación son los que actualmente se encuentran disponibles a la venta para las diferentes tipos de empresas y dicha información fue extraída de Internet, de cada uno de ellos, tanto precio como características, algunas ventajas y desventajas.

## 4.1 Tecnología 3com para pequeña y mediana empresa

Una de las marcas comerciales son 3Com Corporación Empresa dedicada a la fabricación de dispositivos de Hardware para brindar seguridad a las diferentes empresas. A continuación detallaremos algunos productos de Hardware de esta empresa que están orientadas para el uso de PYMES:

- **3Com** Router 3000
- **3Com** IfficeConnect VPN Firewall
- **3Com** OfficeConnect Segure Router.

**Beneficios para la Mediana Empresa**

La familia 3Com Router 3000 incluye tres modelos de routers con diferentes interfaces WAN (*Wide Area Network*) y proporciona los siguientes beneficios entorno a la conectividad y la seguridad:

- Resuelve la complejidad de conectar sitios remotos a oficinas centrales y delegaciones, utilizando una variedad de interfaces WAN públicos y privados.
- Protege los datos que viajan entre oficinas remotas.

- Solución sencilla de utilizar y segura para la conexión a Internet y a la red local tanto para conectividad de área local o de área extensa en un sistema integrado y basado en estándares.

- Soporta los servicios más avanzados, como priorización de tráfico (QoS), IP y Routing IPXS, filtrado avanzado y soporte multicast para asegurar la forma más eficiente de transportar datos, voz y contenidos.

- ***3Com*** OfficeConnect VPN Firewall y3Com OfficeConnect Secure Router, un pequeño router para pequeñas oficinas y entornos domésticos, están diseñados para Pymes que utilizan conexiones de banda ancha (cable o **DSL**) o que ya dispongan de servicio WAN. Estas localizaciones normalmente no requieren tantas prestaciones como las que ofrece la familia Router 3000 (como multicast IP y Calidad de Servicio), pero necesitan un dispositivo sencillo de utilizar y seguro para proteger los datos mientras trabajan a través de conexiones WAN con usuarios, **partners**, proveedores y otros elementos clave para su negocio.

- ***3Com*** OfficeConnect VPN Firewall proporciona seguridad para prevenir los accesos no autorizados y bloquear los ataques de denegación de servicio y otros ataques provenientes de Internet. Diseñado para pequeñas empresas con delegaciones y trabajadores remotos, el firewall **VPN** ayuda a hacer seguras las comunicaciones a través de Internet. **3Com** OfficeConnect Secure Router permite compartir acceso a Internet de una forma económica y segura hasta 253 usuarios a través del módem DSL o cable ya instalado.

**Tabla I. Precio de tecnología 3com mediana empresa**

| NOBRE DISPOSITIVO | EMPRESA PRODUCTORA | PRECIO |
|---|---|---|
| 3Com Router 3016 | 3com | 895 Dólares |
| 3com OfficeConnect Vpn Firewall | 3COM | 155 Dólares |
| 3com Officeconnect SegureRouter | 3COM | 395 Dólares |

## 4.2 Tecnología 3com empresariales

Entre la tecnología 3com daremos a conocer los siguientes dispositivos para brindar seguridad en una red.

- Superstack 3 firewall
- Embedded firewall

**Características y ventajas**

El 3Com SuperStack 3 Firewall, caracterizado por aceleración de hardware VPN, disponibilidad mundial y filtración de contenido, proporciona la protección perimétrica de alto desempeño de 10/100 Mbps. El 3Com SuperStack 3 Firewall confiere seguridad a su red frente a accesos no autorizados y otras amenazas externas con origen en Internet. Esta solución de seguridad viene preconfigurada para detectar y repeler ataques por parte de hackers.

**Tabla II Precio tecnología 3com Empresariales**

| NOBRE DISPOSITIVO | EMPRESA PRODUCTORA | PRECIO |
|---|---|---|
| 3COM Superstack 3 Firewall | 3COM | 2760.50 dolares |
| 3com Embedded Firewall | 3com | 1,000 dolares |

## 4.3 Tecnología cisco *system* para pymes

A continuación mencionaremos algunos modelos de la tecnología **CISCO** que son utilizados para ofrecer mayor seguridad a las redes informáticas, orientadas a pequeña y Mediana empresa:

**Tabla III. Precio Tecnología Cisco System**

| NOBRE DISPOSITIVO | EMPRESA PRODUCTORA | PRECIO |
|---|---|---|
| Cisco PIX Firewall 515E | Cisco | 1469 dólares |
| Cisco 1700 IOS Firewall | Cisco | 674.02 dolares |

## 4.4 Tecnología Cisco System empresariales

### Cisco ASA 5510, 5520 y 5540

En las tecnologías para brindar seguridad mencionaremos algunas de la empresa Cisco System, orientadas a grandes empresas, detallando sus características y precios:

Es una solución de alto rendimiento, con alta disponibilidad (activo/ activo) y conectividad Gigabit Ethernet para grandes y medianas empresas, y proveedores de servicios. Utilizandos sus 4 puertos GE y con soporte hasta 100 VLANs, su negocio puede ser segmentado en numerosas zonas, mejorando la seguridad.

