Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE ASEGURAMIENTO DE REDES UTILIZANDO DMZ´S

Héctor Rodolfo Morales Rabanales
Asesorado por el Phd. Ing. Enrique Edmundo Ruiz Carballo

Guatemala, mayo de 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE ASEGURAMIENTO DE REDES UTILIZANDO DMZ´S

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

HÉCTOR RODOLFO MORALES RABANALES
ASESORADO POR EL PHD. ING. ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO ELECTRÓNICO

GUATEMALA, MAYO DE 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. José Milton De León Bran
VOCAL V	Br. Isaac Sultán Mejía
SECRETARÍA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Armando Alonso Rivera Carrillo
EXAMINADOR	Ing. Julio Cesar Solares Peñate
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
SECRETARÍA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

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

DISEÑO DE ASEGURAMIENTO DE REDES UTILIZANDO DMZ´S,

tema que me fuera asignado por la Coordinación de la Carrera de Ingeniería Electrónica, el 28 de octubre de 2008.

Héctor Rodolfo Morales Rabanales

AGRADECIMIENTOS A:

Dios	Por haberme permitido concluir con esta meta.
Mi familia	Por haberme apoyado en todo lo necesario para llegar hasta aquí.
Mi asesor	Por toda la ayuda y consejo brindado para realizar este trabajo de graduación.
Mis amigos	Por haber pasado juntos tantos momentos buenos durante los proyectos y los desvelos.
La Universidad de San Carlos	Por haberme brindado la oportunidad de ser parte de esta casa de estudios.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES **V**
RESUMEN **VII**
OBJETIVOS **IX**
INTRODUCCIÓN **XI**

1. REDES INFORMÁTICAS **1**

1.1 ¿Qué es una red? 1
1.1.1 Objetivos de las redes 2
1.1.2 Aplicaciones de las redes 3
1.2 Tipos de redes 4
1.2.1 Redes de área personal (PAN) 5
1.2.1 Redes de área local (LAN) 5
1.2.2.1 Conexión *Ethernet* 6
1.2.3 Redes de área extensa (WAN) 8
1.3 Topologías para redes 9
1.3.1 Tipos de arquitecturas 10
1.3.1.1 Arquitectura centralizada 11
1.3.1.1.1 Topología en estrella 12
1.3.1.2 Arquitectura descentralizada 13
1.3.1.2.1 Topología en árbol 15
1.3.1.3 Arquitectura distribuida 16
1.3.1.3.1 Topología en malla 16

2 EQUIPOS DE TELECOMINICACIONES PARA REDES 19

2.1 Modelo OSI 19
2.1.1 Capa física (Capa 1) 22
2.1.2 Capa de enlace de datos (Capa 2) 24
2.1.3 Capa de red (Capa 3) 25
2.1.4 Capa de transporte (Capa 4) 26
2.1.5 Capa de sesión (Capa 5) 28
2.1.6 Capa de presentación (Capa 6) 29
2.1.7 Capa de aplicación (Capa 7) 30
2.1.8 Datagramas de red 30
2.1.9 *Backbone* 32
2.2 *Hub´s* de comunicación 32
2.3 *Switches* de comunicación 34
2.3.1 *Switches* de comunicación capa 2 35
2.3.2 *Switches* de comunicación capa 3 37
2.3.3 *Switches* de comunicación capa 4 38
2.4 *Routers* de comunicación 40
2.4.1 Transmisión de paquetes 42
2.4.2 Enrutamiento de información 42
2.5 *Firewall* 43
2.5.1 Funcionamiento de los *firewall* 45
2.5.2 Beneficios de un *firewall* 46
2.5.3 Limitantes de un *firewall* 47

3 SEGURIDAD INFORMÁTICA **49**

3.1 Importancia de la seguridad informática 49
3.1.1 ¿Por qué es importante la seguridad informática? 50
3.1.2 Amenazas y vulnerabilidades 51
3.2 Métodos de seguridad en redes informáticas 54
3.2.1 Planificación de la seguridad en la red 55
3.2.1.1 Nivel de seguridad 56
3.2.1.2 Configuración de las políticas o normativas 56
3.2.1.3 Prevención 56
3.2.1.4 Autenticación 57
3.2.1.5 Entrenamiento 57
3.2.2 Equipamiento de seguridad 58
3.2.2.1 Seguridad de los servidores 58
3.2.2.2 Seguridad del cableado 59
3.2.3 Modelos de seguridad 59
3.2.3.1 Compartir recursos en forma protegida 60
3.2.3.2 Permisos de acceso 61
3.3 DMZ´s 62
3.3.1 Características de una DMZ 64
3.3.1.1 Filtrado de paquetes 65
3.3.1.2 NAT, mapeo bidireccional 66
3.3.1.3 Colas de tráfico y prioridad 67
3.3.1.4 Salidas redundantes / balanceo de carga 67
3.3.1.5 Filtrado de contenido (*Caching*) 67

4 IMPLEMENTACIÓN DE UNA DMZ CORPORATIVA 69

4.1 Metodología de implementación 69
4.1.1 PMI 69
4.1.2 Gestión de proyectos 70
4.1.3 Características de un proyecto 71
4.1.3.1 Características temporal 72
4.1.3.2 Características productos, servicios o resultados únicos 72
4.1.3.3 Características de elaboración gradual 73
4.1.4 Restricciones de un proyecto 73
4.1.4.1 Restricciones de tiempo 74
4.1.4.2 Restricciones de costo 74
4.1.4.3 Restricciones de alcance 75
4.2 Procedimiento de implementación 75
4.2.1 Definición del alcance del proyecto 77
4.2.2 Definición de recursos necesarios 80
4.2.3 Definición de posibles proveedores 81
4.2.4 Presentación de evaluaciones técnicas y económicas 82
4.2.5 Generación de planificación 84

CONCLUSIONES 89
RECOMENDACIÓN 91
BIBLIOGRAFÍA 93

ÍNDICE DE ILUSTRACIONES

FIGURAS

1	Equipos conectados en red	2
2	Ejemplo de red LAN	6
3	Conexión *Ethernet*	8
4	Ejemplo de red WAN	9
5	Arquitectura centralizada	12
6	Arquitectura centralizada	13
7	Arquitectura de una red descentralizada	14
8	Topología en árbol	15
9	Arquitectura de una red distribuida	16
10	La pila OSI	19
11	Flujo de información por capas	22
12	Datagrama de red	31
13	Conexión de un *backbone*	32
14	Conexión mediante *hubs*	34
15	Comunicación entre *switches* capa 2	37
16	Esquema de comunicación utilizando un *router*	41
17	Funcionamiento de un *firewall*	44
18	Configuración de *firewall* en trípode	63
19	Configuración *firewall* de subred monitoreada	64
20	Flujo para la implementación de proyectos	76
21	Formato para la definición de alcances de un proyecto	78

22	Definición de alcance para proyecto de DMZ´s	79
23	Formato para definición de recursos necesarios	80
24	Definición de recursos necesarios para proyecto de DMZ´s	81
25	Formato para inventario de proveedores	82
26	Formato de evaluación económica	83
27	Formato de evaluación técnica	84
28	Planificación por fechas para proyecto de DMZ´s	86
29	Planificación por diagrama de Gantt para proyecto de DMZ´s	87

TABLA

I	Tecnologías *Ethernet*	7

RESUMEN

La información es el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

Por el enorme número de amenazas y riesgos que existen a lo largo del mundo, la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo. Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

Existen gran cantidad de métodos para asegurar una red informática, uno de los más usados es el de DMZ´s o zonas desmilitarizadas.

Una zona desmilitarizada o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, con el objetivo que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa.

OBJETIVOS

General

- Estudiar el diseño de una arquitectura de seguridad en redes informáticas corporativas utilizando DMZ´s.

Específicos:

1 Analizar el funcionamiento de una red corporativa
2 Conocer la función de los equipos de telecomunicaciones dentro de una red corporativa
3 Analizar y comprender la función de una DMZ dentro de una red corporativa
4 Estudiar el diseño de una DMZ corporativa

INTRODUCCIÓN

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió, y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Podemos entender como seguridad, un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- Integridad, la información sólo puede ser modificada por quien está autorizado
- Confidencialidad, la información sólo debe ser legible para los autorizados
- Disponibilidad, debe estar disponible cuando se necesita
- Irrefutabilidad, que no se pueda negar la autoría (no-rechazo o no repudio)

1 REDES INFORMÁTICAS

1.1 ¿Qué es una red?

El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de una organización se está remplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados que efectúan el mismo trabajo. Estos nuevos modelos se conocen como redes de ordenadores.

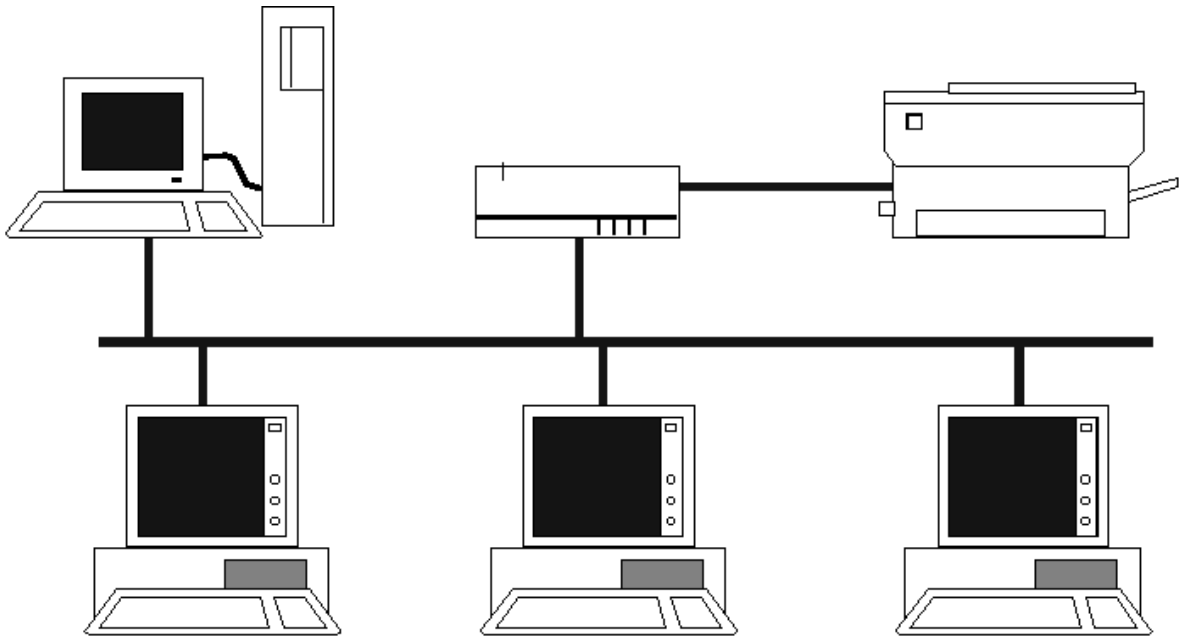
Una red es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, recursos, servicios, etc.

Una red sencilla se puede construir de dos ordenadores agregando un adaptador de la red a cada ordenador y conectándolos mediante un cable especial llamado "cable cruzado". Este tipo de red es útil para transferir información entre dos ordenadores que normalmente no se conectan entre sí por una conexión de red permanente o para usos caseros básicos.

Alternativamente, una red entre dos computadoras se puede establecer sin aparato dedicado adicional usando una conexión estándar tal como el puerto serial en ambos ordenadores. En este tipo de red solo es necesario

configurar una dirección IP, pues no existe un servidor que les asigne IP automáticamente.

Figura 1. Equipos conectados en red



1.1.1 Objetivos de las redes

Las redes en general consisten en compartir recursos, y uno de los objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera en la red que así lo solicite, esto sin importar la localización física del recurso y usuario. En otras palabras, el hecho que el usuario se encuentre a 1000 KM de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Otros de los objetivos es proporcionar una alta fiabilidad, al contar con múltiples suministros alternativos de información sobre la red y generar un ahorro económico al colocar sistemas constituidos por ordenadores poderosos que comparten recursos a gran cantidad de usuarios sobre el sistema.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual, a medida que crece la carga, simplemente añadiendo más procesadores. Con máquinas grandes, cuando el sistema está lleno, deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

1.1.2 Aplicaciones de las redes

La disponibilidad que se tenga sobre una red, nos brinda la posibilidad de introducir y generar nuevas aplicaciones viables y algunas de ellas pueden ocasionar importantes efectos en la sociedad. Para generar una idea más clara sobre los usos que se le pueden dar a una red podemos mencionar:

1. El acceso a programas remotos, que nos permitiría poder acceder desde lugares distantes a información de nuestra compañía.

2. Acceso a bases de datos remotas, que podría permitir a clientes de nuestra compañía conectarse a sus plataformas de negocios y acceder a información personalizada.

3. Facilidades de comunicación, con las que podemos tener intercambio de información entre usuarios como por ejemplo, el tan conocido correo electrónico, que se envía desde una terminal a cualquier persona situada en cualquier parte del mundo que tenga acceso a este servicio.

