SEGURIDAD EN REDES

JULIE MARGARITA GARCES VERGARA
WENDY PAOLA HERRERA ROMERO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍAS ELECTRICA Y ELECTRONICA
CARTAGENA DE INDIAS D. T. Y C.
2007

SEGURIDAD EN REDES

JULIE MARGARITA GARCES VERGARA
WENDY PAOLA HERRERA ROMERO

Trabajo de monografía presentado como requisito para optar al titulo de Ingeniero Electrónico

DIRECTOR
ING. MARGARITA UPEGUI FERRER
MAGISTER EN CIENCIAS COMPUTACIONALES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍAS ELECTRICA Y ELECTRONICA
CARTAGENA DE INDIAS D. T. Y C.
2007

Articulo 105

La Universidad Tecnológica de Bolívar se reserva el derecho de propiedad de los trabajos de grado aprobados y no pueden ser explotados comercialmente sin autorización.

Nota de aceptación:

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Cartagena de indias, septiembre de 2007

Señores
Comité curricular de Ingeniería Eléctrica y Electrónica
Universidad Tecnológica de Bolívar
La Ciudad

Respetados señores:

Por medio de la presente nos dirigimos a ustedes para informarles que la monografía titulada **"SEGURIDAD EN REDES"** ha sido desarrollada conforme a los objetivos establecidos.

Como autores de la monografía consideramos que el trabajo es satisfactorio y merece ser presentado para su estudio, evaluación y posteriormente su aprobación.

Atentamente:

_____	_____
Julie Margarita Garcés Vergara	**Wendy Paola Herrera Romero**
CC # 45.554.706 de Cartagena	**CC # 32.935.249 de Cartagena**

Cartagena D. T. Y C., septiembre de 2007

Señores

COMITÉ DE EVALUACIÓN DE PROYECTOS
Programa de Ingeniería Electrónica

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

La ciudad

Cordial saludo:

A través de la presente me permito entregar la monografía titulada SEGURIDAD EN REDES para su estudio y evaluación la cual fue realizada por los estudiantes JULIE MARGARITA GARCÉS VERGARA y WENDY PAOLA HERRERA ROMERO, de la cual acepto ser su director

Atentamente,

_____

MARGARITA UPEGUI FERRER

Magíster en ciencias computacionales

AUTORIZACIÓN

Yo JULIE MARGARITA GARCÉS VERGARA, identificada con cedula de ciudadanía # 45.554.706 de Cartagena , autorizo a la universidad tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo en línea de la biblioteca.

_____

JULIE MARGARITA GARCÉS VERGARA

AUTORIZACIÓN

Yo WENDY PAOLA HERRERA ROMERO, identificada con cedula de ciudadanía # 32.935.249 de Cartagena, autorizo a la universidad tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo en línea de la biblioteca.

_____

WENDY PAOLA HERRERA ROMERO

DEDICATORIA

Esta dedicatoria va dirigida especialmente a Dios, por permitirme culminar esta etapa de mi vida, por darme sabiduría, fortaleza, por hacerme entender y enseñarme el camino que debía andar.

A mis padres Rubiela Vergara y Rodolfo Garcés quienes centraron todos sus esfuerzos por hacerme una profesional, enseñándome y dándome muchos ejemplos como la perseverancia, la paciencia, la disciplina y la constancia. A mis hermanos Stefany y Leonardo que me apoyaron desde el inicio de mi carrera y siempre estuvieron orgullosos de mi esfuerzo y mi entrega a la ingeniería. A Kenny Fajardo quien con su amor, entrega y experiencia me guió en el desarrollo de este trabajo. A mis familiares, amigos y compañeros quienes me apoyaron todo el tiempo y siempre me brindaron su mejor consejo.

Y finalmente a la universidad Tecnológica de Bolívar y a su grupo de docentes que a lo largo de mi carrera profesional me enseñaron a ser una persona integral y competitiva.

Mil gracias, Julie.

DEDICATORIA

Dedico con todo mi corazón y mi amor este trabajo fruto de mis sueños, mi esfuerzo, mi dedicación principalmente a Dios y a mi familia: a mis padres Carlos Herrera, Nury Romero, Rafael Guerreo y Maritza Romero por su apoyo incondicional, sus enseñanzas, por los valores que desde niña me inculcaron; a mis hermanos Carlos Alberto, Yari, Yuri Carolina, sin su apoyo hubiese sido difícil la realización de mis actividades, especialmente a Yuri Carolina por acompañarme en mis noches de desvelos y brindarme apoyo moral y sentimental; A Raúl Berdugo quien con su amor, paciencia, experiencia, buenos consejos y su ejemplo de perseverancia me ayudo a no desvanecer en la mitad del camino; A mis primos, especialmente a Xamara quien con su amor y espiritualidad me ha dado grandes enseñanzas, a mi sobrinito Diego Andrés por llegar y convertirse en un motivo mas para sonreír, a mis tíos, compañeros, amigos y demás persona que de una u otra forma me acompañaron en este camino.

Este esfuerzo también va dedicado a la familia Universidad Tecnológica de Bolívar, Rectora, Decano, Director de programa, profesores, compañeros.

A todos ustedes le prometo que seré una buena profesional que llevara con orgullo el titulo de Ingeniera electrónica.

“El temor de Dios es el principio de la sabiduría, Y el conocimiento del Santísimo es la inteligencia” PROVERBIOS 9:10

Muchas gracias, WENDY.

AGRADECIMIENTOS

Nosotras: Julie Margarita Garcés Vergara
Wendy Paola Herrera Romero

Agradecemos primero a nuestro Dios todopoderoso, quien con su inmensa misericordia y su infinito amor nos permitió la vida, el espacio y el tiempo para culminar con éxito esta etapa tan importante en nuestras existencias.
El nos prodigó todas las herramientas, la sabiduría, la paciencia y el amor con que forjamos el largo y difícil camino de nuestras vidas profesionales, que gracias a él hoy vemos realizadas.

¡Gracias, Dios!

Gracias a nuestros padres quienes han sido pilares fuertes en quienes nos hemos apoyados en momentos de flaquezas y debilidades, encontrando el aliento para proseguir.
A nuestros hermanos por su voz constante de aliento y sus buenos consejos.
A nuestro director quien con su ayuda profesional, su voz alentadora nos impulso siempre a buscar la excelencia.
A nuestros profesores Gonzalo López y Enrique Vanegas quienes nos guiaron en nuestro desarrollo profesional brindándonos su apoyo y buenos consejos.
A nuestros compañeros de estudio, amigos y todas aquellas personas que de una u otra forma colocaron su granito de arena para que hoy felizmente nosotras llegáramos a la meta.

¡Gracias!

CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

INTRODUCCION

Las redes informáticas o redes de computadoras son la base de la comunicación de los seres humanos y por supuesto de las pequeñas, medianas y grandes compañías. Debido al gran auge que tiene hoy día la tecnología ofrecen a los usuarios o clientes un gran portafolio de servicios. Lo que hace que cada día las compañías sean más dependientes de sus redes informáticas; por eso un problema que afecte a estas por mínimo que sea podría causarle grandes pérdidas.

Dadas las nuevas plataformas de computación disponibles y las cambiantes condiciones, se han abierto nuevos caminos, los cuales conducen a la aparición de grandes atacantes cada vez más organizados. Consecuentemente, muchas organizaciones internacionales gubernamentales y no gubernamentales, han desarrollado reglas, técnicas y herramientas, como la criptografía, los antivirus, los firewalls, para el correcto y debido uso, y de protección de las redes, estos organismos también recalcan la importancia de la atención y vigilancia continua y sistemática por parte de los responsables de la red.

Debido a lo planteado surgen las políticas informáticas como herramientas o normas organizacionales, como primera mediada para asegurar la red. Y como segunda, concientizar a los integrantes de las compañías sobre la importancia que tiene la información. Para lograr todos estos objetivos es necesario contar con el personal calificado y certificado, y de este modo implantar un sistema de administración de seguridad que garantice efectividad y eficiencia en las redes informáticas.

.

1. INTRODUCCION Y CONCEPTOS PREVIOS

1.1 Concepto de red

Una red de computadoras también llamada red de ordenadores o red informática, es un conjunto de computadoras y/o dispositivos conectados por enlaces de un medio físico (medios guiados) ó inalámbricos (medios no guiados) y que comparten información, archivos, recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, Chat, juegos), etc.[1]

1.2 Estructura de una Red

Por lo general una red para interconectarse necesita de elementos básicos como:

Host: Máquinas que ejecutan procesos de usuario.

Sub-Red: Mecanismos que permiten el paso de información de un host a otro, en la mayor parte de las redes de área extendida. Una sub-red consiste de dos componentes diferentes: las líneas de transmisión y los IMP.

Líneas de transmisión; también se denominan circuitos o canales, es el medio físico a través del cual se realiza la transmisión de los datos.

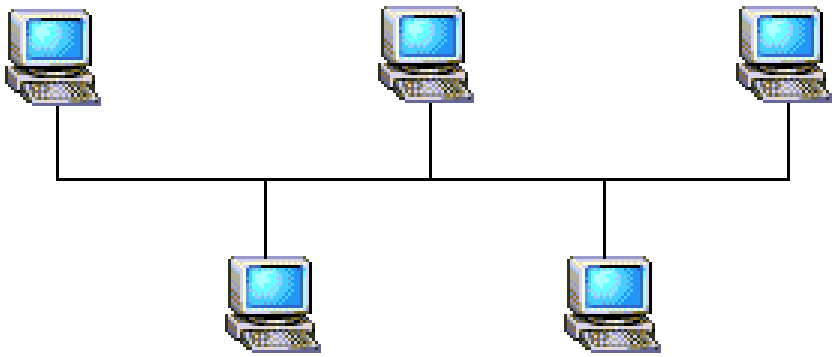
[1] **Articulo Red de Computadores**, Enciclopedia libre wikipedia.com, Groth, David; Toby Skandier

I.M.P. (Interface Message processor): también llamados nodos, conmutadores de paquetes, ordenadores de comunicaciones, intercambiadores de datos, sistemas intermedios, etc. Son ordenadores especializados que sólo ejecutan programas de comunicaciones. Su misión es habilitar una conexión entre en dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos.

1.3 Tipos de Redes

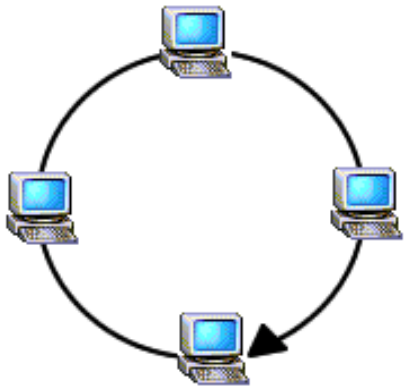
- **Bus:** Esta topología permite que todas las estaciones reciban la información que se transmite; una estación transmite y todas las restantes escuchan. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red. Todos los nodos de la red están unidos a este cable: el cual recibe el nombre de “Backbone Cable”. Tanto Ethernet como Local Talk pueden utilizar esta topología.

FIGURA 1. TOPOLOGIA BUS



- **Anillo:** En esta topología las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se rompe una conexión, se cae la red completa.

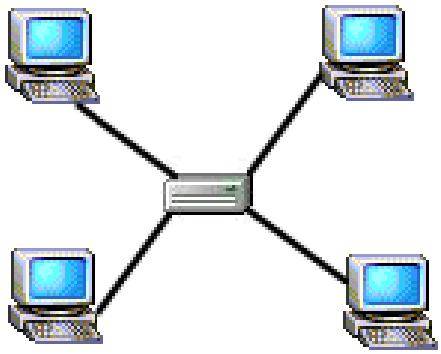
FIGURA 2. TOPOLOGIA ANILLO



- **Estrella:** Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.

  La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

FIGURA 3. TOPOLOGIA ESTRELLA

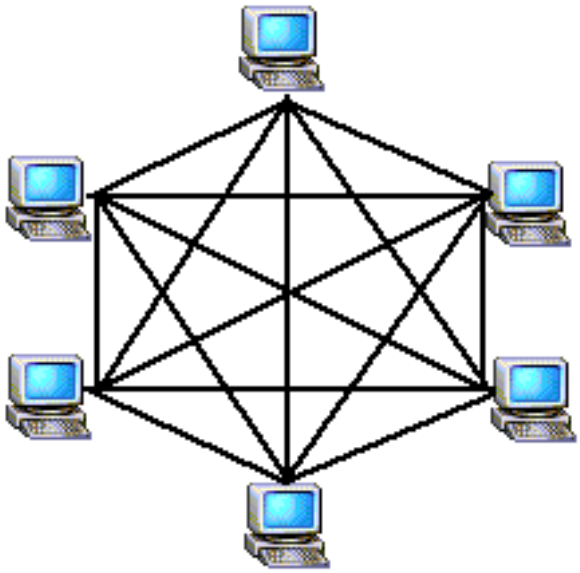


- **Híbridas:** Algunas veces se combinan el bus lineal, la estrella y el anillo para formar combinaciones de redes híbridas.

  - Anillo en Estrella: Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.
  - Bus en Estrella: El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.
  - Estrella Jerárquica: Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.

- **Árbol:** Esta estructura se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las estructuras de redes en los hogares de hoy en día. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

FIGURA 4. TOPOLOGIA ARBOL



- **Trama:** Esta estructura de red es típica de las WAN[2], pero también se puede utilizar en algunas aplicaciones de redes locales (LAN). Las estaciones de trabajo están conectadas cada una con todas las demás.

1.4 Protocolos de Redes

Los protocolos son el conjunto de normas o reglas que rigen como se comunican los ordenadores entre sí.

En Informática y Telecomunicaciones, un protocolo es una convención, o estándar, o acuerdo entre partes que regulan la conexión, la comunicación y la transferencia de datos entre dos sistemas.

[2] **WAN:** Wide Area Network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 Km.

En su forma más simple, un protocolo se puede definir como las reglas que gobiernan la semántica (significado de lo que se comunica), la sintaxis (forma en que se expresa) y la sincronización (quién y cuándo transmite) de la comunicación.

Los protocolos pueden estar implementados bien en hardware (tarjetas de red), software (drivers), o una combinación de ambos:

- **TCP/IP** (Transfer Control Protocol/Internet Protocol).
- **SMTP/POP3** (Email Transfer Protocol)/(Post Office Protocol)
- **MIME** (Multipurpose Internet Mail Extension)
- **HTTP** (Hypertext Transfer Protocol)
- **FTP** (File Transfer protocol)
- **NNTP** (Network News Transfer Protocol)

1.4.1 Propiedades Típicas

Al hablar de protocolos no se puede generalizar, debido a la gran amplitud de campos que cubren, tanto en propósito, como en especificidad. No obstante, la mayoría de los protocolos especifican una o más de las siguientes propiedades:

- Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables).
- Pasos necesarios para comenzar a comunicarse (Handshaking)
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.

- Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad

1.4.2 Estandarización

Los protocolos que son implementados en sistemas de comunicación que tienen un amplio impacto, suelen convertirse en estándares, debido a que la comunicación e intercambio de información (datos) es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo PRE-existente. Esto ocurre tanto de manera informal como deliberada.

Existen consorcios empresariales, que tienen como propósito precisamente el de proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos.

2. SEGURIDAD DEL ENTORNO

2.1 Concepto de Seguridad

En la actualidad, la seguridad en las redes ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles.
La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados. Se puede entender como seguridad un estado de cualquier sistema (informático o no) que nos indique que ese sistema está libre de peligro, daño o riesgo; es decir un sistema libre de todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

La seguridad informática no son más que técnicas desarrolladas para proteger los equipos informáticos individuales conectados a una red, de daños accidentales o intencionados. Dichos daños incluyen el mal funcionamiento del hardware, perdida física de datos o acceso a la base de datos o red de personas no autorizadas.

2.2 Elementos a 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 almacenamiento secundario (cintas, CD-ROMs, USBs…) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional el hardware, tanto en 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 auditoras de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo como el papel de impresora, cintas magnéticas) aunque se considera la seguridad en elementos externos al sistema.

2.3 Ataques

Las redes pueden verse perjudicadas por múltiples elementos como por ejemplo personas, programas o catástrofes naturales.

2.3.1 Personas

La mayoría de los ataques que se presentan en una red provienen de personas que, intencionada o inintencionadamente, pueden causar enormes perdidas.
En esta sección se describen los diferentes tipos de personas que de una u otra forma pueden causar un riesgo para la red; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por la red pero no la 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 la red no es su objetivo, y activos en caso de lo contrario.

- **Empleados**

  Muchas veces las amenazas a la seguridad de una red provenientes del los empleados de la propia empresa no son tomadas en cuenta.

