UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

“FUNDAMENTOS DE INTRANET Y SU UTILIDAD EN EL MANEJO DE INFORMACIÒN PRIVILEGIADA”

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACIÒN
PRESENTA:

JESUS GERARDO OBLE OLIVARES

ASESOR: Ing. Norma Raquel Soto Arredondo

MEXICO , 2009

Agradecimientos

. A Dios por dejarme vivir

. A

Paula Socorro

Modesta

Dolores

gracias por existir.

INDICE DE TEMAS

	Contenido	Página
	Introducción	1
	Capítulo I: Generalidades	
1.1	Definición de red	3
1.2	Clasificaciones de redes	3
1.2.1	Red de área local	4
1.2.2	Red de área metropolitana	5
1.2.3	Red de área extensa	5
1.2.4	Red Intranet	6
1.2.5	Red Extranet	7
1.2.6	Red internet	8
1.3	Redes de equipos	9
1.3.1	Razones para usar una red de equipos	9
1.3.2	Compartir información	11
1.3.2.1	Utilidad para compartir información	11
1.3.2.2	Compartir hardware y software	11
1.3.3	Centralización de la administración y el soporte	12
1.3.4	Redes LAN y WAN	12
1.3.5	Configuración de redes	13
1.4	Redes para trabajo en grupo vs redes basadas en servidor	13
1.4.1	Redes para trabajo en grupo	14

1.4.1.1	Tamaño	14
1.4.1.2	Costes	14
1.4.1.3	Sistemas operativos en redes	14
1.4.1.4	Implementación	15
1.4.1.5	Recomendaciones de uso	15
1.4.1.6	Consideraciones	15
1.4.1.7	Administración	16
1.4.1.8	Compartición de recursos	16
1.4.1.9	Requerimientos del servidor	16
1.4.1.10	Seguridad	16
1.4.1.11	Formación	17
1.4.2	Redes basadas en servidor	17
1.4.3	Topologías de redes	18
1.4.3.1	Jerárquica	19
1.4.3.2	Bus	20
1.4.3.3	Estrella	20
1.4.3.4	Anillo	21
1.4.3.5	Malla	22
1.4.3.6	Topologías híbridas	22
1.5	Razones para utilizar Intranet	23
1.5.1	Herramientas de Intranet	23
1.5.2	Funcionamiento financiero en Intranet	24
	Capítulo II: Estructuras y necesidades empresariales	
2.1	Empresa y organización	25
2.1.1	Empresas	25

2.1.1.1	Definiciones	25
2.1.1.2	Clasificación de las empresas	26
2.1.1.2.1	Según su actividad o giro	27
2.1.1.2.2	Según la forma jurídica	27
2.1.1.2.3	Según su tamaño	28
2.1.1.2.4	Según su ámbito de actuación	28
2.1.1.2.5	Según la titularidad del capital	29
2.1.1.2.6	Según la cuota de mercado que posean	29
2.1.1.2.7	Según el destino de los beneficios	30
2.1.1.3	Características de las empresas	30
2.1.1.4	Gobierno empresarial	31
2.1.1.5	Objetivos empresariales	31
2.1.2	Organizaciones	31
2.1.2.1	Definiciones	31
2.1.2.2	Clasificación de organizaciones	33
2.1.2.3	Observaciones importantes	33
2.2	Organigramas	33
2.2.1	Definiciones	33
2.2.2	Tipos de organigramas	33
2.2.2.1	Por su naturaleza	34
2.2.2.2	Por su ámbito	34
2.2.2.3	Por su contenido	35
2.2.2.4	Por su representación	37
2.3	Medios de comunicación	40
2.4	Oficinas virtuales	41

2.5	El cambio en los negocios	42
2.5.1	La tecnología informática Tradicional Entregada	42
2.5.2	Reingeniería de los procesos en los negocios	43
2.5.3	Fusión de equipos de trabajo	43
2.5.4	Expectativas de los usuarios	44
2.5.5	Aplicaciones multimedia	44
2.5.6	Aprendizaje a distancia	44
2.5.7	Voz y Vídeo en la red	44
	Capítulo III: Manejo de información en Intranet	
3.1	Definición	46
3.2	Visión general de Intranet	48
3.3	Protocolos de Intranet	50
3.3.1	Funcionamiento de TCP/IP e IPX en Intranet	52
3.3.2	Procesamiento de paquetes TCP/IP	54
3.4	Intranet a través del tiempo	54
3.5	Características de Intranet	55
3.6	Ventajas de Intranet	55
3.7	Desventajas de Intranet	56
3.8	Modelo OSI para Intranet	56
3.9	Funcionamiento de puentes o bridges	58
3.10	Funcionamiento de los enrutadores	59
3.10.1	Tablas de encaminamiento	60
3.10.2	Protocolos de encaminamiento	60
3.11	Correo electrónico en redes Intranet	61
3.11.1	Correo electrónico interno de Intranet	61

3.11.2	Correo electrónico entre redes Intranet´s	62
3.12	Funcionamiento de Intranet	63
3.12.1	Servidores de dominio (URL)	63
3.12.2	Java	65
3.12.3	Conversiones IPX en Intranet	66
3.13	Subdivisión de redes Intranet	67
	Capítulo IV: Seguridad en comunicación privada	
4.1	Conceptos importantes	68
4.2	Seguridad en las redes intranet´s	69
4.2.1	Enrutadores para filtrar	71
4.2.2	Firewall´s	73
4.2.3	Servidores sustitutos	75
4.2.4	Anfitriones Bastión	76
4.2.5	Encriptación	77
4.2.6	Contraseñas y sistemas de autenticación	78
4.2.7	Software para examinar virus	79
4.2.8	Bloqueo de sitios indeseables	80
4.3	Software de supervisión de intranets	81
4.4	Redes virtuales seguras	82
	Conclusiones	83
	Glosario	85
	Bibliografía	87

INTRODUCCIÓN

El mundo empresarial es muy complejo; las empresas manejan gran cantidad de información y de datos. Por ello, necesitan de mecanismos que les permitan su manejo y manipulación sin riesgos; es decir, que requieren no solamente de facilidad de manejo, sino de herramientas que les provean de seguridad en diferentes sentidos.

Es necesario hacer notar que, en materia de negocios, la pérdida de información puede resultar muy costosa.

Una herramienta muy útil para apoyar a los empresarios, es el uso de redes informáticas y software de seguridad, así como de manejo y gestión de información.

En su forma más simple, una red se define como un sistema en donde los elementos que lo componen son autónomos y están conectados entre sí por medios físicos y/o lógicos; y que pueden comunicarse para compartir recursos.

Las redes manejan información. Se entiende por información al conjunto de hechos (medibles o no) de los que se puede tener conocimiento.

Entonces, una red informática es un conjunto de ordenadores conectados entre sí a través de un servidor; cada elemento de la red es un terminal autónomo e independiente; es decir, tiene propias funciones y características.

Existen diferentes tipos de redes, tales como: Intranet, Extranet, Internet, etcétera. En el presente trabajo nos apegaremos únicamente a lo que es Intranet.

Se define por Intranet, una red privada de ordenadores basada en los estándares de Internet. Es decir, este tipo de redes utilizan tecnologías de Internet para enlazar los recursos informativos de una organización, que van desde documentos de texto hasta documentos multimedia; desde bases de datos legales hasta sistemas de gestión de documentos.

Cabe mencionar que las Intranet`s pueden incluir:

- Sistemas de seguridad para la red
- Tablones de anuncios
- Motores de búsqueda

Asimismo, una intranet puede extenderse a través de Internet; esto se hace utilizando una red privada virtual (VPN, por sus siglas en inglés)

GENERALIDADES

1.1 Definición de red

Una red se define como la unión de dos o más computadoras que comparten recursos y que son capaces de realizar comunicaciones electrónicas. Las redes se encuentran unidas a través de lo que se denomina medios, que es un enlace no siempre tangible.

Los recursos que se comparten en una red son, entre otros, los siguientes:

- Archivos
- Impresoras
- CD-ROM´s
- Bases de datos

Los medios por los cuales pueden unirse las redes son, entre otros, los siguientes:

- Cable
- Línea telefónica
- Ondas de radio
- Satélites

1.2 Clasificaciones de redes

Las redes pueden dividirse de acuerdo a sus características, funciones, versatilidad, aplicaciones, etcétera.

Una clasificación muy general se resumiría en la que sigue:

- Red de área local
- Red de área metropolitana
- Red de área extensa

La red de área local se divide, a su vez en:

- Intranet
- Extranet

La red de área extensa es representada por la red más grande del mundo: la Internet.

Por supuesto, una Intranet se puede ampliar a grandes extensiones, convirtiéndose en una red de área metropolitana o extensa. Lo anterior lo logra utilizando el Internet.

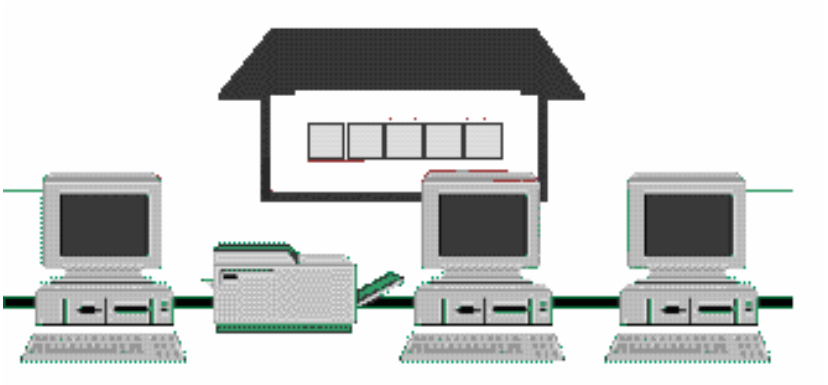
1.2.1 Red de área local

Una red de área local (LAN, por sus siglas en inglés) es una red que cubre una extensión reducida, como es el caso de una empresa, una universidad, un colegio, etcétera.

Dentro de las redes de área local, no existe, por lo general, dos ordenadores con una distancia de más de un kilómetro uno del otro.

Por lo general, las redes de área local son muy utilizadas en los centros de cómputo, en donde las computadoras se encuentran muy juntas entre sí.

Se puede decir que una configuración típica en una red de este tipo, es tener una computadora a manera de servidor, en donde se almacena todo el software correspondiente al control de la red, así como aquel que se comparte con los demás ordenadores de la misma, como lo muestra la siguiente figura:



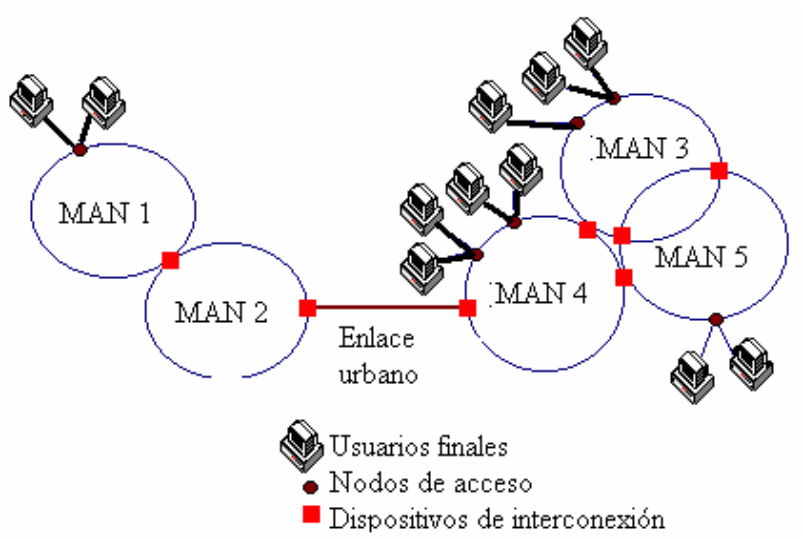
En este caso, las computadoras que no son servidores, reciben el nombre de estaciones de trabajo o terminales. Este tipo de ordenadores suelen ser menos potentes y suelen tener software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red; una en cada equipo

1.2.2 Red de área metropolitana

Las redes de área metropolitana (MAN por sus siglas en inglés), cubren extensiones mayores; como puede ser una ciudad o un distrito.

Si bien una red MAN es más amplia que una red LAN, se vale de ella para distribuir la información a los diferentes puntos del distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

Una forma de representar una red de área metropolitana se muestra en la figura siguiente:

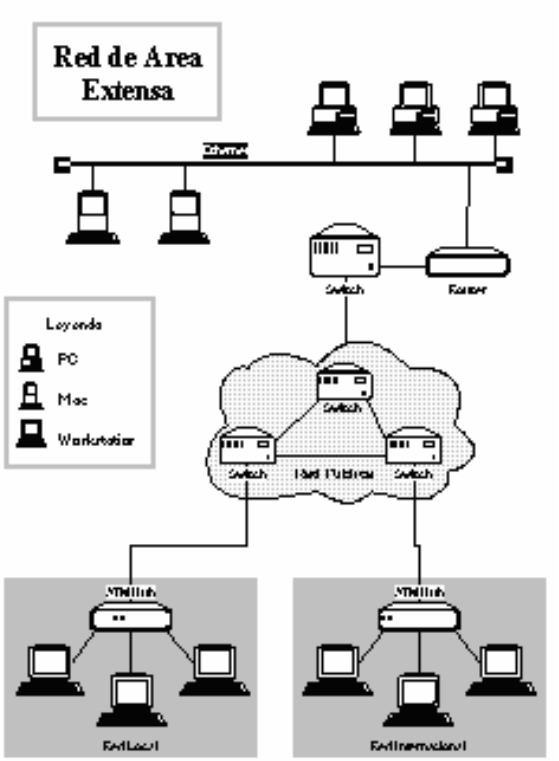


1.2.3 Red de área extensa

Las redes de área extensa (WAN por sus siglas en inglés) cubren grandes regiones geográficas, tales como pueden ser: un país, un continente, el mundo.

Para que este tipo de red tenga una comunicación entre sus terminales, hacen uso de medios más sofisticados, tales como: cables transoceánicos o satélites.

Las formas clásicas para representar a una red WAN son las siguientes:



Como un dato específico, se puede decir que, con el uso de una WAN se puede contactar desde España con Japón sin tener que pagar enormes cantidades de teléfono.

Sin embargo, la implementación de una red de área extensa es muy complicada. Se utilizan multiplexadores para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características puedan comunicarse sin problemas. El mejor ejemplo de una red de área extensa es Internet.

1.2.4 Red Intranet

Una Intranet es una red de ordenadores basada en los estándares de Internet. Esta red es de carácter privado; es decir, es de uso exclusivo de una organización en particular.

Las redes intranet utilizan tecnologías de Internet para enlazar los recursos informativos de una organización que pueden ser:

- Desde documentos de texto hasta documentos multimedia
- Desde bases de datos legales hasta sistemas de gestión de documentos.

Las redes Intranet pueden incluir:

- Sistemas de seguridad para la red
- Tablones de anuncios
- Motores de búsqueda

También, una red intranet puede extenderse a través de Internet utilizando una red privada virtual (VPN).

Una intranet es, entonces, una red de ordenadores de una red de área local (LAN) privada empresarial o educativa que proporciona herramientas de Internet, la cual tiene como función principal proveer lógica de negocios para aplicaciones de:

- Captura
- Reportes
- Consultas
- Etcétera

Ello, con el fin de auxiliar la producción de dichos grupos de trabajo; es también un importante medio de difusión de información interna a nivel de grupo de trabajo. No necesariamente proporciona Internet a la organización; normalmente, tiene como base el protocolo TCP/IP de Internet y, por ser privada, puede emplear mecanismos de restricción de acceso a nivel de programación como lo son usuarios y contraseñas de acceso o incluso a nivel de hardware como un sistema firewall (cortafuegos) que pueda restringir el acceso a la red organizacional.

La Intranet fue creada para mayor seguridad para poder compartir archivos, carpetas y recursos. Es una excelente opción de bajo costo para las empresas.

Las redes internas corporativas son unas potentes herramientas que permiten divulgar información de la compañía a los empleados con efectividad, consiguiendo que estos estén permanentemente informados con las últimas novedades y datos de la organización.

Tienen gran valor como repositorio documental, convirtiéndose en un factor determinante para conseguir el objetivo de oficina sin papeles. Añadiéndoles funcionalidades como un buen buscador, una taxonomía adecuada o un sistema de metatags trabajado se puede conseguir una consulta rápida y eficaz por parte de los empleados de un volumen importante de documentación

1.2.5 Red Extranet

Una extranet (intranet extendida) es una red privada virtual, resultante de la interconexión de dos o más redes Intranet que utilizan Internet como medio de transporte de la información entre sus nodos.

Durante los años 1999 al 2001, hubo una creciente demanda por el desarrollo de Extranet`s, sin contar con los requerimientos necesarios para este fin.

La Extranet permite intercambiar ficheros y acceder a Internet. Un claro ejemplo de una Extranet podría referirse a un banco y sus sucursales.

Un uso muy frecuente de Extranet se da en las oficinas virtuales, que es un concepto que puede tomarse como sinónimo de Extranet.

1.2.6 Red Internet

Internet es un método de interconexión de redes de computadoras implementado en un conjunto de protocolos denominado TCP/IP y garantiza que redes físicas heterogéneas funcionen como una red (lógica) única. De ahí que Internet se conozca comúnmente con el nombre de "red de redes", pero es importante destacar que Internet no es un nuevo tipo de red física, sino un método de interconexión.

Internet aparece por primera vez en 1969, cuando ARPAnet establece su primera conexión entre tres universidades en California y una en Utah. También se usa el término Internet como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.

Cuando se dice red de redes, se hace referencia a que es una red formada por la interconexión de otras redes menores.

Al contrario de lo que se piensa comúnmente, Internet no es sinónimo de World Wide Web (www). Ésta es parte de Internet, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet.

La Web es un sistema de información mucho más reciente, desarrollado inicialmente por Tim Berners Lee en 1989. El www utiliza Internet como medio de transmisión.

Algunos de los servicios disponibles en Internet aparte de la Web son:

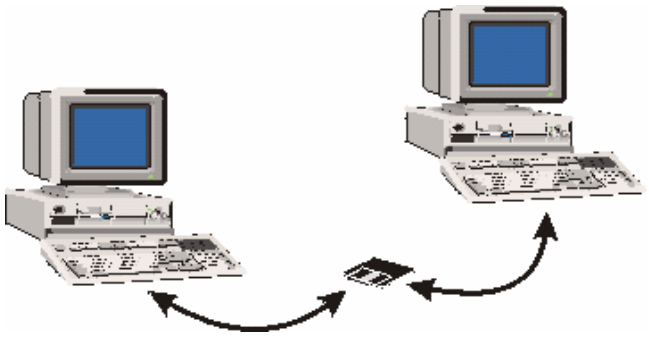
- El acceso remoto a otras máquinas (SSH y telnet)
- Transferencia de archivos (FTP)
- Correo electrónico (SMTP)
- Boletines electrónicos (news o grupos de noticias)
- Conversaciones en línea (IRC y chats)
- Mensajería instantánea
- Transmisión de archivos (P2P, P2M, Descarga Directa)
- Etcétera

El género de la palabra Internet es ambiguo según el diccionario de la Real academia española. Sin embargo, al ser "Internet" un nombre propio, la Real Academia Española recomienda no usar artículo alguno. En caso de usar artículo, se prefieren las formas femeninas, pues Internet es una red y el género de la palabra es femenino. A pesar de esto, es común escuchar hablar de "el Internet" o "la Internet", utilizando el artículo por calco del inglés the Internet.

1.3 Redes de equipos

En su nivel más elemental, una red de equipos consiste en dos equipos conectados entre sí con un cable que les permite compartir datos. Todas las redes de equipos, independientemente de su nivel de sofisticación, surgen de este sistema simple. Aunque puede que la idea de conectar dos equipos con un cable no parezca extraordinaria, al mirar hacia atrás se comprueba que ha sido un gran logro a nivel de comunicaciones.

Esta forma tan "rudimentaria" de conectar redes de computadoras, se muestra en la figura siguiente:



Las redes de equipos surgen como respuesta a la necesidad de compartir datos de forma rápida. Los equipos personales son herramientas potentes que pueden procesar y manipular rápidamente grandes cantidades de datos, pero no permiten que los usuarios compartan los datos de forma eficiente.

Antes de la aparición de las redes, los usuarios necesitaban imprimir sus documentos o copiar los archivos de documentos en un disco para que otras personas pudieran editarlos o utilizarlos. Si otras personas realizaban modificaciones en el documento, no existía un método fácil para combinar los cambios. A este sistema se le denominó "trabajo en un entorno independiente.