Este modelo es capaz de ampliarse si el crecimiento de su negocio requiere ampliar la seguridad, facilitando así el retorno de la inversión. La aplicación de defensa anti-x puede ser extendida utilizando el Módulo de Servicios de Seguridad (SSM). Su empresa puede extender su capacidad IPSec y SSL VPN para soportar mayor número de teletrabajadores y conexiones remotas.

**Tabla IV. Tecnología Cisco System Empresariales**

| Modelo | Rendimiento concurrente | Precio |
|---|---|---|
| Cisco ASA 5510 | Hasta 300 Mbps | A partir de 3,495 dólares |
| Cisco ASA 5520 | Hasta 450 Mbps | A partir de 7,995 dólares |
| Cisco ASA 5540 | Hasta 650 Mbps | A partir de 16,995 dólares |
| Cisco 1700 IOS Firewall | Hasta 450 Mbps | $726.59 - $789.59 dolares |

# 5. EVALUACIÓN Y ANÁLISIS DE SISTEMAS OPERATIVOS

Nuestro propósito es poder evaluar y analizar a los siguientes sistemas operativos con la finalidad de poder elegir según el tipo de empresa y necesidad de computo que se desee, tanto a nivel económico como a nivel de seguridad, describiendo cada una de sus características ventajas y desventajas que ofrece cada uno de los siguientes sistemas operativos.

Los sistemas operativos que a continuación se presentan son los mas conocidos y utilizados en muchas empresas que manejan la información computacional.

## 5.1 UNIX

### Características

- Es un sistema operativo multiusuario, con capacidad de simular multiprocesamiento y procesamiento no interactivo
- Está escrito en un lenguaje de alto nivel: C
- Dispone de un lenguaje de control programable llamado SHELL
- Ofrece facilidades para la creación de programas y sistemas y el ambiente adecuado para las tareas de diseños de software
- Emplea manejo dinámico de memoria por intercambio o paginación
- Tiene capacidad de interconexión de procesos
- Permite comunicación entre procesos
- Emplea un sistema jerárquico de archivos, con facilidades de protección de archivos, cuentas y procesos
- Tiene facilidad para redireccionamiento de Entradas/Salidas
- Contiene 4 aportaciones importantes que han aumentado la viabilidad de los sistemas UNIX como base para los sistemas distribuidos:

- Conectores Berkely
- Los Streams de AT&T
- El sistema de archivos de red NFS
- El sistema de archivos remoto RFS de AT&T

***Seguridad***

Para poder identificar a las personas, UNIX realiza un proceso denominado ingreso (*login*). Cada archivo en UNIX tiene asociados un grupo de permisos. Estos permisos le indican al sistema operativo quien puede leer, escribir o ejecutar como programa determinado archivo. UNIX reconoce tres tipos diferentes de individuos: primero, el propietario del archivo; segundo, el *grupo*; por último, está el *resto* que no son ni propietarios ni pertenecen al grupo, denominados *otros.*

Una computadora UNIX ofrece generalmente una serie de servicios a la red, mediante programas que se ejecutan continuamente llamados daemon (demonio). Por supuesto, para usar estos programas hay que tener primero permiso para usar tal puerto o protocolo, y luego acceso a la máquina remota, es decir, hay que "autentificarse", o identificarse como un usuario autorizado de la máquina. Algunos de estos programas son telnet, rlogin, rsh, ftp, etc.

### 5.2 Microsoft Windows NT

Características de Windows NT Server

- Soporta Sistemas Intel y los basados en RISC.
- Incorpora un NOS (Sistema Operativo de Red) de 32 bits.
- Ofrece una solución de red punto a punto.
- Requiere un mínimo de 16MB en RAM, por lo que es más caro de instalar que la mayor parte de los NOS.