Aunque los ataques puedan ser intencionados, lo normal es que más que 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 de red que se equivoca al teclear una orden y borra todos los sistemas de archivos.

- **Ex – empleados**

Otros posibles atacantes de una red son los antiguos empleados, principalmente aquellos que no abandonaron la empresa por propia voluntad o los que pasaron a una empresa de la competencia. Habitualmente, se trata de personas descontentas con la empresa que pueden aprovechar debilidades de una red que conocen a la perfección para dañarla por venganza, pueden insertar troyanos[3], bombas lógicas, virus o simplemente conectarse al sistema como si aún pertenecieran, pueden causar daños a la red o incluso chantajear a sus ex-compañeros o ex-jefes.

- **Curiosos**

Estos son los atacantes más habituales en las redes. Hay que recordar que los equipos trabajan en entornos donde hay personas que están interesadas por las nuevas tecnologías.

Hay que tener en cuenta 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. Aunque en la mayoría de las veces se trata

[3] **Troyanos:** son un conjunto de programas informáticos maliciosos

de ataques no destructivos, es claro que no benefician en lo absoluto al entorno de fiabilidad que se pueda crear en una determinada red.

- **Crackers**

Los crackers son personas que intentan descubrir información y contraseñas de las redes, violando la seguridad de un sistema informático con fines de beneficio personal o para hacer daño. Generalmente los crackers se aprovechan de redes abiertas, en donde la seguridad no es tenida muy en cuenta; provocando que los equipos conectados a la red sean vulnerables a problemas conocidos como:

- Explotación del robo de passwords
- Puertas traseras
- Fallos de autenticación
- Fallos en protocolos
- Software maligno: virus y gusanos, bomba de tiempo

- **Terroristas Informáticos**

Los terroristas no son simplemente aquellas personas que se dedican a hacer atentados; este concepto también abarca a cualquier persona que ataca a la red simplemente por causar algún tipo de daño. Por ejemplo, borrar las bases de datos o destruir los sistemas de archivos, etc.

- **Intrusos remunerados**

Estos son los atacantes más peligrosos de una red, ellos comúnmente atacan a las grandes redes. Se trata de personas sin autorización para entrar a la red

con gran experiencia en seguridad de redes y con un amplio conocimiento de redes, estas personas son pagadas por terceras personas para robar secretos de las empresas o simplemente para dañar la imagen de esta. Esta clase de ataques son los menos comunes o suceden con menos frecuencia, cuando pasan pueden ocasionar daños fatales a una empresa a través de su red.

2.3.2 Por amenazas lógicas

Este tipo de ataques son los que se presentan por medio de software creados especialmente para causar daños en una red o por medio de errores "bugs[4]".

- **Software incorrecto**

Estos provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.

- **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 unos sistemas o en la subred completa; un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

- **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 esta diseñando. A estos atajos

[4] **Bugs**: un error de software.

se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos. Si un atacante descubre una de estas puertas traseras va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad al sistema.

- **Bombas lógicas**

Programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola.

Ejemplos de condiciones predeterminadas:

- Día de la semana concreto.
- Hora concreta.
- Pulsación de una tecla o una secuencia de teclas concreta.
- Ejecución de un archivo concreto.

Ejemplos de acciones:

- Borrar la información del disco duro.
- Mostrar un mensaje.
- Reproducir una canción.
- Enviar un correo electrónico.

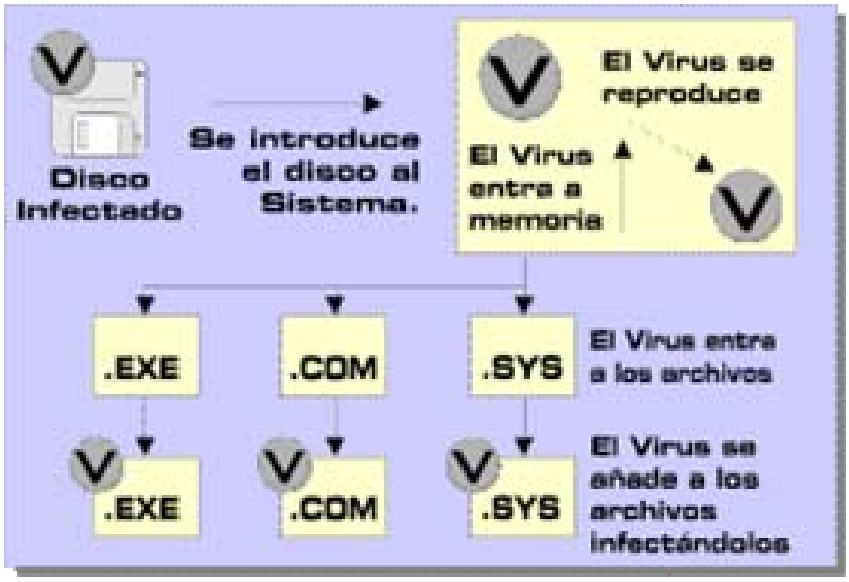
- **Virus**

Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus son programas que se replican y

ejecutan por sí mismos. Habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más benignos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

FIGURA 5. FUNCIONAMIENTO DE UN VIRUS



El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado

de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

Existen dos tipos de virus:

Aquellos que infectan archivos:

- **Virus de acción directa**. En el momento en el que se ejecutan, infectan a otros programas.
- **Virus residentes.** Al ser ejecutados, se instalan en la memoria de la computadora. Infectan a los demás programas a medida que se accede a ellos. Por ejemplo, al ser ejecutados.

Los que infectan el sector de arranque, (*virus de boot*). Hay que recordar que el sector de arranque es lo primero que lee el ordenador cuando es encendido. Estos virus residen en la memoria.

Los virus mas conocidos actualmente son: Gusanos, troyanos, virus de broma y falsos virus.

Según su comportamiento los virus informáticos pueden ser:

- **Kluggers:** Aquellos virus que al entrar en los sistemas de otro ordenador se reproducen o bien se cifran de manera que tan sólo se les puede detectar con algún tipo de patrones.
- **Viddbers:** Aquellos virus que lo que hacen es modificar los programas del sistema del ordenador en el cual entran.

Existen más clasificaciones según su comportamiento, siendo las citadas, parte de las más significativas y reconocidas por la mayoría de los fabricantes de antivirus.

Los virus más enviados según la **ICVS** (Informatic control virus scanner) son:

TABLA 1. VIRUS MÁS ENVIADOS SEGÚN ICVS

Tipos	1998	2000	2003	2007
Troyanos	20%	15%	22%	25%
Gusanos	22%	20%	25%	27%
Boot	5%	1%	4%	2%
Otros	52%	64%	49%	46%

Los virus informáticos afectan en mayor o menor medida a casi todos los sistemas más conocidos y usados en la actualidad.

Las mayores incidencias se dan en el sistema operativo Windows debido a:

- Su gran popularidad, como sistema operativo, entre los computadores personales. Se estima que, actualmente, (2007) un 90% de los computadores personales utilizan Windows. Esta popularidad facilita la vulnerabilidad del sistema.
- Sistema para el desarrollo de los virus, y así atacar sus puntos débiles, que por lo general son abundantes.
- Software como Internet Explorer y Outlook Express, desarrollados por Microsoft e incluidos en forma predeterminada en las últimas versiones de Windows, son conocidos por ser vulnerables a los virus ya que éstos aprovechan la ventaja de que dichos programas están fuertemente

integrados en el sistema operativo dando acceso completo y, prácticamente sin restricciones, a los archivos del sistema.

- La escasa formación de un número importante de usuarios de este sistema lo que provoca que no se tomen medidas preventivas por parte de estos, ya que este sistema está dirigido de manera mayoritaria a los usuarios no expertos en Informática. Esta situación es aprovechada, constantemente, por los programadores de virus.

En otros sistemas operativos como Mac OS X, Linux y otros basados en UNIX las incidencias y ataques son prácticamente inexistentes. Esto se debe principalmente a:

- No existen virus letales para estos sistemas, debido a su poderosa jerarquía de trabajo.
- Tradicionalmente los programadores y usuarios de sistemas basados en Unix[5] han considerado la seguridad como una prioridad por lo que hay mayores medidas frente a virus tales como la necesidad de autenticación por parte del usuario como administrador para poder instalar cualquier programa adicional al sistema.
- Los directorios o carpetas que contienen los archivos vitales del sistema operativo cuentan con permisos especiales de acceso por lo que no cualquier usuario o programa puede acceder fácilmente a ellos para modificarlos o borrarlos. Existe una jerarquía de permisos y accesos para los usuarios.

[5] **Unix:** sistema operativo portable

- Relacionado al punto anterior, a diferencia de los usuarios de Windows, la mayoría de los usuarios de sistemas basados en Unix no pueden normalmente iniciar sesiones como usuarios Administradores, excepto para instalar o configurar software, dando como resultado que si incluso un usuario no administrador ejecuta un virus o algún software malicioso pues este no dañaría completamente el sistema operativo ya que Unix limita el entorno de ejecución a un espacio o directorio reservado llamado comúnmente home.
- Estos sistemas a diferencia de Windows, son usados para tareas más complejas como servidores que por lo general están fuertemente protegidos, razón que los hace menos atractivos para un desarrollo de virus o software malicioso.

- **Gusanos**

  Un gusano es un virus informático que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo.

  Los gusanos siempre dañan la red, mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

  Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Los gusanos se basan en una red de computadoras para enviar copias de sí mismo a otros nodos (es decir, a otras terminales en la red) y es capaz de llevar esto a cabo sin intervención del usuario.

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

- **Caballos de Troya**

Es un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona. Fingiendo ser una utilidad o un juego, los caballos de Troya convencen al usuario de que sean instalados en una PC o en un servidor.

Los caballos de Troya en si no son un virus, aunque sean distribuidos y funcionen como tal. La diferencia fundamental entre un caballo de Troya y un virus, es que los virus pueden causar daños en la computadora, mientras que el caballo de Troya no siempre causa daños a la computadora, el solo intenta controlarla sin que nadie se de cuenta.

Los caballos de Troya entran a la computadora alojados en una imagen, archivo o aplicación, instalándose en esta cuando dicho archivo es abierto o ejecutado.

- **Programas conejo o bacterias**

Reciben este nombre algunos gusanos informáticos, cuyos códigos malignos llenan el disco duro con sus reproducciones en muy poco tiempo y que también pueden saturar el ancho de banda de una red rápidamente.

- **Características de los virus**

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir replicándose. Las redes en la actualidad ayudan a dicha propagación cuando estas no tienen la seguridad adecuada. Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como ejecute este programa y gane un premio.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software pirata o de baja calidad.

2.3.2 Prevenciones y soluciones a los diferentes tipos de ataques

- **Antivirus**: los llamados programas antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

- **Filtros de ficheros**: consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

- **Copias de seguridad**: Mantener una política de copias de seguridad garantiza la recuperación de los datos y una solución cuando nada de lo anterior ha funcionado.

- **Estudiar**: Aprender como es el software de nuestra computadora, buscando y buscando información, en sitios en los que e pueda confiar, sobre software dañino, para así evitarlo.

- **Desconfiar**: Si no conocemos algo o no sabemos lo que hace, será mejor tenerle respeto y no tocarlo hasta aclarar nuestra duda, (en el uso de esta regla es recomendable no abrir archivos de correos de los que se desconoce el remitente, o se sospecha de que pueda contener código malicioso, o que no pidió usted. Aun así, si es de entera confianza, analice siempre con un antivirus el archivo antes de abrirlo). Es aconsejable complementar esta manera de proceder aplicando una política de contraseñas y de seguridad más seguras a su red local o a los parámetros de acceso a Internet. Lo que muchos creadores de virus desean es la sensación de vulnerabilidad al provocar las condiciones de contagio idóneas que permitan una infección del virus a nivel mundial y causar daños sin dejar rastro de su presencia.

- **Hacer reenvíos seguros de e-mail**: Cuando recibamos un mensaje de correo electrónico sospechoso de contener virus o que hable de algo que desconocemos conviene consultar su posible infección o veracidad. Sólo si estamos seguros de la ausencia de virus del mensaje o de que lo que dice es cierto e importante de ser conocido por nuestros contactos lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios. Así evitaremos la propagación de mensajes con virus, así como la del SPAM[6].

    - **Informar a nuestros contactos**: Conviene que hagamos saber lo mencionado en el punto anterior a nuestros contactos en cuanto nos reenvían mensajes con virus o contenido falso.

[6] **SPAM:** son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor.

- **Limpiar y eliminar el virus**: En el caso de que nuestra máquina resulte infectada debemos proceder a su des-conexión inmediata de la red, ya sea local o Internet (esto se hace para evitar contagios a otras máquinas) y, una vez aislada, aplicar un programa Antivirus actualizado para tomar la acción que se corresponda.

- **Restauración completa**: En caso de que el virus sea tan virulento que destruya la lógica de una unidad de almacenamiento, se deberá recurrir a la restauración completa con formateo completo. Téngase en cuenta que esta operación dejará la maquina tal y como estaba el día que se adquirió. Sus configuraciones y demás quedarán borradas permanentemente.

2.3.3 Catástrofes

Las catástrofes son la amenaza menos probable contra los entornos habituales, aunque simplemente por su ubicación geográfica a nadie se le escapa la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad. Esta probabilidad es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generaran los mayores daños.

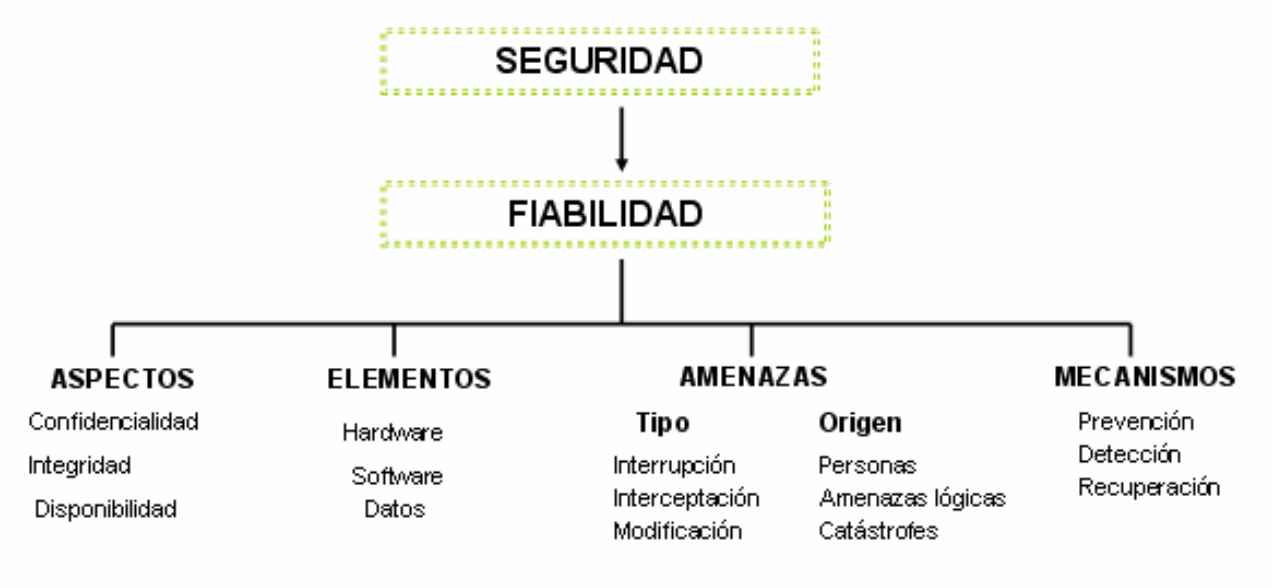
2.3.4 Planes de contingencia

Para proteger nuestra red debemos hacer un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrán generar y la probabilidad de su ocurrencia; a partir de este análisis se deben plantear políticas de seguridad

que den una responsabilidad y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan.

Hay que emplear mecanismos de seguridad al sistema de seguridad, convirtiéndose en herramienta básica para garantizar la protección de los sistemas de la red.

FIGURA 5. VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA



3. SEGURIDAD ENTORNO A OPERACIONES

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial.

3.1 Protección del hardware

El hardware es parte importante de un sistema informático de cualquier organización: universidades, centros tecnológicos y/o de investigación, por lo tanto las medidas encaminadas a asegurar su integridad son posibles soluciones o minimizadoras de amenazas frecuentes. A continuación se citarán algunas de las tantas amenazas posibles a los hardwares.

3.1.1 Acceso físico

La posibilidad de acceder a una máquina físicamente, en realidad lo puede hacer cualquier persona sin tener que violar reglas de seguridad de los sistemas operativos, es tan sencillo, que alguien tenga acceso a la CPU, al disco duro y a la información sin necesidad de utilizar claves de usuario, simplemente puede leer la información, borrarla o cambiarla. Visto esto, parece claro que cierta seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas conectados a ella; evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger. Teniendo parte de los equipos bien protegidos es menos probable recibir ataques a la red.