En ocasiones, al proceso de copiar archivos en disquetes y dárselos a otras personas para copiarlos en sus equipos se le denomina "red de alpargata" (sneakernet). Esta antigua versión de trabajo en red ha sido muy utilizada por diversas personas; aún mucha gente lo usa.

Este sistema funciona bien en ciertas situaciones, y presenta sus ventajas (nos permite tomar un café o hablar con un amigo mientras intercambiamos y combinamos datos), pero resulta demasiado lento e ineficiente para cubrir las necesidades y expectativas de los usuarios informáticos de hoy en día. La cantidad de datos que se necesitan compartir y las distancias que deben cubrir los datos superan con creces las posibilidades del intercambio de disquetes.

Sin embargo, si un equipo estuviera conectado a otros, podría compartir datos con otros equipos y enviar documentos a otras impresoras; acción que se observa en la figura siguiente:

Esta interconexión de equipos y otros dispositivos se llama una red, y el concepto de conectar equipos que comparten recursos es un sistema en red.

1.3.1 Razones para usar una red de equipos

Quizá sea un poco complicado el tratar de explicarles a todas las personas la utilidad que tiene el trabajo en red. La razón principal de esto es que las redes de computadoras no son aplicables a todas las personas ni a todas las empresas.

Las redes de computadoras no son aplicables en los casos en que no se tienen sucursales en un negocio y/o el manejo lo realiza siempre una sola persona. En este caso en particular, la creación de una red implicaría más costo que los beneficios que se supone ofrece.

No obstante, y de forma general, se puede decir que el uso de las redes aumenta la eficiencia y reducen los costos; esto resulta muy sencillo de decir, pero las redes de equipos alcanzan estos objetivos de las siguientes formas:

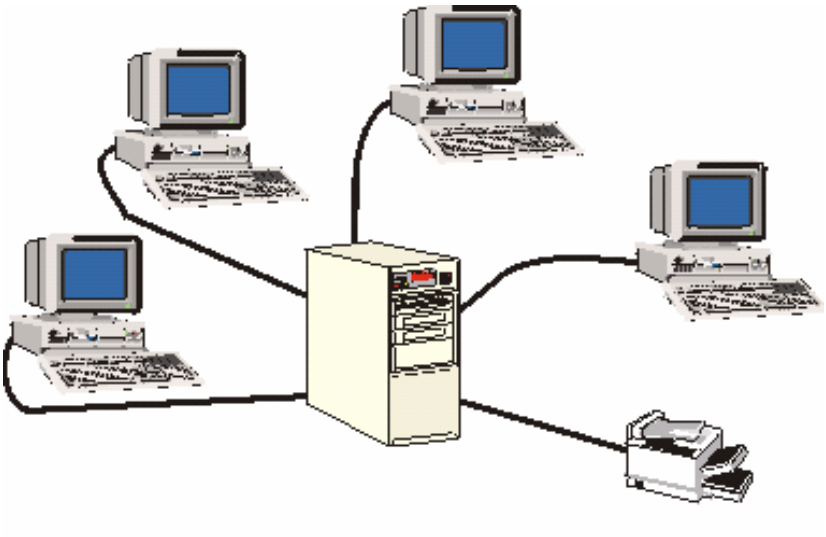
- Compartiendo información o datos.
- Compartiendo hardware y software
- Centralizando la administración y el soporte.

De forma más específica, los equipos que forman parte de una red pueden compartir:

- Documentos (informes, hojas de cálculo, facturas, etcétera)
- Mensajes de correo electrónico
- Software de tratamiento de textos
- Software de seguimiento de proyectos
- Ilustraciones, fotografías, vídeos y archivos de audio
- Transmisiones de audio y vídeo en directo
- Impresoras
- Faxes
- Módems
- Unidades de CD-ROM y otras unidades removibles, como unidades Zip y Jaz.
- Discos duros.

Y existen más posibilidades para compartir. Las prestaciones de las redes crecen constantemente, a medida que se encuentran nuevos métodos para compartir y comunicarse mediante los equipos.

El entorno de una red de equipos se muestra en la siguiente figura:



1.3.2 Compartir información

La capacidad de compartir información de forma rápida y económica ha demostrado ser uno de los usos más populares de la tecnología de las redes. Hay informes que afirman que el correo electrónico es, con diferencia, la principal actividad de las personas que usan Internet. Muchas empresas han invertido en redes específicamente para aprovechar los programas de correo electrónico y planificación basados en red.

1.3.2.1 Utilidad de compartir información

Al hacer que la información esté disponible para compartir, las redes pueden reducir la necesidad de comunicación por escrito, incrementar la eficiencia y hacer que prácticamente cualquier tipo de dato esté disponible simultáneamente para cualquier usuario que lo necesite.

Los directivos pueden usar estas utilidades para comunicarse rápidamente de forma eficaz con grandes grupos de personas, y para organizar y planificar reuniones con personas de toda una empresa u organización de un modo mucho más fácil de lo que era posible anteriormente.

1.3.2.2 Compartir hardware y software

Antes de la aparición de las redes, los usuarios informáticos necesitaban sus propias impresoras, trazadores y otros periféricos; el único modo en que los usuarios podían compartir una impresora era hacer turnos para sentarse en el equipo conectado a la impresora.

Las redes hacen posible que varias personas compartan simultáneamente datos y periféricos. Si muchas personas necesitan usar una impresora, todos pueden usar la impresora disponible en la red.

Las redes pueden usarse para compartir y estandarizar aplicaciones, como:

- Tratamientos de texto
- Hojas de cálculo
- Bases de datos de existencias
- Etcétera

Esto, para asegurarse de que todas las personas de la red utilizan las mismas aplicaciones y las mismas versiones de estas aplicaciones.

Esto permite compartir fácilmente los documentos, y hace que la formación sea más eficiente, bajo la premisa de que es más fácil que los usuarios aprendan a usar bien una aplicación de tratamiento de textos que intentar aprender cuatro o cinco aplicaciones distintas de tratamiento de textos.

1.3.3 Centralización de la administración y el soporte

La conexión en red de los equipos también puede facilitar las tareas de soporte.

Para el personal técnico, es mucho más eficiente dar soporte a una versión de un sistema operativo o aplicación y configurar todos los equipos del mismo modo que dar soporte a muchos sistemas y configuraciones individuales y diferentes.

1.3.4 Redes LAN y WAN

Como se ha mencionado anteriormente, Las redes de equipos se clasifican en dos grupos, dependiendo de su tamaño y función.

Una red de área local (LAN, Local Area Network) es el bloque básico de cualquier red de equipos. Una LAN puede ser muy simple (dos equipos conectados con un cable) o compleja (cientos de equipos y periféricos conectados dentro de una gran empresa). La característica que distingue a una LAN es que está confinada a un área geográfica limitada.

Por otra parte, una red de área extensa (WAN, Wide Area Network), no tiene limitaciones geográficas. Puede conectar equipos y otros dispositivos situados en extremos opuestos del planeta. Una WAN consta de varias LAN interconectadas. Podemos ver Internet como la WAN suprema.

1.3.5 Configuración de redes

En general, todas las redes tienen ciertos componentes, funciones y características en común; entre ellos, podemos mencionar los siguientes:

- Servidores
- Clientes
- Medio
- Datos compartidos
- Impresoras y otros periféricos compartidos
- Recursos

Los servidores son equipos que ofrecen recursos compartidos a los usuarios de la red.

Los clientes son los equipos que acceden a los recursos compartidos de la red, los cuales son ofrecidos por los servidores.

Como medio, se determina a los cables que mantienen las conexiones físicas.

Los datos compartidos son los archivos suministrados a los clientes, por parte de los servidores, a través de la red.

Las impresoras y demás periféricos, son recursos compartidos adicionales ofrecidos por los servidores.

Hablando de recursos, se refiere a cualquier servicio o dispositivo disponible para su uso por los miembros de la red. Estos recursos pueden ser internos o externos al servidor. Dentro del primer grupo encontramos información; dentro del segundo se encuentran los periféricos y dispositivos interconectados en la red.

1.4 Redes para trabajo en grupo vs Redes basadas en Servidor

La diferencia entre las redes para trabajo en grupo y las redes basadas en servidor es muy notoria; puesto que cada una de ellas presenta distintas características.

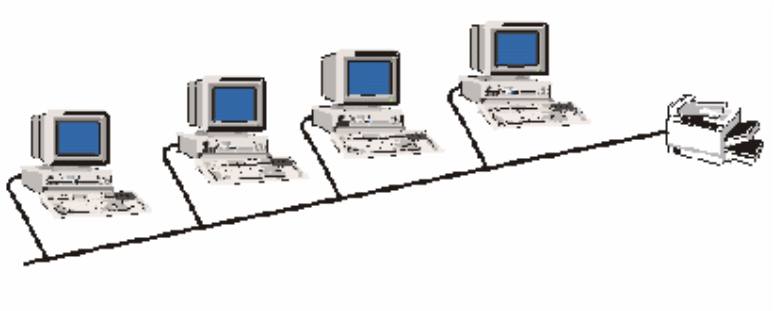
El tipo de red seleccionado para su instalación dependerá de factores tales como:

- El tamaño de la organización
- El nivel de seguridad requerido
- El tipo de negocio
- El nivel de soporte administrativo disponible
- La cantidad de tráfico de la red
- Las necesidades de los usuarios de la red
- El presupuesto de la red

1.4.1 Redes para trabajo en grupo

En una red para trabajo en grupo, no existen servidores dedicados, y no existe una jerarquía entre los equipos. Esto es, todos los equipos son iguales y, por lo tanto, cada equipo actúa como cliente y servidor y no hay un administrador responsable de la red completa.

El usuario de cada equipo determina los datos de dicho equipo que van a ser compartidos en la red. La representación de una red sencilla es la siguiente:



1.4.1.1 Tamaño

Las redes para trabajo en grupo (peer-to-peer) se llaman también grupos de trabajo (workgroups).

El término "grupo de trabajo" implica un pequeño grupo de personas. Generalmente, una red Trabajo en Grupo abarca un máximo de diez equipos.

1.4.1.2 Costes

Las redes Trabajo en Grupo son relativamente simples. Como cada equipo funciona como cliente y servidor, no hay necesidad de un potente servidor central o de los restantes componentes de una red de alta capacidad.

Como una nota aclaratoria, se puede decir que las redes para Trabajo en Grupo pueden ser más económicas que las redes basadas en servidor.

1.4.1.3 Sistemas operativos en redes

En una red punto a punto, el software de red no requiere el mismo tipo de rendimiento y nivel de seguridad que el software de red diseñado para servidores dedicados.

Los servidores dedicados sólo funcionan como servidores, y no como clientes o estaciones.

Las redes para trabajo en grupo están incorporadas en muchos sistemas operativos. En estos casos, no es necesario software adicional para configurar una red para Trabajo en Grupo.

1.4.1.4 Implementación

En entornos típicos de red, una implementación Trabajo en Grupo ofrece las siguientes ventajas:

- Los equipos están en las mesas de los usuarios.
- Los usuarios actúan como sus propios administradores, y planifican su propia seguridad.
- Los equipos de la red están conectados por un sistema de cableado simple, fácilmente visible.

1.4.1.5 Recomendaciones de uso

Las redes para trabajo en grupo resultan una buena elección para entornos que cumplen con las siguientes características:

- Hay como máximo 10 usuarios
- Los usuarios comparten recursos, tales como archivos e impresoras, pero no existen servidores especializados
- La seguridad no es una cuestión fundamental
- La organización y la red sólo van a experimentar un crecimiento limitado en un futuro cercano.

Cuando se dan estos factores, puede que una red para Trabajo en Grupo sea una mejor opción que una red basada en servidor.

1.4.1.6 Consideraciones

Aunque puede que una red para Trabajo en Grupo pueda cubrir las necesidades de pequeñas organizaciones, no resulta adecuada para todos los entornos.

1.4.1.7 Administración

Las tareas de administración de la red incluyen:

- Gestionar los usuarios y la seguridad
- Asegurar la disponibilidad de los recursos
- Mantener las aplicaciones y los datos
- Instalar y actualizar software de aplicación y de sistema operativo.

En una red típica para Trabajo en Grupo, no hay un responsable del sistema que supervise la administración de toda la red. En lugar de esto, los usuarios individuales administran sus propios equipos.

1.4.1.8 Compartición de recursos

Todos los usuarios pueden compartir cualquiera de sus recursos de la forma que deseen. Estos recursos incluyen:

- Datos en directorios compartidos
- Impresoras
- Tarjetas de fax
- Etcétera

1.4.1.9 Requerimientos del servidor

En una red para trabajo en grupo, cada equipo necesita:

- Utilizar un amplio porcentaje de sus recursos para dar soporte al usuario sentado frente al equipo, denominado usuario local.
- Usar recursos adicionales, como el disco duro y la memoria, para dar soporte a los usuarios que acceden a recursos desde la red, denominados usuarios remotos.
- Aunque una red basada en servidor libera al usuario local de estas demandas, necesita, como mínimo, un potente servidor dedicado para cubrir las demandas de todos los clientes de la red.

1.4.1.10 Seguridad

En una red de equipos, la seguridad (hacer que los equipos y los datos almacenados en ellos estén a salvo de daños o accesos no autorizados) consiste en definir una contraseña sobre un recurso, como un directorio, que es compartido en la red.

Todos los usuarios de una red para Trabajo en Grupo definen su propia seguridad, y puede haber recursos compartidos en cualquier equipo, en lugar de únicamente en un servidor centralizado; de este modo, es muy difícil mantener un control centralizado.

Esta falta de control tiene un gran impacto en la seguridad de la red, ya que puede que algunos usuarios no implementen ninguna medida de seguridad.

Bajo estas circunstancias, se hace énfasis en que, si la seguridad es importante, puede que sea mejor usar una red basada en servidor.

1.4.1.11 Formación

Como cada equipo de un entorno para Trabajo en Grupo puede actuar como servidor y cliente, los usuarios necesitan formación antes de que puedan desenvolverse correctamente como usuarios y administradores de sus equipos.

1.4.2 Redes basadas en Servidor

En un entorno con más de 10 usuarios, una red para Trabajo en Grupo (con equipos que actúen a la vez como servidores y clientes) puede que no resulta adecuada. Por tanto, la mayoría de las redes tienen servidores dedicados.

1.4.2.1 Servidores dedicados

Un servidor dedicado es aquel que funciona sólo como servidor, y no se utiliza como cliente o estación; ésta es la razón de su nombre. Por otro lado, estos servidores están optimizados para dar (los servicios necesarios).

Los servidores se llaman «dedicados» porque no son a su vez clientes, y porque están optimizados para dar servicio con rapidez a peticiones de clientes de la red, y garantizar la seguridad de los archivos y directorios. Las redes basadas en servidor se han convertido en el modelo estándar para la definición de redes.

A medida que las redes incrementan su tamaño (y el número de equipos conectados y la distancia física y el tráfico entre ellas crece), generalmente se necesita más de un servidor. La división de las tareas de la red entre varios servidores asegura que cada tarea será realizada de la forma más eficiente posible.

1.4.2.2 Servidores especializados

Los servidores necesitan realizar tareas complejas y variadas. Los servidores para grandes redes se han especializado para adaptarse a las necesidades de los usuarios. Algunos ejemplos de este tipo de servidor son:

- De archivo de impresión
- De aplicaciones

- De correo
- De fax
- De comunicaciones
- De servicios de directorio

Por razones de alcance de esta tesis, no hablaré de ellos.

1.4.2.3 Funciones del software en redes

Un servidor de red y su sistema operativo trabajan conjuntamente como una unidad única. Independientemente de lo potente o avanzado que pueda ser un servidor, resultará inútil sin un sistema operativo que pueda sacar partido de sus recursos físicos.

Los sistemas operativos avanzados para servidor, como los de Microsoft y Novell, están diseñados para sacar partido del hardware de los servidores más avanzados.

1.4.2.4 Ventajas del servidor sobre trabajo en grupo

Aunque resulta más compleja de instalar, gestionar y configurar, una red basada en servidor tiene ventajas sobre una red simple Trabajo en Grupo, tales como son:

- Compartir recursos
- Seguridad
- Copia de seguridad
- Redundancia
- Número de usuarios
- Hardware
- fiabilidad.

1.4.3 Topologías de redes

Las topologías físicas más frecuentes en el mundo de las redes son:

- Jerárquica
- Bus.
- Estrella.
- Anillo.
- Malla.

Éstas se pueden combinar obteniendo una variedad de topologías híbridas más complejas.

1.4.3.1 Jerárquica

La estructura jerárquica fue una de las primeras topologías diseñadas para redes locales (LAN) y una de las más utilizadas en redes WAN.

Ésta consiste en la distribución jerárquica de las unidades en un bus donde la información tiene que llegar siempre a la cabecera de jerarquía.

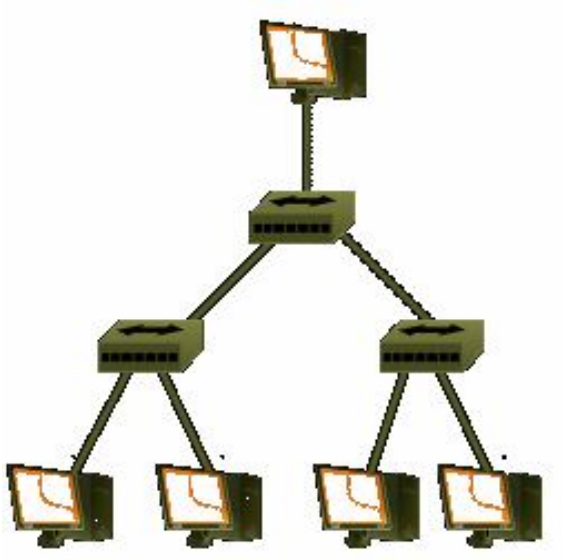
Alguna de las ventajas a resaltar en este tipo de topología son las siguientes:

- Facilidad para cubrir áreas extensas.
- Establecer funciones de gestión de red al disponer de nodos jerárquicos que pueden conocer e informar de las actividades o movimientos.

Entre las desventajas se encuentran:

- Existe la posibilidad de creación de cuellos de botella en un nodo jerárquico por el que pase un tráfico alto.
- La descentralización de la jerarquía puede producir dificultades en la comunicación a través de la red.

La forma de representar una topología jerárquica es la siguiente:

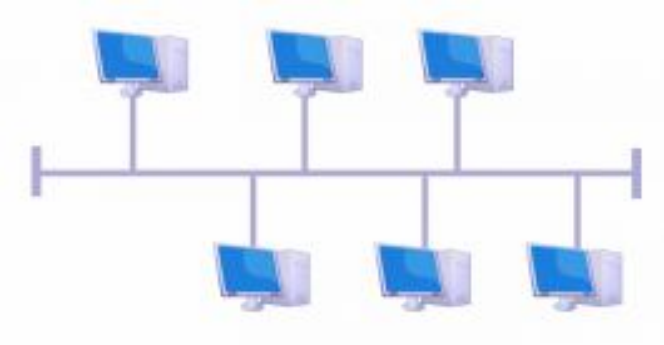


1.4.3.2 Bus

En la topología de bus o bus lineal, los equipos se conectan en línea recta. Consta de un único cable llamado segmento central (trunk; también llamado backbone o segmento) que conecta todos los equipos de la red en una única línea.

Los equipos de una red con topología en bus se comunican enviando datos a un equipo particular, mandando estos datos sobre el cable en forma de señales electrónicas.

La forma de representar a la topología de bus es la siguiente:



1.4.3.3 Estrella

En la topología en estrella, los segmentos de cable de cada equipo están conectados a un componente centralizado llamado hub. Las señales son transmitidas desde el equipo emisor a través del hub a todos los equipos de la red. Esta topología surgió en los albores de la informática, cuando se conectaban equipos a un gran equipo central o mainframe.

La red en estrella ofrece la ventaja de centralizar los recursos y la gestión. Sin embargo, como cada equipo está conectado a un punto central, esta topología requiere una gran cantidad de cables en una gran instalación de red. Además, si el punto central falla, cae toda la red.