- Soporta multitarea simétrica.
- Puede usar hasta 4 procesadores concurrentes.
- Además de ser multitarea, el Windows NT Server también es de lectura múltiple o multilectura.
- Soporta administración centralizada y control de cuenta de usuarios individuales.
- Las multitareas, priorizadas permiten que se ejecute simultáneamente varias aplicaciones.
- Las operaciones de red adquieren prioridad sobre otros procesos menos críticos.
- Incluye extensos servicios para Mac.
- Una computadora Mac puede acceder a Windows NT Server, como si accesara al servidor Appleshare.
- Los archivos se traducen automáticamente de un formato a otro.
- Los usuarios de PC y Mac tienen acceso a las mismas impresoras.
- Incluso una Mac puede imprimir trabajos Postscript en una impresora PC que no sea Postscript.
- Windows NT Server soporta integración con otras redes (Con Software adicional), que incluyen: NetWare, VINES, Lan Manager OS/2, UNIX, VMS y redes SNA.
- Es tolerante a fallas. Posee el reflejado a sistema espejo y separación de discos.
- Proporciona utilerías para administración y control fácil de usar.
- Proporciona acceso remoto por marcación telefónica.

***Seguridad***

Windows NT ofrece gran seguridad por medio del acceso por cuentas y contraseñas. Es decir un usuario debe tener su cuenta asignada y una contraseña para poder tener acceso al sistema.

Contiene protecciones para directorios, archivos, y periféricos, es decir que todo esto se encuentra con una contraseña para poder ser utilizados.
CONCEPTO DE DERECHOS.- Permite a un grupo de usuarios efectuar determinadas operaciones.
CUENTA ADMINISTRADOR.- Controla todos los permisos y con ellas se puede:

- Dar de alta
- Asignar cuentas
- Cancelar derechos

## 5.3 Novell Netware

### Características de NetWare

- Multitarea
- Multiusuario
- No requiere demasiada memoria RAM, y por poca que tenga el sistema no se ve limitado por ej. Netware 4.0 (Requiere 6 Mb de RAM)
- Brinda soporte y apoyo a la MAC
- Apoyo para archivos de DOS y MAC en el servidor
- El usuario puede limitar la cantidad de espacio en el disco duro
- Permite detectar y bloquear intrusos
- Soporta múltiples protocolos

- Soporta acceso remoto
- Permite instalación y actualización remota
- Muestra estadísticas generales del uso del sistema
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios
- Permite realizar auditorias de acceso a archivos, conexión y desconexión, encendido y apagado del sistema, etc.
- Soporta diferentes arquitecturas

**Desventajas de NetWare**

- No cuenta con listas de control de acceso (ACLs) administradas en base a cada archivo.
- Algunas versiones no permiten criptografía de llave pública ni privada.
- No carga automáticamente algunos manejadores en las estaciones de trabajo.
- No ofrece mucha seguridad en sesiones remotas.
- No permite el uso de múltiples procesadores.
- No permite el uso de servidores no dedicados.
- Para su instalación se requiere un poco de experiencia.

**Seguridad del Sistema**

Aunque los fabricantes que se dedican exclusivamente a los sistemas de seguridad de redes pueden ofrecer sistemas más elaborados, NetWare de Novell ofrece los sistemas de seguridad integrados más importantes del mercado. NetWare proporciona seguridad de servidores de archivos en cuatro formas diferentes:

1. Procedimiento de registro de entrada
2. Derechos encomendados

3. Derechos de directorio
4. Atributos de archivo

## 5.5 Linux

### Características

- Es un clon del sistema operativo UNIX por tanto es Multitarea y Multiusuario
- Se puede correr la mayoría del software popular para UNIX, incluyendo el Sistema X-Window
- Cumple los estándares POSIX y de Sistemas Abiertos, esto es que tiene la capacidad de comunicarse con sistemas distintos a él.

### Ventajas de Linux

- Precio. Es una implementación de UNIX sin costo
- Estabilidad
- Libre de virus, es muy difícil que sea infectado por virus
- Seguridad, es mucho más seguro que otros servidores
- Compatibilidad, reconoce la mayoría de los otros sistemas operativos en una red
- Velocidad, es mucho más veloz para realizar las tareas
- Posee el apoyo de miles de programadores a nivel mundial
- El paquete incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades del usuario
- Se puede usar en casi cualquier computadora, desde una 386
- Puede manejar múltiples procesadores. Incluso hasta 16 procesadores
- Maneja discos duros de hasta 16 TeraBytes
- Soporta acceso remoto
- Soporte nativo de TCP/IP (Fácil conexión a Internet y otras redes)

**Desventajas de Linux**

- Carencia de soporte técnico.
- Inconvenientes de hardware, no soporta todas las plataformas, y no es compatible con algunas marcas específicas.