Para prevenir posibles ataques es importante considerar ciertas soluciones, desde las más sencillas y no costosas hasta las más complejas y costosas. Se pueden

emplear normas elementales como cerrar las puertas con llave al salir de un laboratorio o un despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados; o también video cámaras, tarjetas inteligentes o control de las llaves que abren determinada puerta.

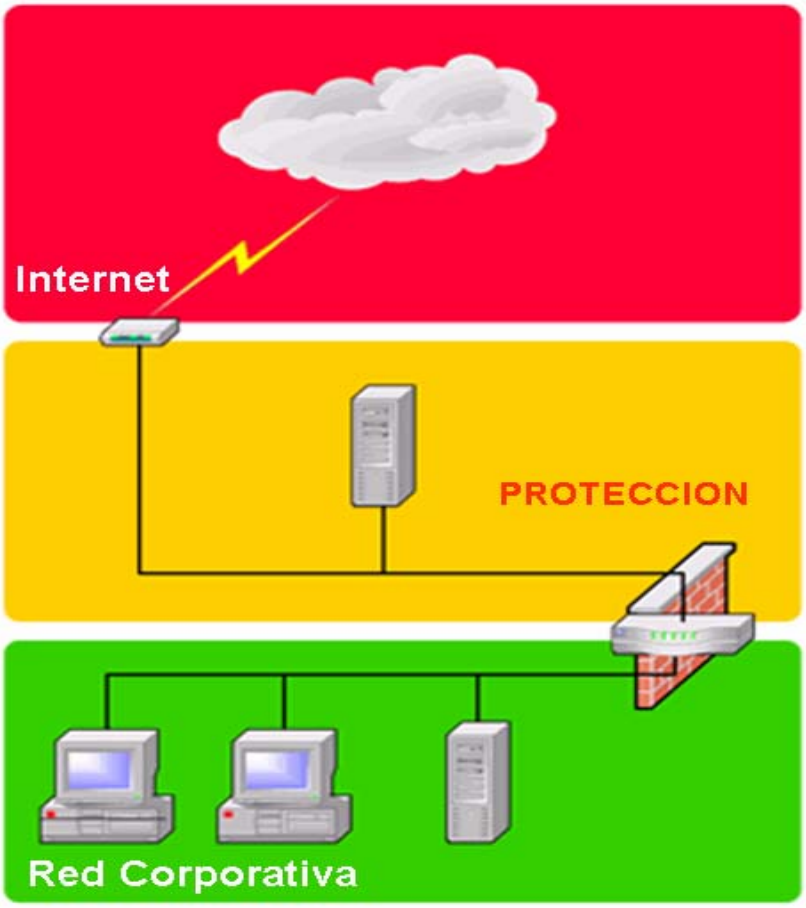
3.1.2 Desastres naturales

Los desastres naturales, no dan previo aviso de cuando van a ocurrir, por ejemplo en caso de terremotos, los elementos más críticos como las CPUs, los monitores o routers pueden sufrir daños si no se ubican en lugares apropiados (por lo general no tan altos), lo que pueden ocasionar consecuencias fatales como pérdida de datos o daños al hardware.

- Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de las maquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones es recomendable utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos.
- Las tormentas eléctricas pueden ocasionar serios problemas, en caso de la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir el hardware incluso protegido contra voltajes elevados. Una medida de seguridad podría ser ubicación de los medios magnéticos, especialmente las copias de seguridad o backups.

- Los niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una maquina. Medidas de protección pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos.

FIGURA 6. PROTECCION CONTRA DESASTRES



3.1.3 Desastres de entorno

Quizás los problemas derivados del entorno de trabajo mas frecuentes son los relacionados con el sistema eléctrico que alimenta a los equipos; cortocircuitos, picos de tensión, cortes de flujo, a diario amenazan la integridad tanto del hardware como de los datos que se almacenan o que circulan por el.
Una medida efectiva es utilizar tomas de tierra para asegurar la integridad los equipos, con esto se evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo de una sala o edificio.

- Otro problema, muchísimo más habitual en redes eléctricas, son los cortes en el fluido eléctrico que llega a los equipos. Aunque un simple corte de corriente no suele afectar al hardware, lo mas peligroso son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, las maquinas pueden sufrir daños. La forma más efectiva de proteger los equipos contra estos problemas de la corriente eléctrica es utilizar una SAI (Servicio de Alimentación Ininterrumpido) conectado al elemento que se quiere proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable, protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen capacidad para seguir alimentando las maquinas incluso en caso de que no reciban electricidad.
- El ruido eléctrico suele ser otro problema, es generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, se transmite a través del espacio o de líneas eléctricas cercanas a las instalaciones. Para prevenir los problemas que el ruido eléctrico puede causar en los equipos lo mas barato es intentar no situar hardware cercano a la maquinaria que puede causar dicho ruido; si no se tiene mas remedio que hacerlo, se puede instalar filtros en las líneas

de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos puede incluso dañar permanentemente a el hardware si tiene la suficiente potencia de transmisión.

- Los incendios pueden provenir de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en un edificio, o en una menos planta, donde se encuentran invertidos millones de pesos en equipamiento. Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor.
- Las temperaturas extremas evitan el buen funcionamiento de los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas. Para controlar la temperatura ambiente en el entorno de operaciones, nada mejor que un aire acondicionado, aparato que también influye positivamente en el rendimiento de los usuarios. Otra condición básica para el correcto funcionamiento de cualquier equipo es que se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU.

3.2 Protección de datos

De pronto en otro contexto la información es algo que no tiene mucho valor debido a su intangibilidad, pero cuando hablamos de computadores, sistemas de información o redes, allí pasa a jugar un papel muy importante. La información es el objeto de mayor valor para una organización, el objetivo es el resguardo de la

información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

Las medidas de seguridad que se tomen para proteger la información no afectan en nada la producción o efectividad de una red, las medidas de seguridad se tienen en cuenta al momento de diseñar una política, porque no solo basta con asegurar los medios físicos sino también la información almacenada y la que se retransmitirá a diferentes equipos. Existen ataques cuya intención no es solo destruir los medios físicos sino conseguir la información almacenada en ellos.

3.2.1 Eavesdropping

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red. Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

El snifing, consistente en capturar tramas que circulan por la red mediante un programa ejecutándose en una maquina conectada a ella o bien mediante un dispositivo (placa) que se engancha directamente el cableado. En la cabecera de los paquetes enviados a través de una red, entre otros datos, se tiene, la dirección del emisor y la del destinatario. De esta forma, independientemente de protocolo usado, las tramas llegan a su destino. Cada maquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino del paquete. Si estas direcciones son iguales asume que el paquete enviado es para ella, en caso contrario libera el paquete para que otras placas lo analicen.

Un Sniffer se colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer). Estos dispositivos, de alta impedancia, se conectan en paralelo con el cable de forma que la impedancia total del cable y el aparato es similar a la del cable solo, lo que hace difícil su detección. Inicialmente este tipo de software, era únicamente utilizado por los Administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

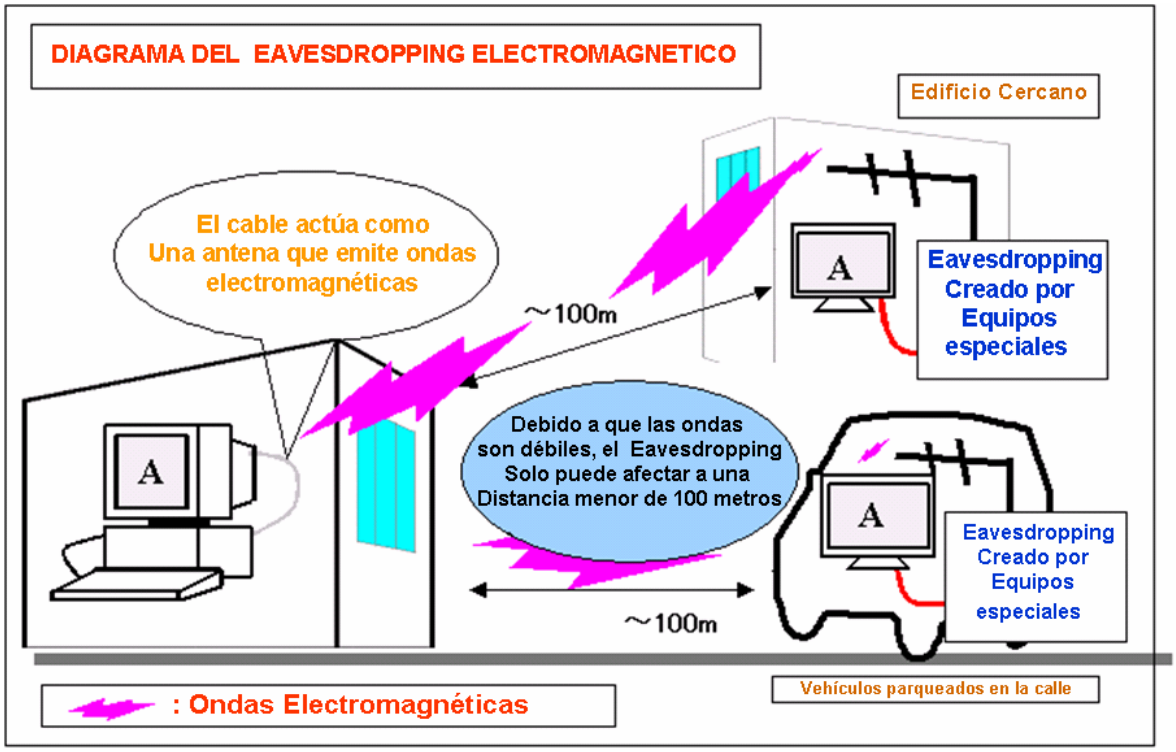
Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos. Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan.

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

Para contrarrestar estos ataques existen varias soluciones que se pueden emplear, una puede ser no permitir existencia de segmentos de red de fácil acceso, lugares donde para un atacante sea fácil de conectar estos aparatos y capture todo el trafico de ellos. Aunque esto resulte difícil en redes ya instaladas y en donde no se puede modificar su arquitectura; una solución podría ser el uso de aplicaciones de cifrado para realizar las comunicaciones o el almacenamiento de la información. Tampoco se debe descuidar las tomas de red libres, donde un

intruso con un portátil puede conectarse para capturar trafico; es recomendable analizar regularmente nuestra red para verificar que todas las maquinas activas estén autorizadas.

FIGURA 7. EAVESDROPPING



3.2.2 Backups

Backups se refiere a la copia de datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una perdida de información, lo que se quiere conseguir es la protección física de la información, en donde a futuro inmediato en caso de cualquier daño causado al hardware, se tenga un salvavidas de la información. Esto se trata no solo de tener una copia de la información, si no una vez copiada o salvada se organice y se guarde de tal forma que no sea accesible a todo tipo de personas, sino que tenga una codificación especial que solo pueda ser interpretada por el personal autorizado para manejar la

información, una idea puede ser, crear un código especial único en una organización en donde solo personal autorizado tenga acceso a ella.

La información guardada debe estar alejada de la sala de operaciones, con esto se busca evitar que en caso de ocurrir un incendio, los discos no se quemen y no se tenga forma de recuperar la información. Se debe alejar también de lugares húmedos o con probabilidades de escape de líquidos inflamables.

Algunos medios en donde se puede guardar información son:

- **Cinta magnética**: La cinta magnética es el medio de almacenaje más común usado para volcar datos almacenados, copias de seguridad, archivadores e intercambio. La cinta ha tenido comúnmente un orden de magnitud mejor de proporción capacidad/precio comparando con los discos duros, pero últimamente esas proporciones entre discos duros y cintas son más cercanas. Hay multitud de formatos, algunos de los cuales son específicos de mercados como unidades principales o a rangos de ordenadores particulares. La cinta es un medio de acceso secuencial, por ello aunque el tiempo de acceso es lento, la tasa de escritura y lectura continua de datos puede ser muy rápida. Algunas unidades de cinta son incluso más rápidas que discos duros actuales.
- **Disco duro:** Estos gracias a la proporción capacidad/precio han sido rápidamente mejorada para muchos años. Esto los ha convertido muy competitivos con las cintas magnéticas como un medio de volcar información. La principal ventaja de los discos duros en la gran capacidad y el corto tiempo de acceso que poseen.
- **Discos ópticos**: Entre los más usados están el CD y el DVD. Un CD puede ser usado como un mecanismo de copia de seguridad. Una ventaja de los CDS es que pueden almacenar hasta 650 MB de datos en 12 cm. Pueden

incluso utilizarse en cualquier maquina con una unidad de CD ROM. Otro de los formatos utilizados es el DVD. Muchos de los formatos de disco ópticos son de tipo de escritura única, lo que los convierte en más útiles para fines de almacenamiento desde que los datos no pueden ser modificados.

- **Disquetes**: Durante la década de los ochenta y principios de los noventa, muchas personas y usuarios de ordenadores personales asociaban la copia de seguridad con los disquetes de copia. La baja capacidad de datos de los disquetes los ha convertido en un caso olvidado en la actualidad.
- **Dispositivos de memoria no volátil:** También conocidos como memorias flash, llaves USB, compact flash, smart media, sticks de memoria, tarjetas Secure Digital, etc., estos dispositivos son relativamente costosos por su baja capacidad, pero ofrecen una manejabilidad excelente en casos de uso.
- **Servicios remotos de copia de seguridad:** A medida que el ancho de banda de Internet se ha convertido más extensa, los servicios de copia de seguridad remota han ganado en popularidad. Copias de seguridad vía Internet a una localización remota, puede protegernos ante hechos diversos como incendios o destrucciones de sistemas de copia de seguridad. La pega al servicio remoto de copia es que la velocidad de la conexión de Internet es menor que la velocidad de los dispositivos de almacenamiento de datos, así puede convertirse en un inconveniente si la cantidad de información es muy grande. Esto también tiene el riesgo de perder el control sobre el personal o sobre los datos más importantes.

3.2.3 Otros elementos

Casi que a diario en muchas organizaciones, la información llega a ser de acceso a un atacante, el caso se presenta cuando se dejan hojas con información sueltas o en la cola de la impresora y/o plotter, facturas y libros de registro.

Esto debido al descuido de cualquier persona que en momento tenga a cargo información valiosa que puede ser utilizada por personal de la organización para beneficio propio o para causar daños; también es apetecida por alguien ajeno a la misma.

Evidentemente, hay que tomar medidas contra estos problemas. En primer lugar, las impresoras, plotters, faxes, o cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos. Sería conveniente que un usuario que recoge una copia se acredite como alguien autorizado a hacerlo.

3.3 Radiaciones electromagnéticas

Las radiaciones electromagnéticas, son otro tipo de ataque a la red, estas se encuentran dentro de los eavesdropping.

Para protegernos de radiaciones electromagnéticas existen gran variedad de soluciones que se pueden aplicar, la primera podría ser: la distancia, debido a que las señales que se transmiten por el espacio son atenuadas conforme aumenta la separación de la fuente, si se tiene un perímetro amplio de seguridad es más difícil para un atacante interceptar a cierta distancia las emisiones. Esta solución

también es válida para las señales inducidas a través de conductores, que aunque también se atenúan por la resistencia e inductancia del cableado, la pérdida no es la suficiente para considerar seguro el sistema.

La confusión es otra posible solución, debido a que si se tiene muchas señales dentro de un mismo medio, es difícil para un atacante filtrar lo que esta buscando, aunque de esta forma no es imposible evitar la interceptación, dificulta el acceso a la maquina que se quiere. Esto se puede conseguir teniendo cerca fuentes emisoras como monitores, cables, radios, etc., de donde se emite información diferente.

Existe también un hardware diseñado para crear ruido electromagnético, con señales de radio que enmascaran las radiaciones emitidas por el equipo a proteger, aunque si se usan frecuencias no permitidas por el gobierno, el uso de estos dispositivos puede ser ilegal, lo que hace necesario tener una licencia para poder trasmitir.

Finalmente se presenta una solución efectiva pero un poco costosa, se hace referencia al uso de dispositivos certificados que aseguran una mínima emisión, esto es instalaciones que apantallan a las radiaciones. En el hardware, hay dos aproximaciones para prevenir las emisiones: una es la utilización de circuitos especiales que apenas emiten radiaciones suprimidas, y la otra es la contención de las radiaciones, por ejemplo aumentando la atenuación; generalmente ambas aproximaciones se aplican conjuntamente. En cuanto a las instalaciones utilizadas para prevenir el eavesdropping, la idea general es aplicar la contención no solo a ciertos dispositivos, sino a una edición o a una sala completa.