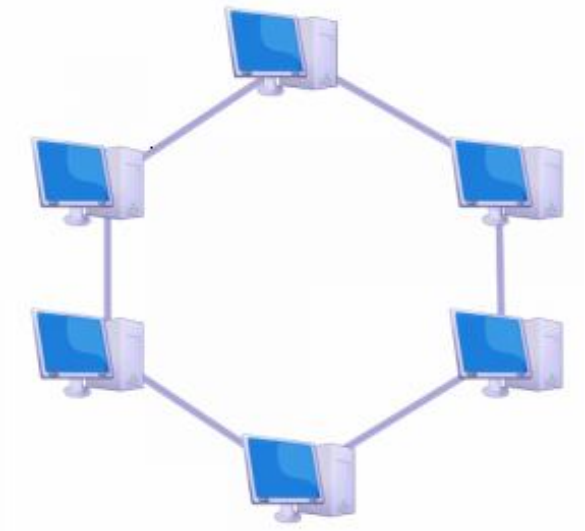
En una red en estrella, si falla un equipo (o el cable que lo conecta al hub), el equipo afectado será el único que no podrá enviar o recibir datos de la red. El resto de la red continuará funcionando normalmente.

La representación de la topología de red es la siguiente:

1.4.3.4 Anillo

La topología en anillo conecta equipos en un único círculo de cable. A diferencia de la topología en bus, no existen finales con terminadores. La señal viaja a través del bucle en una dirección, y pasa a través de cada equipo que puede actuar como repetidor para amplificar la señal y enviarla al siguiente equipo. El fallo de un equipo puede tener impacto sobre toda la red.

La topología física de una red es el propio cable. La topología lógica de una red es la forma en la que se transmiten las señales por el cable. Su representación se muestra a continuación:



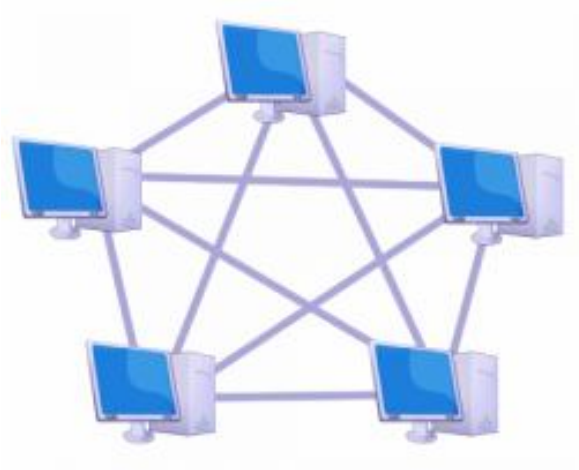
1.4.3.5 Malla

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. En una topología en malla, cada equipo está conectado a todos los demás equipos mediante cables separados.

Sin embargo, esta configuración ofrece caminos redundantes por toda la red, de modo que si falla un cable, otro se hará cargo del tráfico.

Aunque la facilidad de solución de problemas y el aumento de la fiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida.

La topología en malla se representa como sigue:



1.4.3.6 Topologías híbridas

Muchas topologías existentes son combinaciones híbridas de las topologías en bus, estrella, anillo y malla.

Las combinaciones clásicas son:

- Estrella – bus
- Estrella – anillo
- Trabajo en grupo

La topología estrella-bus es una combinación de las topologías en bus y estrella. En una topología en estrella-bus, varias redes con topología en estrella están conectadas entre sí con segmentos de bus lineales.

Si un equipo cae, esto no afectará al resto de la red. Los restantes equipos pueden seguir comunicándose. Si un hub deja de funcionar, todos los equipos conectados a dicho hub no podrán comunicarse. Si un hub está conectado a otros hubs, estas conexiones también se interrumpirán.

La topología de estrella-anillo, también conocida como anillo cableado en estrella parece ser similar a la topología estrella-bus. Tanto la estrella-anillo como la estrella-bus están centradas en un hub que contiene el anillo o bus real. En una red en estrella-bus hay segmentos lineales que conectan los hubs, mientras que los hubs de una red estrella-anillo están conectados en forma de estrella al hub principal.

Por otro lado, es de mencionar que muchas pequeñas oficinas utilizan una red Trabajo en Grupo, una red de este tipo puede configurarse con una topología física de estrella o bus. Sin embargo, como todos los equipos de la red son iguales (cada una puede actuar como cliente y servidor), la topología lógica puede resultar distinta.

1.5 Razones para utilizar Intranet

Una de las razones más sobresalientes por que las empresas instalan una Intranet, es para permitir a sus empleados trabajar mejor juntos. El tipo de software más potente que deja a la gente trabajar juntas está incluido en el extenso apartado de programas para trabajo en grupo y admite que los usuarios empleen la conferencia visual, comparta documentos, participen en discusiones y trabajen juntos de otro modo.

1.5.1 Herramientas de Intranet

Las herramientas de búsqueda y de catalogación, como agentes, arañas, tractores y autómatas, algunas veces denominadas motores de búsqueda, se pueden utilizar para ayudar a la gente a encontrar información y se emplean para reunir información acerca de documentos disponibles en una Intranet.

Estas herramientas de búsqueda son programas que buscan páginas Web, obtienen los enlaces de hipertexto en esas páginas y clasifican la información que encuentran para construir una base de datos.

Cada motor de búsqueda tiene su propio conjunto de reglas. Algunos siguen cada enlace en todas las páginas que encuentran, y después en turno examinan cada enlace en cada una de esas páginas iniciales nuevas, etcétera. Algunos ignoran enlaces que dirigen a archivos gráficos, archivos de sonido y archivos de animación; algunos enlaces a ciertos recursos como las bases de datos WAIS; y a algunos se les dan instrucciones para buscar las páginas iniciales más visitadas.

1.5.2 Funcionamiento financiero en Intranet

Las Intranet se utilizan no sólo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlos; esto es, recibir y rellenar pedidos de bienes y servicios.

Para que lo anterior pueda ocurrir, se debe diseñar una manera segura para enviar la información de la tarjeta de crédito por la notoriamente insegura Internet. Hay muchos métodos para hacer esto pero probablemente el que más se utiliza es un estándar llamado: el protocolo para la Transacción Electrónica Segura (SET), que ha sido aprobado, entre otras compañías, por:

- VISA
- MasterCard
- American Express
- Microsoft
- Nestcape

Es un sistema que permitirá a la gente con tarjetas bancarias hacer negocios seguros por las Intranets.

ESTRUCTURAS Y NECESIDADES EMPRESARIALES

2.1 Empresa y organización

Por lo regular, se suelen confundir los conceptos de empresa y organización; y, aunque existen ciertas diferencias entre ellos, es muy notoria su relación, por lo que es posible que sean manejados como sinónimos.

2.1.1 Empresas

De manera general, se define como empresa a todo grupo social en el que, a través de la administración de capital y el trabajo, se producen bienes y/o servicios pendientes a la satisfacción de las necesidades de la comunidad.

Para cumplir este objetivo, la empresa combina naturaleza y capital. Cada empresa es coordinada por un administrador que se encarga de tomar decisiones en forma oportuna para la consecución de los objetivos para los que fue creada.

2.1.1.1 Definiciones

El concepto de empresa revela un trasfondo filosófico que nos permite conocer la importancia que tienen las personas y sus conversaciones en el funcionamiento de toda empresa; esto, además de las actividades que se realizan y los recursos que son utilizados.

De esta declaración, se hace énfasis en la importancia que tiene el que toda persona que esté vinculada a una empresa, conozca este concepto.

El concepto de empresa puede diferir de acuerdo a quien lo dé; esto proviene de diferentes visiones o puntos de vista.

En este sentido, los conceptos más usuales de empresa son:

- Una empresa es una organización socia que utiliza una gran variedad de recursos para alcanzar determinados objetivos.

- La empresa se puede considerar como un sistema dentro del cual una persona o grupo de personas desarrollan un conjunto de actividades encaminadas a la producción y/o distribución de bienes y/o servicios, enmarcados en un objeto social determinado.

- Una empresa es sólo una conversación, un diálogo que existe y se perpetúa a través del lenguaje usado por quienes la componen.

- En Derecho, es una entidad jurídica creada con ánimo de lucro y está sujeta al Derecho mercantil.

- En Economía, la empresa es la unidad económica básica encargada de satisfacer las necesidades del mercado mediante el uso de recursos materiales y humanos. Se encarga, por lo tanto, de la organización de los factores de producción, capital y trabajo.

Tomando en cuenta los conceptos anteriores, se puede definir a una empresa como una organización social que realiza un conjunto de actividades y utiliza una gran variedad de recursos para lograr determinados objetivos, como la satisfacción de una necesidad o deseo de su mercado meta con la finalidad de lucrar o no; y que es construida a partir de conversaciones específicas basadas en compromisos mutuos entre las personas que la conforman.

2.1.1.2 Clasificación de las empresas

Las empresas tienen características que comparten; también, tienen características que las hacen diferentes y que permiten agruparlas.

Las empresas pueden ser clasificadas de acuerdo con varios criterios, entre los que destacan de acuerdo a:

- La actividad o giro
- La forma jurídica
- Su tamaño
- Su ámbito de actuación
- La titularidad de capital

- La cuota de mercado que posean
- El ámbito de su actividad
- El destino de los beneficios

2.1.1.2.1 Según su actividad o giro

De acuerdo con el sector de actividad de las empresas, éstas pueden ser:

- Del sector primario o extractivas
- Del sector secundario, comercial o industrial
- Del sector terciario o de servicios

Las empresas son extractivas cuando se dedican a la explotación de recursos naturales (renovables o no renovables); ejemplos de ellas son: agricultura, ganadería, caza, pesca, extracción de áridos, agua, minerales, petróleo, etcétera.

Las empresas del sector secundario son aquellas que realizan algún proceso de transformación de la materia prima, tales como: construcción, óptica, maderera, textil, etcétera.

El sector terciario incluye a las empresas cuyo principal elemento es la capacidad humana para realizar trabajos físicos o intelectuales. Comprende a empresas tales como: las de transporte, bancos, comercios, seguros, hotelería, educación, etcétera.

2.1.1.2.2 Según la forma jurídica

La legislación de cada país regula las formas jurídicas que pueden adoptar las empresas para el desarrollo de su actividad, las obligaciones, los derechos y las responsabilidades de la empresa. Así, las empresas se clasifican en:

- Unipersonal
- Sociedad colectiva
- Cooperativas
- Comanditarias
- Sociedad de responsabilidad limitada
- Sociedad anónima

En la unipersonal, el empresario o propietario es la persona con capacidad legal para ejercer el comercio, y es el encargado de responder de forma ilimitada con todo su patrimonio ante las personas que pudiesen verse afectadas por el accionar de la empresa.

La sociedad colectiva es una empresa de más de una persona; en ella, los socios responden también de forma ilimitada con su patrimonio, y existe participación en la dirección o gestión de la empresa.

Las cooperativas no poseen ánimo de lucro y son constituidas para satisfacer las necesidades o intereses socioeconómicos de los cooperativistas, quienes, a su vez, son trabajadores y, en algunos casos, proveedores y/o clientes de la empresa.

En las comanditarias existen dos tipos de socios: los colectivos, con la característica de la responsabilidad ilimitada; y los comanditarios, cuya responsabilidad se limita a la aportación de capital efectuado.

En la sociedad de responsabilidad limitada, los socios propietarios tienen la característica de asumir una responsabilidad de carácter limitada, respondiendo sólo por capital o patrimonio que aportan a la empresa.

La sociedad anónima tiene el carácter de la responsabilidad limitada al capital que aportan, pero poseen la alternativa de tener las puertas abiertas a cualquier persona que desee adquirir acciones de la empresa.

2.1.1.2.3 Según su tamaño

De acuerdo con su tamaño, las empresas puede tipificarse en:

- Grandes empresas
- Medianas empresas
- Pequeñas empresas
- Microempresas

No hay unanimidad entre los economistas a la hora de establecer qué es una empresa grande o pequeña, puesto que no existe un criterio único para medir el tamaño de la empresa. Los principales indicadores son:

- El volumen de ventas
- El capital propio
- Número de trabajadores
- Beneficios
- Etcétera

El más utilizado de los anteriores, suele ser según el número de trabajadores.

2.1.1.2.4 Según su ámbito de actuación

En función del ámbito geográfico en el que las empresas realizan su actividad económica, se pueden clasificar en:

- Locales
- Regionales
- Nacionales
- Multinacionales

- Transnacionales
- Mundiales

2.1.1.2.5 Según la titularidad de capital

Este criterio se refiere a si el capital se encuentra en poder de los particulares, de organismos públicos o, en su caso, de ambos. De acuerdo con él, las empresas se pueden dividir en:

- Privada
- Pública
- Mixta

Se le conoce como privada si el capital se encuentra en manos de accionistas particulares.

Se le llama pública si el capital y el control de éste están en manos del gobierno.

La mixta es el tipo de empresa en la que la propiedad del capital es compartida entre el Estado y los particulares.

2.1.1.2.6 Según la cuota de mercado que posean

De acuerdo con este criterio, las empresas se pueden tipificar en:

- Aspirante
- Especialista
- Líder
- Seguidora

La empresa aspirante es aquella cuya estrategia va dirigida a ampliar su cuota frente al líder y las demás empresas competidoras.

La especialista es aquella empresa que responde a necesidades muy concretas dentro de un segmento de mercado.

La empresa líder es aquella que marca la pauta en cuanto a precios, innovaciones, publicidad, etcétera.

La empresa seguidora es muy pequeña, y no dispone de una cuota suficientemente grande como para inquietar a la empresa líder.

2.1.1.2.7 Según el Destino de los Beneficios

Según el destino que la empresa decida otorgar a los beneficios económicos (excedente entre ingresos y gastos) que obtenga, pueden categorizarse en dos grupos:

- Con ánimo de lucro
- Sin ánimo de lucro

En las primeras, los excedentes pasan a poder de los propietarios y/o accionistas de la empresa. En los segundos, los excedentes se vuelcan a la propia empresa para permitir su desarrollo.

2.1.1.3 Características de las empresas

Una empresa combina, básicamente, tres factores; éstos son:

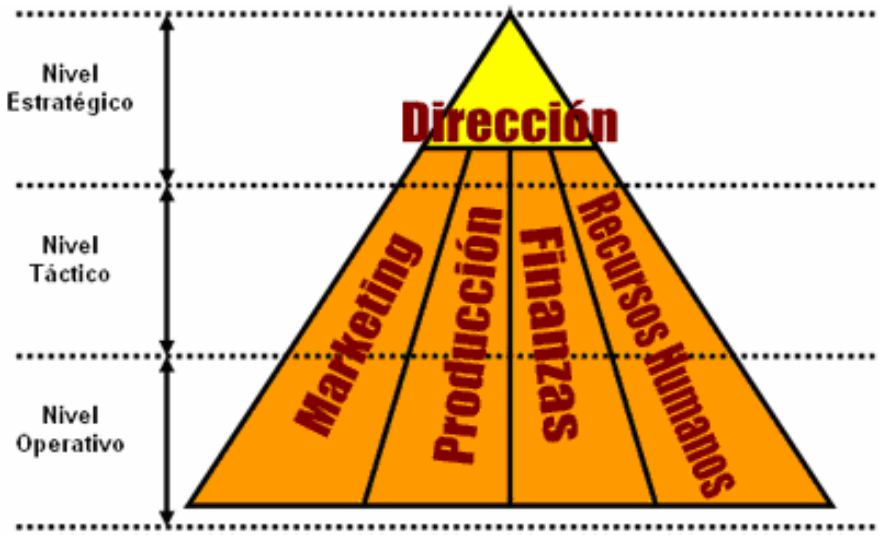
- Factores activos
- Factores pasivos
- Organización

Los factores activos se refieren a los empleados, propietarios, sindicatos, bancos, etcétera.

Los factores pasivos son: las materias primas, transporte, tecnología, conocimiento, contratos financieros, etcétera.

En cuanto a la organización, es la coordinación y el orden entre todos los factores y las áreas.

Las áreas funcionales de una empresa se muestran en la figura siguiente:



2.1.1.4 Gobierno empresarial

Las prácticas de buen gobierno empresarial varían enormemente en cuanto a su detalle y aplicación de país a país. Básicamente su objetivo es generar confianza ante accionistas, empleados, actores económicos y sociedad en general. Los elementos esenciales del "buen gobierno empresarial" son:

- Transparencia informativa
- Informes y auditoria de cuentas
- Códigos éticos
- Gestión del riesgo
- Protección del patrimonio
- Planificación estratégica

Dentro de estos aspectos deben contemplarse como integrantes:

- El buen gobierno de los recursos humanos
- El buen gobierno de la calidad
- El buen gobierno de los sistemas de información y las comunicaciones
- El buen gobierno medioambiental
- El buen gobierno de la tecnología

En el ejercicio de su actividad económica, la empresa moderna ha producido indudables beneficios sociales. En general, ha proporcionado al público un abastecimiento oportuno y adecuado y una distribución más efectiva de bienes y servicios.

A través de la difusión del crédito, ha incrementado la capacidad de compra de grandes sectores de la población y, por medio de la publicidad, les ha llevado el conocimiento de nuevos y útiles productos capaces de satisfacer sus necesidades generales. Además, el aumento en la productividad y la producción en masa le han permitido la reducción de precios.

2.1.1.5 Objetivos empresariales

En realidad, los objetivos de cada empresa son muy particulares, debido a sus propias necesidades y/o características.

De manera general, algunos de los objetivos empresariales son:

- Crear, desarrollar y dar a conocer el sistema de la empresa a todos los integrantes.

- Concientizar a cada miembro de la empresa acerca de que la misma es una organización social

- Administrar adecuadamente cada recurso de la empresa

- Guiar positivamente las conversaciones que se dan en la empresa.

- Incentivar los compromisos que contribuyen positivamente al mejoramiento de la empresa

2.1.2 Organizaciones

Si bien, todos tenemos una idea básica acerca de lo que significa el término organización, no siempre podemos definirlo adecuadamente.

Sin embargo, en el contexto empresarial es importante tener una idea cabal acerca de lo que significa este término para poder referirnos con propiedad, ya sea, a una entidad (organización con o sin fines de lucro) o a una determinada actividad (la organización de una empresa, un evento u otro).

2.1.2.1 Definiciones

La organización, desde diversos puntos de vista, se puede definir de diferentes maneras; algunos ejemplos son:

- Acción y efecto de articular, disponer y hacer operativos un conjunto de medios, factores o elementos para la consecución de un fin concreto.

- Acción y objeto (al mismo tiempo)

- Consiste en ensamblar y coordinar los recursos humanos, financieros, físicos, de información y otros, que son necesarios para lograr las metas, y en actividades que incluyan atraer a la gente a la organización, especificar las responsabilidades del puesto, agrupar tareas en unidades de trabajo, dirigir y distribuir recursos y crear condiciones para que las personas y las cosas funcionen para alcanzar el máximo éxito.

- Cuando es utilizada como sustantivo, implica la estructura dentro de la cual las personas son asignadas a posiciones y su trabajo es coordinado para realizar planes y alcanzar metas.

De acuerdo con lo anterior, se puede deducir que existen dos formas de definir a una organización: como entidad y como actividad.

Como entidad, una organización es un sistema cuya estructura está diseñada para que los recursos humanos, financieros, físicos, de información y otros, de forma coordinada, ordenada y regulada por un conjunto de normas, logren determinados fines.

Como actividad, una organización es el acto de coordinar, disponer y ordenar los recursos disponibles (humanos, financieros, físicos y otros) y las actividades necesarias, de tal manera, que se logren los fines propuestos.

2.1.2.2 Clasificación de organizaciones

Las organizaciones se caracterizan por ser altamente heterogéneas y diversas; por ello, dan lugar a una catalogación de ellas. En este sentido, se pueden tipificar según:

- Fines
- Formalidad
- Grado de centralización

2.1.2.3 Observaciones importantes

Es de mencionar que las organizaciones no son estáticas; esto es, van cambiando de acuerdo a su necesidades, cambio de tamaño, etcétera.

En este sentido, cabe señalar que una misma organización puede tener las características de dos o tres organizaciones al mismo tiempo; lo cual da a conocer sus fines, estructura y características principales.

2.2 Organigramas

El organigrama es una representación gráfica que expresa en términos concretos y accesibles la estructura, jerarquía e interrelación de las distintas áreas que componen una empresa u organización, resulta muy conveniente que todos los que la componen conozcan cuál es su definición, para que de esa manera, tengan un conocimiento básico pero fundamental, acerca de lo que es este sencillo pero valioso recurso.

2.2.1 Definiciones

Básicamente, un organigrama se define como una representación gráfica de la estructura organizacional de cualquier empresa o entidad productiva, comercial, administrativa, etcétera; en él, se muestra e indica, en forma esquemática, la posición de las áreas que la integran, sus líneas de autoridad, relaciones de personal, comités permanentes, líneas de comunicación y de accesoria.