1.2 Tipos de redes

La posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información con bases de datos remotas; cargar aplicaciones desde puntos de ultramar; enviar mensajes a otros países y compartir ficheros, todo ello desde una computadora personal.

Por las áreas físicas que cubren, las redes pueden dividirse en tres grandes grupos, las redes de área personal (PAN), las redes de área local (LAN) y las redes de área extensa (WAN).

1.2.1 Redes de área personal (PAN)

Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con una red de alto nivel y el Internet (un *up link*). Las redes personales del área se pueden conectar con cables, utilizando los buses de la computadora tales como USB y *FireWire*. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como Bluetooth.

1.2.1 Redes de área local (LAN)

Como su nombre lo indica, constituye una forma de interconectar una serie de equipos informáticos y represento uno de los sucesos más críticos para la conexión de equipos de cómputo entre sí.

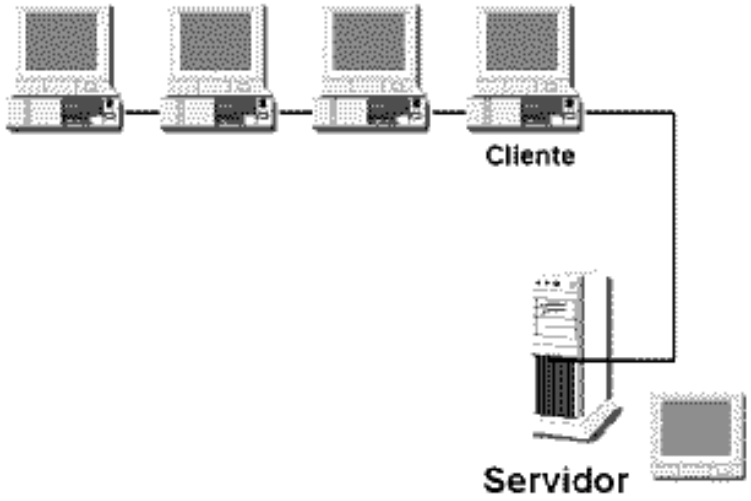
Una LAN no es más que un medio compartido junto con una serie de reglas que rigen el acceso a dicho medio, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas como por ejemplo,

controlar la configuración de equipos dentro de este medio, mediante gestiones de *software*, administración de usuarios y recursos de la red.

Todas las LAN comparten la característica de poseer un alcance ilimitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Una de las LAN más difundida es la Ethernet.

Figura 2. Ejemplo de red LAN



1.2.2.1 Conexión Ethernet

Ethernet es un patrón para la conexión entre dos computadoras para que puedan compartir información y recursos. Su concepto es que cada equipo conectado solo puede utilizar la conexión cuando ningún otro equipo la está

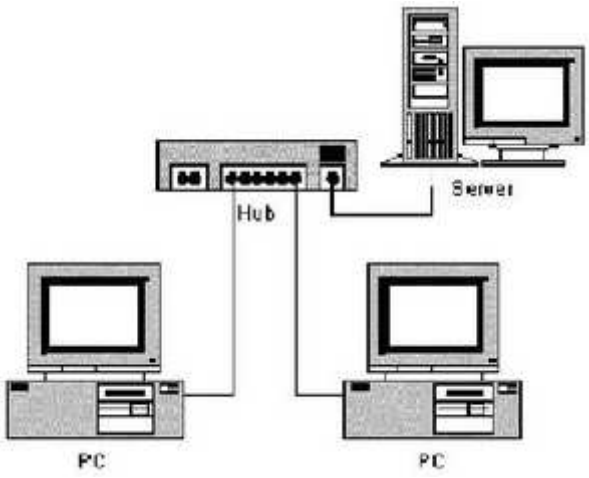
utilizando, si existiese algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante.

Existen gran cantidad de tecnologías *Ethernet*, las cuales pueden ser aplicadas en diferentes topologías, con diferentes velocidades de transmisión y a diferentes distancias. El objetivo de esto es realizar la conexión lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión que están conectados directamente a su destino.

Tabla I. Tecnologías *Ethernet*

Tecnología	Velocidad de trasmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra Óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (Cat. 3UTP)	100 m	Estrella Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100Mbps	Par Trenzado (Cat. 5UTP)	100 m	Estrella Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100Mbps	Fibra Óptica	2000 m	No permite uso de Hubs
1000BAseT	1000Mbps	4 pares Trenzado (Cat. 5e ó 6UTP)	100 m	Estrella Full Dúplex (switch)
1000BaseSX	1000Mbps	Fibra Óptica (multimodo)	550 m	Estrella Full Dúplex (switch)
1000BAseLX	1000Mbps	Fibra Óptica (monomodo)	5000 m	Estrella Full Dúplex (switch)

Figura 3. Conexión *Ethernet*

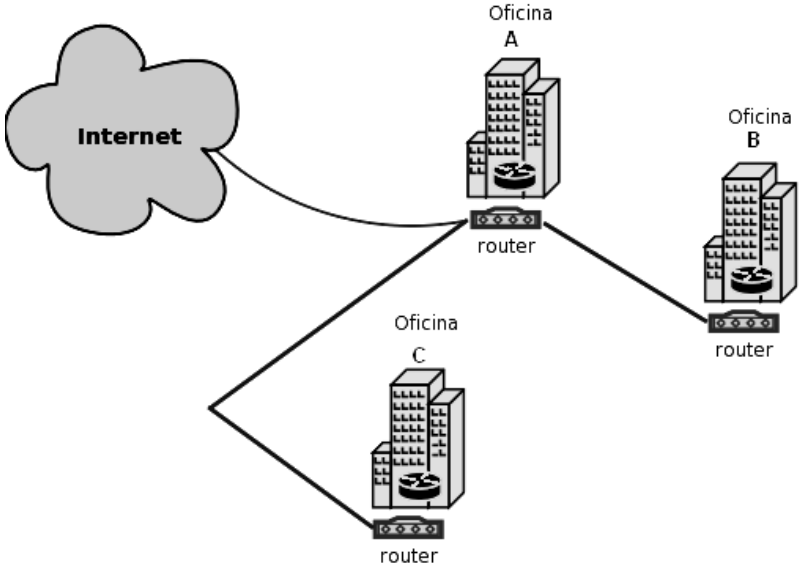


1.2.3 Redes de área extensa (WAN)

Una red de área amplia o WAN (*Wide Area Network*, del inglés), se extiende sobre un área geográfica extensa, a veces un país o un continente, y su función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí. Para ello cuentan con una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continua. Por esta razón también se dice que las redes WAN tienen carácter público, pues el tráfico de información que por ellas circula proviene de diferentes lugares, siendo usada por numerosos usuarios de diferentes países del mundo para transmitir información de un lugar a otro.

Cuando se llega a un cierto punto deja de ser poco práctico continuar con la ampliación de una LAN, y a veces esto viene impuesto por limitaciones físicas de la misma red, En este punto en donde se quiere cubrir grandes distancias es en donde se empieza con la ampliación de la LAN hasta convertirla en una red de área extensa WAN.

Figura 4. Ejemplo de red WAN



1.3 Topologías para redes

La topología de red define la estructura de una red, una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios y la otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

La topología de red o forma lógica de red se define como la cadena de comunicación que los nodos que conforman una red usan para comunicarse, la topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre sí.

Además de la topología estética, se puede dar una topología lógica a la red y eso dependerá de lo que se necesite en un momento dado.

1.3.1 Tipos de arquitecturas

En algunos casos se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de cómo el protocolo considera dicho cableado.

Se han de tener en cuenta una serie de factores al seleccionar como más adecuada una arquitectura, se describen seguidamente:

- Complejidad, factor que afecta la instalación y mantenimiento de todo el cableado
- Respuesta, cantidad de tráfico que puede soportar el sistema
- Vulnerabilidad, susceptibilidad de la arquitectura a fallos o averías
- Aplicación, tipo de instalación más apropiada para la arquitectura

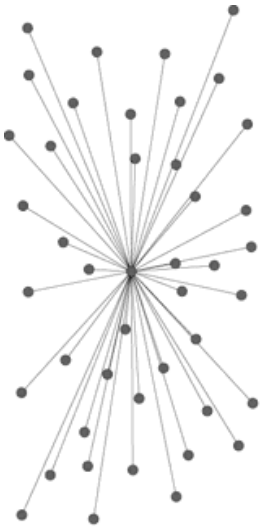
- Expansión, facilidad de ampliar la red y añadir dispositivos para cubrir grandes distancias.

1.3.1.1 Arquitectura centralizada

Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. El tipo de concentrador *hub* se utiliza en esta topología.

La desventaja radica en la carga que recae sobre el nodo central. La cantidad de tráfico que deberá soportar es grande y aumentará conforme vayamos agregando más nodos periféricos, lo que la hace poco recomendable para redes de gran tamaño. Además, un fallo en el nodo central puede dejar inoperante a toda la red. Esto último conlleva también una mayor vulnerabilidad de la red, en su conjunto, ante ataques. Entre estas arquitecturas podemos encontrar la topología de estrella.

Figura 5. Arquitectura centralizada



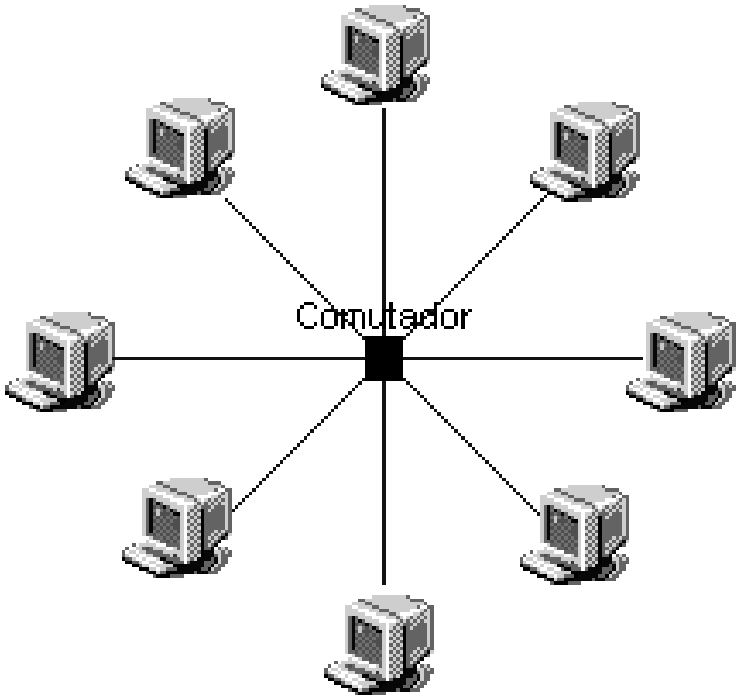
1.3.1.1.1 Topología en estrella

En la topología estrella existe un concentrador central que reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo hacia el nodo central solamente, un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto.

La desventaja de esta topología radica en que la carga recae sobre el nodo central, por ende la cantidad de tráfico que deberá soportar es grande y

aumentará conforme se agregué más nodos periféricos, lo que la hace poco recomendable para redes de gran tamaño. Un fallo en el nodo central puede dejar inoperante a toda la red, esto último conlleva también una mayor vulnerabilidad de la red ante ataques.

Figura 6. Topología en estrella



1.3.1.2 Arquitectura descentralizada

En estas redes no hay un servidor central, los usuarios se interconectan, de tal modo que todos los usuarios comparten archivos y recursos a la vez, ya que los nodos están interconectados entre sí.

Aparece por interconexión los nodos centrales de varias redes centralizadas, como resultado no existe un único nodo central sino un centro colectivo de conectores. La caída de uno de los nodos centralizadores, conlleva la desconexión de uno o más nodos del conjunto de la red mientras que la caída del nodo centralizador produciría necesariamente la ruptura o desaparición de la red, entre esta arquitectura podemos encontrar la topología en árbol.

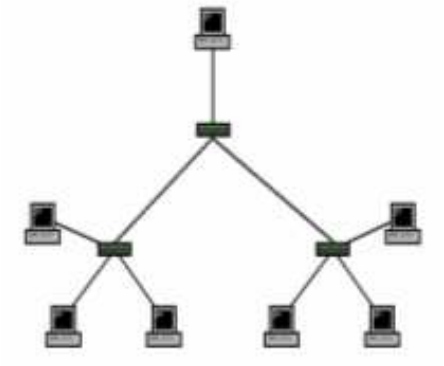
Figura 7. Arquitectura de una red descentralizada

1.3.1.2.1 Topología en Árbol

Esta topología también conocida como topología jerárquica, puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales, que requieren transmitir y recibir de otro nodo sin necesidad de actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir.

Como en las redes en estrella convencionales, los nodos individuales pueden quedar aislados de la red por un fallo puntual en la ruta de conexión del nodo, si falla un enlace que conecta con un nodo hoja, ese nodo hoja queda aislado; si falla un enlace con un nodo que no sea hoja, la sección entera queda aislada del resto.