Una solución muy utilizada son las jaulas de Faraday sobre lugares donde se trabaja con información sensible, conceptualmente hace referencia a un efecto que provoca que el campo electromagnético en el interior de un conductor en

equilibrio sea nulo, anulando el efecto de los campos externos. Esto se debe a que, cuando el conductor sujeto a un campo electromagnético externo, se polariza de manera que queda cargado positivamente en la dirección en que va el campo electromagnético, y cargado negativamente en la dirección contraria. Puesto que el conductor se ha polarizado, este genera un campo eléctrico igual en magnitud pero opuesto en dirección al campo electromagnético, luego la suma de ambos campos dentro del conductor será igual a 0. Específicamente se trata de separar el espacio en dos zonas electromagneticamente aisladas (por ejemplo, una sala y el resto del espacio) de forma que fuera de una zona no se puedan captar las emisiones que se producen en su interior. Para implementar esta solución se utilizan materiales especiales, como algunas clases de cristal, o simplemente un recubrimiento conductor conectado a tierra.

Las radiaciones electromagnéticas no son riego importante en la mayoría de las organizaciones, por lo tanto estas soluciones son aplicables a los entornos donde se trabaja con información altamente confidencial, como empresas militares o de inteligencia.

4. POLÍTICAS DE SEGURIDAD

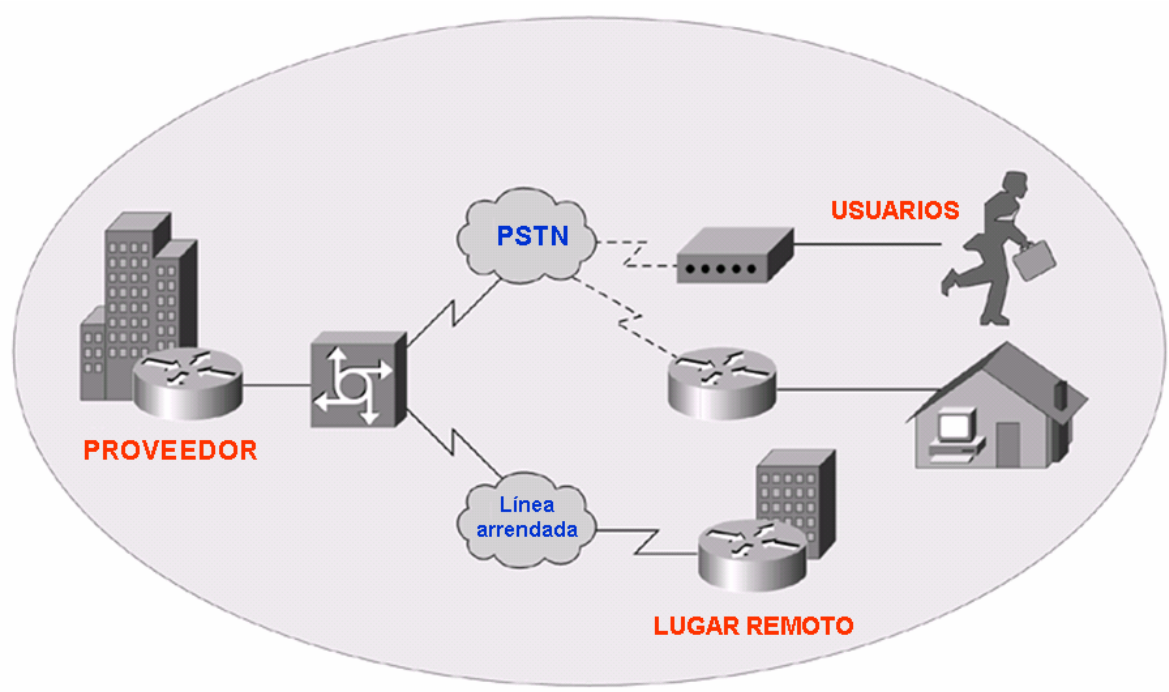
4.1 Concepto de políticas de seguridad

Las políticas de seguridad son mecanismos que resumen cómo se utilizara y cómo se protegerá los recursos de una computadora y de la red, los cuales ayudan a establecer la comunicación entre usuarios, recursos y servicios informáticos de una organización de manera confiable. Estas no involucran sanciones, ni reglamentaciones a los usuarios, más bien es una descripción formal de las reglas a seguir para tener acceso a los activos de la información y a la información de una organización.

Si una compañía desea proteger adecuadamente su red, debe poner una política de la seguridad en ejecución. Es importante establecer un buen equilibrio entre el nivel de la seguridad y la capacidad de usuarios de conseguir la información que necesitan.

En la figura 8, se muestra una red con disponibilidad a Internet y redes públicas; se puede ver que la red tiene acceso tanto a redes públicas y como privadas, por lo tanto, asegurar estas redes ha llegado a ser fundamental e importante. Con el desarrollo de estas redes, ha habido un aumento enorme en amenazas de la seguridad. Las amenazas de la seguridad han aumentado no sólo porque los hackers han descubierto más vulnerabilidades, sino que también han llegado a ser más fáciles de utilizar y el conocimiento técnico más simple aprender.

FIGURA 8. RED CON DISPONIBILIDAD A INTERNET



La seguridad se ha movido a la vanguardia de la puesta en práctica y de la gerencia de red; está permitiendo el acceso abierto a los recursos de la red y a asegurarse de que los datos y que los recursos sean seguros para la supervivencia de muchos negocios. La necesidad de la seguridad está llegando a ser más importante debido a lo siguiente:

- Es importante para las organizaciones, porque los datos confidenciales que viajan por la red necesitan ser protegidos.
- Se requiere para comunicar y hacer de ambientes de negocio seguridad, ya que algunos son potencialmente inseguros.

Establecer una política de seguridad debe ser el primer paso en la migración de una red a una infraestructura segura.

4.2 Importancia de una política de seguridad

Las políticas de la seguridad proporcionan muchas ventajas y valen el tiempo y el esfuerzo necesitados para desarrollarlas. Las políticas de la seguridad son importantes para las organizaciones por un número de razones, incluyendo las siguientes:

- Crea una guía actual de la seguridad en la red.
- Fija un marco para la puesta en práctica de la seguridad en la red.
- Define el comportamiento permitido y rechazado.
- Ayuda a determinar las herramientas necesarias y los procedimientos.
- Define cómo manejar incidentes de la seguridad en la red.

Estas razones conducen directamente a preguntarse que debe contener una buena política de seguridad; a continuación se hace una breve descripción de los componentes dominantes o de las secciones para una política de seguridad:

- ✓ **Declaración de la autoridad y del alcance:** Identifica a los patrocinadores de la política de seguridad y de los asuntos que se cubrirán.
- ✓ **Aceptación del uso de la política de seguridad:** Explica lo que admite y no admite la compañía al mirar la infraestructura de la información.
- ✓ **Política de la identificación y de la autentificación:** Específica qué tecnologías y que equipos se utilizaran para asegurarse de que solamente los individuos autorizados tengan acceso a los datos de la organización.
- ✓ **Política del acceso a Internet:** Define el uso ético y apropiado de las capacidades de acceso del Internet de la organización.
- ✓ **Política de acceso en el campo de trabajo:** Define cómo los usuarios locales deben utilizar la infraestructura de los datos.

- ✓ **Política de acceso en un lugar remoto:** Describe cómo los usuarios alejados deben tener acceso a la infraestructura de los datos de la organización.
- ✓ **Procedimientos en caso de un incidente:** Especifica como la organización crea los mecanismos de respuesta en caso de que ocurra un incidente y los procedimientos que se utilizaran durante y después de que ocurra.

Hay que tener en cuenta que cada política de seguridad de una compañía es única y debe resolver los objetivos de la compañía.
El propósito principal de una política de seguridad es informar a los usuarios al personal y a la gerencia, su obligación de proteger los activos de la tecnología y de la información de una organización. La política debe indicar los mecanismos a través de los cuales estos requisitos pueden ser resueltos. Una política de seguridad debe ser tan explícita como sea posible evitar ambigüedad o el malentendido.

4.3 Proceso de desarrollo

Todos los sitios deben tener un plan comprensivo de la seguridad. Este plan debe estar en un nivel más alto que políticas. El plan de la seguridad se debe hacer a mano como marco de las amplias pautas en las cuales las políticas específicas caben. Es importante tener este marco en lugar de modo que las políticas individuales sean constantes con la arquitectura total de la seguridad del sitio. Hay que tener una política fuerte en el acceso corporativo, y establecer restricciones para quienes intenten acceder a la organización y utilizar las computadoras.

Dos filosofías opuestas pueden ser adoptadas al definir un plan de seguridad: niegue todos y permita todos. Ambos alternativas tienen puntos fuertes y débiles, y la opción entre ellos depende de la necesidad de la seguridad de un sitio en particular. La primera opción es negar todo y después permitir selectivamente servicios sobre una base. Esto dificulta un poco el acceso pero lo hace mas seguro.

El otro modelo, se refiere que como permite todos, es mucho más fácil de poner en ejecución lo que quiere, puede ser generalmente menos seguro que el negar todo el modelo. Este es generalmente el defecto en un sistema huésped ya que permite que todos los protocolos viajen a través de límites de la red. Ambos modelos se pueden utilizar en el mismo tiempo.

Para hacer eficaz una política de seguridad, es importante designar a un equipo de desarrollo, el cual necesita tener la aceptación y la ayuda de todos los niveles de empleados dentro de la organización. Es importante que la gerencia corporativa apoye completamente el proceso de la política de seguridad. Cuando se crea una política de seguridad en una organización, deben tenerse en cuenta los siguientes aspectos para tener un equipo que respalde las políticas implantadas:

- Administrador de seguridad del sitio.
- Personal técnico de la tecnología de información.
- Administradores de grandes grupos de usuarios.
- Equipo de apoyo en caso de incidentes.
- Representantes de los grupos de usuarios afectados por la política.
- Gerencia responsable.

- Recursos humanos.

4.4 Incidentes que se manejan en el proceso

En caso de ocurrir incidentes durante el proceso es recomendable considerar la siguiente lista que identifica los objetivos para ocuparse de incidentes

- Determínese qué sucedió.
- Planee cómo evitar un ataque y como evitar que se repita.
- Evite el progreso del incidente.
- Determine el impacto y el daño del incidente.
- Recupérese del incidente.
- Políticas y procedimientos de la actualización según lo necesitado.
- Identifique los autores.

Dependiendo de la naturaleza del incidente, analice las prioridades entre la fuente original del problema y la restauración de sistemas y de servicios.
Para parar o para prevenir el acceso desautorizado y para proteger la información se usan siguientes métodos:

- La autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.
- Criptografía es un método para asegurar el secreto, la integridad, y la autenticidad de las comunicaciones de datos a través de una red.
- El cortafuego (firewall) es un sistema de servicios relacionados, situado en una entrada de la red, que protege los recursos de una red privada contra usuarios de otras redes. Los cortafuegos pueden también ser dispositivos independientes o se pueden configurar.

5. CRIPTOLOGIA

Es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un transmisor y un receptor a través de un canal de comunicaciones (red de computadoras en nuestro caso). Engloba tanto las técnicas de cifrado, como sus técnicas complementarias. Esta ciencia esta dividida en dos grandes ramas:

La Criptografía que es una de las ciencias considerada de las más antiguas del mundo, es la encargada de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de información o mensajes de manera que sólo puedan ser leídos por los usuarios a quienes van dirigidos. Y el Criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de descifrar la información o mensajes originales en ausencia de la clave, rompiendo así el criptosistema.

5.1 Aplicaciones de la criptografía

La principal aplicación de la criptografía es proteger la información para evitar que sea accesible por personas o usuarios NO autorizados para acceder a la red, proteger datos de la red, pero también tiene otras aplicaciones como son:

- Modificar un mensaje de tal forma que sea completamente ilegible por cualquier persona a menos que dicha persona posea la clave para volver a ponerlo en su estado original.
- Verificar que un mensaje NO ha sido modificado "*intencionalmente*" por una persona o usuario ajeno a la red.
- Verificar que "alguien" es quien realmente dice ser.

5.2 Criptosistemas

Matemáticamente un criptosistema es una cuaterna de elementos formada por:

- Un conjunto finito llamado alfabeto, que según unas normas sintácticas y semánticas, permite emitir un mensaje en claro así como su correspondiente criptograma.
- Un conjunto finito denominado espacio de claves formado por todas las posibles claves, tanto de encriptación como de desencriptación, del criptosistema.
- Una familia de aplicaciones del alfabeto en sí mismo que denominamos transformaciones de cifrado.
- Una familia de aplicaciones del alfabeto en sí mismo que denominamos transformaciones de descifrado.

Pero un criptosistema informático se esta formado por los siguientes cuatro elementos:

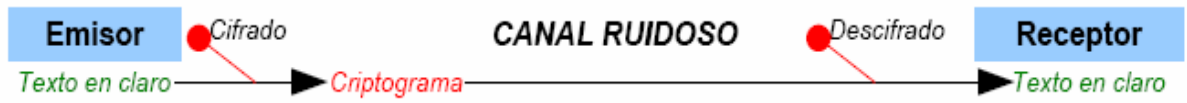
- Un conjunto finito denominado *alfabeto*, que permite representar tanto el texto en claro como el criptograma. A bajo nivel hablaríamos de *bits*, y a más alto nivel podríamos hablar de caracteres ASCII o MIME.
- Un conjunto finito denominado espacio de claves. Estaría constituido por la totalidad de las claves posibles del criptosistema.
- Una familia de transformaciones aritmético-lógicas que denominamos transformaciones de cifrado.
- Una familia de transformaciones aritmético-lógicas que denominamos transformaciones de descifrado.

Es adaptar un criptosistema a las posibilidades y limitaciones de una computadora.

El alfabeto o espacio de caracteres suele ser un estándar de representación de información (típicamente MIME o UNICODE por motivos de compatibilidad) y a más bajo nivel, por bits. Las transformaciones de cifrado y descifrado se ciñen a las normas de computación de los ordenadores actuales. En realidad, para efectos prácticos no existe mucha diferencia entre criptosistema matemático e informático, pues los matemáticos suelen diseñarse pensando en representaciones computacionales (pues solamente los ordenadores tienen la potencia necesaria para soportar los complejos algoritmos), y los informáticos se desarrollan siempre con una base matemática.

En un criptosistema la información sigue un flujo siempre fijo como se observa en la figura 9.

FIGURA 9. FLUJO DE INFORMACIÓN EN UN CRIPTOSISTEMA



El emisor cifra el texto en claro (cualquier información que resulte legible por cualquier persona) para obtener el criptograma, que viaja por un canal ruidoso. El receptor descifra el criptograma y obtiene de nuevo el texto en claro que el emisor le envió. Durante toda la transmisión, el mensaje es incomprensible.

5.3.1 Criptosistemas de clave secreta

Son aquellos en los cuales la clave de cifrado (clave secreta, única o simétrica) se puede conocer o calcular a partir de la clave de descifrado y viceversa. En la mayoría de estos sistemas, ambas claves coinciden, y lógicamente han de mantenerse como un secreto entre emisor y receptor:
Si un atacante descubre la clave utilizada en la comunicación, entonces se dice que se ha roto el criptosistema. Los criptosistemas de clave secreta son matemáticamente menos complicados que los clave pública.

Los sistemas de cifrado de clave única se dividen a su vez en dos grandes grupos de criptosistemas: por una parte tenemos los *cifradores de flujo*, que son aquellos que pueden cifrar un sólo bit de texto claro al mismo tiempo, y por tanto su cifrado se produce bit a bit, y por otro lado tenemos los *cifradores de bloque*, que cifran un bloque de bits (habitualmente, cada bloque es de 64 bits) como una única unidad.

5.3.1.2 DES

DES (Data Encryption Standard) es un algoritmo simétrico de cifrado en bloques de 64 bits basado en LUCIFER (criptosistema interno de IBM).
Fue ideado por IBM y aceptado por el NIST (National Institute of Standars and Technology) en 1976. Se trata de un algoritmo de 64 bits de clave de los cuales 56 bits componen la clave de cifrado propiamente dicha, mientras los 8 restantes son de paridad y se usan para corrección de errores. DES puede ser implementado tanto en software como en chips con tecnología VLSI (Very Large Scale Integration), como en hardware, alcanzando aquí una velocidad de hasta 50 Mbs.

DES actualmente ya no es estándar criptográfico y fue roto en Enero de 1999 con un sistema de cómputo que analizaba 250.000.000.000 claves por segundo. Su principal ventaja es la rapidez de cálculo y la sencillez de su implementación.
Sus principales defectos son la poca longitud de clave que maneja, unido a la incapacidad de manejar claves de longitud variable; y su debilidad en un uso continuado de la misma clave, pues si se disponen de suficientes criptogramas, mediante criptoanálisis diferencial es posible romper la clave en 2^47 iteraciones.