2.3.2 Tipos de organigramas

Los organigramas pueden clasificarse, de manera general, de la siguiente forma:

- Por su naturaleza
- Por su ámbito

- Por su contenido
- Por su presentación

2.2.2.1 Por su naturaleza

Dentro de esta clasificación se encuentran:

- Organigramas microadministrativos
- Organigramas macroadministrativos
- Organigramas mesoadministrativos

Los organigramas microadministrativos corresponden a una sola organización, y pueden referirse a ella en forma global o mencionar alguna de las áreas que la conforman.

Los macroadministrativos involucran a más de una organización.

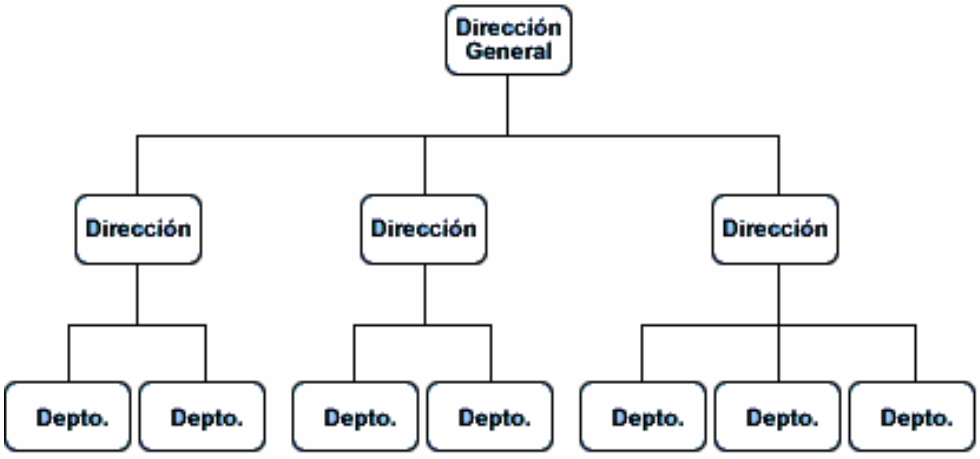
Los organigramas mesoadministrativos consideran una o más organizaciones de un mismo sector de actividad o ramo específico.

2.2.2.2 Por su ámbito

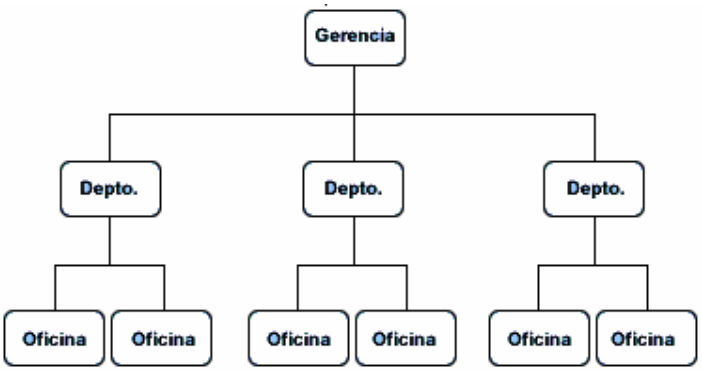
De acuerdo con su ámbito, los organigramas pueden ser:

- Generales
- Específicos.

Los organigramas generales contienen información representativa de una organización hasta determinado nivel jerárquico, según su magnitud y características. Su esquema se observa en la siguiente figura:



Los organigramas específicos muestran en forma particular la estructura de un área de la organización; su representación es la siguiente:

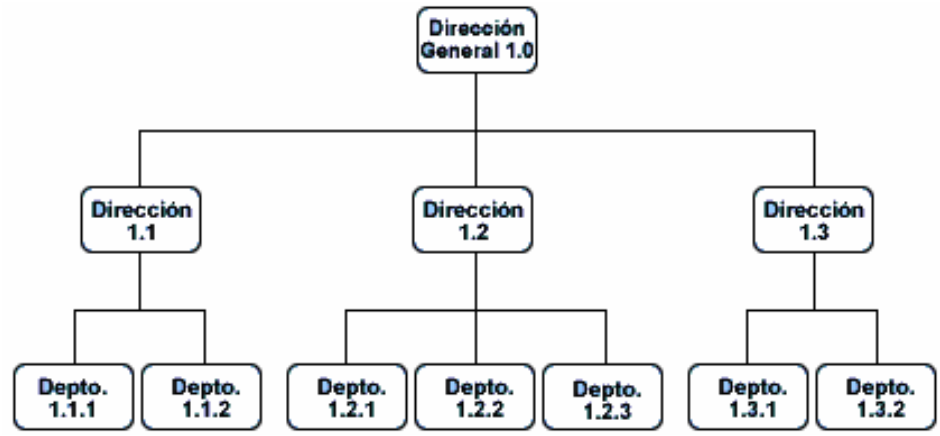


2.2.2.3 Por su contenido

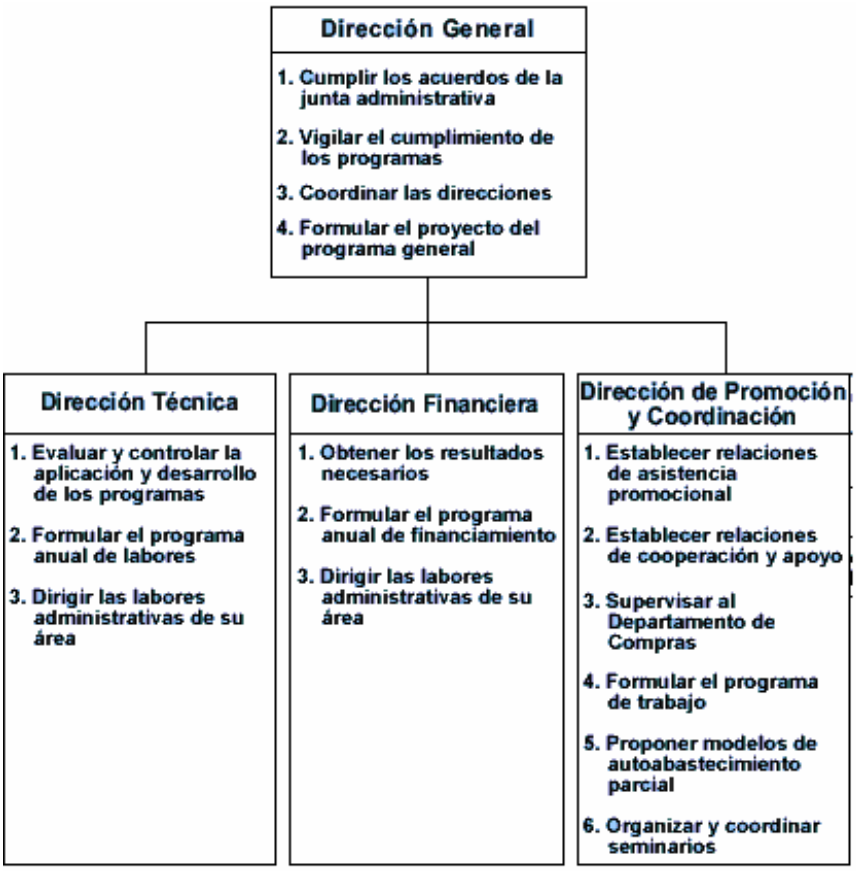
De acuerdo con su contenido, un organigrama puede ser:

- Integral
- Funcional
- De puestos, plazas y unidades.

Los organigramas integrales son representaciones gráficas de todas las unidades administrativas de una organización y sus relaciones de jerarquía o dependencia, tal como lo muestra la figura siguiente:

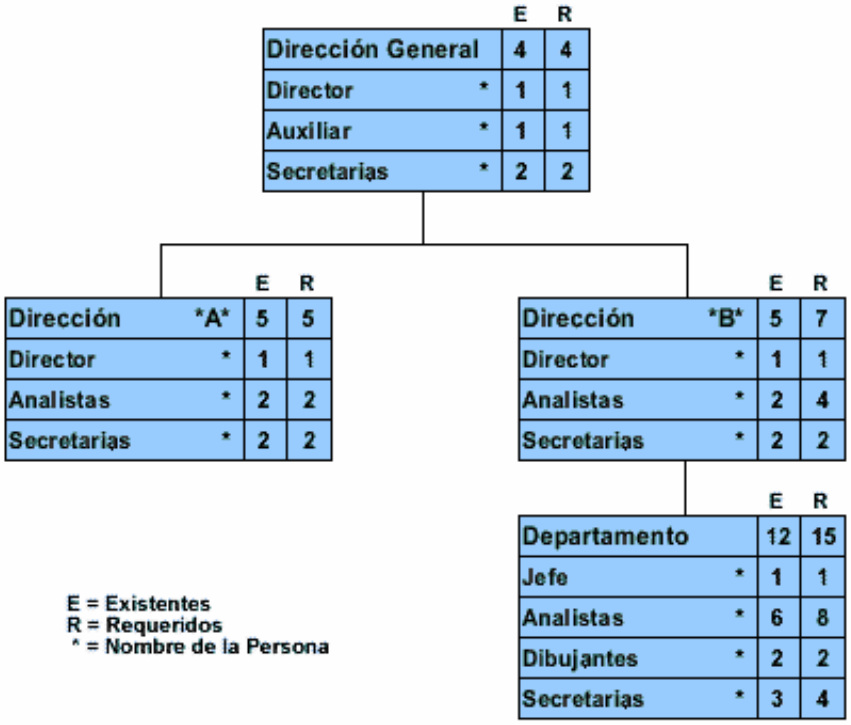


Los organigramas funcionales incluyen las principales funciones que tienen asignadas, además de las unidades y sus interrelaciones. Su representación se muestra en la siguiente figura:



Los organigramas de puestos, plazas y unidades, indican las necesidades en cuanto a puestos y el número de plazas existentes o necesarias para cada unidad consignada.

También se pueden incluir los nombres de las personas que ocupan las plazas; lo anterior se muestra en la figura siguiente:



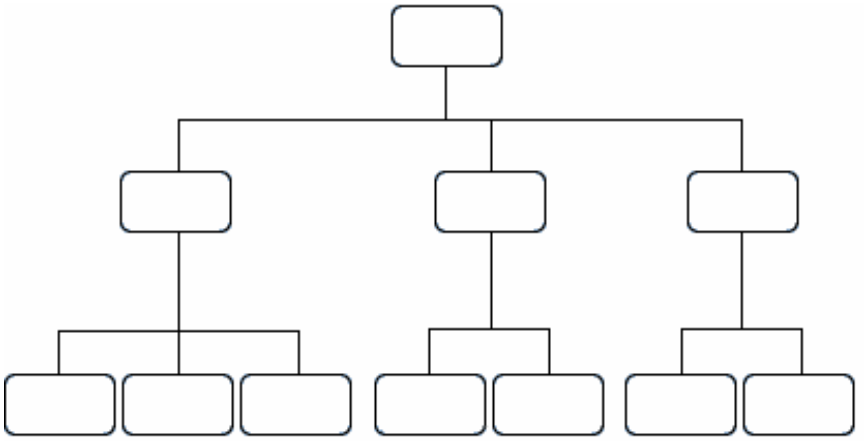
2.3.2.4 Por su presentación

De acuerdo con su presentación, los organigramas pueden ser:

- Verticales
- Horizontales
- Mixtos
- De bloque

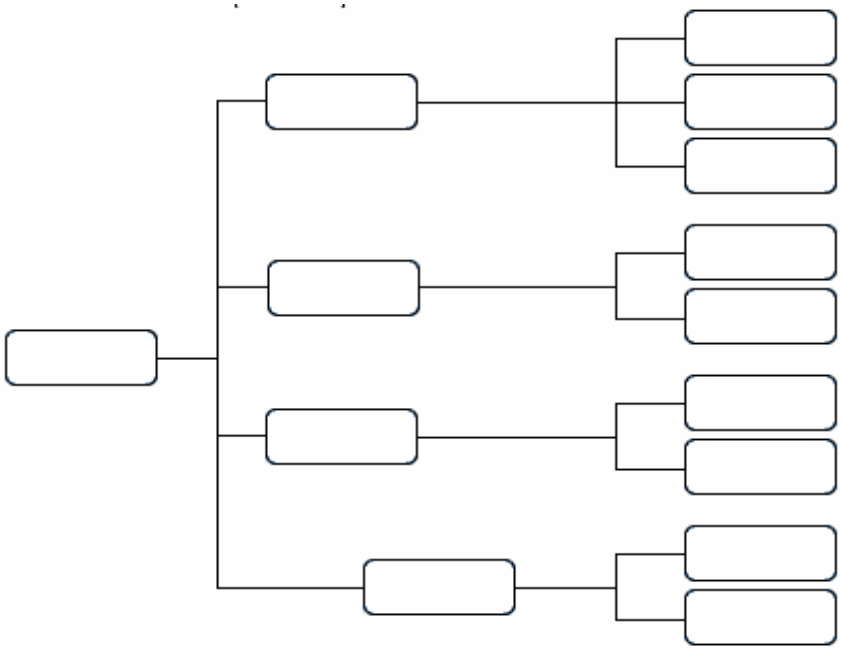
Los verticales presentan las unidades ramificadas de arriba hacia abajo a partir del titular, en la parte superior; y desagregan los diferentes niveles jerárquicos en forma escalonada.

Estos organigramas son los más usuales en la administración. Una representación de este tipo de organigramas es la que se muestra a continuación:

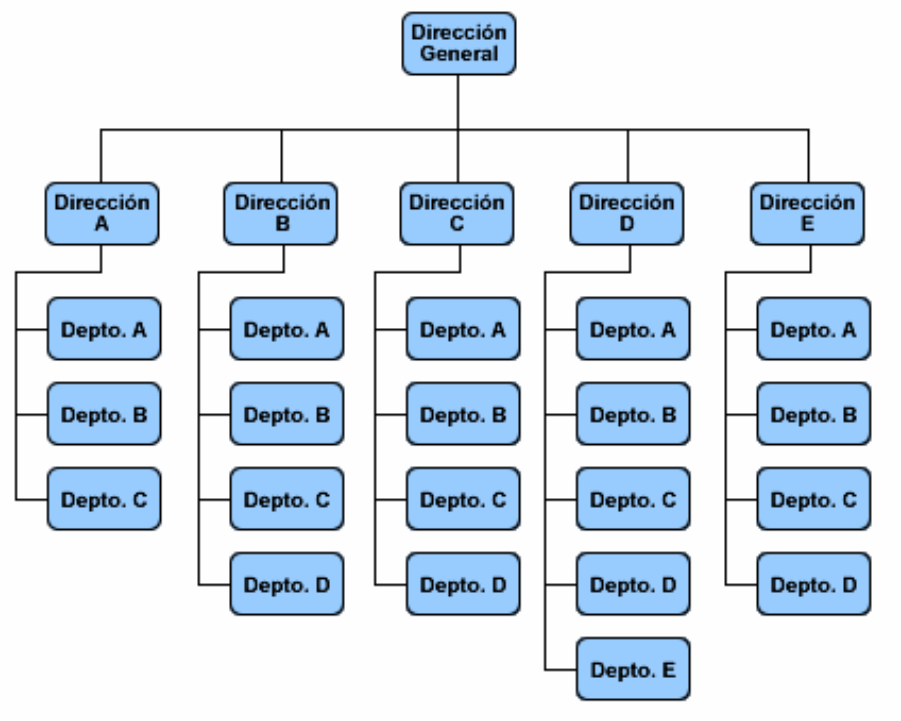


Los horizontales despliegan las unidades de izquierda a derecha, y colocan al titular en el extremo izquierdo. Los niveles jerárquicos se ordenan en forma de columnas, en tanto que las relaciones entre las unidades se ordenan por líneas dispuestas horizontalmente; de ahí su nombre.

La forma de representar a este tipo de organigramas, es el siguiente:

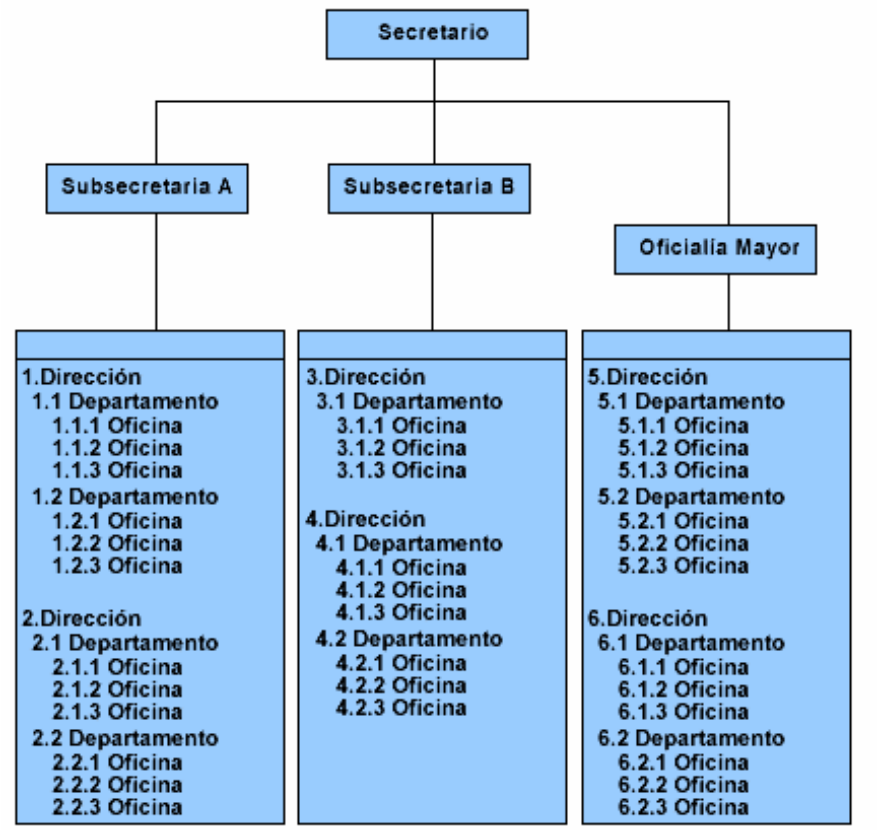


Los organigramas mixtos utilizan combinaciones de los dos anteriores; esto con el fin de ampliar las posibilidades de graficación. Su uso es recomendado en el caso de organizaciones con un gran número de unidades en la base. Su representación se puede ver en la figura siguiente:



Finalmente, los organigramas de bloque son también una variante de los verticales y tienen la particularidad de integrar un mayor número de unidades en espacios que pueden ser sumamente reducidos.

Por su cobertura, permiten que aparezcan unidades ubicadas en los últimos niveles jerárquicos. Una forma de representarlos es como sigue:



2.3 Medios de comunicación

Los medios de comunicación son el canal que mercadólogos y publicistas utilizan para transmitir un determinado mensaje a su mercado meta, por tanto, la elección del o los medios a utilizar en una campaña publicitaria es una decisión de suma importancia porque repercute directamente en los resultados que se obtienen con ella.

Por ello, tanto mercadólogos como publicistas deben conocer cuáles son los diferentes tipos de medios de comunicación, en qué consisten y cuáles son sus ventajas y desventajas, con la finalidad de que puedan tomar las decisiones más acertadas al momento de seleccionar los medios que van a utilizar.

Los medios de comunicación se pueden tipificar, de forma general, en:

- Medios masivos
- Medios auxiliares
- Medios alternativos

Los medios masivos o medidos, son aquellos que afectan a un mayor número de personas en un momento dado. De entre ellos, se pueden destacar los siguientes:

- Televisión
- Radio
- Periódico
- Revista
- Gate Folder
- Booklets
- Cuponeo
- Muestreo
- Internet
- Cine

Los medios auxiliares, complementarios o no medidos, afectan a un menor número de personas en un momento dado. De entre ellos destacan:

- Medios exteriores o de publicidad exterior
- Publicidad interior
- Publicidad directa o correo directo

Los medios alternativos son aquellas formas nuevas de promoción de productos; algunas de ellas son ordinarias, mientras que otras resultan muy innovadoras. De ellos, están los siguientes ejemplos:

- Fax
- Carritos de compras con vídeo en las tiendas comerciales
- Protectores de pantalla de computadoras
- Discos compactos
- Kioscos interactivos en tiendas comerciales
- Anuncios que pasan antes de las películas en los cines.

2.4 Oficinas virtuales

Las oficinas virtuales son oficinas integrales que prestan servicios secretariales, asistenciales y de comunicación (tales como: teléfono, correo electrónico, comunicación vía fax, teleconferencias, Internet, etcétera) a empresarios, profesionistas, tele-trabajadores y prestadores, aunque de forma externa (lo que recibe el nombre, en el ámbito financiero, de outsourcing); este es un campo de aplicación para las Intranet´s.