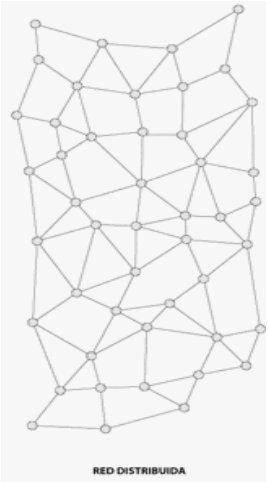
Figura 8. Topología en árbol



1.3.1.3 Arquitectura Distribuida

Todos los nodos se conectan entre sí, sin tener que pasar por uno o varios nodos centrales, esto aumenta la disponibilidad de la red, lo que la hace más robusta ante caída de nodos, ya que ningún nodo al ser extraído generará desconexiones de otro nodo. Entre esta arquitectura podemos encontrar la topología de malla.

Figura 9. Arquitectura de una red distribuida



1.3.1.3.1 Topología en malla

Las redes de malla se diferencian de otras redes en que los elementos de la red, más comúnmente llamados nodos, están conectados con todos los demás nodos, mediante cables separados. Esta configuración ofrece caminos

redundantes por toda la red de modo que, si falla un cable, otro se hará cargo del tráfico.

Esta topología, a diferencia de otras, como la topología en árbol y la topología en estrella, no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento y la posibilidad de que un error en un nodo, no implique la caída de toda la red.

La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto, en consecuencia, la red malla, se transforma en una red muy confiable.

2 EQUIPOS DE TELECOMINICACIONES PARA REDES

2.1 Modelo OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, conocido mundialmente como Modelo OSI (*Open System Interconnection*), fue creado por la ISO (Organización Estándar Internacional), y en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes, y estandarizar la interconexión de sistemas abiertos en un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Figura 10. La pila OSI

A principios de la década de 1980 el desarrollo de redes sucedió con desorden en muchos sentidos, se produjo un enorme crecimiento en la cantidad y el tamaño de las redes y a medida que las empresas tomaron conciencia de las ventajas de usar tecnologías de conexión, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

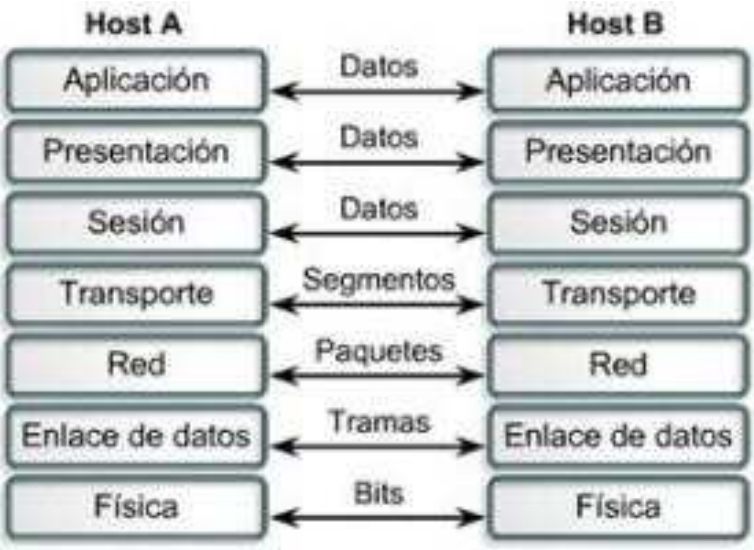
Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión, esto de la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgió con las empresas que desarrollaban tecnologías de conexión privada o propietaria, las tecnologías de conexión que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO), investigó modelos de conexión como la red de *Digital Equipment Corporation* (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

- Capa física (Capa 1)
- Capa de enlace de datos (Capa 2)
- Capa de red (Capa 3)
- Capa de transporte (Capa 4)
- Capa de sesión (Capa 5)
- Capa de presentación (Capa 6)
- Capa de aplicación (Capa 7)

Figura 11. Flujo de información por capas



2.1.1 Capa física (Capa 1)

La capa física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico, características del medio, y la forma en la que se transmite la información.

Esta capa dispone del control del medio físico y especifica bits de control, mediante:

- Definir conexiones físicas entre computadoras
- Describir el aspecto mecánico de la interfaz física

- Describir el aspecto electrónico de la interfaz física
- Describir el aspecto funcional de la interfaz física
- Definir la técnica de transmisión
- Definir el tipo de transmisión
- Definir la codificación de línea
- Definir la velocidad de transmisión
- Definir el modo de operación de la línea de datos.

Por ser el primer nivel del modelo OSI, en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación.

Cuando actúa en modo de emisión, se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión, estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos, dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es

inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

2.1.2 Capa de enlace de datos (Capa 2)

Conocido también como nivel de trama (*Frame*) o marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

Este nivel ensambla los datos en tramas y las transmite a través del medio, es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. Es en este nivel y mediante algoritmos, donde se podrá validar la integridad física de la trama; mas no será corregida a este nivel sino que se le notificará al transmisor para su retransmisión.

En el nivel de enlace de datos, se lleva a cabo el direccionamiento físico de la información; es decir, se leerán los encabezados que definen las direcciones de los nodos (para el caso de una WAN) o de los segmentos (para el caso de una LAN) por donde viajarán las tramas. Decimos que son direcciones físicas, ya que las direcciones lógicas o de la aplicación que pretendemos transmitir serán direccionadas o enrutadas en un nivel superior llamado nivel de red. En este nivel de enlace sólo se da tratamiento a las direcciones MAC para el caso de LAN y a las direcciones de las tramas síncronas para el caso de una WAN.

2.1.3 Capa de Red (Capa 3)

Este nivel define el enrutamiento y el envío de paquetes entre redes, tiene la responsabilidad de establecer, mantener y terminar las conexiones. Proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Capa de Transporte) o bien al nivel 2 (Capa de Enlace de Datos).

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre en inglés (*routers*), en ocasiones enrutadores.

Una función importante de este nivel o capa es la normalización del sistema de señalización y sistema de numeraciones de terminales, estos son elementos básicos en una red conmutada. Traduce direcciones lógicas o nombres en direcciones físicas, conmuta, enruta y controla la congestión de los paquetes de información en una sub-red. Define el estado de los mensajes que se envían a nodos de la red.

Los *routers* trabajan en esta capa, aunque pueden actuar como *switch* de capa 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de maquinas.

En este nivel se determina la ruta de los datos (Direccionamiento físico) y su receptor final IP.

2.1.4 Capa de transporte (Capa 4)

La capa de transporte es el cuarto nivel del modelo OSI, encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, así como de mantener el flujo de la red. Es la base de toda la jerarquía de protocolo.

El objetivo final de la capa transporte es proporcionar un servicio eficiente, confiable y económico a sus usuarios, que normalmente son procesos de la

capa de aplicación. Para lograr este objetivo, la capa de transporte utiliza los servicios proporcionados por la capa de red.

El hardware o software de la capa de transporte que se encarga del trabajo se llama entidad de transporte, la cual puede estar en el núcleo del sistema operativo, ubicada en un proceso independiente dentro de un paquete de biblioteca o en la tarjeta de red.

Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento, además, garantiza una entrega confiable de la información y asegura que la llegada de datos de la capa de red encuentre las características de transmisión y calidad de servicio requerido por el nivel 5 (Capa de sesión).

Las actividades que desarrolla esta capa son las siguientes:

- Define como direccionar la localidad física de los dispositivos de la red
- Asigna una dirección única de transporte a cada usuario
- Define una posible multicanalización (puede soportar múltiples conexiones)
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos

- Determina el protocolo que garantiza el envío del mensaje

- Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas

2.1.5 Capa de sesión (Capa 5)

Proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles. No obstante en algunas aplicaciones su utilización es ineludible.

Esta capa establece, gestiona y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta)

- Control de la concurrencia (que dos operaciones críticas no se efectúen al mismo tiempo)

- Mantener puntos de verificación (*checkpoints*), si se presenta una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación, en lugar de repetirla desde el principio.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

Los *firewall* actúan sobre esta capa, para bloquear los accesos a los puertos de un computador.

2.1.6 Capa de Presentación (Capa 6)

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (*little-endian* tipo Intel, *big-endian* tipo Motorola), sonidos o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar el contenido de la comunicación, pero no en cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de

representación de datos necesarias para la correcta interpretación de los mismos. Permite cifrar los datos y comprimirlos, en pocas palabras es un traductor.

2.1.7 Capa de aplicación (Capa 7)

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP).

Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación, suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

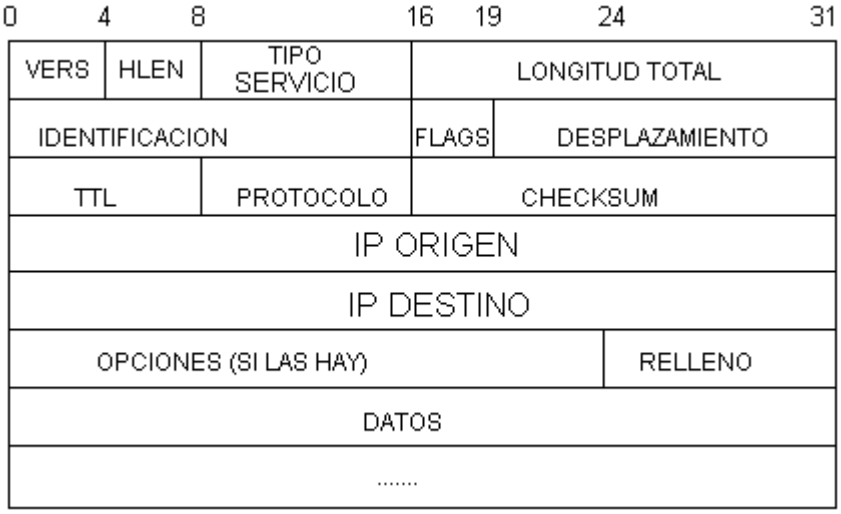
2.1.8 Datagramas de Red

Es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el

equipo terminal de datos receptor, de manera independiente a los fragmentos restantes.

Un datagrama tiene una cabecera de IP que contiene información de direcciones de la capa 3 (capa de red), los encaminadores examinan la dirección de destino de la cabecera de IP y dirigen los datagramas al destino. La capa de IP se denomina no orientada a conexión, ya que cada datagrama se encamina de forma independiente y la capa de IP no garantiza una entrega fiable, ni en secuencia, de los mismos. IP encamina su tráfico sin tener en cuenta la relación entre aplicaciones a la que pertenece un determinado datagrama.

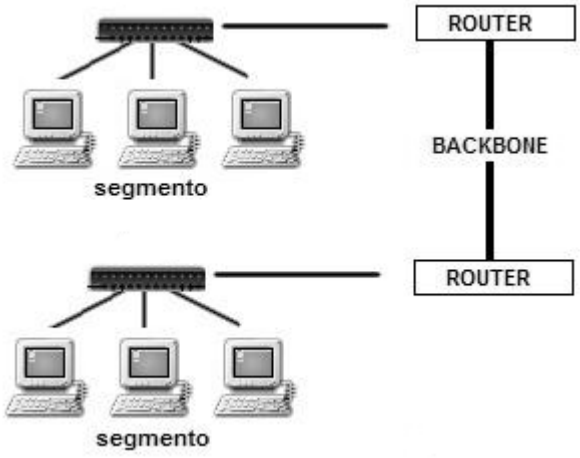
Figura 12. Datagrama de red



2.1.9 *Backbone*

No es más que el cableado troncal o subsistema vertical en una instalación de una LAN, que sigue la normativa de cableado estructurado. La gran mayoría de redes grandes pueden estar compuestas por múltiples LAN, y se conectan entre sí a través del *backbone*, que es el principal conducto que permite comunicar segmentos entre sí.

Figura 13. Conexión de un *backbone*



2.2 Hub´s de comunicación

Denominados como concentradores o repetidores, son dispositivos de emisión bastante sencillos, los concentradores no logran dirigir el tráfico que llega a través de ellos, y cualquier paquete de entrada es transmitido a otros puertos (que no sea el puerto de entrada). Dado que cada paquete está siendo

enviado a través de cualquier otro puerto, aparecen colisiones de paquetes como resultado, que impiden en gran medida la fluidez del tráfico.

Su único objetivo es recuperar los datos binarios que ingresan a un puerto y enviarlos a los demás puertos, el concentrador funciona en el nivel 1 del modelo OSI y es por ello que a veces se lo denomina repetidor multipuertos. Es un elemento de hardware que permite concentrar el tráfico de red que proviene de múltiples *host* y regenera la señal.