5.3.1.2 Triple – DES

Dada la capacidad de cómputo actual y la relativa facilidad que supone romper el algoritmo DES, se desarrolló un sistema de triple aplicación al algoritmo DES, con tres claves diferentes para aplicar sucesivamente (en realidad se usa una clave externa dividida para aplicación intermedia dado que DES matemáticamente no es grupo, y su aplicación repetida ocasionaría un aumento efectivo de tamaño).
Mediante este sistema se obtiene un cifrado de 192 bits (168 efectivos y 24 de paridad) con tres claves que resulta mucho más complejo de vulnerar.

5.3.2 Criptosistemas de clave publica

Son aquellos en los cuales la clave de cifrado es conocida, pero la clave de descifrado (clave privada) si mantiene en secreto. Ambas claves se complementan, pero aun conociendo la pública no se puede deducir o conocer la privada sin tener información adicional. Este hecho hace que estos sistemas también sean conocidos como asimétricos.

Cuando un receptor quiere recibir una información o mensaje cifrado, le envía a todos sus posibles emisores su clave pública, para que estos le envíen la

información cifrada con su clave, así él será el único que podrá descifrar la información o mensaje, mediante su clave privada.

5.3.2.1 El criptosistema RSA

Este criptosistma de clave pública nació en 1978, fue creado por Ron Rivest, Adi Shamir y Leonard Adleman, en honor a ellos es conocido con las siglas RSA78. Se trata de un algoritmo de cifrado asimétrico basado en el problema de la factorización entera, y aunque la descripción de este algoritmo fue propuesta en 1973 por Clifford Cocks, fue secreta hasta 1978 cuando se publicó RSA. Este algoritmo fue patentado, pero dicha patente expiró en el año 2000, por esto actualmente se trata de un algoritmo libre.

En la Tabla 2 se observan los pasos del algoritmo RSA:

TABLA 2. ALGORITMO RSA

1	Escoger dos números primos muy grandes p y q (secretos) y calcular el número n (público) correspondiente a su producto, $n = p * q$
2	Escoger la clave de descifrado constituida por un gran número entero d (secreto), que es primo con el número $\Phi(n)$ (secreto) obtenido mediante: $\Phi(n) = (p-1) * (q-1)$
3	Calcular el entero e (público) tal que $1 \leq e \leq \Phi(n)$, mediante la fórmula: $e * d = 1 \pmod{\Phi(n)}$
4	Hacer pública la clave de cifado (e, n)
5	Para cifrar texto, es necesario previamente codificar el texto en un sistema numérico en base b dividiéndolo en bloques de tamaño $j-1$ de forma que $b^{j-1} < n < b^j$
6	Cifrar cada bloque M_i transformándolo en un nuevo bloque de tamaño j C_i de acuerdo con la expresión $C_i \equiv M_i^e \pmod{n}$
7	Para descifrar el bloque C_i, se usa la clave privada d según la expresión: $M_i \equiv C_i^d \pmod{n}$

Ahora observen un ejemplo práctico de cómo generar un criptosistema RSA:

1. Seleccionamos dos números primos ***p = 11*** y ***q = 3***.
2. Calculamos ***N = p * q*** y ***Φ = (p-1) * (q-1) = 10 * 2 = 20***
3. Elegimos el exponente ***e = 3*** comprobando ***mcd (e, p-1) = mcd (3, 10) = 1*** y...***mcd (e, q-1) = mcd (3, 2) = 1*** , lo que implica que...
   mcd (e, Φ) = mcd (e, (p-1) (q-1)) = mcd (3, 10, 2) = 1
4. Calcular ***d*** tal que ***e * d = 1 (mod Φ(n))*** , por ejemplo ***d = 7*** (comprobamos ***e * d-1 = 3 * 7-1 = 20*** que es divisible por ***Φ***)
5. ***Clave Pública = (n, e) = (33, 3)***
   Clave Privada = (n, d) = (33, 7)

Ahora se puede observar un ejemplo de cómo generar un mensaje cifrado con RSA:

1. Queremos encriptar el mensaje ***m = 7***

2. Calculamos el cifrado ***c = me mod n = 73 mod 33 = 343 mod 33 = 13***

3. Nuestro texto cifrado es ***c = 13***

4. Calculamos el descifrado ***m' = cd mod n = 137 mod 33 = 7***

5. El mensaje descifrado es ***m' = 7***

En la actualidad día RSA es el algoritmo de criptosismas de clave público más utilizado, en conexiones de Internet y protocolos seguros, como también en cifrado de datos (por ejemplo en el sistema PGP). Las longitudes de las claves pueden estar desde 512 hasta los 4096 bits, aunque por lo general se usan claves de 1204 y a que son consideradas como más seguras.

El sistema RSA ha permanecido invulnerable hasta hoy, a pesar de los numerosos ataques de criptoanalistas.

5.3.2.2 El criptosistema de ElGamal

Este criptosistema de clave pública fue desarrollado entre los años de 1984 y 1985 por ElGamal, se basa en la intratabilidad computacional del problema del logaritmo discreto.

Normalmente no se utiliza de forma directa, ya que la velocidad de cifrado y autenticación es inferior a la obtenida con el criptosistema RSA, y además las firmas producidas son más largas (el doble de largo que el texto original), el algoritmo de ElGamal es de gran importancia en el desarrollo del DSS (Digital Signature Standard), del NIST. En este criptosistema, para generar un par de claves pública/privada, se escoge un número primo grande y dos enteros.
Para firmar un determinado mensaje, el emisor elige un entero aleatorio no usado con anterioridad y con la restricción que sea relativamente primo.
La característica principal que distingue es criptosistema de los demás es que en el cifrado se utiliza aparte de la clave pública del receptor, la clave privada del emisor.

5.3.2.3 Criptosistema de McEliece

Fue creado por McEliece en 1978, se conoce por sus siglas MCE78. Se fundamenta en la *Teoría de la codificación algebraica*, Basa su potencia en el hecho de que la decodificación de un código lineal general es un problema NP-completo. Un punto importante a la hora de entender la complejidad computacional de este algoritmo es el hecho de que no trabaje con cifras enteras, sino con matrices. Además, se introduce un gran factor de expansión de datos, en función de las palabras del código de Goppa, y se produce un desorden intencionado mediante la adición de ruido.

Por desgracia su aplicación de momento no pasa del ámbito teórico, y no se han desarrollado criptosistemas de clave pública sobre este algoritmo, aunque está siendo investigado hoy en día.

5.4 Criptoanálisis

Es otra rama de estudio de la criptología la cual estudia el camino inverso de la criptografía, dedicando sus esfuerzos a descubrir los secretos que la criptografía se empeña en mantener ocultos. Consiste en descifrar un mensaje o información sin conocer el método por el cual fue cifrado, y hallar la forma de violar sistemas criptográficos.

Para diseñar un algoritmo robusto de cifrado, se debe utilizar criptoanálisis para encontrar y para corregir cualquier debilidad.
Suponiendo conocidos los algoritmos de encriptación el criptoanálisis consiste en comprometer la seguridad de un sistema criptográfico. El criptoanálisis consiste en buscar los puntos débiles de un sistema criptográfico.

Existen diferentes formas de atacar un sistema criptográfico:

- ***Ataque por fuerza bruta***, si se tiene un criptograma mediante este método se probaran todas las claves posibles para obtener el texto plano. Si el conjunto de posibles claves es alto este sistema es inviable. Normalmente a este tipo de ataques no se les suele considerar como una forma de criptoanálisis ya que no busca puntos débiles, únicamente utiliza todas las claves posibles.

- ***Ataque por texto plano escogido***, consiste en elegir varios textos planos y obtener sus criptogramas asociados. Esto implica tener acceso al dispositivo de encriptación, pero no a la clave de encriptación

- ***Ataque a partir de texto plano***, el atacante tiene acceso a textos planos y a sus correspondientes criptogramas.

- ***Análisis por frecuencias***, este tipo de ataque es utilizado para romper sistemas criptográficos simétricos y se basa en estudiar la frecuencia con la que aparecen los distintos símbolos en un lenguaje determinado y luego estudiar la frecuencia con la que aparecen en los criptogramas, y de esta manera establecer una relación y obtener el texto plano.

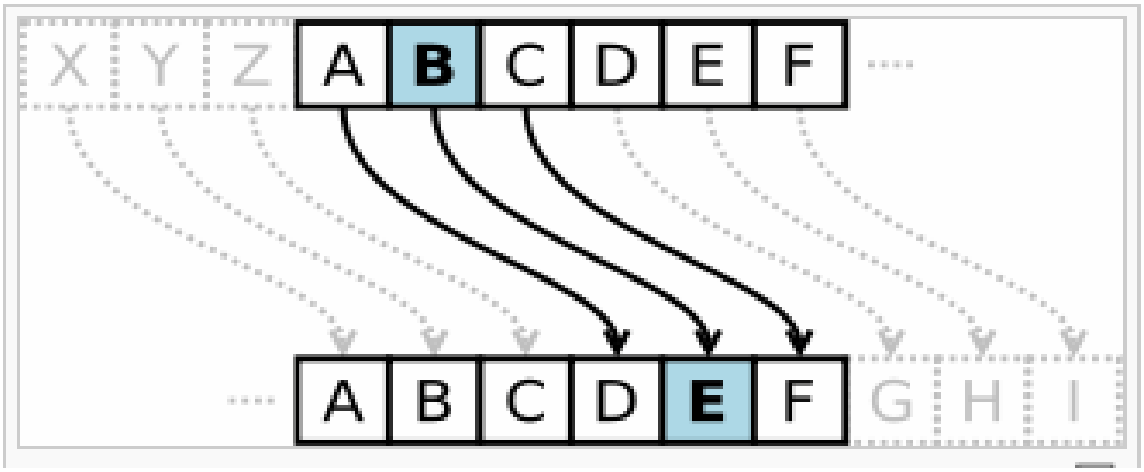
5.5 Criptografía clásica

Se basan en conceptos que podríamos denominar clásicos como son los de transposición y sustitución con una clave privada, si bien en estos sistemas la operación se realiza sobre una cadena de bits y no sobre caracteres.

5.5.1 El sistema Caesar o César

Es una de las técnicas más sencillas y de las más utilizadas, también conocida como *cifrado por desplazamiento*, Debe su nombre al emperador Julio Cesar, que lo utilizo para establecer comunicaciones seguras con sus generales durante las guerras. Es un cifrado por sustitución, en el cual una letra en el texto original es reemplazada por otra letra que se encuentra en una posición que está un número determinado de espacios más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería reemplazada por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etcétera. Como se observa en la figura 10.

FIGURA 10. EJEMPLO DE CIFRADO CAESAR



El cifrado Caesar tiene 26 claves diferentes utilizando el alfabeto ingles.

5.5.2 El criptosistema de Vigenere

Es un sistema poli alfabético o de sustitución múltiple. Este tipo de criptosistemas es un cifrado basado en diferentes series de caracteres o letras de Caesar, que presentaban ciertas debilidades frente al ataque de los criptoanalistas relativas a la frecuencia de aparición de elementos del alfabeto. El principal elemento de este sistema es la llamada Tabla de Vigenere, una matriz de caracteres cuadrada, con dimensión 26 x 26, que se muestra en la siguiente figura 11.

FIGURA 11. MATRIZ DE VIGENERE

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Este cifrado es fácil de entender e implementar, además parece irrompible.

5.6 Funciones resumen

La criptografía asimétrica utilizan las llamadas funciones resumen para identificar un mensaje se. El resultado de aplicar una función resumen a un texto es un número grande, que tiene las siguientes características:

- Todos los números resumen generados con un mismo método tienen el mismo tamaño sea cual sea el texto plano.

- Dado un texto plano, es fácil y rápido (para un ordenador) calcular su número resumen.
- Es imposible reconstruir el texto plano a partir del número resumen.
- Es imposible que dos textos planos diferentes tengan el mismo número resumen.

Una de las aplicaciones criptográficas mas importante de las funciones resumen es sin duda la verificación de integridad de archivos. Una función resumen puede generar claves iguales para objetos diferentes, ya que el rango de posibles claves es mucho menor que el de posibles objetos a resumir. Hay muchos algoritmos de este tipo. Uno de los más conocidos es SHA, que se utiliza habitualmente para firmas digitales.

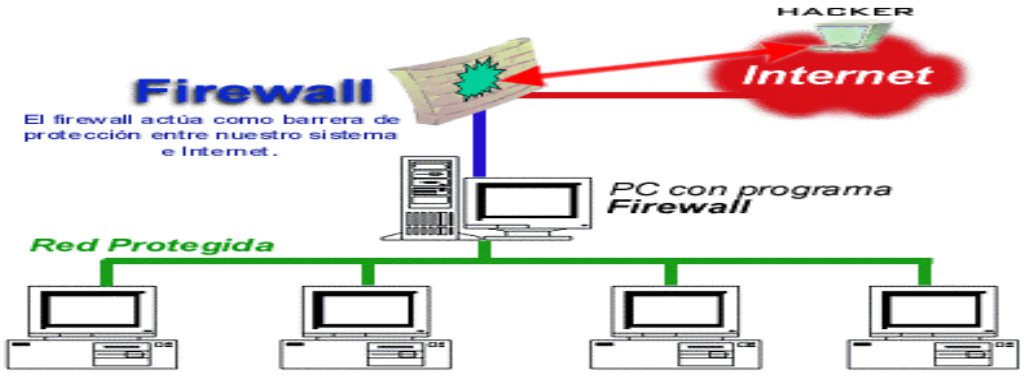
6. FIREWALL

6.1 Concepto de firewall

También es conocido como cortafuegos, es un elemento de hardware o software utilizado en las redes para permitir o prohibir algunos tipos de comunicaciones de acuerdo por las políticas de red. Es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra.

Un firewall puede ser un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar computadores muy potentes y con softwares específicos que lo único que hacen es monitorizar las comunicaciones entre redes. Un uso característico de los cortafuegos es ubicarlos entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. En la figura 12 se puede observar la ubicación de un firewall dentro de una red.

FIGURA 12. UBICACIÓN DE UN FIREWALL DENTRO DE UNA RED



Los firewalls se crean como objetivo principal para tratar las innumerables amenazas planteadas a una red de una organización, permitiendo el acceso solamente al tráfico válido.

6.1.1 Firewall de capa de red o de filtrado de paquetes

Es uno de los principales tipos de firewalls. Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.

Este tipo de firewalls toman decisiones según la dirección de transmisión, dirección de recepción y el puerto de cada uno de los paquetes IP. Un ejemplo de un firewall de capa de red puede ser un router. Cuentan con una dirección IP valida. Los firewalls tienden a ser muy rápidos, y sobre todo, invisibles al usuario.

6.1.2 Firewall de capa de aplicación

Trabaja en el nivel de aplicación (nivel 7) de la pila de protocolos (TCP/IP). Analizando todo el tráfico de HTTP, (u otro protocolo), puede interceptar todos los paquetes que llegan o salen desde y hacia las aplicaciones que corren en la red. Este tipo de cortafuegos usa ese conocimiento sobre la información transferida para proveer un bloqueo más selectivo y para permitir que ciertas aplicaciones autorizadas funcionen adecuadamente. A menudo tienen la capacidad de modificar la información transferida sobre la marcha, de modo de engañar a las aplicaciones y hacerles creer que el cortafuego no existe.

Un firewall de capa de aplicación puede ser un host con servidores proxy, que no permiten el tráfico pase directamente entre dos redes. Los firewalls de capa de aplicación también se utilizan como traductores de direcciones de red; Estos sistemas proporcionan informes de auditoria más detallados que los firewalls de capa de red; se usan cuando la política de control de acceso es más conservadora.

6.1.3 Firewall personal

Este tipo firewalls o cortafuegos se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

6.2 Ventajas de un firewall

- Los firewalls en Internet permiten administran los posibles accesos de Internet a una red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet.

- Los firewall permiten al administrador de una red establecer un "choke point" (punto de obstrucción), para así controlar el acceso de los usuarios no autorizados (hackers, crakers, espías, etc) fuera de la red, restringiendo el acceso de entrada o salida a los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.