**Tabla V. Comparación de las Características Generales de los Sistemas Operativos**

| Sistema Operativo | Conectividad | Confiabilidad | Estabilidad | Escalabilidad | Multi-usuario | Multi-plataforma | POSIX | Propietario |
|---|---|---|---|---|---|---|---|---|
| UNIX | Excelente | Muy Alta | Excelente | Muy Alta | Si | Si Múltiple | Si | Si |
| Windows NT | Muy Buena | Baja | Regular | Media | Inseguro | Parcial | Limitada | Si |
| Netware | Excelente | Alta | Excelente | Alta | Si | Si | No | Si |
| Linux | Excelente | Muy Alta | Excelente | Muy Alta | Si | Si Múltiple | Si | No |

**Tabla VI. Precio de Algunas Versiones de los Sistemas Operativos**

| Sistema Operativo | Propietario | Precio |
|---|---|---|
| UNIX<br><br>Mac OS X Server 10.2 | Apple | US $499.00 (10 usuarios)<br><br>US $999.00 (sin limite de usuarios) |
| Windows 2000 Advanced Server | Microsoft | US $809 (5 usuarios)<br>US $1,129 (10 Usuarios) |
| Netware 6.0 | Novell | US $1,395 (5 usuarios)<br><br>US $47,995 (1000 usuarios) |
| Linux Red Hat 8.0 | | Gratis o sobre US $49.95 para una distribución en CD-ROM |

**Tabla VII. Comparación de la Seguridad de los Sistemas Operativos**

| Sistema Operativo | Seguridad |
|---|---|
| UNIX | Realiza un proceso denominado ingreso (login). Cada archivo en UNIX tiene asociados un grupo de permisos. Hay que "autentificarse", o identificarse como un usuario autorizado de la máquina. UNIX reconoce tres tipos diferentes de individuos: primero, el propietario del archivo; segundo, el "grupo"; por último, el "resto" que no son ni propietarios ni pertenecen al grupo, denominados "otros". |
| Windows NT | El usuario debe tener su cuenta asignada y una contraseña para poder tener acceso al sistema. El sistema está protegido del acceso ilegal a las aplicaciones en las diferentes configuraciones. Ofrece la detección de intrusos. Permite cambiar periódicamente las contraseñas.<br><br>No permite criptografía de llave pública ni privada. |
| Netware | Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios. Permite detectar y bloquear intrusos.Algunas versiones no permiten criptografía de llave pública ni privada. |
| Linux | Presenta las mismas características que UNIX lo que lo hace mucho más seguro que otros servidores. |

Analizando cada una de las tablas anteriores podemos llegar a la conclusión que para una **Empresa Mediana** tomando en encuentra tanto en el punto de vista económico, como el tamaño de información a manejar, un Sistema Operativo **LINUX**, seria un sistema operativo que nos brinda buena seguridad como la de **Unix**, ya que es un clon de el.

A nivel seguridad podemos confiar en todas las características de nos ofrece Linux, ya que actualmente en la Web la mayoría de servidores están en Linux.

En el caso de una **Empresa Corporativa** podríamos hablar de Unix, porque nos ofrece un nivel alto de seguridad, como también estabilidad en el manejo de las transacciones de datos. Y un soporte técnico por software propietario. Lo que hace mas confiable el poderlo adquirir.

Este análisis se hace desde el punto de vista de los sistemas operativos que actualmente en Guatemala pueden ser adquiridos fácilmente, y que son mas conocidos.

# 6. DISEÑO DE REDES PARA MEDIANA Y GRANDE EMPRESA

Lo que se pretende con los diseños que a continuación se proponen para las diferentes tipos de empresas, son tanto precio cómodo de la configuración y seguridad necesaria según sea el tipo de empresa, tomando en cuenta los siguientes factores técnicos a la hora del diseño:

1. Utilización de dispositivos de Conexión según la necesidad de la empresa, a nivel de manejo de datos, para brindar seguridad.
2. Elección de los dispositivos de Hardware de seguridad según el tipo de empresa.
3. Utilización de Software de Seguridad según el tipo de empresa, para optimizar costos, ya que actualmente suele ser mas barato el uso de software de seguridad que Hardware de seguridad.
4. En el caso de software nos basaremos mas en el sistema operativo a elegir según la necesidad y tipo de empresa.

## 6.1 Diseño básico de un red C/B Mediana empresa

Normalmente una mediana Empresa, no tiene sucursales, solo esta ubicada en un lugar, y hay algunas que tienen acceso a Internet para que sus clientes puedan interactuar con ella, ya sea para comprar sus productos, o poder ofertar sus productos, en el diseño siguiente supondremos que nuestra mediana empresa estará conectada a Internet y que contara con un Servidor Web, en la cual sus clientes podrán realizar ciertas operaciones.

Una solución intermedia para brindar seguridad , sería montar un router linux, que cambie las ips, anulando la red 192.168.0.0/255.255.255.0, y crear nosotros subredes de clase B, 172.16.0.0/255.255.255.0 a partir del firewall.

Es decir, tendremos una clase C (192.168.0.0), solo hasta el firewall, y el resto de la red privada, será un clase B (172.16.0.0). La clase B, permitirá aislar y crear subredes.