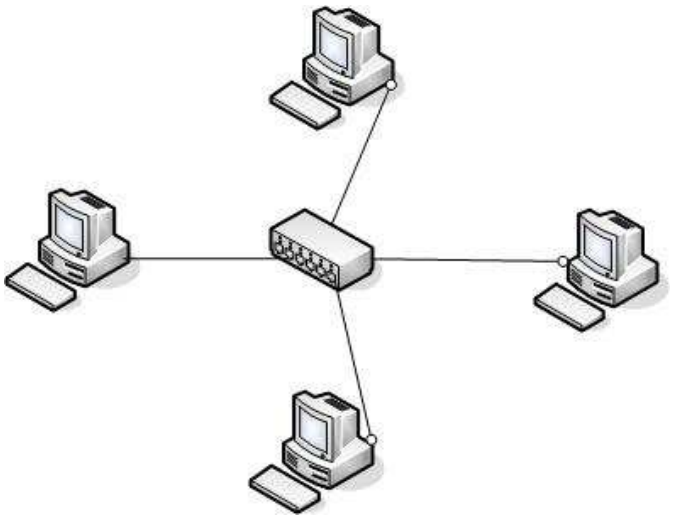
Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos, también se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan, existen 3 clases:

- Pasivo, no necesita energía eléctrica
- Activo, necesita alimentación
- Inteligente, también llamados *smart hubs*, son *hubs* activos que incluyen microprocesador

Uno de los usos más frecuentes que se le da a los concentradores es por ejemplo, la conexión de un analizador de protocolos conectado a un conmutador no siempre recibe todos los paquetes desde que el conmutador separa los puertos en los diferentes segmentos, la conexión del analizador de protocolos con un concentrador permite ver todo el tráfico en el segmento.

Figura 14. Conexión mediante *Hubs*



2.3 *Switches* de comunicación

Denominado en castellano como “conmutador”, es un dispositivo analógico que utiliza lógica de interconexión de redes, opera. Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los *switches* se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LAN (*Local Area Network*- Red de Área Local). El *switch* conmuta paquetes desde los puertos (interfaces) entrantes a los puertos salientes, suministrando a cada puerto el ancho de banda total.

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de los dispositivos alcanzables, a través de cada uno de sus puertos. Un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC, esto permite que, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino.

2.3.1 *Switches* de comunicación capa 2

Este es el tipo de *switch* de red de área local (LAN) más básico, el cual opera en la capa 2 del modelo OSI. Su antecesor es el bridge, por ello, muchas veces al *switch* se le refiere como un bridge multipuerto, pero con un costo más bajo, con mayor rendimiento y mayor densidad por puerto.

El *switch* capa 2 hace sus decisiones de envío de datos con base a la dirección MAC destino contenida en cada *frame*. Estos, al igual que los *bridges*, segmentan la red en dominios de colisión, proporcionando un mayor ancho de banda por cada estación.

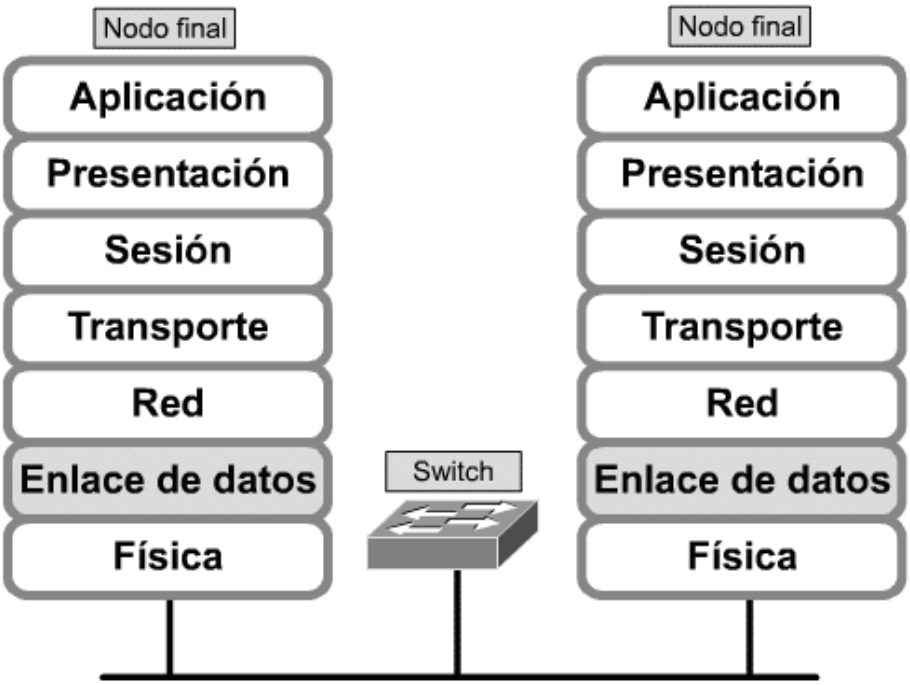
El uso de procesadores especializados incrementó la velocidad de conmutación de los *switches*, en comparación con los bridges, porque pueden enviar los datos a todos los puertos de forma casi simultánea.

Estos *switches* siguen, principalmente, dos esquemas para envío de tráfico, los cuales son:

- *Cut-trough*, comienzan el proceso de envío antes que el *frame* sea completamente recibido. En estos *switches* la latencia es baja, porque sólo basta con leer la dirección MAC destino para comenzar a transferir el *frame*. La desventaja de este esquema es que los *frames* corruptos (corruptos, enanos, con errores, etc.) son también enviados

- *Store-and-forward*, lee y valida el paquete completo antes de iniciar el proceso de envío. Esto permite que el *switch* descarte paquetes corruptos y se puedan definir filtros de tráfico. La desventaja de este esquema es que la latencia se incrementa con el tamaño del paquete.

Figura 15. Comunicación entre *switches* capa 2



2.3.2 *Switches* de comunicación capa 3

Este tipo de *switches* integran *routing* y *switching* para producir altas velocidades, esta es una tecnología nueva, a los cuales los vendedores se refieren muchas veces como: *Netflow, tag switching* y *Fast* IP.

Este nuevo tipo de dispositivos es el resultado de un proceso de evolución natural de las LAN, ya que combinan las funciones de los *switches* capa 2 con las capacidades de los *routers*, se pueden encontrar como *packet-by-packet* (PPL3) o como *cut-trought* (CTL3).

En ambos tipos de *switches*, se examinan todos los paquetes y se envían a sus destinos y la diferencia real entre ellos es el rendimiento. PPL3 enruta todos los paquetes, en tanto que los *switches* CTL3 efectúan la entrega de paquetes de una forma un poco distinta, estos *switches* investigan el destino del primer paquete en una serie y una vez que lo conoce, se establece una conexión y el flujo es conmutado en capa 2, lo cual hace que este último tenga una eficiencia de un *switch* capa 2.

Las actividades que desarrolla un *switch* capa 3 son las siguientes:

- Procesamiento de rutas, esto incluye construcción y mantenimiento de la tabla de enrutamiento.

- Envío de paquetes, una vez que el camino es determinado, los paquetes son enviados a su dirección destino y las direcciones MAC son resueltas y el *checksum* IP es calculado.

- Servicios especiales, traslación de paquetes, prioritización, autenticación, filtros, etc.

2.3.3 *Switches* de comunicación capa 4

La información en los encabezados de los paquetes comúnmente incluyen direccionamiento de capa 2 y 3, pero hay también información relevante a las capas superiores, como lo es el tipo de protocolo de capa 4 (UDP, TCP, etc.) y

el número de puerto (valor numérico que identifica la sesión abierta en el host, a la cual pertenece el paquete).

La información del encabezado de capa 4 permite clasificar de acuerdo a secuencias de paquetes manejados por aplicación. Ahora bien, dependiendo del diseño del *switch*, éste puede prioritizar servicios o garantizar ancho de banda por aplicación.

Algunos de los diseños de capa 4 son:

- Arquitectura basada en *Crossbard*, generalmente, sólo proveen prioritización por flujos porque tienen un esquema de *buffering* y de planificación muy compleja.

- *Switches* con memoria compartida y cola de salida, son capaces de manejar múltiples niveles de prioridades. Resultando con problemas en proveer servicios cuando el número de flujos excede el número de colas disponibles.

- *Switches* con colas por "flujos", son capaces de garantizar ancho de banda y manejar bien la congestión y pudiendo hacer la clasificación por flujos porque existe una cola por cada uno.

2.4 *Routers* de Comunicación

También denominado enrutador, ruteador o encaminador, es un dispositivo de *hardware* para interconexión de red de ordenadores que opera en la capa tres (Capa de Red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. El *router* une las Redes del emisor y el destinatario de una información determinada y además solo transmitirá entre las mismas la información necesaria.

Un *router* tiene dos misiones distintas aunque muy relacionadas y son:

- El *router* se asegura de que la información no va a donde no es necesario

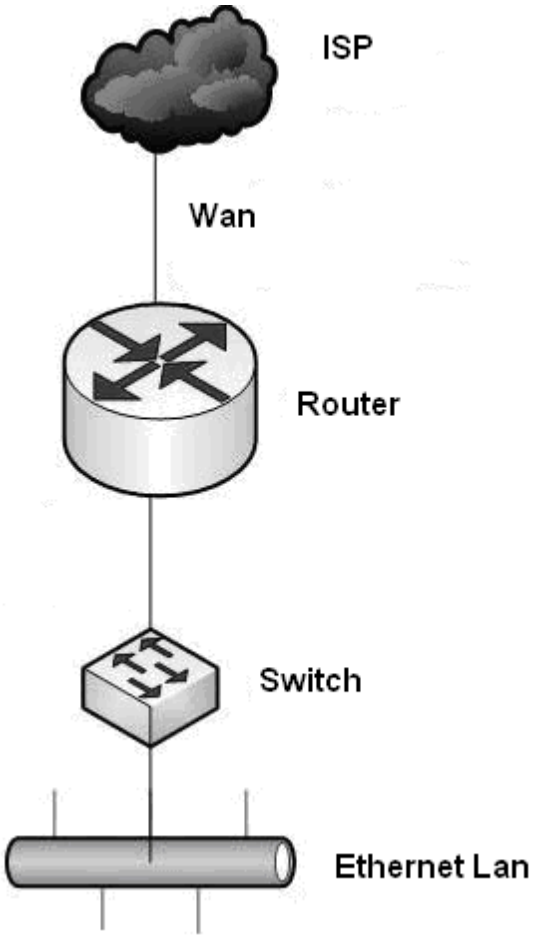
- El *router* se asegura que la información si llegue al destinatario

Los *routers* más sofisticados, y de hecho los más utilizados, hacen algo más, entre otras cosas protegen nuestra red del tráfico exterior, éstos son capaces de manejar bastante tráfico. Es por ello que son la opción más típica en redes, e incluso, en usuarios domésticos.

Los *routers* más potentes, que se están utilizando dentro de grandes empresas para gestionar el tráfico, manejan un volumen de millones de paquetes de datos por segundo y optimizan al máximo los caminos entre origen y destino.

Además de su función de enrutar, los *routers* también se utilizan para manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra. Como no todas las redes pueden manejar el mismo tamaño de paquetes de datos, los *routers* deben fragmentar los paquetes de datos para que puedan viajar libremente.

Figura 16. Esquema de comunicación utilizando un *router*



2.4.1 Transmisión de paquetes

El movimiento de información en a través de una red funciona dividiendo en pequeñas unidades o “paquetes” (de unos 1.500 bytes por paquete) cada uno de los mensajes. Cada paquete lleva información del origen, el destinatario y lugar de ese paquete en el total de la información transmitida (para que luego el mensaje pueda ser reconstruido correctamente) e información de cómo confirmar su llegada al destino.

El *router* se encargará de analizar paquete por paquete el origen y el destino buscando de esta manera el camino más corto de uno a otro. Esta forma de transmitir información tiene grandes ventajas:

- El *router* es capaz de ver si una ruta no funciona y buscar una alternativa

- El *router* es capaz incluso de buscar la ruta más rápida (por ejemplo la que tenga menos tráfico) en caso de poder escoger entre varias posibilidades

2.4.2 Enrutamiento de información

Existen gran cantidad de formas para enrutar la información sobre una red, los dos tipos de enrutamiento principales son:

- Los *routers* del tipo vector de distancias, generan una tabla de enrutamiento que calcula el "costo" (en términos de número de saltos) de cada ruta y después envían esta tabla a los *routers* cercanos. Para cada solicitud de conexión el *router* elige la ruta menos costosa.

- Los *routers* del tipo estado de enlace, escuchan continuamente la red para poder identificar los diferentes elementos que la rodean. Con esta información, cada *router* calcula la ruta más corta (en tiempo) a los *routers* cercanos y envía esta información en forma de paquetes de actualización. Finalmente, cada *router* confecciona su tabla de enrutamiento calculando las rutas más cortas hacia otros *routers*.