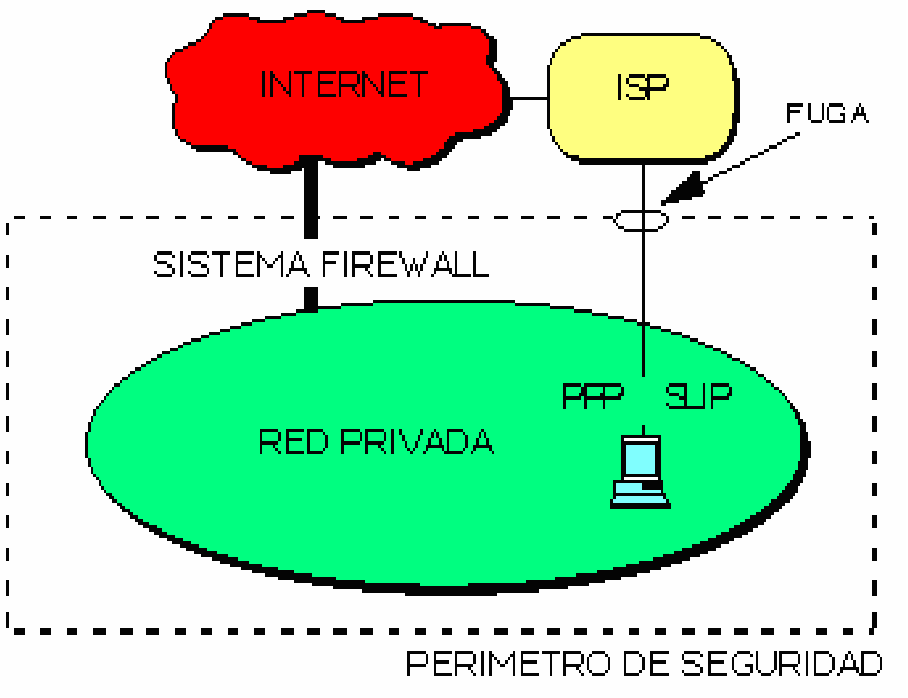
- Los firewall ofrecen un punto donde la seguridad puede ser monitoreada y si surge o identifican alguna actividad sospechosa, este generara una alarma ante la posibilidad de que suceda un ataque.

- Permiten establecer los niveles de acceso a la información de los usuarios de la red, de tal forma que cada usuario de una red tenga acceso solo a la información que le compete o que sea necesaria.
- Los firewalls permiten identificar los elementos internos de una red y optimizar que la comunicación entre ellos sea más directa.

6.3 Limitaciones de un firewall

- Un firewall no se puede proteger contra los ataques que se generen fuera de su punto de operación, como se observa en la siguiente figura 13.

FIGURA 13. LIMITACIONES DE UN FIREWALL



- No proveen casi ninguna protección contra protocolos de alto nivel.
- No brinda protección contra virus contenidos en archivos transferidos con FTP.

- No protege contra ataques desde el interior.
- No protege contra *back doors*.
- No protege contra nuevos tipos de ataques a menos que la política sea que todo está prohibido a menos que se permita explícitamente.
- Un firewall no puede protegerse de las amenazas a las que es sometido por traidores o usuarios inconscientes. El cortafuego no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA.
- Un firewall no puede protegerse de los ataques de ingeniería social.
- Los firewall no pueden protegerse de los ataques causados a la red por virus. La solución a ello se instalando softwares antivirus en cada computador de la red para protegerse de los virus que lleguen a esta.
- Los firewall no protegen la red de los fallos de seguridad de los servicios y protocolos de los cuales se permite el tráfico.

6.4 Ataques a un firewall

Identificar tráfico válido en una red es una tarea difícil, y por lo tanto el personal de la seguridad debe estar bien enterado de técnicas y de ataques existentes por parte de los intrusos. Los atacantes de un firewall son los mismos atacantes que se pueden presentar a una red, los cuales fueron tratados en el capitulo 2.

6.5 Políticas de un firewall

Existen dos políticas básicas en la configuración de un firewall, las cuales conllevan a una buena seguridad de la red:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está permitido. El firewall obstruye todo el tráfico y hay que habilitar únicamente el tráfico de los servicios que se necesiten.
- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio considerado peligroso deberá ser aislado caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es más segura que la permisiva, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

6.6 Ejemplos Firewall

Actualmente algunos de los cortafuegos pueden examinar los paquetes de datos hasta la capa 4 (capa del TCP/IP). Otros pueden examinar todas las capas (incluyendo capas más altas) y se refieren como cortafuegos profundos del paquete. En esta sección se define y explica algunos de estos cortafuegos. Los tres tipos de metodologías de inspección son las siguientes:

- Filtros de paquetes y filtros de pocos estados
- Filtros de muchos estados
- Inspección profunda de la capa de paquete

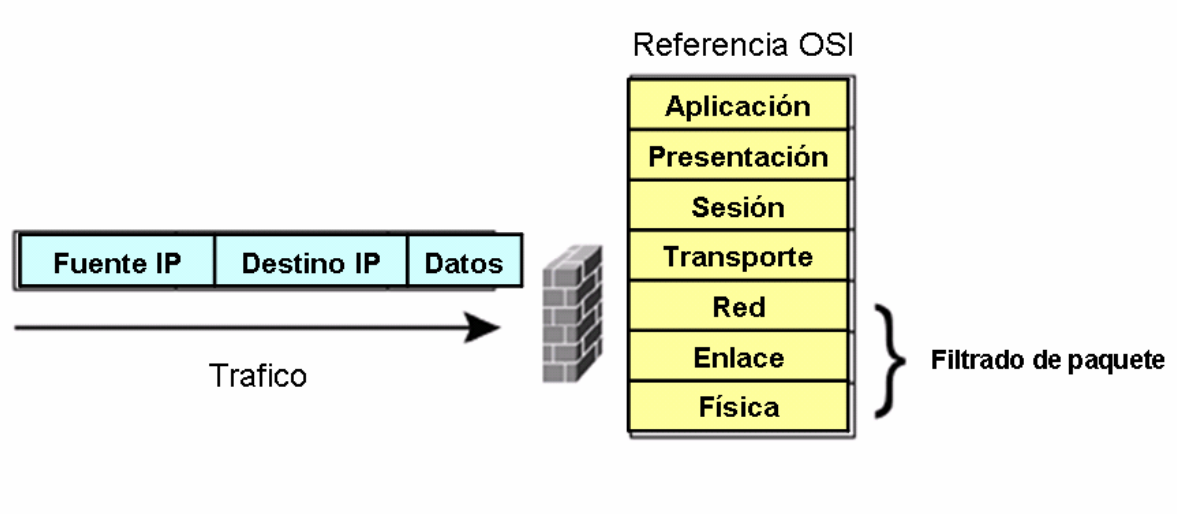
Los filtros del paquete (acceso básico – enumerar los filtros en los routers) son fáciles a la hora de romperse, por lo tanto la introducción de los servidores proxy atacan el limite de un solo dispositivo. Un servidor proxy es un servidor que se sienta entre un uso del cliente, tal como un web browser, y un servidor verdadero. Intercepta todas las peticiones al servidor verdadero para ver si puede satisfacer

las peticiones del mismo. Si no, transmite la petición al servidor verdadero. Un proxy solicita una conexión al Internet basado en peticiones de recursos internos u ocultos. Los servidores Proxy son de bajo uso, lentos, y difíciles de manejar en las grandes redes de IP.

La siguiente generación de los filtros del paquete es stateless firewall. Básicamente, permite solo el recibo de los paquetes de la información que están bajo el origen de la dirección y del puerto de las redes de confianza.

Los stateless firewall fueron introducidos para agregar más flexibilidad y escalabilidad a la configuración de una red. Un stateless firewall examina la información de la red basada en el origen y la dirección de destino. En la figura 13 se observa a profundidad la inspección de un filtro del paquete o stateless firewall. Los paquetes se examinan hasta la capa 3 del modelo de OSI, que es la capa de red. Por lo tanto, los stateless firewall pueden examinar direcciones IP del origen y destino, protocolo de origen y puertos de destino.

FIGURA 14. STATELESS FIREWAL

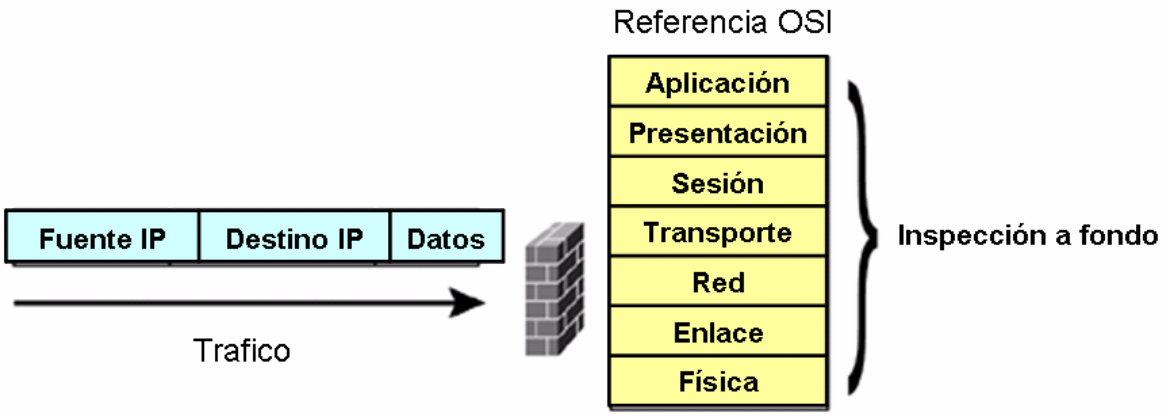


Un stateful firewall limita la información de la red bajo el origen de la dirección IP de destino, origen de la dirección IP, el puerto de origen TCP/UDP, y el puerto de destino TCP/UDP. Los stateful firewall pueden también examinar el contenido y la comprobación para de los datos para saber si hay anomalías del protocolo. Por ejemplo, un stateful firewall se equipa mucho mejor que un filtro de proxy o el filtro de paquete, para detectar y detener un ataque del negación de servicio. Un filtro del proxy o el filtro del paquete son incapaces de detectar tal ataque. Porque el origen y la dirección de destino son válidos, los datos son permitidos y pasan bien a través si son legítimos o intentan cortar contra la red. La figura 14 ilustra la profundidad de la inspección de un stateful firewall. Los paquetes se examinan hasta la capa 4 del modelo de OSI, que es la capa de transporte. Por lo tanto, los stateful firewall pueden examinar anomalías del protocolo.

Con la inspección profunda de la capa del paquete, el cortafuego examina la información de origen de la red a un destino bajo la dirección en el IP de destino, la dirección IP de origen, el puerto de origen TCP/UDP, y el puerto de destino TCP/UDP. También examina conformidad del protocolo, comprueba para saber si hay aplicaciones – bajo ataques, y asegura la integridad de los datos flujo entre cualquier dispositivo de TCP/IP. En la figura 15 se puede observar la forma cómo un dispositivo examina los paquetes con la inspección profunda de la capa del paquete.

- Asegúrese que los paquetes concuerden con el protocolo
- Asegúrese que los paquetes concuerden con las especificaciones
- Asegúrese que los paquetes no sean aplicaciones de ataques
- Mantener la integridad impidiendo las fallas

FIGURA 15. DEEP PACKET LAYER FIREWALL



Típicamente, estas funciones se realizan en hardware o son basadas en ASIC y son extremadamente rápidas. Cualquier dato que empareje los criterios tales como eso definidos para el DOS se cae inmediatamente y se puede registrar a un almacenador intermediario interno, e-mails, a los ingenieros de seguridad, o puede enviar trampas a un servidor externo de la dirección de la red (NMS).

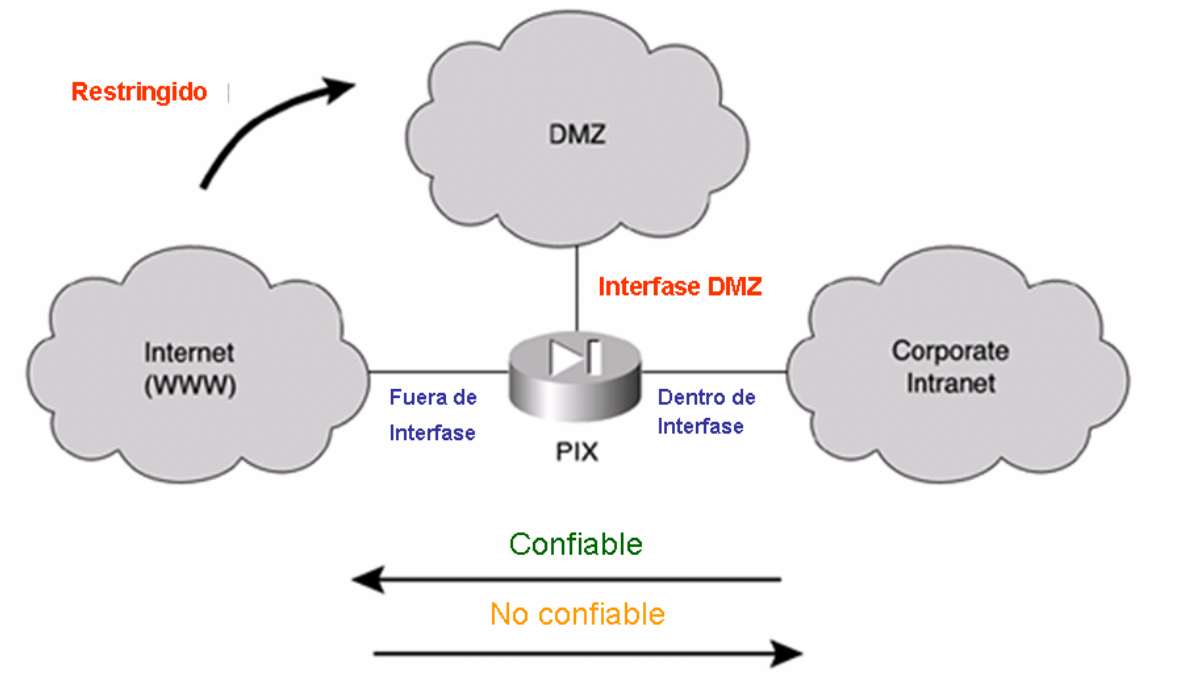
A continuación se describen dos hardwares de cortafuegos, lo más comunes del mercado actual, el cortafuego privado del intercambio del Internet de CiscoSecure (PIX) y el cortafuego de NetScreen.

6.6.1 PIX

El PIX es un dispositivo hardware dedicado al establecimiento de una red que se diseña para asegurar solamente el tráfico que empareja un sistema de criterios el cual permite para tener acceso a recursos de las redes definidas con cierto grado de seguridad.

El cortafuego PIX se diseño para llevar más lejos el nivel de la seguridad de una red. Previene conexiones desautorizadas entre dos o más redes. También puede apoyar redes exteriores o de múltiples perímetros en las zonas desmilitarizadas (DMZ).

FIGURA 16. INTERFACES PIX



Comúnmente la conexión del Internet se da el nivel más bajo de la seguridad, y un PIX se asegura de que solamente el tráfico de redes internas esté confiado en para enviar datos. En la figura 16 se ilustra las diversas interfaces y las conexiones de PIX. Un cortafuego de PIX permite una política conexión basada de la seguridad. El renombre del cortafuego de PIX proviene el hecho de que está dedicado solamente a la seguridad. El cortafuego PIX es un dispositivo stateful de la inspección.

6.6.2 NetScreen Firewall

Los cortafuegos NetScreen son cortafuegos profundos en la inspección que proporcionan la protección del uso de la capa, mientras que el PIX se puede configurar como cortafuegos stateful o stateless que proporcionan la protección de la red y el transporte de la capa.
NetScreen fue creado con la visión de proporcionar tecnologías de seguridad integradas que ofrecen funcionamiento de la velocidad del alambre y es fácil de desplegar a través de una red.

Los cortafuegos de NetScreen funcionan con Ethernet solamente. No hay ayuda para el token ring o el ISDN de alta velocidad.

El cortafuego de NetScreen puede realizar las funciones siguientes:

- Soporte para NAT y políticas basadas en NAT
- Soporte para la traducción de direcciones de puerto (PAT)
- Habilidad para soportar inconvenientes tanto en las conexiones tipo host
- Capacidad de apoyar conexiones de entrada a los anfitriones tales como en los servidores FTP
- Soporte para VPN
- DHCP
- Filtrado del URL
- Gerencia vía un simple de la interfaz web de HTTP
- Soporte para encaminamiento de protocolos tales como BGP (solamente 8000 entradas), OSPF y RipV

7. ESPECIALIZACIONES Y CERTIFICACIONES EN SEGURIDAD INFORMATICA

En la informática no solo basta con conocer de tecnologías, sistemas operativos y bases de datos; es importante que personas tanto interesadas como especializadas en estos temas adquieran certificaciones que acrediten que son competentes en el esta área, con conocimientos no solo de los problemas sino con múltiples soluciones a los que se presentan hoy en día.