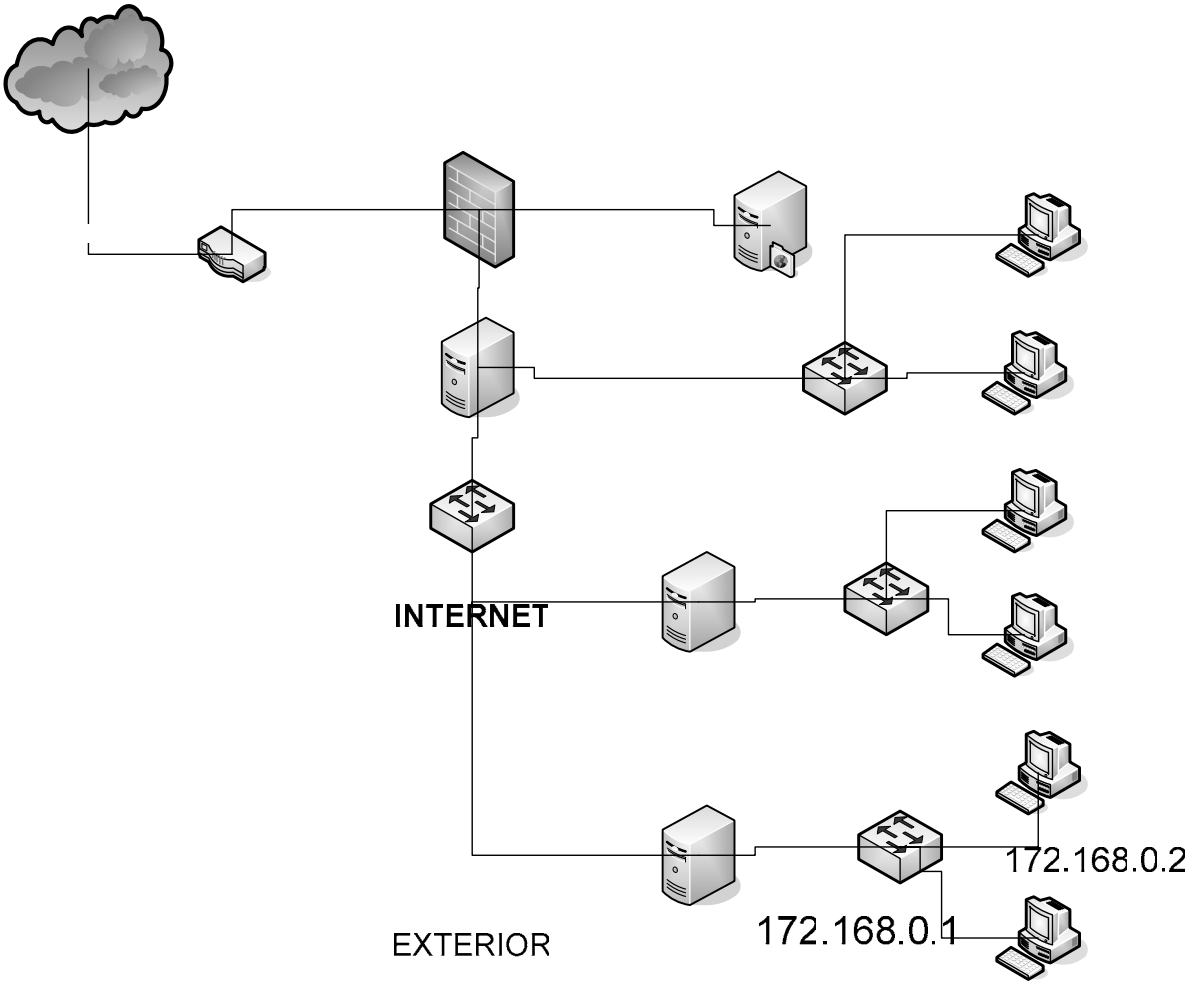
Ventajas:

1. Fácil de instalar y mantener. Sólo hay que activar el dhcp en los pcs.
2. Se bloquea el acceso de las sub-redes a otros pcs.
3. Se podría instalar un Proxy transparente en cada servidor de subdepartamento y encadenarlos.
4. Red segura, ya que todas las máquinas no tienen tienen acceso a toda la red.
5. Tiene un gran tráfico de paquetes de **broadcast** más bajo.

Inconvenientes:

1. Los routers linux que tienen varias ips, deben tener su tabla de rutas.
2. No se pueden poner servidores web al exterior, por tener el acceso al router bloqueado.
3. El dhcp se hara segmentado por subredes.
4. Hay que añadir un firewall.