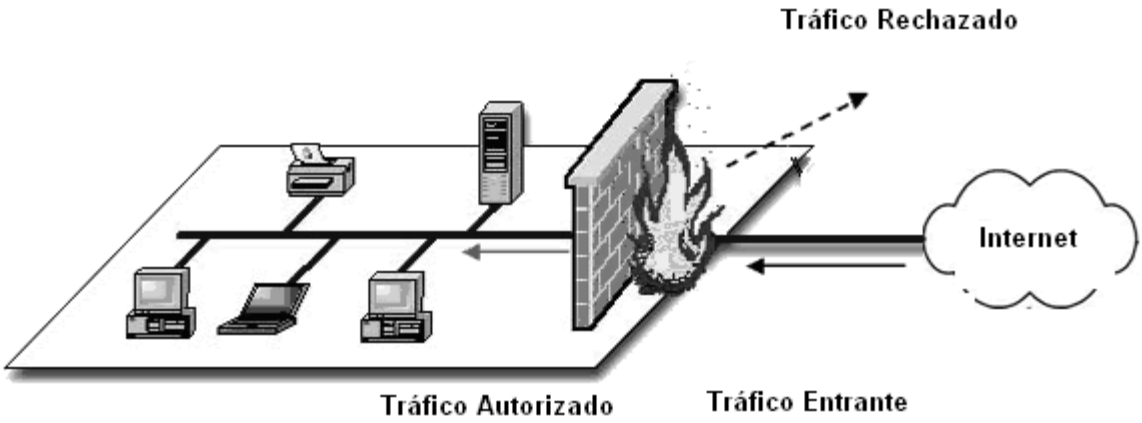
2.5 *Firewall*

Un *firewall* es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que el usuario necesite, permite o deniega su paso. Para permitir o denegar una comunicación el *firewall* examina el tipo de servicio al que corresponde, como pueden ser *web* o el correo. Dependiendo del servicio, el *firewall* decide si lo permite o no. Además, el *firewall* examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no, es un elemento de *hardware* o *software* que se utiliza en una red de computadoras para controlar las comunicaciones,

permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Figura 17. Funcionamiento de un *firewall*



Un *firewall* puede permitir desde una red local hacia Internet servicios *web*, correo y ftp, pero no restringe tráfico que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la *web*. Dependiendo del *firewall* que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Puede ser un dispositivo *software* o *hardware*, es decir, una caja 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 módem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con *software* específico, que lo único que hacen es monitorear las comunicaciones entre redes.

2.5.1 Funcionamiento de los *firewall*

Los *firewall* manejan la conectividad por zonas (seguras o no) o bien por niveles de seguridad, los que establece el usuario, según el grado de permisividad que le imponga al equipo. Los *firewall* sólo deben configurarse según las necesidades o gustos del usuario, cosa que no termina con la instalación. Tras esta, una vez que el usuario se conecta a Internet (o aún antes) comienza a trabajar el programa. Los primeros días de uso pueden ser un tanto engorrosos, ya que tanto el usuario como el programa "aprenden" mutuamente. El usuario aprende las funciones y el programa qué cosas debe dejar pasar, qué bloquear y qué programas dejar conectar, por eso al principio son puras preguntas, hasta que se van conformando las reglas de uso en la medida que el usuario haga determinadas acciones con las alarmas. Con este tipo de aviso el programa pide que se defina la regla que se va a aplicar entre alguna de las posibles.

Una vez que se determina qué hacer con esa acción (por ejemplo permitir que un programa se conecte siempre a Internet), con cada cartel de

alerta se van configurando las reglas ya que luego ese aviso no va a volver a aparecer. Con el tiempo estos avisos se reducen al mínimo. Por cada acción crean un registro de la actividad (*log*) para el posterior análisis del usuario.

Las políticas de accesos en un *firewall* se deben diseñar poniendo principal atención en sus limitaciones y capacidades, pero también pensando en las amenazas y vulnerabilidades presentes en una red externa. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad, también es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

2.5.2 Beneficios de un *firewall*

Los *firewall* manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

Otra causa que ha hecho que el uso de *firewall* se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en

crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el *firewall*.

También son importantes los *firewall* para llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

2.5.3 Limitantes de un *firewall*

La limitación más grande que tiene un *firewall*, es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los *firewall* no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje *Back Doors*, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

El *firewall* no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El *firewall* no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (diskettes, memorias, etc.) y sustraerlas del edificio.

No pueden proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y *software*. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

3 SEGURIDAD INFORMÁTICA

3.1 Importancia de la Seguridad Informática

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{Riesgo} = \frac{\text{Amenaza X Vulnerabilidad}}{\text{Contramedidas}}$$

Una definición muy útil para conocer lo que implica el concepto de seguridad informática es, garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos. En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales. Es por esto que la información se puede reconocer como:

- Crítica, indispensable para garantizar la continuidad operativa de la organización

- Valiosa, es un activo corporativo que tiene valor en sí mismo

- Sensitiva, debe ser conocida por las personas que necesitan los datos

3.1.1 ¿Por qué es importante la seguridad informática?

Por lo valiosa que se convierte la información en las empresas, existen personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Tales personajes pueden incluso formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales

amenazas combinadas. El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor incalculable dentro de la empresa. La seguridad informática debe garantizar:

- La disponibilidad de los sistemas de información
- La recuperación rápida y completa de los sistemas de información
- La integridad de la información
- La confidencialidad de la información

3.1.2 Amenazas y vulnerabilidades

Por vulnerabilidad entendemos la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y *hackers*; no obstante, con el crecimiento de las comunicaciones a nivel mundial, los riesgos han evolucionado y ahora las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "*hackeo*", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

En los ataques de negación de servicio es evidente que los riesgos están en la red y no en el equipo, ya que este no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el sitio *web* de la compañía.

Por el enorme número de amenazas y riesgos que existen a lo largo del mundo, la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo. Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos. Las políticas deberán basarse en los siguientes pasos:

- Identificación y selección de lo que se debe proteger (información sensible)

- Establecer niveles de prioridad e importancia sobre esta información

- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles

- Identificar las amenazas, así como los niveles de vulnerabilidad de la red

- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla

- Implementar respuesta a incidentes y recuperación para disminuir el impacto

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente se habrá identificado y definido los sistemas y datos a proteger. Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional utilizando firewalls, autenticación, antivirus, controles, políticas, procedimientos, análisis de vulnerabilidad, entre otros.

Un esquema de seguridad empresarial contempla la seguridad física y lógica de una compañía. La primera se refiere a la protección contra robo o daño al personal, equipo e instalaciones de la empresa; y la segunda está relacionada con el tema que del cual estamos adentrando: la protección a la información, a través de una arquitectura de seguridad eficiente. Esta última debe ser proactiva, integrar una serie de iniciativas para actuar en forma rápida y eficaz ante incidentes y recuperación de información, así como elementos

para generar una cultura de seguridad dentro de la organización. Entre estos elementos podemos mencionar:

- Implementación de políticas de seguridad informática
- Identificación de problemas
- Desarrollo de planes de seguridad informática
- Análisis de la seguridad en equipos de computo
- Auditoría y revisión de sistemas

3.2 Métodos de seguridad en redes informáticas

La seguridad, protección de los equipos conectados en red y de los datos que almacenan y comparten, es un hecho muy importante en la interconexión de equipos. Cuanto más grande sea una empresa, más importante será la necesidad de seguridad en la red. La seguridad es bastante más que evitar accesos no autorizados a los equipos y a sus datos, incluye el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto de la red. La planificación de la seguridad es un elemento importante en el diseño de una red, es más sencillo implementar una red segura a partir de un plan, que recuperar los datos perdidos.

3.2.1 Planificación de la seguridad en la red

En un entorno de red debe asegurarse la privacidad de los datos sensibles, no sólo es importante asegurar la información, sino también, proteger las operaciones de la red de daños no intencionados o deliberados. El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear este equilibrio. Las cuatro amenazas principales que afectan a la seguridad de los datos en una red son:

- Acceso no autorizado
- Soborno electrónico
- Robo
- Daño intencionado o no intencionado

La seguridad de los datos no siempre se implementa en forma apropiada, precisamente por la seriedad de estas amenazas. La tarea del administrador es asegurar que la red se mantenga fiable y segura, en resumen, libre de amenazas.

3.2.1.1 Nivel de seguridad

La magnitud y nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red. Una red que almacena datos para un banco importante, requiere una mayor seguridad, que una LAN que enlaza equipos en una pequeña organización de voluntarios.

3.2.1.2 Configuración de las políticas o normativas

Generar la seguridad en una red requiere establecer un conjunto de reglas, regulaciones y políticas. El primer paso para garantizar la seguridad de los datos es implementar las políticas que establecen los matices de la seguridad y ayudan al administrador y a los usuarios a actuar cuando se producen modificaciones, planificadas y no planificadas, en el desarrollo de la red.

3.2.1.3 Prevención

La mejor forma de diseñar políticas de seguridad es elegir una perspectiva preventiva, los datos se mantienen seguros cuando se evitan accesos no autorizados. Un sistema basado en la prevención requiere que el administrador

conozca todas las herramientas y métodos disponibles que permiten mantener la seguridad de los datos.

3.2.1.4 Autenticación

Para acceder a la red, un usuario debe introducir un nombre de usuario y una contraseña válida. Dado que las contraseñas se vinculan a las cuentas de usuario, un sistema de autenticación de contraseñas constituye la primera línea de defensa frente a usuarios no autorizados. Es importante no permitir un exceso de confianza en este proceso de autenticación engañándonos con una falsa idea de seguridad. Esto sólo puede proporcionar a un usuario acceso completo a la red, de forma que cualquier cosa que se comparta está disponible para este usuario. La autenticación funciona sólo en una red basada en servidor, donde el nombre y contraseña de usuario debe ser autenticada utilizando para ello la base de datos de seguridad.

3.2.1.5 Entrenamiento

Los errores no intencionados pueden implicar fallos en la seguridad. Un usuario de red perfectamente entrenado probablemente va a causar, de forma accidental, un número menor de errores que un principiante sin ningún tipo de experiencia.

El administrador debería asegurar que alguien que utiliza la red esté familiarizado con sus procedimientos operativos y con las tareas relativas a la seguridad. Para lograr esto, el administrador puede desarrollar una guía breve y clara que especifique lo que necesitan conocer los usuarios y obligar a que los nuevos usuarios asistan a las clases de entrenamiento apropiadas.

3.2.2 Equipamiento de seguridad

El primer paso en el mantenimiento de la seguridad de los datos es proporcionar seguridad física para el hardware de la red. La magnitud de la seguridad requerida depende de:

- El tamaño de la empresa
- La importancia de los datos
- Los recursos disponibles

3.2.2.1 Seguridad de los servidores

En un sistema centralizado, donde existe una gran cantidad de datos críticos y usuarios, es importante garantizar la seguridad en los servidores de amenazas accidentales o deliberadas. La solución más sencilla pasa por

encerrar los servidores en una habitación de equipos con acceso restringido. Esto puede no resultar viable dependiendo del tamaño de la empresa. No obstante, encerrar los servidores en una oficina incluso en un armario de almacén es, a menudo, viable y nos proporciona una forma de intentar garantizar la seguridad de los servidores.

3.2.2.2 Seguridad del cableado

La información transportada en los medios de transmisión físicos se puede monitorear con dispositivos electrónicos de escucha. Además, un cable de cobre se puede intervenir pudiendo robar la información que transmite.

Sólo el personal autorizado debería tener acceso al cable que transporta datos sensibles. Una planificación apropiada puede garantizar que el cable sea inaccesible al personal no autorizado. Por ejemplo, el cable puede instalarse dentro de la estructura del edificio a través del techo, paredes y cielos falsos.

3.2.3 Modelos de seguridad

Después de implementar la seguridad en los componentes físicos de la red, el administrador necesita garantizar la seguridad en los recursos de la red, evitando accesos no autorizados y daños accidentales o deliberados. Las

políticas para la asignación de permisos y derechos a los recursos de la red constituyen el corazón de la seguridad de la red.

Se han desarrollado dos modelos de seguridad para garantizar la seguridad de los datos y recursos hardware:

- Compartir recursos en forma protegida por contraseña
- Permisos de acceso o seguridad a nivel usuario

3.2.3.1 Compartir recursos en forma protegida

La implementación de un esquema para compartir recursos protegidos por contraseñas requiere la asignación de una contraseña a cada recurso compartido. Se garantiza el acceso a un recurso compartido cuando el usuario introduce la contraseña correcta.

En muchos sistemas, se pueden compartir los recursos con diferentes tipos de permisos, como por ejemplo:

- Solo lectura, los usuarios que conocen la contraseña tienen acceso de lectura a los archivos de este directorio, pero no pueden modificar los documentos originales

- Total, los usuarios pueden visualizar, modificar, añadir y borrar los archivos del directorio compartido

- Depende de la contraseña, implica configurar los recursos compartidos para que utilicen niveles de contraseñas

El esquema de compartir utilizando contraseña es un método de seguridad sencillo que permite a alguien que conozca la contraseña obtener el acceso a un recurso determinado.

3.2.3.2 Permisos de acceso

La seguridad basada en los permisos de acceso implica la asignación de ciertos derechos usuario por usuario. Un usuario escribe una contraseña cuando entra en la red. El servidor valida esta combinación de contraseña y nombre de usuario y la utiliza para asignar o denegar el acceso a los recursos compartidos, comprobando el acceso al recurso en una base de datos de accesos de usuarios en el servidor.