Es importante que administradores de redes, de servidores Web, de firewall; analistas de intrusiones, directivos y auditores de sistemas, así como a ingenieros de sistemas y telecomunicaciones, vivan actualizándose en congresos, especialización y diplomados en temas muy reconocidos como: administración y seguridad en Windows, seguridad de redes, técnicas de intrusión y análisis de vulnerabilidades, detección de intrusos y sobre todo que conozcan y apliquen estándares de planeación y administración de la seguridad informática, que son los que garantizan la efectividad y eficiencia de la seguridad informática

En este capitulo se mencionarán los diferentes tipos o líneas de certificaciones que se han impulsado a muchas personas interesadas en el área a actualizarse en cuanto a cultura de seguridad informática y al mejoramiento de redes, sistemas operativos y bases de datos; y los hardware y software que han sido diseñados para seguridad en redes.

Entre los diferentes tipos de certificaciones de seguridad tenemos las siguientes:

1. Certificación en administración y seguridad en Windows
2. Certificación en seguridad perimetral y red.
3. Certificación en técnicas de intrusión y análisis de vulnerabilidades.

4. Certificación en detección de intrusos y tecnologías *honeypots*[7].
5. Certificación de estándares, planeación y administración de la seguridad informática.

Estas certificaciones por lo general están basadas en los principios básicos de administración y seguridad informática.

7.1 Certificación en administración y seguridad en Windows

En esta certificación se dan a conocer los aspectos mas importantes relacionados con la instalación, configuración y monitoreo de sistemas Windows 2000/XP/2003 mediante el empleo de distintas técnicas en cada una de estas secciones. La idea es citar las prácticas mas sofisticadas de seguridad aplicables a los sistemas Windows, así como las distintas herramientas de protección, detección de vulnerabilidades y aquellas que ayuden a mejorar la administración de la seguridad informática.

Adicionalmente proporciona conocimientos necesarios para lograr que los servicios de red de Windows como el DNS[8] funcionen con un nivel de seguridad adecuado.

Se citan entre los temas más relevantes de esta certificación los aspectos necesarios para instalar, configurar y administrar de forma segura una red Windows con Active Directory[9] para proporcionar mecanismos de protección contra los principales ataques cibernéticos que puedan poner en riesgo la seguridad de la información en una organización. Entre otras, ofrece las

[7] **Honeypots**: programa informático para captar ataques.
[8] **DNS:** base de datos distribuida que almacena información asociada a nombres de dominio en redes como Internet.
[9] **Active Directory**: nombre utilizado por Microsoft para referirse a su implementación de seguridad en una red distribuida de computadores

herramientas necesarias para realizar una implementación de actualizaciones de seguridad de forma automática en todos los equipos de la organización, además de proporcionar las bases para que el administrador de red pueda diseñar e implementar una infraestructura de llave pública, con el fin de que una red cumpla con los requerimientos de seguridad para su organización y proporcione a los clientes y servidores una seguridad óptima para su mejor implementación y administración en la red.

Criterios más destacados en esta certificación:

- **Directivas de grupo:** son mecanismos basados en Active Directory para asegurar y administrar centralizadamente un gran número de usuarios y de equipos, con estos se logra un alto grado de control administrativo sobre los usuarios y equipos en la red. Así mismo, proporciona conocimientos sobre las nuevas características de seguridad agregadas en el Service Pack[10] para Windows Server 2003 como lo es la herramienta Security Configuration Wizard y las nuevas características del Firewall Personal.

- **Actualizaciones de la seguridad:** permite realizar las gestiones de distribución y actualización que se publican en Microsoft en los equipos de red corporativa, permitiendo una mejora en la instalación de actualizaciones de seguridad.

- **Seguridad en Windows:** está orientada a identificar áreas vulnerables y fáciles de atacar en los servidores Windows 2000/XP/2003, así como de proporcionar los conocimientos necesarios para establecer un nivel de seguridad óptimo mediante el reforzamiento de las configuraciones de seguridad y herramientas adicionales.

[10] **Service park:** grupo de parches que actualizan, corrigen y mejoran aplicaciones y sistemas operativos.

- **Infraestructura de llave pública:** esta tecnología es considerada como elemento fundamental de infraestructura confiable; permite administrar la seguridad a través del manejo de certificados digitales. Debido a su integración con la plataforma de Windows y a su bajo costo provee una solución efectiva para extender la seguridad de la red a todos los objetos de ésta. Finalmente lo que se quiere es que la persona sea capaz de instalar, configurar y administrar una PKI (llave pública) que utilice el servicio de directorio de Active Directory para almacenar los certificados digitales, los cuales, pueden utilizarse para asegurar las comunicaciones de distintos servicios como Web, correo electrónico, VPNs, comunicaciones inalámbricas, entre otros.

- **Administración y seguridad en Internet**: este espacio es ideal para que una persona se especialice en describir los principales pasos a seguir para la instalación de los servicios World Wide Web (WWW) y File Transfer Protocol (FTP) de una forma básica y segura, garantizando la funcionalidad de estos servicios. La idea es manejar escenarios de acceso anónimo y acceso controlado; tener los conocimientos para realizar una instalación segura, manejar permisos en carpetas y archivos, crear listas de control de acceso, configuración de registros, publicación de páginas estáticas y dinámicas, control de servicios y de aplicaciones, empleo de antivirus y uso de firewall.

7.2 Certificación en seguridad perimetral y de red

Lo que se quiere conseguir con personas especializadas e esta área es que sean capaces de analizar como primera medida el perímetro en el que se encuentra una red, ya que es la parte donde es más vulnerable a un ataque, el ataque

puede provenir del interior o del exterior de la red, por eso es indispensable manejar temas relacionados con técnicas y herramientas para detectar y eliminar ataques frecuentes.

Para que alguien especializado en este tema pueda realizar técnicas de detección de ataques es recomendable tener en cuenta lo siguiente:

- **Diseñar un perímetro seguro:** conocer los principios de implementación de seguridad en un perímetro o red y la elección de hardware, software y topología de red entre otras.
- **Equipos:** es fundamental conocer el o los equipos que componen la red, así como también las situaciones que lo amenazan y las estrategias de defensa existentes.
- **Técnicas:** manejar los conceptos de técnicas como detección y mitigación de ataques en la estructura de red, mediante el uso de herramientas y la configuración de equipos de ruteo.
- **Monitoreo:** para medir el comportamiento de las técnicas y herramientas aplicadas y equipos configurados**.**
- **Evaluación**: para conocer la eficacia de detección de ataques.

7.3 Certificación en técnicas de intrusión, análisis de vulnerabilidades

Las técnicas de intrusión y las vulnerabilidades cada vez son más frecuentes; el agresor por lo general conoce paso a paso la metodología que emplean sus victimas, lo cual hace más fácil el éxito de sus ataques.

En la certificación de técnicas de intrusión y análisis de vulnerabilidades se mencionan los dos principales pasos que usan los intrusos para poder explorar los sistemas: reconocimiento del sistema y sistema de escaneo.

Lo que se quieres es que la persona interesada tenga presente que las redes de cómputo proporcionan gran cantidad de información, la cual puede ser empleada para explotar o buscar posibles huecos y fallas en cada sistema y así lograr obtener datos e información. Esta búsqueda de datos e información se realiza en sistemas con deficiente administración y seguridad, acceso a módems inseguros, incluso hasta los que cuentan con firewalls o detectores de intrusos, o algo que día con día se va popularizando como son los accesos inalámbricos con deficiente configuración y acceso.

Los ataques a los sistemas de cómputo han ido en aumento, a medida que surgen nuevas técnicas desarrolladas por los intrusos que mejoran sus habilidades de obtención de datos e información de diferentes sistemas.

Los intrusos emplean una gran variedad de técnicas para poder atacar un sistema de cómputo, dichos ataques van desde el nivel de red, hasta nivel aplicación. Lo que busca esta certificación es abordar a fondo los ataques que se llevan a cabo en estos niveles, detallando cómo operan los desbordamientos de buffer (buffer Overflow) y técnicas de desbordación de cadenas, hasta el robo de sesión, incluso usando protocolos seguros.

Este tipo de ataque resulta muy complejo y para poder mitigarlo cuando se presenta, es necesario conocer a fondo la forma de operar de diversas técnicas de negación de servicios, así como las defensas que pueden ser aplicadas.

Una vez que se cuenta con un amplio conocimiento sobre las técnicas de intrusión, éstas deberán acoplarse a una metodología enfocada a las pruebas de

penetración. Las metodologías de pruebas de penetración serán el instrumento para llevar a cado dichas pruebas. Estas pruebas deben realizarse a servicios Web, a redes, a sistemas operativos y a bases de datos.

No obstante hay que recordar que los ataques están presentes en nuevas tecnologías como voz sobre IP, RFID[11] y bluetooth, lo que hace aún mas imprescindible que los ingenieros y personal administrativo de redes estén capacitados para afrontar las estrategias de los atacantes.

7.4 Certificación en detección de intrusos y tecnologías honeypots

La certificación de detección de intrusos y tecnología honeypots abarca principios de funcionamiento del protocolo TCP/IP, útiles para la detección de intrusos, así como de las tareas de análisis de tráfico. Estos temas permitirán que los asistentes identifiquen el tráfico normal, sospechoso o malicioso, mediante el uso de herramientas libres, incluyendo el detector de intrusos Snort. Es importante reconocer el funcionamiento interno que está detrás de todo sistema de detección de intrusiones, para luego ser capaz de utilizar las herramientas que le permitan hacer la valoración del tráfico observado en la red y tomar una decisión de acuerdo a las políticas y necesidades de una organización.

Entre los temas mas relevantes se tiene:

- **TCP/IP para la detección de intrusos:** es necesario para aprender a trabajar con herramientas libres con el fin de realizar tareas básicas de análisis de tráfico que permitan identificar las características de una trama de tráfico TCP/IP.

[11] **RFID:** identificación por radiofrecuencia.

- **Análisis de tráfico de red:** la persona interesada aprenderá a examinar tramas a nivel de bit, examinando e interpretando la intención del paquete, culminando con el análisis de múltiples paquetes de eventos del mundo real; para identificar e interpretar tráfico anómalo que pueda representar un riesgo para una infraestructura de red. Es fundamental tener conocimientos básicos sobre Tcpdump que es una herramienta poderosa para el análisis de paquetes de red y puede ser utilizado junto con un NIDS (Sistema de Detección de Intrusiones en Red) para realizar un análisis exhaustivo del tráfico, con la finalidad de minimizar el falseo e identificar patrones en tráfico sospechoso.

- **Monitoreo**: las estrategias de monitoreo de una red permiten reducir el tiempo de respuesta para una posible intrusión.

- **Snort:**: el sistema de detección de intrusos Snort permite desarrollar y crear reglas que ayuden a identificar el control de tráfico malicioso o sospechoso en ambientes de trabajo, es por eso que se considera parte integral de la certificación de detección de intrusos.

Honeypot: considerados una nueva categoría de herramientas de defensa de una estructura de red, permiten conocer las amenazas existentes, como también los motivos, herramientas y tácticas utilizadas. Es importante conocer herramientas que ayuden a identificar amenazas desconocidas en el interior de la red y el uso de este tipo de herramientas para el monitoreo de de seguridad de redes en ambientes de producción e investigación y la forma como puede verse beneficiada la información capturada por este tipo de tecnología para mejorar la seguridad de una organización.

7.5 Certificación en estándares, planeacion y administración de la seguridad

La adquisición de tecnologías en base a resultados de análisis de riesgos y la planeación de tecnologías requieren de procesos administrativos que consideren la seguridad como asunto prioritario, sin embargo, esto no es tarea fácil, ya que no solo se trata de adquirir productos tecnológicos, sino de administrar la infraestructura tecnológica de seguridad y el personal especializado, para esto existen reglas claras y aplicadas ampliamente alrededor del mundo.

Las soluciones tecnológicas deben ser sustentadas por sistemas de administración de la seguridad real y operable.

Para elaborar estos Sistemas de Administración de la Seguridad se requiere conocer los conceptos y modelos de seguridad que pueden ser aplicables en las organizaciones, a fin de seleccionar cuál se adapta a los requerimientos de la organización y que garantice que la inversión en tecnología sea un retorno de inversión.

- **Estándares de seguridad ISO 27001**: los estándares de seguridad son una herramienta que apoya la gestión de la seguridad informática, ya que los ambientes cada vez más complejos requieren de modelos que administren las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad. Además es importante estudiar las últimas versiones del estándar ISO 27001 y su estado.

- **Análisis de riesgos**: los análisis de riegos basados en al ISO 27001 identifican las vulnerabilidades potenciales de seguridad de los procesos de la organización, para la definición de los planes de mitigación.

- **Administración de la seguridad**: La mala administración de la seguridad puede generar un gasto o un esfuerzo inválido para una organización, por lo tanto hay que planear la administración de la seguridad y se tiene que saber integrar los componentes tecnológicos de la seguridad implementados.

- **Políticas y procedimientos de seguridad**: la implementación de la ISO 27001 requiere de una adecuada documentación, y como consecuencia de esto se tiene que elaborar documentos y mecanismos de actualización para analizar los documentos.

- **Métricas de seguridad**: al realizar la gestión de la seguridad es necesario medir si lo que se esta haciendo esta dando los resultados esperados, por lo que hay que desarrollar parámetros de medición en la implementación de un buen sistema de administración de la seguridad.

7.6 Hardware y software para seguridad en redes

En la tabla 3 se puede observar una breve descripción de algunos software y hardware que existen en la actualidad para la seguridad en redes.

TABLA 3. HARDWARE Y SOFTWARE PARA SEGURIDAD EN REDES

Nombre	Tipo	Descripción	Pagina Web del Fabricante
PANDA INTERNET SECURITY 2008	Software	• Protege contra todo tipo de virus. • Bloquea y elimina spyware. • Impide el acceso a hackers. • Blinda frente al robo de información bancaria. • Tecnologías TruPrevent: Doble protección.	http://www.pandasecurity.com/spain/homeusers/solutions/internet-security/?sitepanda=particulares
PANDA ENTERPRISECURE CON TECNOLOGÍAS TRUPREVENT	Software	• Detecta y elimina los virus, spyware, gusanos, etc. • Protege completamente las estaciones de trabajo, servidores de archivos y correo de Exchange y Dominio, pasarelas de correo SMTP y servidores perimetrales.	http://www.pandasecurity.com/spain/enterprise/solutions/enterprisecure/
AVG ANTI-MALWARE NETWORK EDITION	Software	• Protección de seguridad controlada centralmente contra virus, gusanos, troyanos, spyware y adware combinada con protección de firewall de escritorio contra ataques de hackers y otros intrusos.	http://www5.grisoft.com/doc/products-avg-anti-malware-network-edition/la-es/crp/4
ZONEALARM SERVIDOR DE SEGURIDAD	Software	• Protege el perímetro de la red de los ataques, tanto entrantes como salientes. • Impide que el software espía y otros programas dañinos transmitan sus datos personales a sitios de Internet. • El modo completamente silencioso le mantiene invisible ante cualquier usuario de Internet. • Protege sus programas del código dañino.	http://www.zonealarm.com/store/content/catalog/products/sku_list_za.jsp

KERIO	Software	• Kerio Firewall está diseñado para proteger tu sistema tanto de otros computadores conectados en red local, como de ataques procedentes de sistemas remotos.	http://www.ca.com/us/products/product.aspx?ID=5785
AGNITUM	Software	• Agnitum Outpost Firewall es un potente firewall que impide que nadie invada la intimidad de su PC sin tu consentimiento.	http://www.agnitum.com/products/outpost/index.php
PANDA GATEDEFENDER INTEGRA 100 Y 300	Hardware	• Dispositivo hardware con un software dedicado, que instalado en la conexión entre la red de la empresa e Internet proporciona una protección unificada contra todo tipo de amenazas. • Incluye todas las protecciones necesarias en un único dispositivo: Firewall, Sistema de prevención contra Intrusiones (IPS), VPN, Anti-malware, Content Filter, Anti-spam y Filtrado web.	http://www.pandaantivirus.com.ar/gatedefender/gatedefender_integra.php
ASTARO SECURITY APPLIANCES	Hardware	• Son dispositivos Gateway que combinan facilidad de uso junto con una protección de red completa.	http://www.astaro.com/
WATCHGUARD FIREBOX X EDGE e-SERIES	Hardware	• proveen una protección poderosa para las redes de empresas pequeñas, oficinas o sucursales remotas y teletrabajadores. • Integra un firewall dinámico, VPN, protección "Zero Day", defensa antispyware, antispam, antivirus, prevención de intrusiones y filtrado de URLs. • También incluye avanzadas habilidades de administración de redes y tráfico para maximizar la configurabilidad de la red.	http://www.watchguard.com/products/edge-e.asp
IBM PROVENTIA MFS SERIES	Hardware	• Son dispositivos unificados de gran alcance con costos rentables. Para todo tipo de amenazas de Internet antes de que penetren en su red y	http://www-935.ibm.com/services/us/index.wss/detail/iss/a1027200?cntxt=a1027111

		afecten su negocio. • Aseguran que su red esté conectada, mejorando productividad de la mano de obra bloqueando virus, gusanos, hackers, el Spam y el contenido indeseado de la navegación.	
MCAFEE INTRUSHIELD	Hardware	• Dispositivos IPS para redes. • Proteje de forma preventiva sus puntos extremos e infraestructuras de red frente a ataques de día cero, de ataques de denegación de servicio (DoS), de programas espía, de voz sobre IP (VoIP), de botnet (red de robots), de programas malintencionados, de robos de identidad (phishing) y de ataques cifrados.	http://www.mcafee.com/mx/small/products/network_intrusion_prevention/intrushield_network_appliances.html

8. EMPRESAS QUE PROPORCIONAN SERVICIOS DE SEGURIDAD INFORMÁTICA

Debido a la gran importancia de las redes en las comunicaciones, los portafolios de servicios de empresas en la actualidad son muchos, por lo tanto hay organizaciones o empresas dedicas a brindar servicios de seguridad para las redes; en este capitulo mencionaremos algunas de ellas y sus portafolios de servicios.