**Figura 19. Red de clase C/B Mediana Empresa**




Router Internet

172.16.253.2

172.16.100.100



INTERIOR

## 6.2 Diseño de red clase b con DMZ y firewall, red segura para grande Empresa

En el caso de una empresa corporativa normalmente tienen diferentes sedes, como también tecnologías para resguardar los datos, por lo que sus redes en la mayoría de casos son unidas por una línea dedicada de Internet, en la cual pueden hasta utilizar tecnologías VPN, en el siguiente diseño supondremos que cada una de las redes que a continuación se describen cada una esta en un lugar diferente, unidas por una línea dedicada de Internet.

Suponemos que queremos varias subredes por departamentos, en cada una de las LAN. Queremos que los PCS de los departamentos se vean entre ellos (esto deberá contemplarse en el cuadro de encaminamientos).

Usaremos la red de tipo B privada para una de las redes y tipo C para la otra que representaría el otro extremo de la red, ya que las redes corporativas normalmente tienen diferentes sedes en la cual su red es bastante grande y manejan servicio dedicado de Internet, como también redes virtuales.

172.16.0.0 / 255.255.255.0 o lo que es lo mismo 172.16.0.0 /24

Esto significa que tenemos, esta máscara:

11111111. 11111111.11111111.00000000

Es decir, podemos tener:

- Subredes : 2 elevado a 8 (11111111 del tercer número de la máscara) =256

- Hosts: 2 elevado a 8 - 2 : (00000000 del cuarto número de la máscara) =256-2=254

**Tabla VIII. Subredes para 172.16.0.0/255.255.255.0**

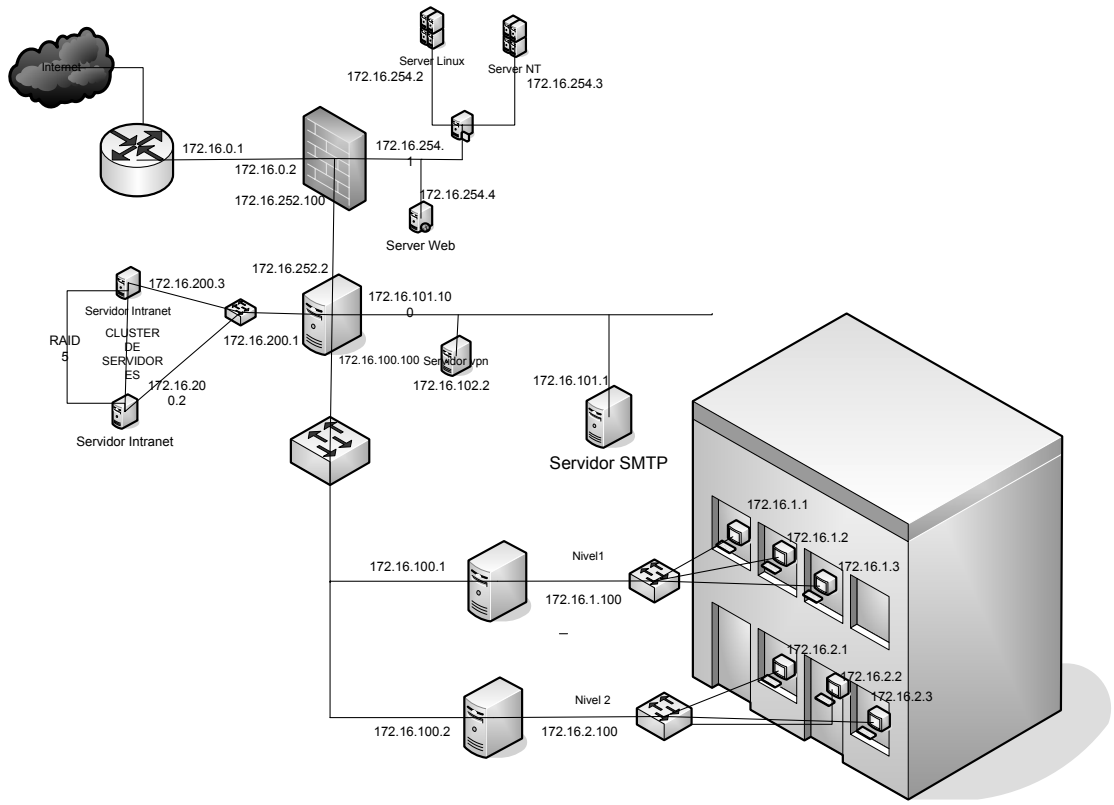
| Subred | De | A | Broadcast | Mascara |
|---|---|---|---|---|
| 172.16.1.0 | 172.16.1.1 | 172.16.1.254 | 172.16.1.255 | 255.255.255.0 |
| 172.16.2.0 | 172.16.2.1 | 172.16.2.254 | 172.16.2.255 | 255.255.255.0 |
| 172.16.3.0 | 172.16.3.2 | 172.16.3.254 | 172.16.3.255 | 255.255.255.0 |
| ... | ... | ... | ... | ... |
| 172.16.254.0 | 172.16.254.0 | 172.16.254.254 | 172.16.254.255 | 255.255.255.0 |

No se toman en cuenta la red 172.16.0.0 por representar la red, ni la 172.16.255.0, por representar el broadcasting.