La seguridad de los permisos de acceso proporciona un alto nivel de control sobre los derechos de acceso. La seguridad a nivel de usuario es el modelo preferido en las grandes organizaciones, puesto que se trata de la seguridad más completa y permite determinar varios niveles de seguridad.

3.3 DMZ´s

Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores *web*, servidores de correo electrónico, servidores FTP), es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer la seguridad de la compañía.

El término "zona desmilitarizada" o DMZ hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

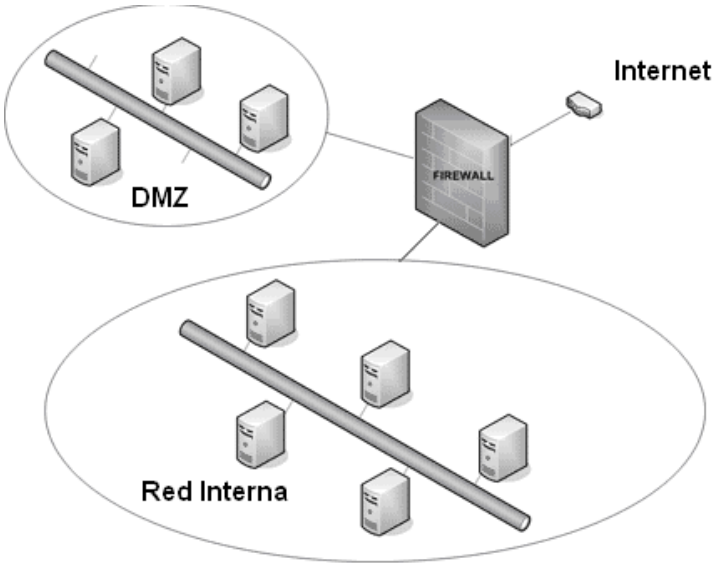
Una zona desmilitarizada o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet aunque puede ser cualquier otra red externa que se conecte a nuestra LAN. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa. Los equipos en la DMZ no pueden conectar con la red interna, lo que permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Por lo general, las políticas de seguridad para las DMZ son las siguientes:

- El tráfico de la red externa a la DMZ está autorizado

- El tráfico de la red externa a la red interna está prohibido
- El tráfico de la red interna a la DMZ está autorizado
- El tráfico de la red interna a la red externa está autorizado
- El tráfico de la DMZ a la red interna está prohibido
- El tráfico de la DMZ a la red externa está denegado

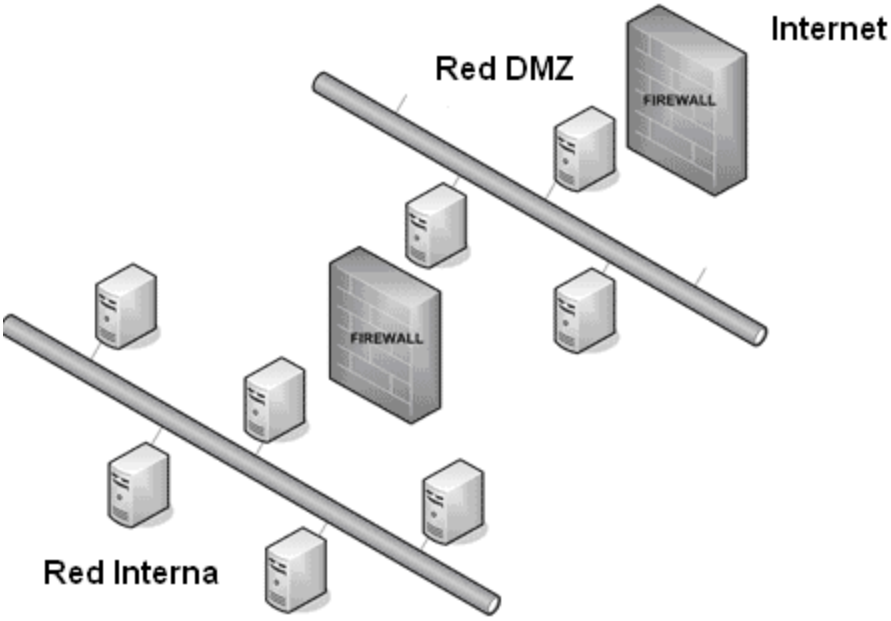
Una DMZ se crea a menudo a través de las opciones de configuración del *firewall*, donde cada red se conecta a un puerto distinto de éste dispositivo. Esta configuración se llama *firewall* en trípode (*three-legged firewall*).

Figura 18. Configuración de *firewall* en trípode



Un planteamiento más seguro es usar dos *firewall*, donde la DMZ se sitúa en medio y se conecta a ambos *firewall*, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado *firewall* de subred monitoreada (*screened-subnet firewall*).

Figura 19. Configuración *firewall* de subred monitoreada



3.3.1 Características de una DMZ

Entre las características más comunes dentro de las DMZ´s podemos encontrar las siguientes:

- Filtrado de paquetes
- NAT, mapeo bidireccional
- Colas de tráfico y prioridad
- Salidas redundantes / balanceo de carga
- Filtrado de contenido

3.3.1.1 Filtrado de paquetes

La acción de filtrar paquetes es bloquear o permitir el paso de datos en forma selectiva, según van llegando a una interfaz de red. Los criterios que se usan para inspeccionar los paquetes, son tomados de la información existente en la capa 3 (IPv4 y IPv6) y en la capa 4 (TCP, UDP, ICMP, y ICMPv6) de las cabeceras de los paquetes.

Los criterios que más se utilizan son los de la dirección de origen y de destino, el puerto de origen y de destino, y el protocolo. Las reglas de filtrado especifican los criterios con los que debe concordar un paquete y la acción a seguir, bien sea bloquearlo o permitir que pase, que se toma cuando se encuentra una concordancia.

Las reglas de filtrado se evalúan por orden de secuencia, de la primera a la última. La última regla que concuerde será la que dictamine qué acción se tomará con el paquete. Al principio del grupo de reglas de filtrado hay un *pass all* implícito que indica que si algún paquete no concuerda con ninguna de las reglas de filtrado, la acción a seguir será dejarlo pasar, o sea permitirle el acceso.

3.3.1.2 NAT, mapeo bidireccional

La traducción de direcciones de red, o NAT (*Network Address Translation*) es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. NAT es necesario cuando la cantidad de direcciones IP que nos han asignado hacia una red externa es inferior a la cantidad de equipos que necesitamos accedan a dicha red.

Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT. La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder:

- Invertir los cambios en los paquetes devueltos

- Asegurarse de que los paquetes devueltos pasen a través del *firewall* y no sean bloqueados

3.3.1.3 Colas de tráfico y prioridad

Poner algo en cola es almacenarlo en orden, a la espera de ser procesado. Dentro de una DMZ, cuando se envían paquetes desde un servidor, éstos entran en un sistema de colas en el que permanecen hasta ser procesados por el sistema.

3.3.1.4 Salidas redundantes / balanceo de carga

Para poder llevar acabo esta acción el sistema DMZ, reserva en grupo de direcciones cuyo uso comparten un grupo de usuarios. Una reserva de direcciones puede aparecer como la dirección de redirección, como la dirección de traducción en las reglas nat y como la dirección de destino en las opciones *route-to, reply-to,* y *dup-to* de las reglas de filtrado de paquetes.

3.3.1.5 Filtrado de contenido (*Caching*)

La ventaja del *caching* consiste en que cuando varios clientes solicitan el mismo objeto, este puede proporcionárseles desde el caché. De este modo, los clientes obtiene los datos de una forma más rápida y se reduce al mismo tiempo el volumen de transferencias en la red.

Además del *caching*, ofrece múltiples prestaciones tales como:

- la definición de jerarquías de servicios para distribuir la carga del sistema

- establecer estrictas reglas de control de acceso para los clientes que quieran acceder

- permitir o denegar el acceso a determinadas páginas *web* con ayuda de aplicaciones adicionales

4 IMPLEMENTACIÓN DE UNA DMZ CORPORATIVA

4.1 Metodología de implementación

Como lo hemos descrito en capítulos anteriores, el aseguramiento de redes informáticas mediante el uso de DMZ´s es una muy buena opción para el resguardo de información sensible dentro de una empresa. El uso de este tipo de seguridad se volvió muy común por la facilidad y los bajos costos que representan implementar uno de estos sistemas.

Para la implementación de una DMZ (red desmilitarizada) corporativa, se utilizará el sistema respaldado por el PMI (*Project Management Institute*), para la implementación de proyectos a nivel internacional, esta es una asociación que rige gestiones para la implementación de proyectos.

4.1.1 PMI

El *Project Management Institute* (PMI) es considerado la asociación profesional para la gestión de proyectos sin fines de lucro más grande del mundo. Su oficina central está ubicada en la localidad de *Newtown Square*, a las afueras de la ciudad de Filadelfia en Pennsylvania, Estados Unidos. Entre

sus principales objetivos se encuentran formular estándares profesionales, generar conocimiento a través de la investigación, y promover la Gestión de Proyectos como profesión a través de sus programas de certificación.

4.1.2 Gestión de proyectos

La gestión de proyectos es la disciplina de organizar y administrar recursos de manera tal que se pueda culminar todo el trabajo requerido en el proyecto dentro del alcance, el tiempo, y costos definidos. Un proyecto es un esfuerzo temporal, único y progresivo, emprendido para crear un producto o un servicio también único.

Tomando como referencia a la economía, es posible demostrar que el desarrollo empresarial guarda una relación directa con la inversión, lo que determina que mayores niveles de inversión reportan mayores índices de crecimiento empresarial. Al mismo tiempo podemos afirmar que la capacidad de crecimiento de una empresa no depende exclusivamente de la dimensión de la inversión, sino que también de la calidad de la misma. Por lo tanto, se precisa contar con instrumentos e infraestructura idóneos que permitan identificar los proyectos de inversión y seleccionar aquellos que garanticen mayor crecimiento económico empresarial y bienestar para la sociedad.

A través de un proceso inteligente conocido como "identificación, formulación, evaluación y gestión de proyectos", que se suele enmarcar en un concepto más amplio de "planeación" se pretende orientar la utilización

adecuada de los recursos buscando siempre objetivos de crecimiento empresarial y social. Por lo tanto, para asignar mejor los recursos se requiere mayor información sobre la rentabilidad (financiera, económica y social) de los proyectos e idear mecanismos que permitan programar la inversión en función de dichas rentabilidades.

Formular un proyecto en este contexto significa, verificar los efectos económicos, técnicos, financieros, institucionales, jurídicos, ambientales, políticos y organizativos, de asignar recursos hacia el logro de unos objetivos.

4.1.3 Características de un proyecto

Es de suma importancia para el éxito de un proyecto poder definir sus características, entre las más importantes podemos mencionar las siguientes:

- Característica temporal
- Característica de productos, servicios o resultados únicos
- Característica de elaboración gradual

4.1.3.1 Características Temporal

Significa que cada proyecto tiene un comienzo definido y un final definido. El final se alcanza cuando se han logrado los objetivos del proyecto o cuando queda claro que los objetivos del proyecto no serán o no podrán ser alcanzados, o cuando la necesidad del proyecto ya no exista. Temporal no necesariamente significa de corta duración; muchos proyectos duran varios años. En cada caso, sin embargo, la duración de un proyecto es limitada. Los proyectos no son esfuerzos continuos.

4.1.3.2 Características de Productos, Servicios o Resultados Únicos

Un proyecto crea productos entregables únicos. Productos entregables son productos, servicios o resultados. Los proyectos pueden crear:

- Un producto o artículo producido, que es cuantificable, y que puede ser un elemento terminado o un componente

- La capacidad de prestar un servicio como, funciones del negocio que respaldan la producción o la distribución

- Un resultado como, salidas o documentos. Por ejemplo, de un proyecto de investigación se obtienen conocimientos que pueden usarse para

determinar si existe o no una tendencia o si un nuevo proceso beneficiará a la sociedad.

4.1.3.3 Características de Elaboración Gradual

Característica de los proyectos que acompaña a los conceptos de temporal y único. “Elaboración gradual” significa desarrollar en pasos e ir aumentando mediante incrementos. El alcance de un proyecto se define de forma general al comienzo del proyecto, y se hace más explícito y detallado a medida que el equipo del proyecto desarrolla un mejor y más completo entendimiento de los objetivos y de los productos entregables.

4.1.4 Restricciones de un Proyecto

Los proyectos necesitan ser ejecutados y entregados bajo ciertas restricciones. Tradicionalmente, estas restricciones han sido alcance, tiempo y costo. Esto también se conoce como el Triángulo de la Gestión de Proyectos, donde cada lado representa una restricción. Un lado del triángulo no puede ser modificado sin impactar a los otros. Un refinamiento posterior de las restricciones separa la calidad del producto del alcance, y hace de la calidad una cuarta restricción.