Adicionalmente, algunas oficinas virtuales suelen proporcionar un domicilio social.

2.5 El cambio en los negocios

Es de notarse que los negocios han ido cambiando paulatinamente; algunos cambios, por supuesto, son más notorios que otros debido al impacto que estos causan a los procesos de la empresa.

Cabe mencionar el gran impacto que ha tomado la tecnología informática (IT) hacia el interior de las compañías.

Las empresas buscan optimizar su infraestructura de Tecnología Informática, (IT). Ésta, al igual que las telecomunicaciones debe ser constantemente revisada y evaluada por los mandos medios y superiores de las compañías para lograr el equilibrio entre economía y eficiencia. Todavía, se espera encontrar aplicaciones más robustas y complejas de esta nueva tecnología. "Voice LAN", proporciona una forma para facilitar:

- Los procesos de reingeniería de los negocios.
- Manejar el "núcleo" de los equipos de trabajo.
- Operar las aplicaciones de multimedia en un entorno cliente/servidor.
- Controlar los costos de operación.

Se puede hacer la declaración categórica de que, en los negocios de hoy, "lo único constante es el cambio". Las compañías están operando en la actualidad de una forma más volátil y con mercados en movimiento, en comparación a como se hacían negocios en el pasado inmediato.

Estas demandas requieren flexibilidad tanto en los servicios como en los productos. Ahora, el lapso de tiempo en que los productos llegan a los nuevos mercados en muy corto. Por lo que, ahora es el momento en que el cliente debe estar preparado para obtener respuestas.

2.5.1 La Tecnología Informática Tradicional Entregada

Actualmente, los negocios están luchando para tener mejores inversiones en Tecnología Informática, el sentimiento generalizado es que aún, no se han podido deshacer de la Tecnología tradicional y esto significa, no poder crecer al ritmo que ellos esperarían.

En vez de modelarse a sí misma en los negocios, la Tecnología Informática ha dejado crecer las expectativas de lo que finalmente podría ser el ambiente real de los negocios.

En el ambiente cliente/servidor que utilizan los usuarios, ha sido difícil integrar los sistemas con los equipos de trabajo. Sin embargo, los usuarios que trabajan en la misma tarea siempre se encuentran ubicados en la misma oficina o en el mismo edificio, o al menos en el mismo continente.

Actualmente, los usuarios distribuidos y establecidos en varios lugares requieren colaborar en el mismo proyecto. Y, requieren más que un correo electrónico y de telefonía convencional: los usuarios necesitan compartir documentos en tiempo real, mostrar hoja(s) de cálculo, cambiar imágenes en documentos y la comunicación en grupos.

2.5.2 Reingeniería de los Procesos en los Negocios

Las empresas requieren, para mantenerse al día, la implantación de la llamada Reingeniería de los Procesos en los Negocios ("Business Process Reengineering", BRP); una tecnología que realmente proporcione ventajas competitivas a los negocios (trabajar con los negocios y no contra ellos), además de dar a los usuarios todo lo que ellos necesitan.

La BRP (reingeniería de los procesos en los negocios) ha presionado a los departamentos de Tecnología Informática de los negocios a ser por sí mismos rentables y comerciales al igual que ser más responsables hacia las necesidades y requerimientos de los usuarios.

Los usuarios no son ya una multitud dócil para el Departamento de Tecnología Informática; es decir, los usuarios se han revelado. Ellos esperan respuestas rápidas y sistemas que les ayuden en los requerimientos del negocio.

2.5.3 Fusión de Equipos de Trabajo

Para que el manejo de la fusión entre equipos de trabajo sea exitoso, se requiere involucrar y educar al equipo de voz en Red de Área Local (LAN) y aplicaciones de datos, mientras que el equipo experto en datos tiene que aprender los fundamentos de las telecomunicaciones.

Con este entrenamiento en puerta, el equipo entero es preparado para un nuevo escenario en el cual la voz, al igual que otro contenido de multimedia como el video, es un ejemplo especializado del manejo de datos.

Los sistemas tradicionales con PBX estarán soportados al lado de nuevos sistemas, requiriendo las gerencias de los equipos de voz y datos combinar el conocimiento de lo antiguo con lo moderno (lo viejo con lo nuevo).

Pero esto no debe ser una dura carga. Moviendo los PBX basados en servidores se disminuirá la dificultad de transición en la gerencia de cada equipo de trabajo, y la situación más dura es igual a ser una compañía que intenta ir de un equipo centralizado en PBX hacia un ambiente de "VoiceLAN" en un único paso.

El punto importante a tratar aquí, es ahora dar un paso alejado del modelo centralizado de voz. Esto salvará a muchos de infartos en algunos años. En el "corazón" del manejo de "VoiceLAN" se tiene un reconocimiento muy complejo y elaborado para las máquinas de escritorio.

2.5.4 Expectativas de los Usuarios

Los usuarios, quienes hace sólo algunos pocos años fueron "enchufados" con sistemas de cómputo que sólo podían mostrar letras en color verde sobre fondo negro, ahora esperan que sus equipos realicen más "milagros" día a día.

Efectivamente, el usuario ha cambiado radicalmente su postura de una pregunta como ¿qué es esto?, y ahora, pregunta ¿por qué no puedo hacer esto o aquello?

Por esa razón, los equipos y los medios de comunicación deben, no sólo estar enfocados a las necesidades de los usuarios, sino adaptarse a los más mínimos cambios en los requerimientos de ellos.

2.5.5 Aplicaciones Multimedia

Las aplicaciones Multimedia han dado mucho de que hablar en términos de tecnología. Ahora, se requiere una sinergia entre datos, voz e imagen para finalmente, combinarlos todos de manera eficiente para hacer más robustos los sistemas y resolver problemas de aplicación de los usuarios. A pesar de que Multimedia es un entorno relativamente nuevo, algunas aplicaciones están mostrando claramente sus beneficios.

2.5.6 Aprendizaje a Distancia

La capacitación es un tópico importante en los negocios de hoy, se tienen compañías tratando de seguir las habilidades que la actual mano de obra necesita en cuanto a capacitación.

Con las normas establecidas, Multimedia puede dar el entrenamiento o capacitación a través del uso de video, tutores en "vivo", entrenamiento interactivo y la posibilidad de correr cursos donde actualmente el usuario está de forma presencial.

2.5.7 Voz y Video en la Red

La educación a distancia es sólo la parte delgada de la cuña. Hay otras aplicaciones que pueden tomar "vida" en cuanto el video, la voz se puedan transmitir tan bien como se hace con los datos en los actuales equipos de escritorio.

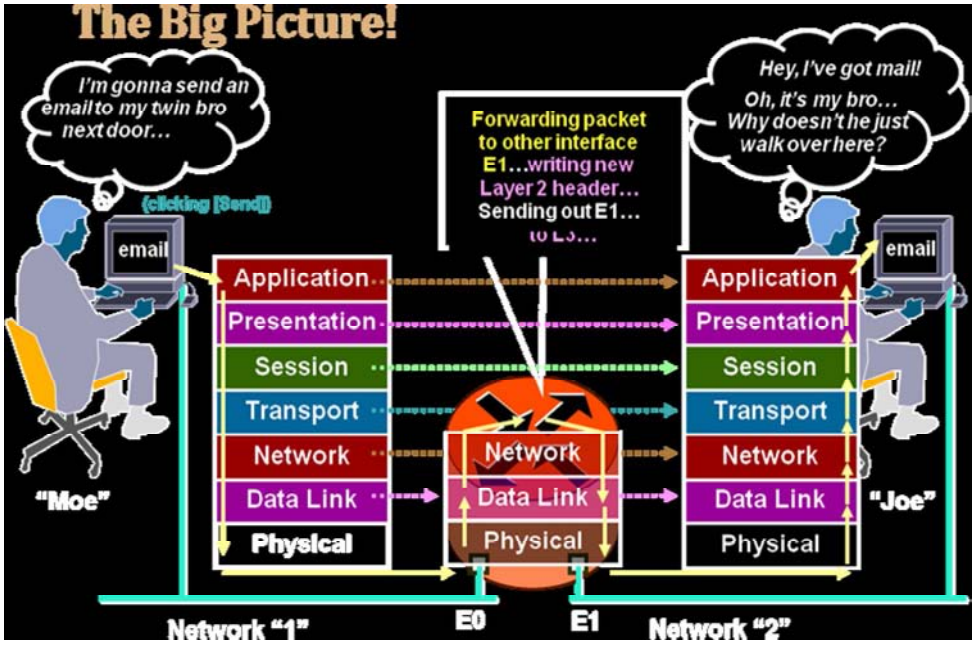
Esto es especialmente cierto para el Video sobre una LAN o una Intranet; ahora LAN ofrece un mayor ancho de banda, que el que tradicionalmente han usado las interfaces de la generación previa en sus comunicaciones. Esto ha mejorado las actuales aplicaciones. Algunas de las mejoras incluyen:

- Servicios nuevos de información como la posibilidad de conocer información financiera de primera mano.

- Videoconferencia en equipos de escritorio acoplados con técnicas compartidas semejantes a la del pizarrón blanco.

Estas aplicaciones traen un nuevo juego de requerimientos para la red. Éstas comparten un pequeño retraso en la transmisión.

MANEJO DE INFORMACIÓN EN INTRANET



3.1 Definición

Una Intranet es una red de ordenadores privada basada en los estándares de Internet. Esto implica que la primera es inevitablemente dependiente de la segunda; sin embargo, existen diferencias entre ellas.

Las Intranet´s utilizan tecnologías de internet para enlazar los recursos informativos de una organización:

- Desde documentos de texto a documentos multimedia
- Desde bases de datos legales a sistemas de gestión de documentos.

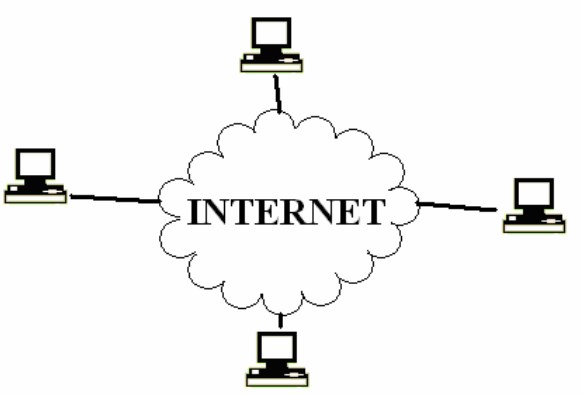
Las Intranet´s pueden incluir:

- Sistemas de seguridad para la red
- Tablones de anuncios
- Motores de búsqueda.

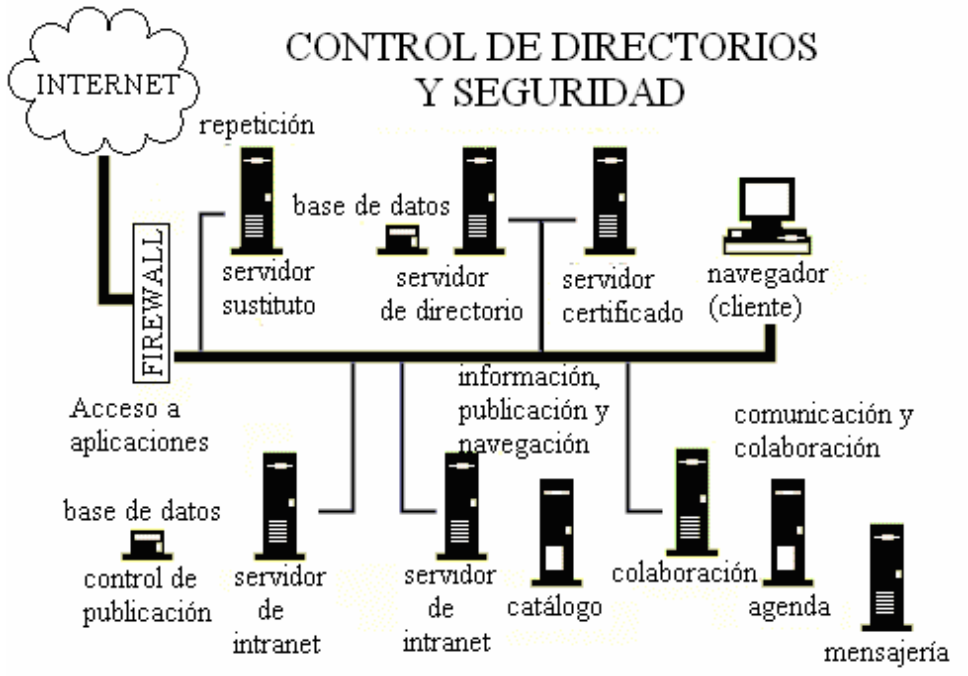
Una Intranet puede extenderse a través de Internet. Esto se hace generalmente usando una red privada virtual (VPN).

Desde un punto de vista objetivo, la Intranet se puede ver como un conjunto de contenidos compartidos por un grupo bien definido dentro de una organización. Se trata de un concepto relativo al acceso del contenido; por esta razón, podría considerarse como lo opuesto al término Web, el cual está conformado por contenidos de acceso libre y sin restricciones para cualquier tipo de público.

Para tener una idea más clara sobre esta distinción, en las figuras siguientes se observa la globalidad de la red Internet y las restricciones de seguridad de la red Intranet.



Red Internet



Red Intranet

3.2 Visión general de Intranet

Una Intranet es una red privada empresarial o con fines educativos, la cual utiliza los protocolos TCP/IP de Internet para su transporte básico. Estos protocolos pueden ejecutar una variedad de hardware de red; al mismo tiempo, pueden coexistir con otros protocolos de red; un ejemplo de estos podría ser IPX.

Aquellos empleados que están dentro de una Intranet pueden acceder a los amplios recursos de Internet, pero aquellos en Internet no pueden entrar en la Intranet, puesto que ésta tiene acceso restringido.

Frecuentemente, una Intranet se compone de un número de redes diferentes dentro de una empresa que se comunica con otra mediante TCP/IP. Estas redes separadas reciben el nombre de subredes.

Es de mencionar que el software que permite a las personas comunicarse entre ellas vía e-mail (correo electrónico) y tablones de mensajes públicos, así como colaborar en la producción usando software de grupos de trabajo, se encuentra entre los programas más poderosos de Intranet.

Las aplicaciones que permiten a los distintos departamentos empresariales enviar información, y a los empleados el rellenar formularios de la empresa (por ejemplo, las hojas de asistencia) así como el utilizar la información corporativa financiera de la organización, son muy populares.

La mayoría del software que se utiliza en las Intranet´s es estándar; de entre ellos se puede citar a los siguientes:

- Software de Internet

    1. Netscape
    2. Navigator
    3. Explorer para Web de Microsoft

- Programas personalizados

Los programas personalizados se construyen frecuentemente utilizando el lenguaje de programación JAVA y el de guión de CGI.

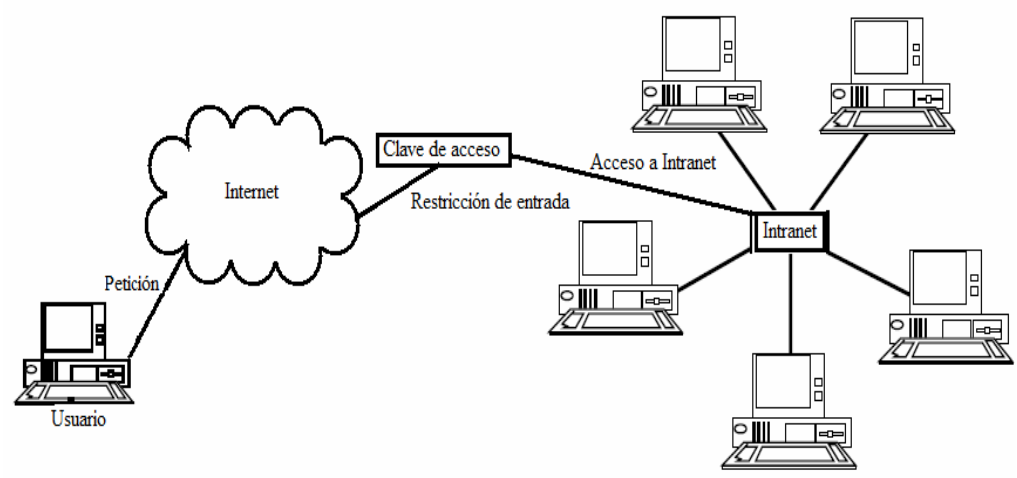
Las Intranet´s también se pueden utilizar para permitir a las empresas llevar a cabo transacciones de negocio a negocio como:

- Hacer pedidos
- Enviar facturas
- Efectuar pagos

Para mayor seguridad, estas transacciones de Intranet a Intranet no necesitan nunca salir a Internet, pero pueden viajar por líneas alquiladas privadas. Son un sistema poderoso para permitir a una compañía hacer negocios en línea, por ejemplo, permitir que alguien en Internet pida productos.

Cuando alguien solicita un producto en Internet, la información se envía de una manera segura desde Internet a la red interna de la compañía, donde se procesa y se completa el encargo.

La información enviada a través de una Intranet alcanza su lugar exacto mediante los enrutadores, que examinan la dirección IP en cada paquete TCP/IP y determinan su destino. Después envía el paquete al siguiente direccionador. Si éste tiene que entregarse en una dirección en la misma subred de la Intranet desde la que fue enviado, llega directamente sin tener que atravesar otro enrutador. Lo anterior se muestra en la siguiente figura:



Por otro lado, si tiene que mandarse a otra subred de trabajo en la Intranet, se enviará a otra ruta. Si el paquete tiene que alcanzar un destino externo a la Intranet en otras palabras, Internet se envía a un enrutador que conecte con Internet.

Con el fin de proteger la información corporativa delicada, y para asegurar que los piratas (hackers) no perjudiquen a los sistemas informáticos ni a los datos, las barreras de seguridad llamadas firewalls protegen a una Intranet de internet.

La tecnología firewall utiliza una combinación de enrutadores, servidores y otro hardware y software para permitir a los usuarios de una Intranet utilizar los recursos de internet, pero no es una función recíproca. El firewall evita que los intrusos se introduzcan el la Intranet.

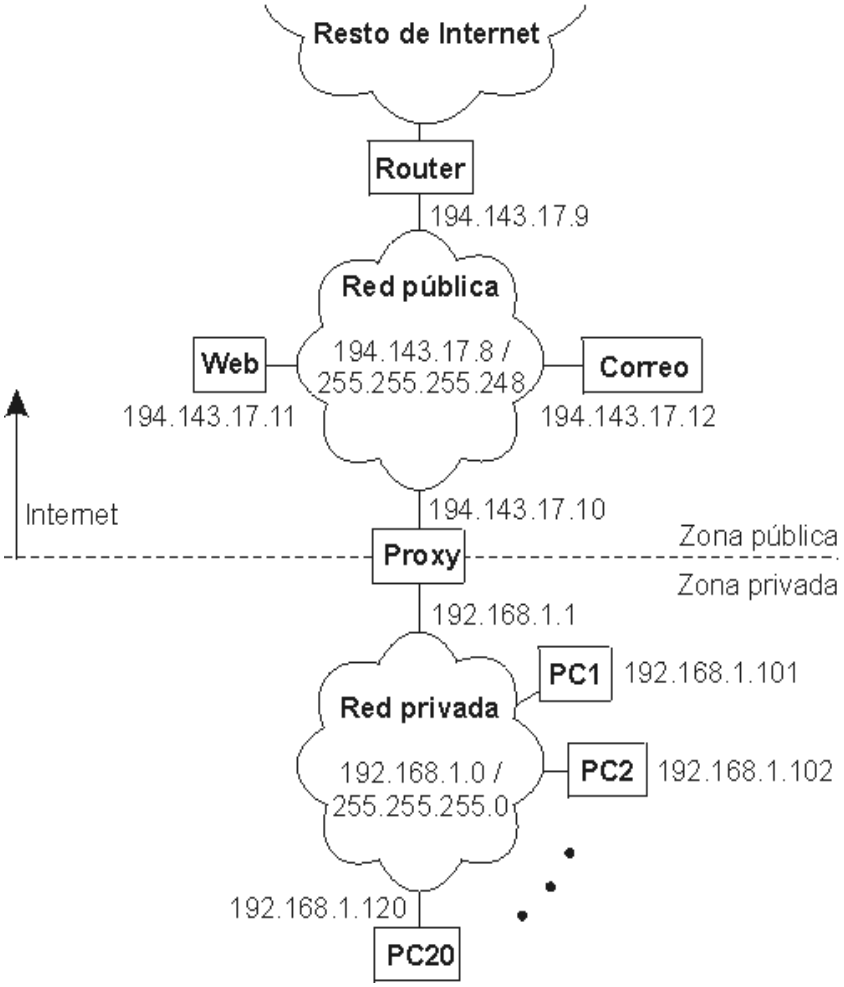
Muchas Intranet´s se ven en la necesidad de conectarse a los que se denomina “sistemas patrimoniales”; es decir, el hardware y las bases de datos que fueron creadas antes de construir la red.