A nivel nacional se encuentran:

8.1 Millennium Systems Ltda.

Es una empresa con base en Cartagena dedicada al diseño, instalación y desarrollo de proyectos como Integrador de soluciones de tecnologías de información, comunicaciones y seguridad para diversas empresas industriales, organismos gubernamentales y educativos de la Costa Atlántica.

Cuenta con un portafolio de servicios en cuanto a soluciones se refiere y de productos.

Soluciones:

- Soluciones LAN
- Soluciones WAN
- Soluciones MAN
- Soluciones Wireles LAN (Redes Inalámbricas)
- Soluciones de Telefonía IP Soluciones de Almacenamiento en Red
- Soluciones VPN
- Soluciones de Acceso
- Soluciones de Seguridad
- Soluciones Control de Horarios
- Soluciones de video
- Soluciones DSL
- Soluciones de Convergencia
- Soluciones Long Reach Ethernet
- Soluciones de Licenciamiento Microsoft
- Soluciones de Infraestructura de Microsoft

- Soluciones de Sistemas de Cableado Estructurado

Productos:

- **Hardware** (Estaciones de trabajo, Portables, Servidores, Impresoras y Ayudas Multimediales)
- **Software** (Licenciamiento, Soporte y Entrenamiento)
- **Comunicaciones** (LAN/ WAN/ MAN, Wireless LAN, Telefonía Análoga e IP , Acceso y Seguridad)
- **Seguridad** (Informática, Vigilancia Digital, Foto Identificación, Control de Acceso y Alarmas)

8.2 TELKUS Ltda.

Ofrece servicios de redes IP, desarrolla soluciones, comercializa equipos y productos, y presta servicios en los campos de las telecomunicaciones, computación e informática, con énfasis en el área de transmisión de datos.
Nació en el 2005 con base al desarrollo de las tecnologías de ***Telkus Group,*** una multinacional que cuenta con profesionales de América y Europa con mas de 25 años de experiencia en telecomunicaciones informáticas e Internet.

Portafolio de servicios:

- Redes inalámbricas
- Voz IP
- Redes IP
- Seguridad y Vigilancia IP

8.3 SIRCOM soluciones integrales en redes y comunicaciones Ltda.

Esta enteramente dedicada y comprometida a satisfacer plenamente las necesidades de los clientes en el ámbito de las comunicaciones e informática, consolidando así, relaciones comerciales estables y duraderas, lo cual garantiza un constante crecimiento dentro del mercado local y Nacional.[12]

Portafolio de servicios:

- Redes
- Soporte de Hardware y Software
- Soporte de Hardware y Software Avanzado
- Servicios de Mantenimiento Preventivo
- Servicios de Mantenimiento Correctivo
- Seguridad en redes
- Instalación, Mantenimiento, Ampliación y Reparación de Plantas Telefónicas
- Suministro, Mantenimiento y Reparación de Hardware
- Sistemas Eléctricos
- INSTALACION de CCTV (Circuito cerrado de Televisión)

8.4 Caribbean Dolphin LTDA.

Empresa dedicada a la comercialización e instalación de equipos de comunicaciones, seguridad, sistemas logísticos para pequeñas, medianas y grandes industrias.

[12] http://www.sircom.com.co/index.htm

Portafolio de servicios:

- Seguridad Biométrica
- Montaje de redes
- Desarrollo de aplicaciones
- Soluciones empresariales

8.5 NewNet S.A

No solo brinda servicios de seguridad sino que también ofrece servicios de conectividad. Trabaja bajo los estándares internacionales ISO/IEC 17799, BS 7799-2, ISO/IEC 13335, ISO/IEC 15408.
Su sede principal se encuentra ubicada en la ciudad de Bogota, también cuenta con sedes en Medellín, Pereira y Cali.
Portafolio de servicios:

Consultoría en Seguridad Informática

- Análisis de Riesgos de Seguridad Informática
- Análisis de Requerimientos organizacionales de Seguridad Informática
- Diseño de una solución de Seguridad Informática
- Desarrollo de una guía de implementación de la solución de seguridad informática en la organización
- Desarrollo de un programa de Administración del Riesgo en Seguridad informática
- Desarrollo de un programa de Administración Operativa de la Seguridad informática
- Desarrollo de un programa de Planeación Estratégica de la Seguridad Informática
- Desarrollo de un programa de Sensibilización y Capacitación organizacional en Seguridad Informática

Servicios de Seguridad Informática

- Análisis de Riesgos y Requerimientos organizacionales de Seguridad Informática.
- Pruebas de penetración/intrusión (Hacking ético, intrusión física e ingeniería social).
- Aseguramiento de Plataformas computacionales y Redes de Datos
- Aseguramiento de Sitios Web, y Servicios Web-enabled
- Implantación de Dispositivos de Control de Acceso y de Seguridad Informática
- Implantación de soluciones en Seguridad Informática
- Interventoría de Proyectos en Seguridad Informática

- Desarrollo de términos de referencia para la contratación de soluciones en seguridad informática
- Capacitación y Sensibilización Organizacional en Seguridad Informática

8.6 Password S.A. Seguridad Informática

Pertenece a la red de empresas de base tecnológica de ParqueSoft. Su sede principal se encuentra en la ciudad de Popayán. Su portafolio de servicios se encuentra dividido en cuatro fases las cuales se describen a continuación:

Fase I “Diagnostico de seguridad informática”

- Análisis de Riesgo en Redes
- Auditoria de seguridad informática

Fase II “Planeación”

- Diseño de una Infraestructura de Seguridad Informática
- Políticas de Seguridad Informática
- Talleres de Concientización
- Planes de Contingencia
- Asesoramiento Sobre la Calidad en el Diseño e Implementación de Sistemas Informáticos
- Orientados a Seguridad

Fase III “Implementación de arquitecturas de seguridad”

- Restricción de Accesos Firewall
- Detección de Intrusos
- BlackBox: Herramienta de Integración de Seguridad para Redes
- AntiSpam
- Antivirus
- Tecnología en Llaves Públicas PKI
- VPN

Fase IV “Soporte permanente en seguridad informática”

- Análisis, Notificación y Alertas
- Servicio Temprano Anti-Phising
- Análisis Periódico de Seguridad
- Log Security Inspector

8.7 Colredes De Occidente

Es una organización comprometida con la satisfacción de los clientes, integrando soluciones en tecnología con productos y servicios de calidad, talento humano competente, implementando procesos para el mejoramiento continuo. Su sede principal se encuentra ubicada en Cali, tiene otras sedes en las ciudades de Cartagena, Barranquilla y Bogotá.

Portafolio de servicios:

- Cableado estructurado
- Potencia
- Conectividad
- Seguridad informática
- Voz
- Seguridad electrónica y automatización
- IT
- Outsourcing

8.8 Colvatel

La Compañía Colombiana de Servicios de Valor Agregado y Telemáticos S.A. ESP.- **COLVATEL S.A. ESP-** es una filial de ETB, creada en 1992 con el fin de desarrollar productos de voz y datos.

Actualmente, Colvatel comercializa las tarjetas prepago integradas de ETB, administra los teléfonos públicos de ETB instalados en Bogota y municipios aledaños, así como ofrece soluciones de conectividad y servicios de redes.[13]

[13] http://www.colvatel.com/contenido/capitulo.asp?chapter=76

Portafolio de servicios:

- Sistemas de seguridad perimetral (Firewalls)
- Soluciones de autenticación
- Sistemas de detección de intrusos (IDS)
- Sistemas de prevención de intrusos (IPS)
- Soluciones antivirus, antispam
- Sistemas de control de navegación en Internet

A nivel internacional se encuentran:

8.9 SonicWALL, Inc.

Su sede corporativa esta ubicada en, 1143 Borregas Avenue Sunnyvale, CA 94089-1306 USA.

Fue fundada en 1991, diseña, desarrolla y fabrica soluciones de gestión y directivas, seguridad para redes, acceso remoto seguro, seguridad de correo electrónico y Web y protección de datos continúa. La completa gama de soluciones de SonicWALL, que incluye productos basados en dispositivos y servicios de suscripción de valor añadido, proporciona soluciones para protección de datos e Internet de calidad empresarial sin comprometer el rendimiento de redes.

Con el objetivo de satisfacer las necesidades de sus clientes, independientemente del tamaño de la red, SonicWALL ofrece un servicio técnico 24 horas al día, los 7 días de la semana, así como servicios detallados de diseño y consultoría y cursos de certificación y formación técnica. Estos servicios pretenden ayudar a los

clientes a planificar, desplegar y gestionar con eficacia sus infraestructuras de seguridad.[14]

8.10 VeriSign Inc.

Proporciona infraestructura digital que posibilita y protege cada día miles de millones de interacciones en las redes de datos y voz de todo el mundo. Su sede principal se encuentra ubicada en España.

Portafolio de servicios:

Servicios de seguridad

- Certificados SSL
- Managed security services
- VeriSign idefense security intelligence service
- VeriSign identity potection
- Programa Verisign secured seal
- Firma de código
- Digital ID para secure Email

Servicios de comunicaciones

- Servicios de análisis y autoservicios
- Conjunto de servicios GSM
- Servicios internacionales

[14] http://www.sonicwall.com/es/Company.html

Servicios de información

- Servicios digital Brand Management
- Servicios DNS Assurance

8.11 VILAmedi

Servicios informáticos de Barcelona, ofrece a las empresas una solución tecnológica que incluye todas las fases de su gestión informática, desde la planificación integral hasta la puesta en marcha, el mantenimiento y la actualización.

Portafolio de servicios:

- Sistemas de Backups
- Sistemas antivirus
- Sistemas firewall
- Entornos redundantes

8.120

Ofrece gran diversidad de servicios y productos informáticos.

Portafolio de servicios:

- Seguridad informática
- Biometría
- Li Security Gateway
- Encriptación

8. CONCLUSIONES

La eficiencia y efectividad de una red consta de aspectos muy importantes como la confidencialidad, control de acceso, integridad y fiabilidad, que comúnmente se ven averiados por la exposición que tienen las redes informáticas a continuos ataques presentados por personas y amenazas lógicas y vulnerabilidades al momento de configuración, instalación o en el momento en que un atacante se aproveche de la debilidad de las mismas. Es muy importante conocer las tecnologías, equipos, y medios de las redes informáticas; pero también es indispensable identificar los tipos de ataques a redes, a sistemas operativos y a bases de datos; analizar las posibles consecuencias y evitar que se presenten, todo con el fin de proteger la información ya que está al igual que los demás recursos, tiene un valor muy importante en las organizaciones o empresas.

La información existe en muchas formas, puede ser escrita, en imágenes, hablada o en medios físicos, transmitida o utilizada por medios electrónicos, cualquier forma de información debe ser protegida adecuadamente. Para eso, existen técnicas que protegen la información de organizaciones y sitios trabajos, como los firewalls y la criptografía, que integrados con un plan de administración de seguridad pueden llevar al éxito de las redes informáticas manteniendo la confiabilidad, integridad y disponibilidad de la información.

Hoy en día a nivel mundial existen especializaciones y certificaciones en distintas áreas de la informática que son de gran apoyo para los ingenieros y administradores de redes. O si se prefiere, se pude contar con empresas consultoras de la seguridad de redes como *Versing*, *Consoltic, Satec*, entre otras, que buscan garantizar que cada nivel de la infraestructura de información de una organización cumpla con los objetivos de seguridad de información de un cliente

específico, aplicando políticas internas de los clientes y estándares como la ISO 27001 e IRAM-ISO IEC 17799 para crear un análisis centrado en las carencias que identifiquen áreas de alto riesgo y aporte a las soluciones recomendadas.

GLOSARIO

B

Bit Dígito del sistema de numeración binario

Bugs Errores de software

C

CD Disco compacto

CD-ROM Disco Compacto de Memoria de Sólo Lectura

D

DES Estándar De Cifrado De Datos

DMZ Zona desmilitarizada o red perimetral

Dirección MAC Control de dirección de acceso al medio

DVD Disco Versátil Digital

F

FTP Protocolo de transferencia de archivos

G

Gateway Es un nodo en una red informática que sirve de punto de acceso a otra red

H

http	Protocolo de transferencia de hipertexto

I

I.M.P.	Procesador de interfaz de mensajes
ISDN	Red Digital de Servicios Integrados

L

LAN	Red de área local

M

MAN	Red de área metropolitana
MIME	Extensiones de Correo Internet Multipropósito
Módem	Equipo electrónico que sirve para transmitir y recibir información digital a distancia, mediante la modulación y demodulación de la señal digital.

N

NAT	Traducción de Dirección de Red
NNTP	Protocolo De Transporte De las Noticias De la Red

P

Packet sniffer	Programa de captura de las tramas de red
Plotter	También conocido como *trazador gráfico*, es un dispositivo de impresión conectado a una computadora, y diseñado específicamente para trazar gráficos vectoriales ó dibujos lineales: planos, dibujos de piezas, etc.
POP3	Protocolo oficial de correo versión 3

R

Router	Dispositivo de hardware para interconexión de redes de las computadoras, funciona en la capa 3 del modelo OSI.
RAM	Memoria de acceso aleatorio ó memoria de acceso directo

S

SAI	Servicio de Alimentación Ininterrumpido
Servidor proxy	Permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
SMTP	Protocolo simple de transferencia de correo electrónico
SPAM	Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor.

T

TCP/IP	Protocolo de control de transmisión / Protocolo de Internet

U

UNIX	Sistema operativo portable

V

VLSI	Integración en escala muy grande
VPN	Red privada virtual

W

WAN	Red de área amplia

BIBLIOGRAFÍA

- Comunicaciones y Redes de computadores, William Stanllings, Prentice Hall

- Seguridad en redes, 2º edición, William Stanllings, Prentice Hall

- Organization for Economic Cooperation and Development Guidelines for Security of Information Systems.

- SWANSON, (National Institute of Standard and Technology. General Principles for Information and systems Security Policies.

- CHAPMAN, B y ZWICKY, Construya Firewalls para Internet. O'Really. Edición en Español por McGraw Hill.

- WILSON, Marketing and Implementing Computer Security.

- Blake, I.; Seroussi, G.; and Smart, N. Elliptic Curves in Cryptography. Cambridge: Cambridge University Press,.

PAGINAS WEB

- http://www.vsantivirus.com/especial-seguridad2004b.htm
- es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf
- www.coit.es/pub/ficheros/redes_wlan_bafc12cb.pdf?PHPSESSID=9905e4262df6d2fed1023eeed0471d34
- http://www.diatel.upm.es/investigacion/Seguridad.html
- http://www.redestelecom.com/Actualidad/Noticias/Seguridad/Vulnerabilidades/20070320074
- www.inf.utfsm.cl/~rmonge/seguridad/cripto-07-bn.pdf
- www.pwc.com/uy/spa/pdf/SeguridadRedesInternas.pdf
- es.tldp.org/Presentaciones/200203jornadassalamanca/jadebustos/conferencia-criptografia.pdf
- http://www.delitosinformaticos.com/01/2007/seguridad-informatica/informe-de-seguridad-de-redes-informaticas-en-2007-de-sophos
- http://antivirusgratis.com.ar/firewall/
- www.millennium-systems.biz
- www.telkus-ip.com
- www.sircom.com.co
- www.newnetsa.com
- http://password.com.co
- http://www.colredes.com

- http://www.colvatel.com
- http://www.sonicwall.com
- http://www.verisign.es
- http://www.vilamedi.com