- La restricción de tiempo, se refiere a la cantidad de tiempo disponible para completar un proyecto

- La restricción de costo, se refiere a la cantidad presupuestada para el proyecto

- La restricción de alcance, se refiere a lo que se debe hacer para producir el resultado final del proyecto

4.1.4.1 Restricciones de Tiempo

El tiempo se descompone para propósitos de análisis en el tiempo requerido para completar los componentes del proyecto que es, a su vez, descompuesto en el tiempo requerido para completar cada tarea que contribuye a la finalización de cada componente. Cuando se realizan tareas utilizando gestión de proyectos, es importante partir el trabajo en pedazos menores para que sean fáciles de seguir.

4.1.4.2 Restricciones de Costo

El costo de desarrollar un proyecto depende de múltiples variables incluyendo costos de mano de obra, costos de materiales, administración de riesgo, infraestructura (edificios, máquinas, etc.), equipo y utilidades. Cuando se

contrata a un consultor independiente para un proyecto, el costo típicamente será determinado por la tarifa de la empresa consultora multiplicada por un estimado del avance del proyecto.

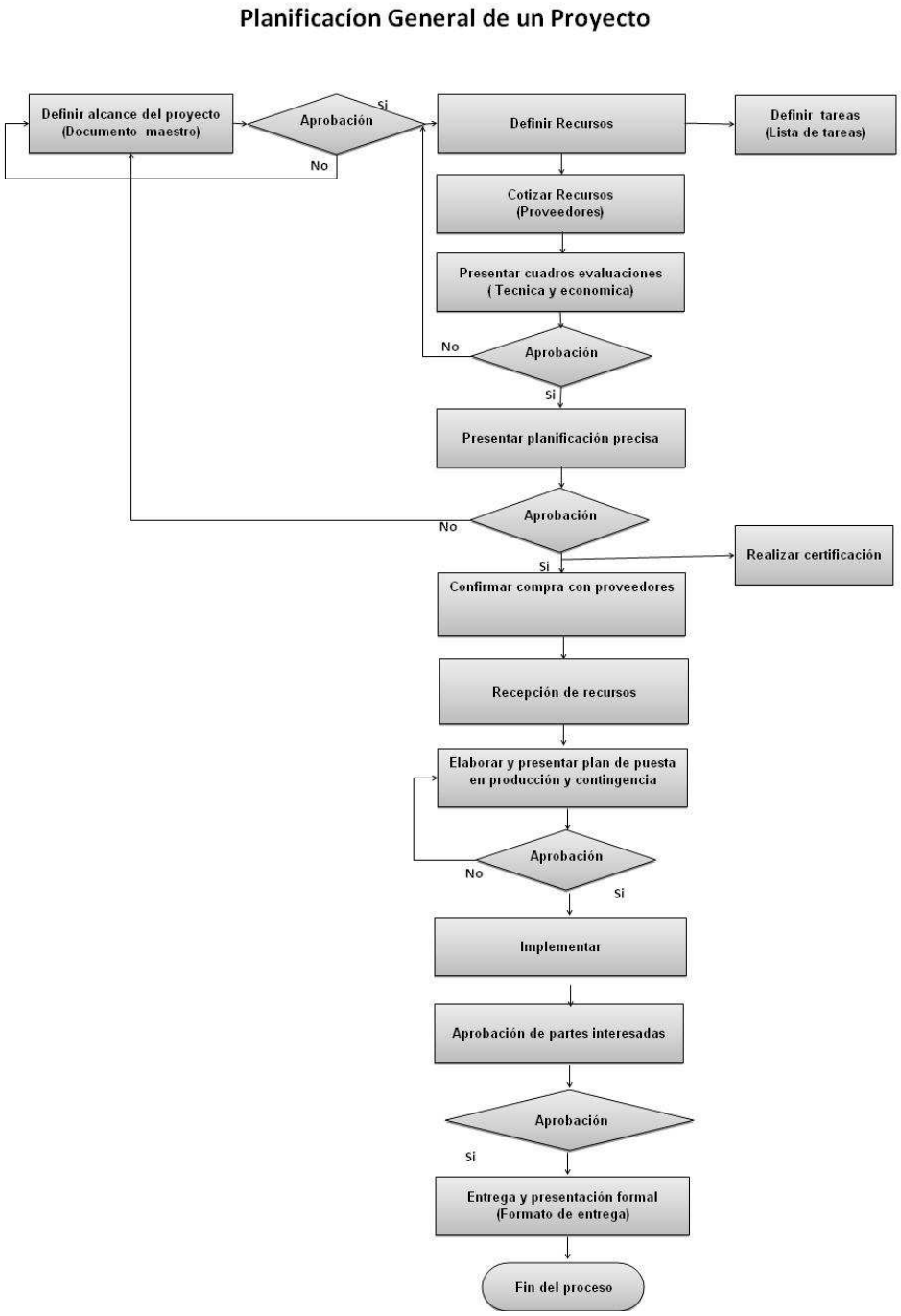
4.1.4.3 Restricciones de Alcance

La definición global de lo que se supone que el proyecto debe alcanzar y una descripción específica de lo que el resultado final debe ser o debe realizar. Un componente principal del alcance es la calidad del producto final. La cantidad de tiempo dedicado a las tareas individuales determina la calidad global del proyecto. Algunas tareas pueden requerir una cantidad dada de tiempo para ser completadas adecuadamente, pero con más tiempo podrían ser completadas excepcionalmente. A lo largo de un proyecto grande, la calidad puede tener un impacto muy significativo en el tiempo y en el costo (o viceversa).

4.2 Procedimiento de Implementación

Para la implementación definiremos un flujo de pasos los cuales debemos de seguir y cumplir a cabalidad para poder obtener el óptimo resultado de la ejecución de un proyecto.

Figura 20. Flujo para la implementación de proyectos



4.2.1 Definición del alcance del proyecto

En es un punto crucial para la implementación de un proyecto, es en donde se da una descripción general del proyecto proyectando las necesidades que se tienen, se define el alcance, el impacto, las áreas de oportunidad, factores críticos, restricciones, fases y tiempo estimado del proyecto.

Presentaremos un formato base en el cual se puede definir el alcance del proyecto.

Figura 21. Formato para la definición de alcances de un proyecto

[Nombre del Proyecto]		
A.	**Descripción General del Proyecto**	
	Declaración del problema (Problem Statement)	
	[Describa la razón(es) para iniciar el proyecto, enfocándose en una mejora o problema].	
B.	**Alcance del proyecto**	
	Metas y objetivos del proyecto (Valores cuantificables)	
	[Describa el alcance del proyecto. Definir limites e identificar los servicios o productos entregados por el proyecto , establecer el alcance del proyecto]	
	Impacto:	
	[Describa el Impacto que el proyecto tendra en donde se implementará]	
	Factores criticos de exito (Critical Success Factors)	
	[Describa los factores o caracteristicas consideradas como criticas para el exito del proyecto, como los que en su ausencia el proyecto podria fallar]	
	Partes interesadas del proyecto:	
	Area(s):	[Area donde se implementará el proyecto]
C.	**Implementacion del proyecto:**	
	Fases del proyecto	
	[Describa las fases o las partes en las que se desarrollá el proyecto]	
D	**Estimaciones del proyecto**	
	Tiempo Estimado:	
	Inicio del proyecto:	[fecha objetivo]
	Termación del proyecto:	[fecha estimada]
	Recursos requeridos:	
	Equipo y recursos de soporte:	
	Estimacion de costos:	

Para el caso de una implementación de una DMZ corporativa, tomando en cuenta este formato, se presenta el siguiente formulario en donde se define el alcance del proyecto.

Figura 22. Definición de alcance para proyecto de DMZ´s

Aseguramiento de Redes Mediante DMZ´s		
A.	**Descripción General del Proyecto**	
	Declaración del problema (Problem Statement)	
	Mantener un sistema que controle las conexiones seguras y que mantenga la alta disponibilidad de información sensible para la corporación.	
B.	**Alcance del proyecto**	
	Metas y objetivos del proyecto (Valores cuantificables)	
	El sistema podrá dar seguridad sobre conexiones externas que puedan en dado momento atentar contra información interna de la corporación y estabilizará el funcionamiento de la red.	
	Impacto:	
	Dará un apoyo al área de administración de IT, con lo referente a la administración y seguridad de la red interna.	
	Factores críticos de éxito (Critical Success Factors)	
	Una administración confiable, un aceptación por las áreas de auditoria interna y una alta disponibilidad de los colaboradores para auto capacitarse en la administración de este sistema.	
	Partes interesadas del proyecto:	
	Area(s):	Administración de Sistemas IT
C.	**Implementación del proyecto:**	
	Fases del proyecto	
	Este proyecto constará de una sola fase, ya que solo requiere una configuración completa	
D	**Estimaciones del proyecto**	
	Tiempo Estimado:	2 meses
	Inicio del proyecto:	Septiembre del presente año
	Termación del proyecto:	Diciembre del presente año
	Recursos requeridos:	2 Ingenieros dedicados
	Equipo y recursos de soporte:	Equipos de Telecomunicaciones dedicados
	Estimación de costos:	$48,000

4.2.2 Definición de recursos necesarios

Se define un formato en donde se documentará que tipo de recurso es el que se necesita para la implementación de este proyecto, el formato que utilizaremos es el siguiente:

Figura 23. Formato para definición de recursos necesarios

LISTADO DE RECURSOS		
No.	**Detalle**	**Proveedor (interno \ externo)**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Para nuestro caso en específico, únicamente necesitaremos apoyo de dos recursos internos. Estos recursos deben de estar dedicados a la implementación del sistema.

Figura 24. Definición de recursos necesarios para proyecto de DMZ´s

LISTADO DE RECURSOS		
No.	**Detalle**	**Proveedor (interno \ externo)**
1	Ing. De Proyectos	Interno
2	Ing. De Proyectos	Interno
3		
4		
5		
6		
7		
8		
9		
10		

4.2.3 Definición de posibles proveedores

Se debe de tener un inventario de posibles proveedores, que cumplan con estándares de calidad para poder ser tomados en cuenta y de esta forma tener la certeza de que podrán atender nuestros requerimientos sin ningún problema. El inventario de proveedores debe de esquematizarse de la siguiente manera:

Figura 25. Formato para inventario de proveedores

INFORMACIÓN DE PROVEEDORES					
Nombre de la Empresa	Nit	Dirección	Infraestructura que ofrece	Marcas que distribuye	Contactos y teléfonos
Proveedor #1	7653762-1	Ave Reforma 12-33 zona 2	Servidores , computadoras, equipo de comunicación, soluciones de negocio	IBM, Cisco, Lexmark	
Proveedor #2	7673264-5	23 ave 31-01 zona 3	Equipo eléctrico, equipo de seguridad informática	Stediwatt	
Proveedor #3	643543-9	14 AVENIDA 7-12 ZONA 5	SOLUCIONES EMPRESARIALES PARA INFRAESTRUCTURA INFORMATICA: EQUIPO, PERIFERICOS Y SUMINISTROS DE COMPUTO;INFRAESTRUCTURA PARA CONECTIVIDAD DE REDES; INFRAESTRUCTURA DE SERVICIOS SOBRE SERVIDORES DE DATOS Y APLICACIONES; SEGURIDAD; RECUPERACION DE DESASTRES; ADMINISTRACION DE SISTEMAS; DISEÑO, IMPLEMENTACIÓN Y SERVICIOS DE SOPORTE DE NIVEL DE ENTRADA, AVANZADO Y DE MISIÓN CRÍTICA; SERVICIOS DE OUTSOURCING Y CONSULTORÍA	MICROSOFT, SYMANTEC, VMWARE, INTEL, HP, EPSON, APC, TRIPPLITE, CDP, FORZA, D-LINK, INTEL, JUNIPER NETWORKS, LG, SAMSUNG, KINGSTON, SEAGATE, WESTERN DIGITAL, TOSHIBA, GENIUS, BENQ, CREATIVE, CANON, TARGUS, IMATION,	

4.2.4 Presentación de evaluaciones técnicas y económicas

Este tipo de evaluaciones son cruciales para tomar la decisión de la implementación de un sistema, estas deben de evaluarse en forma independiente. Se debe de tomar el tiempo que se considere prudente para la evaluación de este punto, ya que de acá puede desprenderse gran parte de los resultados que se obtendrán al analizar los objetivos que cada proyecto hubiese proyectado a un inicio.