Generalmente, los denominados sistemas patrimoniales utilizan tecnologías más antiguas y no basadas en los protocolos TCP/IP de las Intranet´s. Existen diversos modos en que las Intranet´s se pueden unir a sistemas patrimoniales; uno de los más comunes es el usar los guiones CGI para acceder a la información de las bases de datos y colocar esta información en texto HTML formateado; esto lo hace asequible a un navegador de Web.

3.3 Protocolos de Intranet

Como se ha mencionado, una Intranet es una red privada derivada de Internet y maneja sus características y también los protocolos TCP/IP. Esta red puede o no, tener salida a Internet. En el caso de que sí cuente con ésta, el direccionamiento IP permite la salida de las direcciones privadas, pero impide el acceso desde Internet.

La vista de trabajo de una red Intranet se puede observar en la figura siguiente:



De manera objetiva, la Intranet es una red privada que la tecnología internet utilizó como arquitectura elemental. Una red interna se construye usando los protocolos TCP/IP para la comunicación de internet, los cuales pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable.

El hardware fundamental no es lo que construye la Intranet; en este caso, lo que importa son los protocolos de software.

Con el enorme crecimiento de internet, un gran número de personas en las empresas utilizan internet para:

- Comunicarse con el mundo exterior
- Reunir información
- Hacer negocios

A la gente no le lleva mucho tiempo el reconocer que los componentes que funcionan tan bien en internet, también pueden utilizarse dentro de las empresas, sin perder su valor en funcionamiento y facilidad de manejo. Esta es la razón por la que las redes Intranet se han vuelto muy populares.

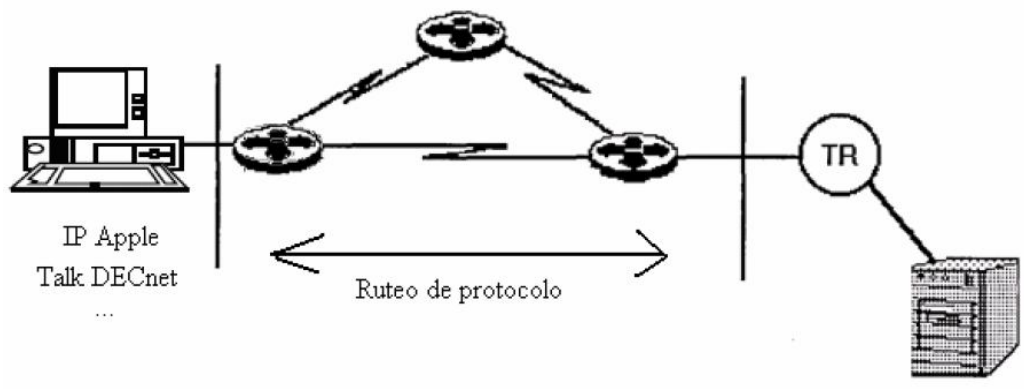
Algunas corporaciones no cuentan con redes TCP/IP, que es el protocolo requerido para acceder a los recursos de internet; en estos casos, la creación de una Intranet en la que toda la información y recursos se puedan usar sin interrupciones, ofrece muchos beneficios.

Las Intranet´s permiten a los usuarios trabajar juntos de un modo sencillo y efectivo. El programa conocido como trabajo en grupo, es una parte importante de las redes internas; puesto que permite:

- Colaborar en proyectos
- Compartir información de manera segura
- Llevar a cabo conferencias visuales
- Establecer procedimientos seguros para el trabajo de producción

El software del servidor y del cliente gratuito y la multitud de servicios como los grupos de noticias, estimulan a la expansión de internet. La consecuencia de ese crecimiento marcó la pauta para el desarrollo de las redes Intranet.

Para tener una idea de lo anteriormente descrito, en la siguiente figura se muestran los protocolos de internet utilizados por una Intranet:



3.3.1 Funcionamiento de TCP/IP e IPX en Intranet

Lo que distingue a una Intranet de cualquier otro tipo de red privada es el hecho de que se basa en TCP/IP; es decir, utiliza los mismos protocolos que se usan en internet.

TCP/IP se refiere a los dos protocolos que trabajan juntos para transmitir datos: El protocolo de control de transmisión (TCP) y el protocolo de internet (IP).

Cuando se envía información a través de una Intranet, los datos se fragmentan en pequeños paquetes.los paquetes llegan a su destino, y se vuelven a fusionar en su forma original.

El protocolo de control de transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El protocolo de internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

En algunas empresas, puede haber una mezcla de Intranet´s basadas en TCP/IP y redes basadas en otra tecnología (como Netware, por ejemplo). En este caso, la tecnología TCP/IP de una Intranet se puede utilizar como intermediario para enviar datos entre Netware y otras redes, utilizando una técnica llamada IP canalizado.

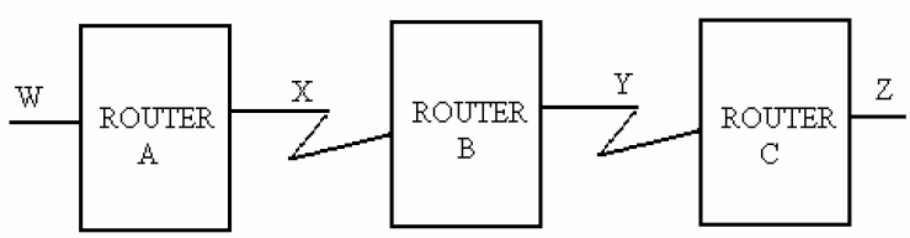
Las redes Netware usan el protocolo IPX (intercambio de paquetes en internet) como medio de entregar datos.

Los datos enviados dentro de una Intranet deben separarse en paquetes menores de 1500 caracteres. TCP divide los datos en paquetes. A medida que crea cada paquete, calcula y añade un número de control a estos. El número de control se basa en los valores de los bytes; es decir, en la cantidad exacta de datos contenidos en el paquete.

Cada paquete, junto al número de control, es colocado en envases IP separados. Estos envases contienen información que detalla exactamente donde se van a enviar los datos dentro de la Intranet o de internet. Todos los envases de una clase de datos determinada, tienen la misma información de direccionamiento; de esta forma, se pueden enviar a la misma localización con el fin de reagruparse.

Los paquetes viajan entre redes Intranet´s gracias a enrutadores de Intranet´s. Los enrutadores examinan todos los envases IP y estudian sus direcciones. Estos direccionadores determinan la ruta más eficiente para enviar cada paquete a su destino final.

El trabajo de los enrutadores se muestra en la siguiente figura:



En razón de que el tráfico de una Intranet varía de manera frecuente, los paquetes se pueden enviar por caminos diferentes y pueden llegar desordenados, y puede ocurrir una de dos condiciones posibles:

- Si el enrutador observa que la dirección está localizada dentro de la Intranet, el paquete se puede enviar directamente a su destino o, en su defecto, puede enviarse a otro enrutador.

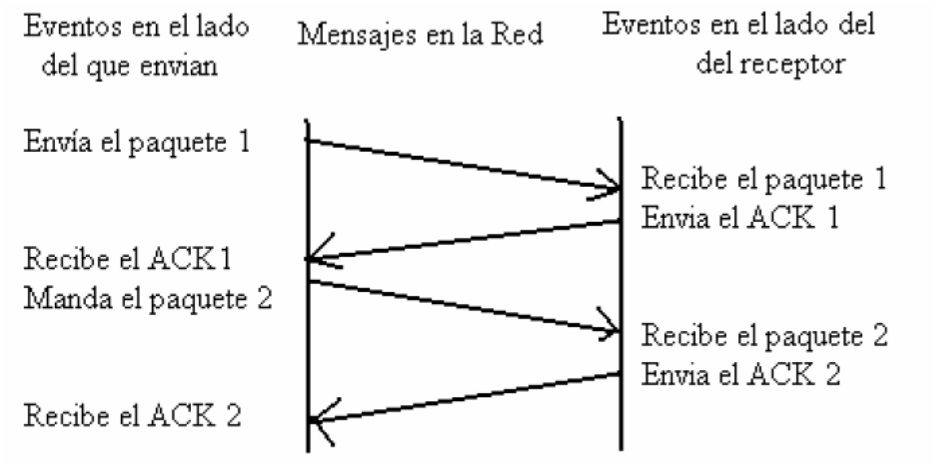
- Si la dirección se localiza fuera de la internet, se enviará a otro enrutador para que se pueda enviar a través de ésta.

A medida que los paquetes llegan a su destino, TCP calcula el número de control para cada uno. Después compara este número de control con el que se ha enviado en el paquete. Si no coinciden, el protocolo TCP sabe que los datos en el paquete se han degradado durante el envío. Posteriormente, descarta el paquete y solicita la retransmisión del paquete original.

TCP incluye la habilidad de comprobar paquetes y determinar que se han recibido todos. Cuando se reciben los paquetes no degradados, TCP los agrupa en su forma original, unificada. La información de cabecera de los paquetes comunica el orden de su colocación.

Una Intranet trata el paquete IP como si fuera otro, y envía el paquete a la red Netware receptora; un servidor TCP/IP Netware abre el paquete IP, y lee el paquete IPX original.

Ahora, puede usar el protocolo IPX para entregar los datos en el destino exacto. La transmisión del mensaje se puede representar en su forma gráfica, de la forma:



3.3.2 Procesamiento de paquetes TCP/IP

Los protocolos como TCP/IP determinan la manera en que las computadoras se comunican entre sí. Estos protocolos funcionan conjuntamente y, si se sitúan por encima de otro en lo que se conoce comúnmente como pila de protocolo. Cada pila de protocolo se diseña para llevar a cabo un propósito especial en la computadora emisora y en la receptora, como se muestra a continuación:

La pila TCP combina las pilas de aplicación, presentación y sesión en una también denominada pila de aplicación.

3.4 Intranet a través del tiempo

Intranet nace hace relativamente poco tiempo; surge de la necesidad de las empresas en la privacidad de su información.

Intranet es una red privada en donde la información que circula puede únicamente ser accedida por el personal registrado y tiene restricciones para usuarios no autorizados.

3.5 Características de Intranet

Uno de los aspectos más destacados de la Intranet es la seguridad de la información. Para que solamente los miembros de una organización puedan acceder a la información, cualquier conexión que no tenga una autorización debe ser automáticamente bloqueada, con el fin de evitar accesos indeseados y/o fuga de información importante.

Así, las características básicas que definen a Intranet son:

- Totalmente basada en Web
- Foros internos de discusión según temáticas.
- Carpetas para todos los temas relevantes.
- Determina códigos de acceso según niveles de seguridad.
- Crea lugares para publicar notas, artículos, opiniones, etcétera.
- El administrador determina a las personas que tienen acceso a la información, previo convenio o instrucción de quien origina ésta.
- Facilita y agiliza la realización de encuestas internas.
- Mantiene políticas específicas de seguridad.
- Calendario personal.
- Agenda de contactos; es decir, base de datos sobre los contactos de la empresa.
- Publica eventos destacados, novedades, etcétera.

3.6 Ventajas de Intranet

Intranet ofrece ciertas ventajas en su manejo, lo que influye en su implantación; entre éstas podemos destacar las siguientes:

- Es una forma muy eficiente y económica de distribuir la información interna, sustituyendo los medios clásicos.
- Fácil adaptación y configuración a la infraestructura tecnológica de la organización, así como gestión y manipulación. Disponible en todas las plataformas informáticas.

- Adaptación a las necesidades de diferentes niveles: Empresas, departamentos, áreas de negocios, etcétera. Centraliza el acceso a la información actualizada de la organización, al mismo tiempo que puede servir para organizar y acceder a la información de la competencia dispuesta en Internet.

- Sencilla integración de multimedia y rápida formación del personal.

- Posibilidad de integración con las bases de datos internas de la organización en particular.

- Acceso a Internet y uso de estándares públicos y abiertos, independientes de empresas externas.

3.7 Desventajas de Intranet

Los principales inconvenientes del uso de una Intranet son:

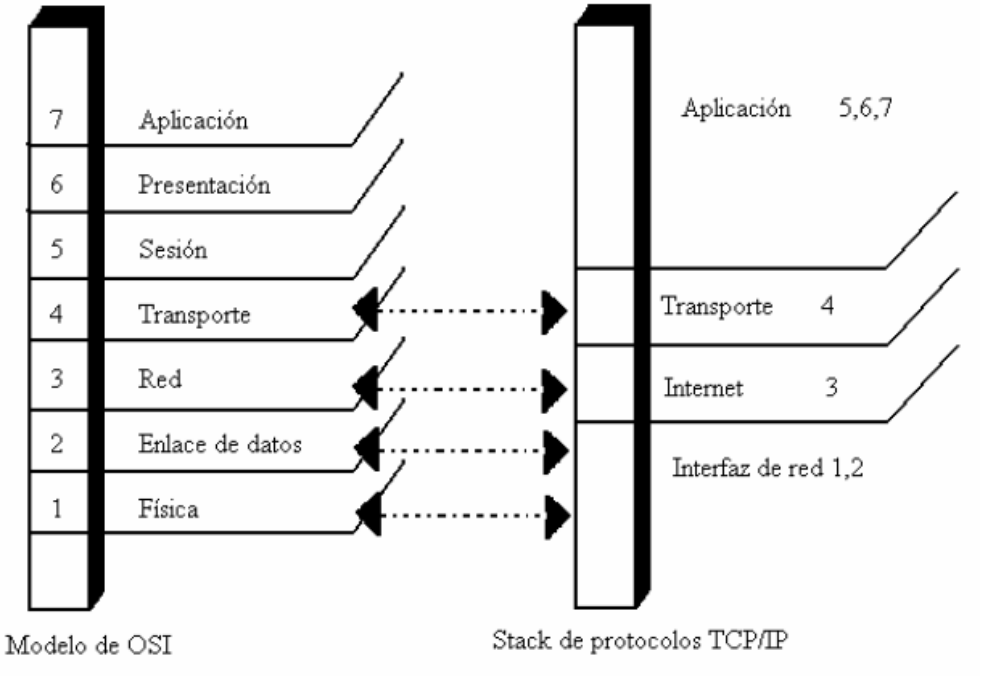
- No se puede poner en marcha si no se conocen las necesidades específicas, tanto de la Intranet como del personal a cargo.

- Las Intranet´s son redes expuestas a notables riesgos de seguridad.

3.7 Modelo OSI para Intranet

La Organización Internacional para la Normalización (ISO), ha creado el modelo de referencia "Interconexión de Sistemas Abiertos" (OSI), el cual describe siete pilas de protocolos para las comunicaciones informáticas. Cada pila es independiente de las demás, por lo que la información contenida en cada una de ellas también lo es.

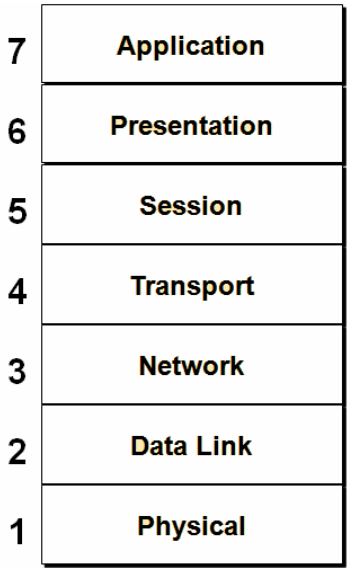
TCP combina las pilas de aplicación, presentación y sesión del modelo OSI en una que también se llama pila de aplicación. Esto se muestra en la siguiente figura:



Dentro de este proceso, se dan las características del envasado que tiene lugar para transmitir datos.

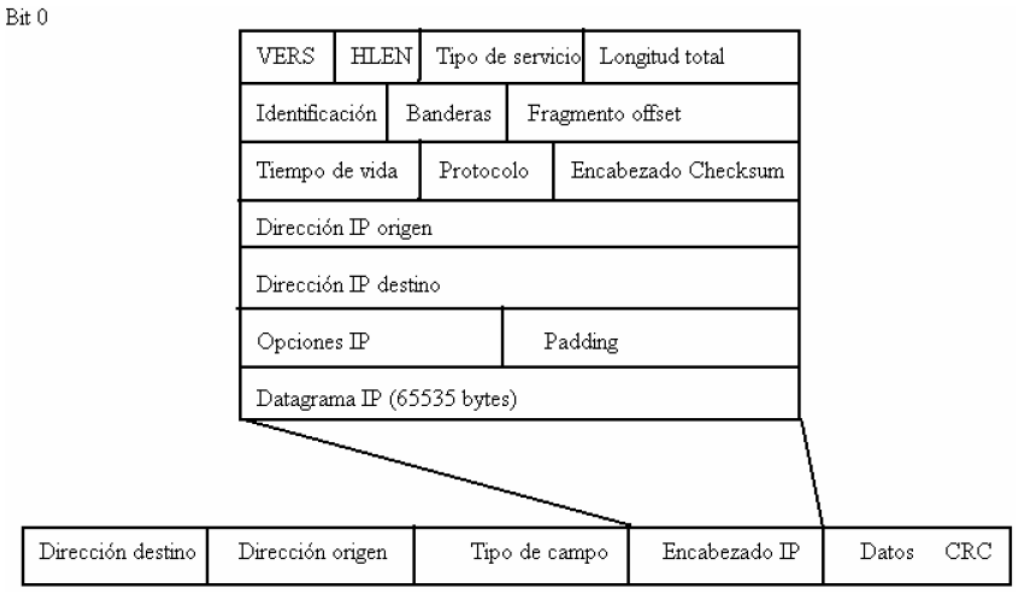
La pila de aplicación TCP formatea los datos que se están enviando para que la pila inferir (la de transporte) los pueda remitir. La pila de aplicación TCP realiza las operaciones equivalentes que llevan a cabo las tres pilas de OSI superiores: Aplicaciones, Presentación, Sesión.

Estas capas se grafican en niveles, de la forma:



La siguiente pila es la de transporte, la cual es responsable de la transferencia de datos y asegura que los datos enviados y recibidos son, de hecho, los mismos; es decir, que no han surgido errores durante el envío. TCP divide los datos que obtiene de la pila de aplicación en segmento. También, agrega una cabecera que contiene información que será utilizada cuando se reciban los datos, con el fin de garantizar que no han sido alterados en el proceso.

La tercera pila prepara los datos para la entrega introduciéndolos en datagramas IP, y determinando la dirección exacta para estos. El protocolo IP trabaja en la pila de internet; coloca un envase IP con una cabecera en cada segmento. La cabecera IP incluye información específica. Una graficación del datagrama se muestra a continuación, junto con el encabezado general IP:



En este punto, se añade un orden secuencial porque el datagrama podría sobrepasar posiblemente el tamaño permitido a los paquetes de red y, de esta manera, necesitaría dividirse en paquetes más pequeños. En este sentido, el incluir el orden secuencial les permitirá volver a combinarse de forma apropiada.

3.9 Funcionamiento de puentes o bridges

Los puentes son combinaciones de hardware y software que conectan distintas partes de una red, como las diferentes secciones de una Intranet. Conectan redes de área local (LAN´s) entre ellas. No obstante, no se utilizan generalmente para conectar redes enteras entre ellas. Por ejemplo:

- Para conectar una Intranet con internet
- Para conectar una Intranet con otra Intranet
- Para conectar una subred completa con otra.

Para ello, se utilizan piezas de tecnología más sofisticada, lo que se conoce como enrutadores.

Cuando hay una gran cantidad de tráfico en una red, los paquetes pueden chocar entre ellos, reduciendo la eficacia de la red, y atrasando el tráfico de la red; en este caso, los paquetes pueden colisionar entre todas las estaciones de trabajo conectadas.

Para reducir el riesgo y/o la cantidad de colisiones, una red se puede subdividir en dos o más redes. Los puentes se usan para enlazar dichas subredes.

Cada paquete de datos en una Intranet posee más información que la de IP. También incluye información de direccionamiento requerida para otra arquitectura de red básica. Los puentes comprueban esta información de la red externa y entregan el paquete en la dirección exacta en una LAN.