**Tabla IX. Subredes 192.168.0.0/255.255.255.0**

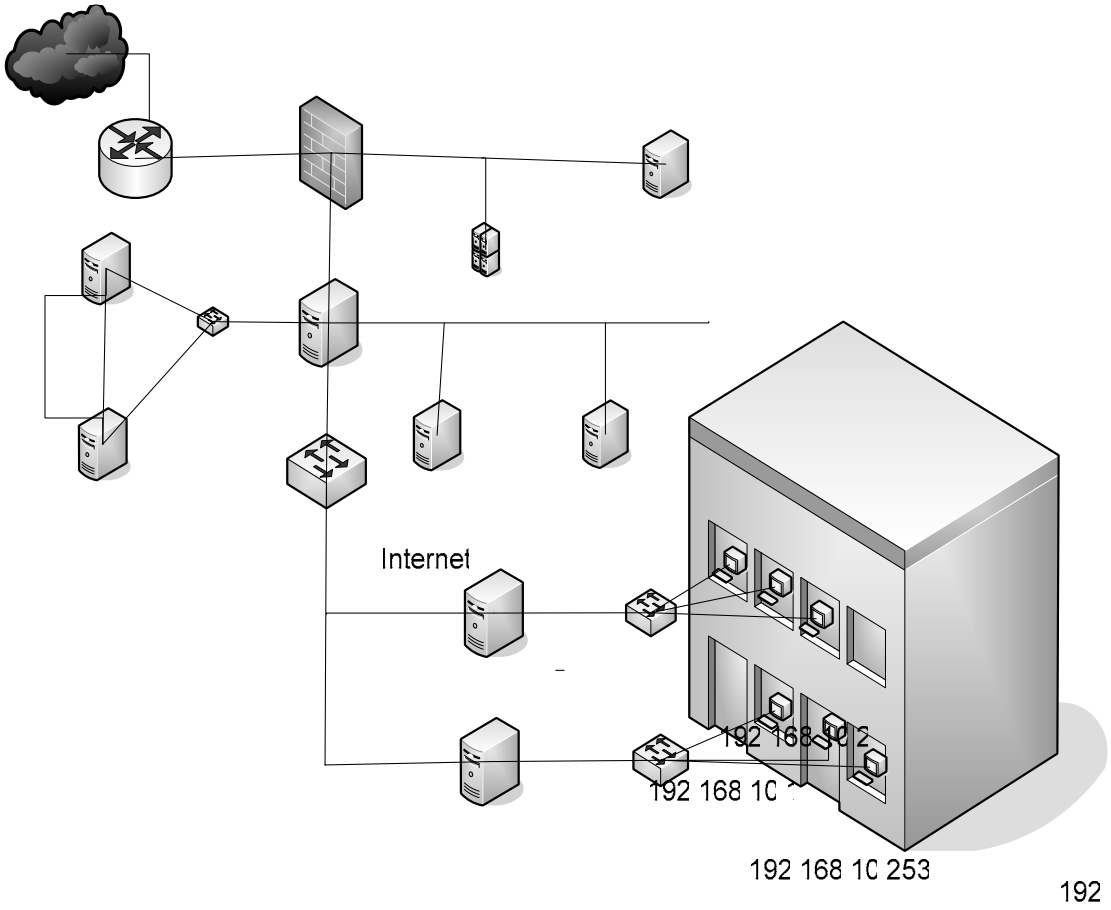
| Subred | De | A | Broadcast | Mascara |
|---|---|---|---|---|
| 192.168.1.0 | 192.168.1.1 | 192.168.1.254 | 192.168.1.255 | 255.255.255.0 |
| 192.168.2.0 | 192.168.2.1 | 192.168.2.254 | 192.168.2.255 | 255.255.255.0 |
| 192.168.3.0 | 192.168.3.2 | 192.168.3.254 | 192.168.3.255 | 255.255.255.0 |
| ... | ... | ... | ... | ... |
| 192.168.254.0 | 192.168.254.0 | 192.16.254.254 | 192.168.254.255 | 255.255.255.0 |

**Figura 20. Red con DMZ Sede Principal**




- La red 172.16.2.0/24, se encuentra accesible por la ip del router del Depto 2, 172.16.2.100
- Para el resto de redes, ir a la 172.16.100.100