El formato definido para una evaluación económica es el siguiente:

Figura 26. Formato de evaluación económica

[Nombre del proyecto] Fecha de Presentación: [fecha]						
	Opción # 1: [Proveedor 1]			Opción #2: [Proveedor 2]		
Descripción	Cantidad	Costo Unitario	Costo Total	Cantidad	Costo Unitario	Costo Total
Gran total						

	Detalle Financiero:
1.-	Presupuesto:
2.-	

	Justificación:
1.-	
2.-	

	Notas [Proveedor #1]
1.-	
2.-	

	Notas [Proveedor 2]
1.-	
2.-	

El formato definido para una evaluación técnica es el siguiente:

Figura 27. Formato de evaluación técnica

Evaluación Técnica de Ofertas							
[Nombre del Proyecto]							
Elementos a Evaluar	Descripción por Producto		Punteo Asigando	[Proveedor 1]		[Proveedor 2]	
	[Proveedor 1]	[Proveedor 2]I					
Estructura							
				0	0	0	0
				0	0	0	0
				0	0	0	0
				0	0	0	0
Servicios							
				0	0	0	0
				0	0	0	0
				0	0	0	0
				0	0	0	0
Funciones							
				0	0	0	0
				0	0	0	0
				0	0	0	0
				0	0	0	0
Generales del Fabricante							
				0	0	0	0
				0	0	0	0
				0	0	0	0
				0	0	0	0
Generales del Proveedor							
				0	0	0	0
				0	0	0	0
				0	0	0	0
				0	0	0	0
Punteo Total					**0**		**0**

4.2.5 Generación de planificación

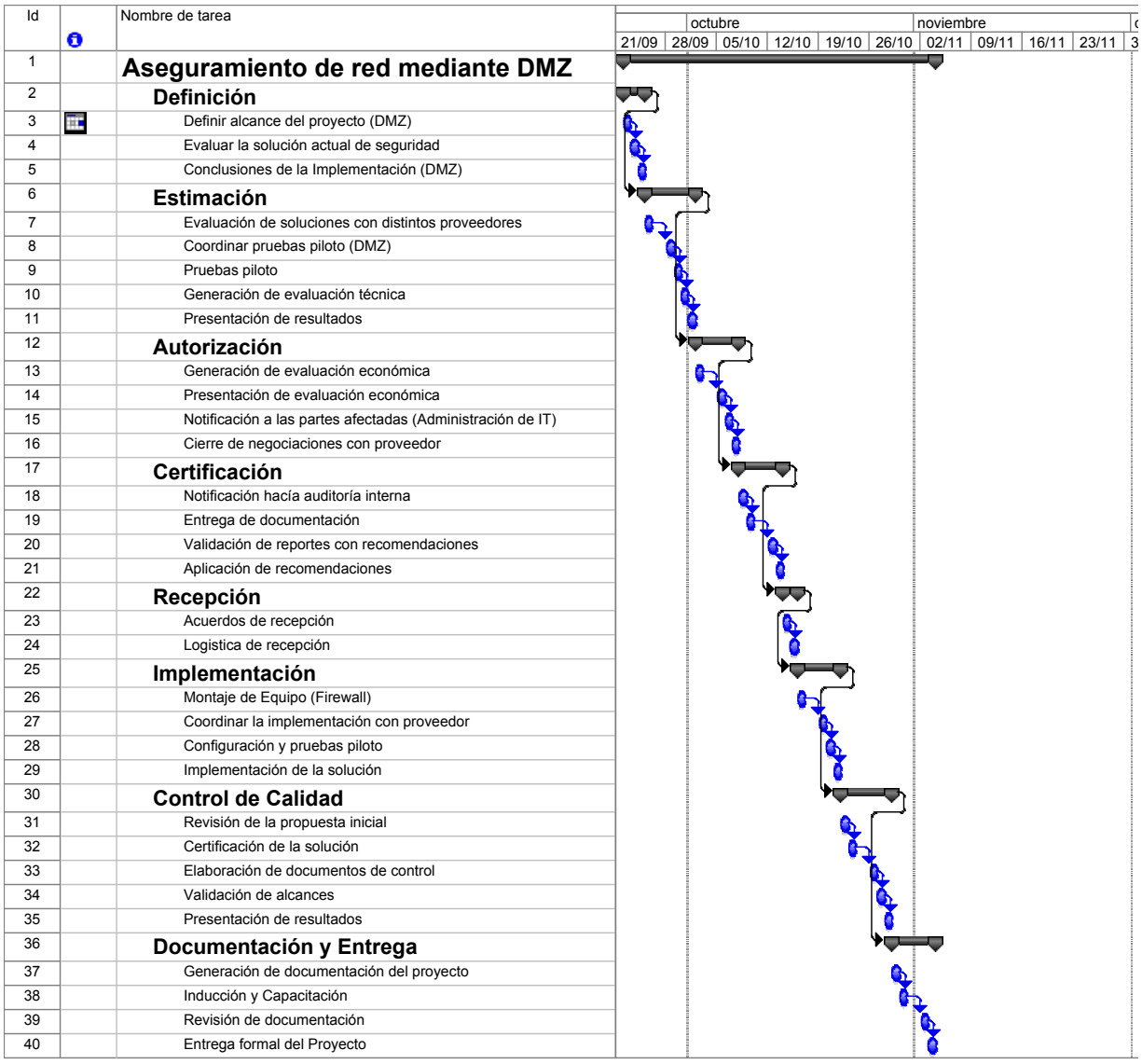
La planificación es la parte más importante dentro de la implementación de un proyecto, esta debe de estar definida con tiempos prudentes para la finalización de cada una de las actividades que el proyecto necesite. Para la generación se deben de tomar en cuenta un listado de actividades que se deben de incorporar. Las actividades son las siguientes:

- Definición de alcance y objetivo
- Estimación de recursos y actividades
- Autorización de infraestructura
- Certificación de auditoría
- Confirmación y recepción de recursos (Actividad paralela a la anterior)
- Implementación
- Control de Calidad
- Documentación final y entrega a áreas responsables (Actividad paralela a la anterior)

Figura 28. Planificación por fechas para proyecto de DMZ´s

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Aseguramiento de red mediante DMZ**	**31 días?**	**mar 22/09/09**	**mar 03/11/09**
2	**Definición**	**3 días?**	**mar 22/09/09**	**jue 24/09/09**
3	Definir alcance del proyecto (DMZ)	1 día?	mar 22/09/09	mar 22/09/09
4	Evaluar la solución actual de seguridad	1 día?	mié 23/09/09	mié 23/09/09
5	Conclusiones de la Implementación (DMZ)	1 día?	jue 24/09/09	jue 24/09/09
6	**Estimación**	**5 días?**	**vie 25/09/09**	**jue 01/10/09**
7	Evaluación de soluciones con distintos proveedores	1 día?	vie 25/09/09	vie 25/09/09
8	Coordinar pruebas piloto (DMZ)	1 día?	lun 28/09/09	lun 28/09/09
9	Pruebas piloto	1 día?	mar 29/09/09	mar 29/09/09
10	Generación de evaluación técnica	1 día?	mié 30/09/09	mié 30/09/09
11	Presentación de resultados	1 día?	jue 01/10/09	jue 01/10/09
12	**Autorización**	**4 días?**	**vie 02/10/09**	**mié 07/10/09**
13	Generación de evaluación económica	1 día?	vie 02/10/09	vie 02/10/09
14	Presentación de evaluación económica	1 día?	lun 05/10/09	lun 05/10/09
15	Notificación a las partes afectadas (Administración de IT)	1 día?	mar 06/10/09	mar 06/10/09
16	Cierre de negociaciones con proveedor	1 día?	mié 07/10/09	mié 07/10/09
17	**Certificación**	**4 días?**	**jue 08/10/09**	**mar 13/10/09**
18	Notificación hacía auditoría interna	1 día?	jue 08/10/09	jue 08/10/09
19	Entrega de documentación	1 día?	vie 09/10/09	vie 09/10/09
20	Validación de reportes con recomendaciones	1 día?	lun 12/10/09	lun 12/10/09
21	Aplicación de recomendaciones	1 día?	mar 13/10/09	mar 13/10/09
22	**Recepción**	**2 días?**	**mié 14/10/09**	**jue 15/10/09**
23	Acuerdos de recepción	1 día?	mié 14/10/09	mié 14/10/09
24	Logistica de recepción	1 día?	jue 15/10/09	jue 15/10/09
25	**Implementación**	**4 días?**	**vie 16/10/09**	**mié 21/10/09**
26	Montaje de Equipo (Firewall)	1 día?	vie 16/10/09	vie 16/10/09
27	Coordinar la implementación con proveedor	1 día?	lun 19/10/09	lun 19/10/09
28	Configuración y pruebas piloto	1 día?	mar 20/10/09	mar 20/10/09
29	Implementación de la solución	1 día?	mié 21/10/09	mié 21/10/09
30	**Control de Calidad**	**5 días?**	**jue 22/10/09**	**mié 28/10/09**
31	Revisión de la propuesta inicial	1 día?	jue 22/10/09	jue 22/10/09
32	Certificación de la solución	1 día?	vie 23/10/09	vie 23/10/09
33	Elaboración de documentos de control	1 día?	lun 26/10/09	lun 26/10/09
34	Validación de alcances	1 día?	mar 27/10/09	mar 27/10/09
35	Presentación de resultados	1 día?	mié 28/10/09	mié 28/10/09
36	**Documentación y Entrega**	**4 días?**	**jue 29/10/09**	**mar 03/11/09**
37	Generación de documentación del proyecto	1 día?	jue 29/10/09	jue 29/10/09
38	Inducción y Capacitación	1 día?	vie 30/10/09	vie 30/10/09
39	Revisión de documentación	1 día?	lun 02/11/09	lun 02/11/09
40	Entrega formal del Proyecto	1 día?	mar 03/11/09	mar 03/11/09

Figura 29. Planificación por diagrama de Gantt para proyecto de DMZ´s



Id	Nombre de tarea
1	**Aseguramiento de red mediante DMZ**
2	**Definición**
3	Definir alcance del proyecto (DMZ)
4	Evaluar la solución actual de seguridad
5	Conclusiones de la Implementación (DMZ)
6	**Estimación**
7	Evaluación de soluciones con distintos proveedores
8	Coordinar pruebas piloto (DMZ)
9	Pruebas piloto
10	Generación de evaluación técnica
11	Presentación de resultados
12	**Autorización**
13	Generación de evaluación económica
14	Presentación de evaluación económica
15	Notificación a las partes afectadas (Administración de IT)
16	Cierre de negociaciones con proveedor
17	**Certificación**
18	Notificación hacía auditoría interna
19	Entrega de documentación
20	Validación de reportes con recomendaciones
21	Aplicación de recomendaciones
22	**Recepción**
23	Acuerdos de recepción
24	Logistica de recepción
25	**Implementación**
26	Montaje de Equipo (Firewall)
27	Coordinar la implementación con proveedor
28	Configuración y pruebas piloto
29	Implementación de la solución
30	**Control de Calidad**
31	Revisión de la propuesta inicial
32	Certificación de la solución
33	Elaboración de documentos de control
34	Validación de alcances
35	Presentación de resultados
36	**Documentación y Entrega**
37	Generación de documentación del proyecto
38	Inducción y Capacitación
39	Revisión de documentación
40	Entrega formal del Proyecto

CONCLUSIONES

1. Un alto porcentaje de la información sensible de una empresa se encuentra viajando diariamente sobre su red informática, es por ello que asegurar dichas redes es un tema crítico para el óptimo funcionamiento de una corporación.

2. Cada uno de los equipos de telecomunicaciones mencionados en este trabajo tiene una función específica al conformar una red empresarial, para poder hacer una elección correcta en la adquisición, primero es saber cuáles son las necesidades que tiene cada empresa, para manipular dicha información.

3. Es necesario poder garantizar que los recursos informáticos de una empresa, estén disponibles para poder cumplir sus propósitos; esto se logra mediante procedimientos de seguridad que se deben de implementar internamente en cada empresa.

4. Existen gran cantidad de métodos para asegurar una red informática dentro de una empresa. Uno de los que se usa con más frecuencia, por su alto desempeño y por su factibilidad de acoplarse con la mayoría de las redes, es el aseguramiento mediante redes desmilitarizadas (DMZ).

5. la información es el elemento principal a proteger, resguardar y recuperar dentro de una red empresarial; esto ya que la información es crítica, valiosa y sensible.

RECOMENDACIÓN

1. Dentro de cada empresa, no importando el tamaño, ni el volumen de información sensible que maneje; es recomendable hacer un análisis de factibilidad para colocar una red desmilitarizada que pueda proteger la información que se maneja dentro de cada empresa. Si este análisis fuese favorable, se recomienda colocar una configuración de *firewall* de Subred Monitoreada, para prevenir así configuraciones erróneas que permitan el acceso desde una red externa hacia la red interna. Estas recomendaciones se dan para poder garantizar el uso adecuado de la información interna de cada empresa.

BIBLIOGRAFÍA

1. Robert J. Shimoski. ***Building DMZs for Enterprise Networks*.** Estados Unidos: Syngress, 2003.

2. Cherie Amon. ***The Best Damn Firewall Book Period***. Estados Unidos: O´Reilly Media, 2004.

3. Syngress. ***Building DMZs*.** Inglaterra: Syngless, 2003.

4. Gary A. Donahue. ***Network Warrior*.** Estados Unidos: O´Reilly Media, 2007.

5. Hal Flynn. ***Designing and Building Enterprices DMZs*.** Estados Unidos: Syngress, 2006.