Los puentes consultan una tabla de aprendizaje que contiene las direcciones de todos los nodos de la red. Si un puente descubre que un paquete pertenece a su red LAN, mantiene el paquete en ella. Si descubre que la estación de trabajo está en otra red de área local, envía el paquete. El puente se encarga de actualizar constantemente la tabla de aprendizaje a medida que controla y encamina el tráfico.

Los puentes pueden conectar redes de área local de varias formas diferentes. Éstos, se combinan algunas veces con enrutadores en un compuesto denominado Brouter, el cual, ejecuta las tareas de ambos de manera inteligente y automatizada.

3.10 Funcionamiento de los enrutadores

Los enrutadores son los guardias de tráfico de las Intranet´s. Se aseguran que de que todos los datos se envíen a donde se supone que tienen que ir y de que lo hagan por la ruta más eficaz. Los enrutadores son también herramientas útiles para sacar el mejor rendimiento de la Intranet. Se emplean para desviar el tráfico y ofrecer rutas. Utilizan la encapsulación para permitir el envío de los distintos protocolos a través de redes incompatibles.

Los enrutadores abren el paquete IP para leer la dirección de destino, calcular la mejor ruta y después enviar el paquete hacia el destino final. El enrutador considera factores como la congestión de tráfico y el número de saltos.

Los enrutadores tienen dos o más puertos físicos:

- Puertos de recepción o de entrada
- Puertos de envío o de salida

Aunque, por lo regular, cada puerto es bidireccional y puede recibir o enviar datos. Cuando se recibe un paquete en un puerto de entrada, se ejecuta una rutina de software denominada proceso de encaminamiento; este proceso investiga la información de cabecera en el paquete IP y encuentra la dirección a la que se están enviando los datos.

Posteriormente, compara esta dirección con una base de datos llamada tabla de encaminamiento, la cual posee información detallando a qué puertos deberían enviarse los paquetes con varias direcciones IP.

Con base en lo que se encuentra en la tabla de encaminamiento, envía el paquete en un puerto de salida específico. Este puerto de salida envía después los datos al siguiente enrutador o al destino.

3.10.1 Tablas de encaminamiento

Las tablas de encaminamiento pueden ser:

- Estáticas
- Dinámicas

Una tabla de encaminamiento estático permite a un administrador de Intranet´s añadir o eliminar entradas en ésta.

Las tablas de encaminamiento dinámico son las más sofisticadas. Deben usarse cuando hay más de una manera para enviar datos desde un enrutador al destino final, y en Intranet´s más complejas. Estas tablas cambian constantemente a medida que varía el tráfico de la red y las condiciones; de tal manera que siempre encaminan datos del modo más eficiente posible, teniendo en cuenta el estado actual del tráfico de la Intranet.

3.10.2 Protocolos de encaminamiento

El protocolo de encaminamiento más común que realiza los cálculos, se conoce como RIP (protocolo de información de encaminamiento).

Cuando RIP determina la ruta más eficaz para enviar los datos por el camino con el menor número de saltos, asume que cuantos menos saltos haya, más eficaz un número de saltos mayor a 16, descartará la ruta.

Por otro lado, el protocolo de pasarela exterior (EGP) se usa en internet, en donde se puede tener que atravesar muchos más enrutadores antes de que un paquete alcance su destino final. El factor a tener en cuenta sobre Intranet´s y tecnología de encaminamiento, es que no existe una única relación entre ellas, puesto que existe una gran diversidad de tecnologías de encaminamiento, y que su uso depende de las necesidades particulares de la red.

En este sentido, algunas de las partes de una red pueden requerir de encaminamiento estático, mientras que otras partes pueden necesitar tablas de encaminamiento dinámico.

3.11 Correo electrónico en redes Intranet

Uno de los servicios más comunes dentro y fuera de las organizaciones, es sin duda el correo electrónico o e-mail, que es un medio de comunicación "informal" aunque sumamente útil; se utiliza en la transferencia de información entre usuarios de una red, y entre usuarios de la misma empresa u organización, pero en distintas redes.

3.11.1 Correo electrónico interno de Intranet

Probablemente, la parte más utilizada dentro de una red Intranet no son las bases de datos ni las páginas Web ostentosas o contenidos de multimedia, que si bien son servicios muy solicitados y pueden ser imprescindibles, lo que generalmente busca el usuario es la facilidad de uso y la estandarización en cuanto a conocimientos en la aplicación.

El servicio más utilizado es el correo electrónico. Las Intranet´s empresariales pueden utilizar diferentes versiones de éste; tales como:

- Mail
- Microsoft mail
- Lotus notes
- Etcétera

La arquitectura más común que sirve de base al uso de e-mail de las redes internas es el llamado Protocolo simple de transferencia por correo, o SMTP. SMTP se utiliza para repartir correo dentro de una Intranet.

Como ocurre con muchas de las aplicaciones en Intranet y de internet, SMTP utiliza una arquitectura cliente/servidor. Cuando alguien quiere crear un mensaje, usa un agente usuario de correo o agente usuario (MUA o UA), que es software cliente que se ejecuta en un ordenador para crear un fragmento de correo electrónico.

Después de finalizar el mensaje, el MUA lo nada a un programa que se está ejecutando en un servidor llamado agente de transferencia de correo (MTA), el cual, examina la dirección del receptor del mensaje, y lo manda al destinatario dentro de la red Intranet o al destinatario externo, a través de internet.

Por supuesto, existen otras muchas formas de manejar el e-mail, y diferentes protocolos para ayudar en la comunicación.

3.11.2 Correo electrónico entre redes Intranet´s

Frecuentemente, un e-mail creado en una Intranet, no se entregará a una computadora de la misma red, sino a alguien externo a ella, que puede ser:

- En internet
- En otra Intranet
- En un servidor en línea

Los pasos para enviar un mensaje desde Intranet a un agente externo son:

1. Un mensaje e-mail se crea usando SMTP. Como ocurre con toda la información enviada a través de Internet, el mensaje es dividido por el Protocolo TCP de Internet en paquetes IP. La dirección la examina el agente de transferencia de correo de la Intranet. Si la dirección se encuentra en otra red, el agente de transferencia de correo enviará el correo a través de la Intranet mediante enrutadores al agente de transferencia de correo en la red receptora.

2. Antes de que se pueda enviar el correo a través de Internet, puede que primero tenga que atravesar un firewall, una computadora que protege a la Intranet para que los intrusos no puedan acceder a ella. El firewall sigue la pista de los mensajes y los datos que entran y salen de la Intranet.

3. El mensaje deja la Intranet y se envía a un enrutador Internet. El enrutador examina la dirección, determina dónde debería mandarse el mensaje, y después lo pone en camino.

4. La red receptora obtiene el mensaje e-mail. Aquí utiliza una pasarela para convertir los paquetes IP en un mensaje completo. Después la pasarela traduce el mensaje al protocolo particular que emplea la red (como el formato de correo de Compu-Serve), y lo pone en camino. Puede que el mensaje también tenga que atravesar un firewall en la red receptora.

5. La red receptora examina la dirección e-mail y envía el mensaje al buzón específico donde el mensaje está destinado a ir, o emplea el Protocolo de Oficina de Correo (POP) para entregarlo a un servidor de correo.

6. Las pasarelas realmente pueden modificar los datos (si se necesita) para la conectividad. Para el e-mail, puede convertir el protocolo Compu-Serve en SMTP. Las pasarelas también se utilizan para conectar PC con sistemas centrales IBM, por ejemplo, ASCII con EBCDIC.

3.12 Funcionamiento de Intranet

El centro de una Intranet es la World Wide Web. Las Intranet´s están basadas en las arquitectura cliente/servidor. El software cliente es un navegador para Web que se ejecuta en una computadora local; y el software servidor es una Intranet anfitriona. El software cliente está disponible para:

- PC (computadora personal)
- Macintosh
- Estaciones de trabajo UNIX

El software servidor se ejecuta en:

- UNIX
- Windows NT
- Otros sistemas operativos

El software cliente y el software servidor son independientes y no necesitan ejecutarse juntos ni en el mismo sistema operativo.

Cuando los navegadores se ponen en marcha, visitarán una cierta localización predeterminada. En una Intranet, esta localizaciones una página Web; sea ésta departamental o por toda la compañía.

Debido a que las Intranet´s suelen construirse usando cables de alta velocidad y todo el tráfico interno se conduce por ellos, la conexión internet puede ser mucho más lenta debido al tráfico de internet, y porque puede haber varias conexiones de baja velocidad que la petición desde la Intranet deberá atravesar. Los paquetes que componen la petición se encaminan hacia un enrutador de la internet, que envía en turnos la petición al servidor Web.

3.12.1 Servidores de dominio (URL)

Los URL son servidores de dominio, los cuales constan de varias partes:

- http:// . detalla qué protocolo Internet se debe de usar.

- www.znet.com varía en longitud e identifica el servidor Web con el que se debe contactar.

- Una parte final que identifica en directorio específico en el servidor y una página inicial, documento u otro objeto de internet o de la Intranet.

Algunos puntos interesantes de mencionar del proceso, son los siguientes:

- Cuando hay que conectar con un URL en particular, la dirección con el URL debe ser igual que la dirección IP verdadera. Web irá primero a un servidor DNS local en la Intranet de la empresa para obtener esta información si la dirección IP es local, el servidor DNS podrá resolver el URL con la dirección IP. Este enviará la dirección IP auténtica a tu computadora.

- Tu navegador para Web tiene ahora la dirección IP verdadera del lugar que estás intentando localizar. Utiliza esa dirección IP y contacta con el sitio. El sitio te envía la información que has solicitado.

- Si la información que has solicitado no está en tu Intranet, y si tu servidor DBS local no tiene la dirección IP, el servidor DNS de Intranet´s debe obtener la información desde un servidor DNS en Internet. El servidor DNS de Intranet´s contacta con lo que se denomina servidor de dominio raíz, que se mantiene por un grupo llamado InterNiC. EL servidor raíz de dominio le dice al servidor de Intranet´s qué servidor primario de nombres y qué servidor secundario de nombres tiene la información sobre el URL solicitado.

- El servidor de Intranet´s contacta ahora con el servidor primario de nombres. Si la información no se puede encontrar en el servidor primario de nombres, el servidor DNS de Intranet´s contacta con el servidor secundario. Uno de esos servidores de nombres tendrá la información exacta. Después devolverá la información al servidor DNS de Intranet´s.

- El servidor DNS de Intranet´s te devuelve la información, tu navegador para Web usa ahora la dirección IP para contactar con el sitio exacto.

Cuando alguien en una Intranet quiere contactar con una localización, por ejemplo, visitar un sitio Web, escribirá una dirección, como www.metahouse.com.

Aunque de hecho, Internet no utiliza realmente estas direcciones alfanuméricas. En lugar de eso, emplea direcciones IP, que son direcciones numéricas, en cuatro números de 8 bits separados por puntos, como 123.5.56.255.

Un servidor DNS, llamado también un servidor de nombres, empareja, direcciones alfanuméricas con sus direcciones IP, y te permite contactar con la localización exacta.

3.12.2 Java

Al usar Java, los programadores pueden vincular datos corporativos desde una Intranet, permitiendo el uso de sistemas patrimoniales como bases de datos. Los programadores, editores y artistas pueden también utilizar Java para crear programación multimedia.

Además, Java será capaz de crear programas personalizados de Intranet´s de todo tipo desde informática para grupos de trabajo a comercio electrónico.

Java es similar al lenguaje informático C++, y está orientado a objetos, lo que significa que se pueden crear programas usando muchos componentes preexistentes, en lugar de tener que escribir todo el programa desde el principio. Esto será una gran ayuda para las Intranet´s, puesto que permitirá a los programadores de la empresa compartir los componentes y de ese modo construir aplicaciones personalizadas mucho más rápido.

Java es un lenguaje compilado, lo que significa que después de ser escrito el programa, éste debe ejecutarse a través de un compilador para transformarlo en un lenguaje que pueda entender la computadora.

En otros lenguajes compilados, los compiladores específicos de la computadora crean un código ejecutable distinto para todos los computadores diferentes en los que se puede ejecutar el programa.

Por el contrario, en Java se crea una sola versión compilada del programa llamada: código de bytes Java. Los intérpretes en los distintos computadores entienden el código de bytes Java y ejecutan el programa. De este modo, un programa Java se puede crear una vez, y usarse después en muchos tipos diferentes de computadora. Los programas Java diseñados para ejecutarse dentro un navegador para Web se denominan apliques.

Los apliques son un subconjunto de Java y por razones de seguridad no pueden leer o escribir archivos locales, mientras que Java lo puede hacer. Los navegadores que admiten Java posen intérpretes del código de bytes Java.

Después de que un aplique Java está compilado en códigos de bytes, se copia en un servidor Web de Intranet´s y el enlace necesario se introduce en HTML.

Cuando alguien en una Intranet visita una página inicial con un aplique Java en ella, éste se recibe automáticamente en su computadora; es decir, no espera la invitación. Por eso hay tanta preocupación por los virus que se están incrustando en los apliques.

Puesto que los apliques Java son programas que se pueden ejecutar en cualquier ordenador, podrían ser portadores de un virus como cualquier otro programa informático. Para asegurar la no infección al recibir un aplique, éste pasa primero a través de la verificación. Sin embargo, los apliques no se pueden leer o escribir en archivos locales que están normalmente involucrados en ataques víricos, así que esto debería reducir substanciales el riesgo de infección.

Después de que los códigos de bytes se hayan verificado, el intérprete Java en el navegador los introduce en un área restringida de la memoria del ordenador y los ejecuta. Se toman medidas adicionales para que ningún virus pueda perjudicarle.

Java tiene Interfaces para Programas de Aplicación (API) y otro tipo de software "enganchado" para permitir a los programadores de Intranet´s integrar más fácilmente programas de Intranet´s como los navegadores para Web en bases de datos y redes corporativas existentes.

3.12.3 Conversiones IPX en Intranet

La mayoría de las Intranet´s no están construidas desde cero. Muchas son redes existentes, como Novell Netware, que tienen que convertirse en una Intranet. A menudo, el primer paso en el movimiento hacia una Intranet puede introducirse en la propia red existente. Después, la tecnología de Intranet´s puede introducirse en la propia red y convertirse en una Intranet.

Cuando una computadora en la red quiere conectar con Internet y solicitar información de ella, se envía una petición a un navegador en la Intranet. Este navegador enviará la petición al destino exacto en Internet. En la red Netware, el sistema operativo Netware se utiliza para manejar el tráfico de la red y la administración. Como método para encaminar paquetes a través de la red, Netware emplea al protocolo IPX (Intercambio de Paquetes Internet).

Aunque IPX se denomina intercambio de paquetes Internet, no ofrece realmente acceso a Internet o transporta la información de Internet. Las estaciones de trabajo pertenecientes a la red Netware, y los servidores en la red, necesitan tener cargado IPX en la memoria para usar la red.

Para que las estaciones de trabajo en la red Novell consiga acceder a Internet o a la Intranet, necesitan ejecutar los protocolos TCP/IP que forman la base de Internet. Para hacer eso, debe instalarse una pila TCP/IP en cada computadora que permitirá la entrada a la Intranet. Esto significa que cada computadora tendrá instalado IPX y una pila TCP/IP, para permitir el acceso a Internet y a la red Ethernet.

Básicamente, esto da como resultado "RAM de bote en bote" y es uno de los dolores de cabeza más fuertes para cualquiera que intente ejecutar ambas pilas de protocolos. Una unidad de servicio de canal/Unidad de Servicio de Datos (CSU/DSU) realiza la conexión física entre el enrutador de la Intranet y el Proveedor de Servicio Internet (IPS).

EL ISP ofrece la autentica conexión Internet y servicios. Varias líneas digitales pueden conectar la CSU/DSU con el ISP, incluyendo una línea alquilada de 56 Kbps, una línea T1 de alta velocidad, o incluso una líneat3 de mayor velocidad.

La información solicitada se devuelve a través del CSU/DSU y del enrutador, y después se encamina a la computadora que pidió la información. Si la información está ubicada en una Intranet dentro de la compañía, el enrutador enviará la petición al anfitrión exacto, que después devolverá la información al solicitante. Algunos productos como Netware/IP permitirán a las computadoras acceder a servicios de Netware y a Internet. Esto significa que no tienen que ejecutar los protocolos IPX y TCP/IP, eliminando los problemas de memoria producidos por las múltiples pilas.

3.13 Subdivisión de redes Intranet

Cuando las Intranet´s sobrepasan un cierto tamaño, o se extienden por varias localizaciones geográficas, empiezan a ser difícil manejarlas como una sola red. Para resolver el problema, la Intranet se puede subdividir en varias subredes, subsecciones de una Intranet que las hacen más fáciles de administrar. Para el mundo exterior, la Intranet aparece todavía como su fuera una sola red.

Cuando una Intranet se conecta con Internet, un enrutador realiza el trabajo de enviar los paquetes desde Internet a la Intranet.

Cuando las Intranet´s crecen, se necesita algún método para manejar el tráfico de red. Puede ser poco práctico y físicamente imposible encaminar todos los datos necesarios entre muchas computadoras diferentes extendidos por un edificio o por el mundo. Se necesita crear una segunda red denominada subred de trabajo o subred.

Para tener un enrutador que dirija todo el tráfico de entrada para un Intranet subdividida, se utiliza el primer byte del campo de la hostid. Los bits que se usan para distinguir subredes se llaman números de subred.

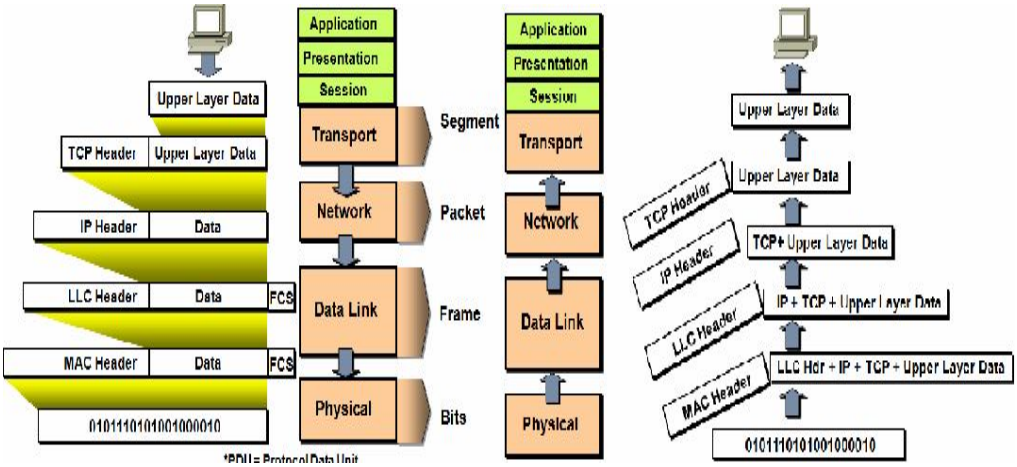
Cada computadora en cada subred recibe su propia dirección IP, como en una Intranet normal. La combinación del campo de la hostid, el número de subred, y un número de anfitrión, forman la dirección IP.

El enrutador debe ir informado de que el campo de la hostid en las subredes tienen que tratarse de modo diferente que los campos de la hostid no subdivididos, si no en así, no podrá encaminar adecuadamente los datos.

Para hacer esto, se emplea una mascara de subred. Una máscara de Subred es un número de 32 bits como 255.255.0.0, que se utiliza conjuntamente con los números en el campo de la hostid.

Cuando se efectúa un cálculo usando la máscara de subred y la dirección IP, el enrutador sabe donde encamina el correo. La máscara de subred está incluida en los archivos de configuración de la red de los usuarios.

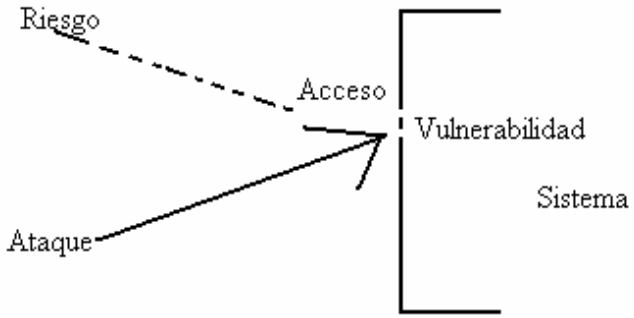
SEGURIDAD EN COMUNICACIÓN PRIVADA



4.1 Conceptos importantes

En materia de informática, la seguridad se define como el tomar las medidas necesarias para lograr que los equipos y los datos almacenados en ellos estén a salvo de daños y/o accesos no autorizados.