**Figura 21. Red con DMZ Sucursal**



# CONCLUSIONES

1. Los diferentes tipos de configuración de Firewall, dará una mejor idea de cómo diseñar nuestras redes seguras para nuestros servidores de datos, según el tipo de empresa.
2. Los diseños y topologías de red segura realizada, para una mediana empresa y grande, pueden ser implementados, pues el objetivo es que sea útil para las empresas.
3. Los precios de las herramientas de Hardware, darán una idea de cómo andan los precios en el mercado actual de dichas herramientas.
4. Todos los Sistemas Operativos analizados en el presente trabajo representan opciones viables para la implementación de seguridad en los servidores. Linux es un Sistema Operativo, el cual debe considerarse seriamente, ya que, presenta numerosas ventajas, además de lo económico de su adquisición, las herramientas de seguridad que incluye hacen factible su configuración como servidor Web.
5. Las técnicas de protección estudiadas son soluciones eficientes a los problemas de seguridad, ya que, son una combinación de Hardware y Software capaces de detectar, prevenir y atenuar cualquier situación de peligro para el sistema. La decisión sobre su implantación al sistema está en dependencia de las necesidades de la empresa o del grado de seguridad que se desee adquirir. Agregando métodos de seguridad no significa necesariamente un aumento en la seguridad.

6. Para un desempeño óptimo del servidor deben tomarse muy en cuenta las consideraciones técnicas enunciadas ya que proporcionan un incremento en el rendimiento del sistema, según las características de éste.

# RECOMENDACIONES

1. La seguridad de un sistema de información no sólo está en dependencia de la ***calidad*** del software o del hardware que se utiliza, es parte fundamental seguir ciertas recomendaciones que garantizarán la verdadera seguridad de los sistemas de información.
2. El desarrollo de políticas de seguridad
   Cualquier política de seguridad debería estar construida con estas características como pautas.

   - Sencilla y no compleja, mientras más sencilla y clara la política de seguridad, más fácil será que las pautas sean respetadas y el sistema permanezca seguro.
   - Fácil de mantener y no difícil, como todo, los métodos y herramientas de seguridad pueden cambiar dependiendo de necesidades y retos nuevos. La política de seguridad debería construirse con un enfoque hacia la minimización del impacto que los cambios tendrán en su sistema y en sus usuarios.
   - Promover la ***libertad*** a través de la confianza en la integridad del sistema en vez de una sofocante utilización de sistema, evitar métodos y herramientas de seguridad que limiten, innecesariamente, la utilidad del sistema. Los métodos y herramientas de seguridad de calidad son casi siempre una ventaja segura y ofrecen más elecciones a los usuarios, cada vez que sea posible.

- El reconocimiento de la factibilidad, en lugar de una falsa sensación de seguridad, una de las maneras más exitosas de atraer un problema de seguridad es a través de la creencia que el sistema no podría tener un problema como ese. En lugar de acomodar la postura, hay que estar siempre alerta.
- El enfoque debería estar en los problemas reales en lugar de problemas teóricos. Emplear tiempo y esfuerzo ocupándose de los problemas reales más grandes y luego proseguir con los menores.
- La inmediatez en lugar de la desidia, resolver los problemas como vayan surgiendo y determinar que equivalen a un riesgo. No creer que es posible ocuparse del problema más tarde. En realidad no hay mejor momento que ahora mismo, especialmente cuando se trata de una amenaza a la incolumidad del sistema.

3. La importancia de contraseñas seguras

Una buena contraseña debe tener las siguientes cualidades:

- tener por lo menos ocho caracteres;
- estar hecha de caracteres, números y símbolos;
- ser única .

Se deben evitar contraseñas que:

- sean palabras que se encuentran en el diccionario;
- tengan que ver con sus datos personales;
- no pueda ser escrita rápidamente.

# REFERENCIAS ELECTRÓNICAS


1. http://www.pello.info/filez/firewall/iptables.html(23/03/2005)
2. http://andercheran.aiind.upv.es/toni/personal/unixsec.pdf(23/03/2005)
3. http://www.aui.es/biblio/documentos/proteccion_datos/intro/intro.htm (23/03/2005)
4. http://www.cysco.com(23/04/2005)
5. http://www.3com.com(23/04/2005)
6. http://www.monografias.com(23/03/2005)
7. http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/(23/03/2005)
8. http://www.redes.upv.es/~mperez/rc2/trabajos/FireWallstxt.pdf (23/03/2005)
9. http://es.tldp.org/COMO-INSFLUG/COMOs/Cortafuegos-Como/Cortafuegos-Como.html(23/03/2005)
10. http://members.fortunecity.es/mardedudascom/Informatica/_inf_redes/seguridadredes.htm(23/03/2005)
11. http://tdg.lsi.us.es/~sit02/res/papers/echevarria.pdf(23/03/2005)