Es importante mencionar que todos los sistemas son vulnerables; es decir, están expuestos a riesgos y ataques, como lo muestra la siguiente figura:



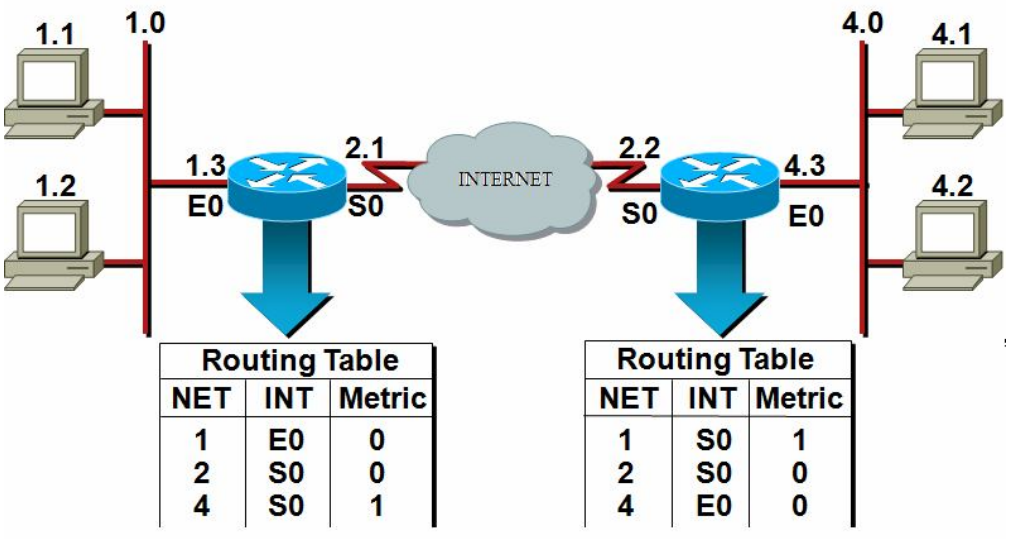
En una red de equipos, la seguridad consiste en definir una contraseña sobre un recurso, como un directorio, que es compartido en la red.

Todos los usuarios de una red de trabajo en grupo definen su propia seguridad, y puede haber recursos compartidos en cualquier equipo, en lugar de únicamente en un servidor centralizado. Esta falta de control implica un gran impacto en la seguridad de la red, ya que puede que algunos usuarios no implementen ninguna medida de seguridad.

Si la seguridad es importante, es recomendable utilizar una red basada en servidor.

4.2 Seguridad en las redes Intranet´s

Cualquier Intranet es vulnerable a los ataques de personas que tengan el propósito de destruir o de robar los datos empresariales. La naturaleza abierta y sin límites de la Internet y los protocolos TCP/IP, exponen a una empresa a este tipo de ataques. Lo anterior se muestra en la figura siguiente:



Por ello, las Intranet´s requieren de varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionen:

- El control del tráfico
- La encripción o encriptación de los datos
- Las contraseñas para convalidar usuarios
- Las herramientas del software para evitar y curar virus
- Las herramientas para el bloqueo de sitios indeseables

El término técnico genérico para denominar a una línea de defensa contra intrusos, recibe el nombre de firewall; éste, es una combinación de hardware y de software que controla el tipo de servicios permitidos hacia y/o desde la Intranet.

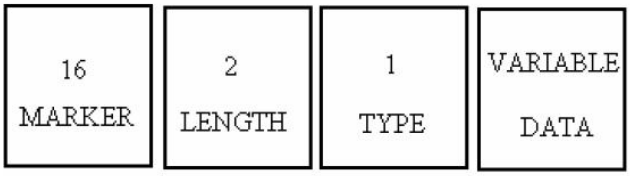
Los servidores sustitutos son otra herramienta de uso común para construir un firewall. Un servidor del tipo sustituto, permite a los administradores de sistemas seguir la pista de todo el tráfico que circula en la Intranet; ya sea que entre o que salga.

Básicamente, un firewall es un servidor bastión que configura para oponerse y evitar el acceso a los servicios no autorizados. Generalmente, se encuentra aislado del resto de la Intranet, en su propia subred de perímetro. De este modo, si el servidor es, de alguna forma, atacado, el resto de la red no estará en peligro.

Los sistemas de autenticación son una parte muy importante en el diseño de la seguridad de cualquier red Intranet. Éstos se emplean para asegurar que a cualquiera de sus recursos acceda sólo la persona con acceso autorizado. Estos sistemas utilizan, generalmente:

- Nombres de usuario
- Contraseñas
- Sistemas de encriptación.

El encabezado para la autenticación tiene una cabecera específica, la cual se muestra en la siguiente figura:



Marker: contiene información de autenticación del mensaje del receptor.

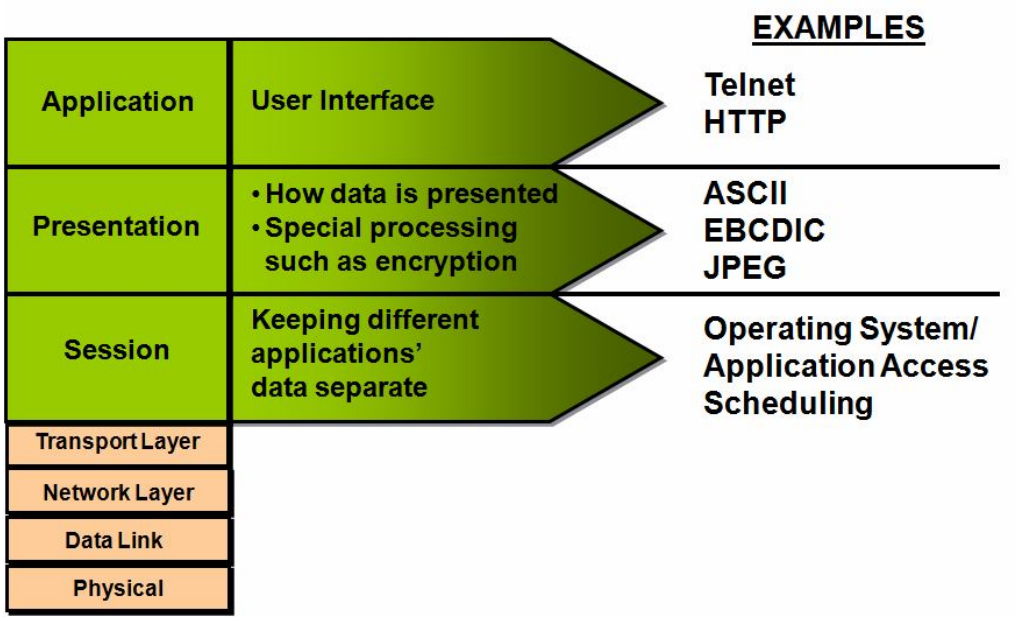
Lenght: longitud total del mensaje en bytes

Type: el tipo de mensaje: Open, Update, Notification, Keep-alive

Data: Información para las capas superiores. Este campo es opcional

El software para el bloqueo de sitios basados en el servidor, puede prohibir a los usuarios de una Intranet la obtención de materiales indeseables.

El software de control rastrea donde ha ido la gente y qué servicios han utilizado (http, para el acceso a la Web, por ejemplo).por otro lado, el software para detectar virus basado en el servidor puede comprobar cualquier archivo que entra en la Intranet para asegurarse de que esté libre de virus. Este servicio se enmarca en la siguiente figura:



Una manera de asegurarse de que las personas no autorizadas o los datos erróneos no puedan accede a la Intranet, es el uso de un enrutador para filtrar. Éste es un tipo especial de enrutador que examina la dirección IP y la información de cabecera de cada paquete que entra en la Intranet; y solamente permite el acceso a aquellos paquetes que tengan direcciones u otros datos, como el correo electrónico, que el administrador del sistema ha decidido previamente que pueden acceder a la red Intranet.

4.2.1 Enrutadores para filtrar

Los enrutadores para filtrar, son denominados generalmente como enrutadores de selección, y son la primera línea de defensa contra ataques a la Intranet. Los enrutadores para filtrar, examinan cada paquete que se mueve entre redes en una Intranet.

Un administrador de Intranet establece las reglas que utilizan los enrutadores para tomas decisiones sobre los paquetes que deben ser admitidos y los que han de ser denegados para la red.

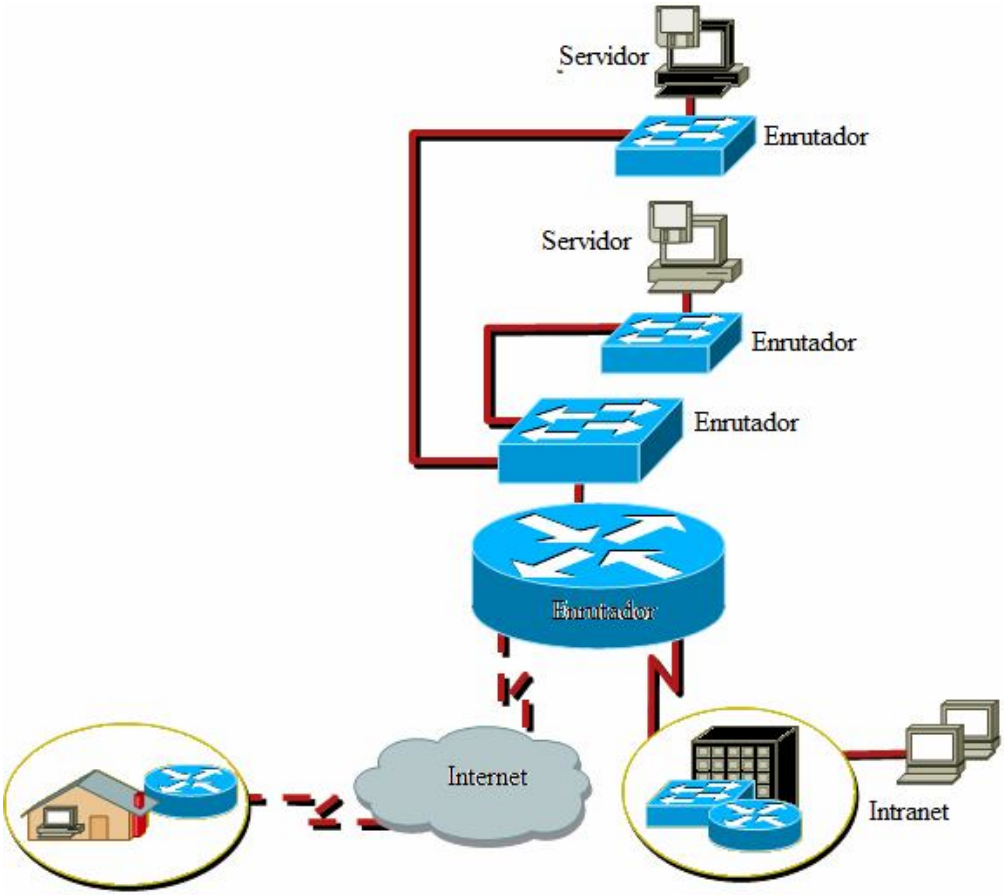
Las distintas reglas se pueden establecer para paquetes que entran y que salen, de manera que los usuarios de la red Intranet puedan acceder a los servicios de Internet; mientras que, al mismo tiempo, cualquiera en Internet tendría prohibido el acceso a ciertos datos y servicios de la Intranet.

Los enrutadores para filtrar pueden llevar un registro sobre la actividad de filtración. Comúnmente, siguen la pista a los paquetes sin permiso para pasar entre la red Internet y la Intranet, que indicarán la medida en que una Intranet ha estado expuesta al ataque externo, que puede ser local o remoto.

Las direcciones de origen se leen desde la cabecera IP y se comparan con la lista de direcciones de origen en las tablas de filtros. Ciertas direcciones pueden ser conocidas por ser peligrosas y, al estar incluidas en la tabla, permiten al enrutador denegar ese tráfico. El enrutador examina los datos en la cabecera IP que envuelve los datos y la información de cabecera de la pila de transporte. Eso significa que cualquier paquete contendrá datos y dos conjuntos de cabeceras:

- Una cabecera para la pila de transporte
- Una cabecera para la pila de Internet

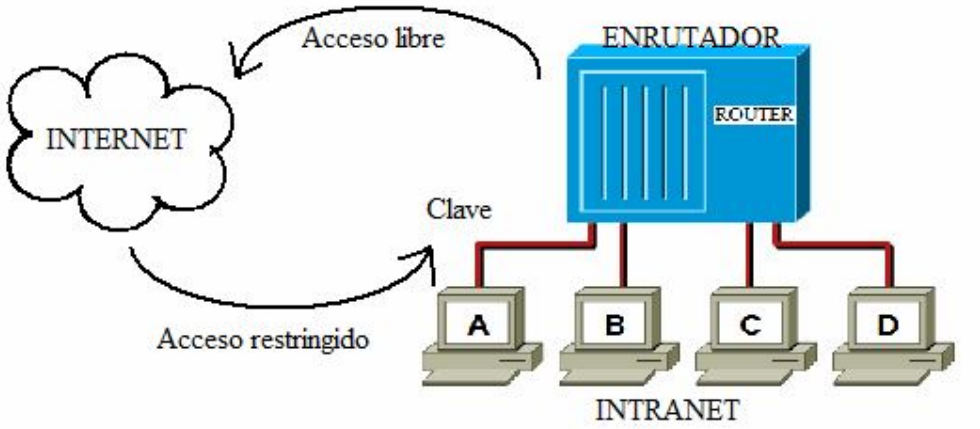
El funcionamiento básico de los enrutadores se muestra en la siguiente figura:



Los enrutadores pueden tener diversos tipos de reglas para las subredes, ya que pueden necesitar distintos niveles de seguridad.

Una subred que contenga información privada y/o competitiva, puede tener muchas restricciones; mientras que una subred de ingeniería puede tener menos restricciones en las actividades que entran o salen de ella.

Un enrutador para filtrar puede permitir a los usuarios tener acceso a servicios como Telnet y FTP, mientras que restringe el uso de Internet de estos servicios para acceder a la Intranet, como lo muestra la siguiente figura:



Esta misma técnica se puede emplear para evitar que los usuarios internos accedan a los datos restringidos de la Intranet. Hay que tomar en cuenta que ciertos tipos de servicios son más importantes que otros.

Trucar direcciones es un método de ataque muy común. Para trucarlas, alguien externo a la Intranet falsifica una dirección de origen de modo que al enrutador le parezca que la dirección de origen es realmente de alguien autorizado, lo que puede ocasionar que los archivos privados puedan ser enviados fuera de la Intranet.

Por ello, se puede establecer una regla que comunique al enrutador examinar la dirección de origen en cada cabecera IP que entre, pero que no salga. Si la dirección de origen es interna, pero el paquete proviene del exterior, el enrutador no admitirá el paquete.

4.2.2 Firewall´s

Los firewall´s protegen a las Intranet´s de los ataques iniciados contra ellas desde Internet. Están diseñados para proteger a una Intranet del acceso no autorizado a la información de una empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a servicios de Internet que puedan ser peligrosos.

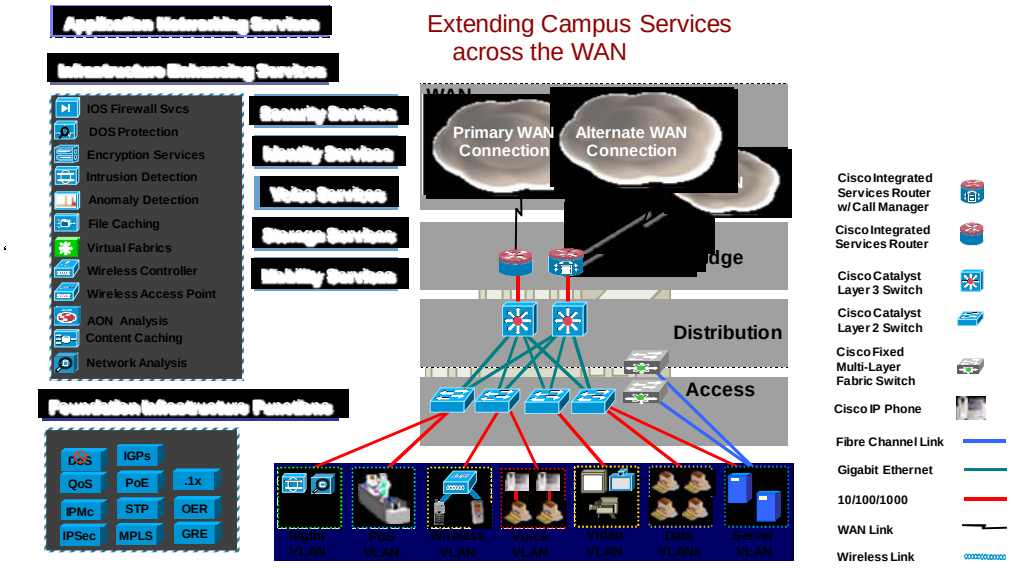
Las computadoras de una Intranet sólo tienen permiso para acceder a Internet después de atravesar un firewall. Las peticiones tienen que traspasar un enrutador interno de selección, el cual evita que el tráfico de paquetes sea interceptado de manera remota. Este enrutador examina la información de todos los paquetes (principalmente, su origen

y su destino); después, compara la información que encuentra con las reglas en una tabla de filtros y, basándose en estas reglas, admite o no, el paquete.

Cuando una Intranet está protegida por un firewall, están disponibles los servicios internos usuales de la red, como:

- Correo electrónico
- Acceso a las bases de datos corporativas
- Acceso a servicios de la red (limitados)
- El uso de programas para el trabajo en grupo

El funcionamiento básico de un firewall se puede graficar de la forma:



Los firewall´s seleccionados de la subred tienen una manera más para proteger la Intranet: un enrutador exterior de selección, también denominado enrutador de acceso. Este enrutador selecciona paquetes entre Internet y la red de perímetro utilizando el mismo tipo de tecnología que el enrutador interior de selección.

Puede seleccionar paquetes basándose en las mismas reglas que aplica el enrutador interior de selección y puede proteger a la red incluso si el enrutador interno llaga a fallar. Sin embargo, el enrutador externo también puede tener reglas adicionales para la selección de paquetes, diseñadas eficazmente para proteger al anfitrión bastión.

Como un modo adicional para proteger a una Intranet del ataque, el anfitrión bastión se coloca en una red de perímetro, una subred, dentro de un firewall. Si el anfitrión bastión estuviera directamente en la Intranet en vez de en una red de perímetro y fuera, el intruso podría obtener acceso a la Intranet.

El anfitrión bastión es el punto de contacto principal para las conexiones provenientes de Internet para todos los servicios, como el correo electrónico, el acceso FTP y cualquier otro tipo de datos o peticiones.

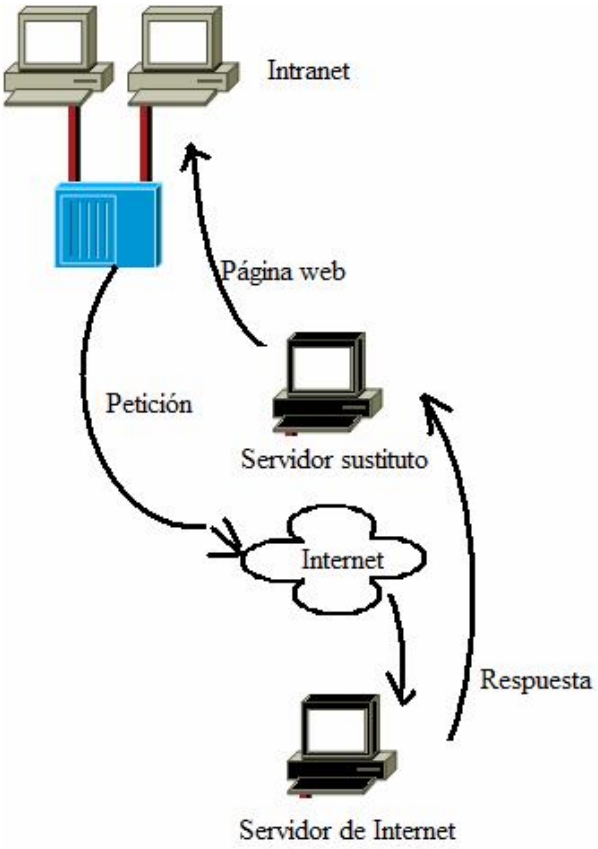
El anfitrión bastión atiende todas estas peticiones, las personas en la Intranet sólo se ponen en contacto con este servidor, y no contactan directamente con otros servidores de Intranet´s. De esta forma, los servidores de Intranet´s están protegidos del ataque. Éstos también pueden configurarse como servidores sustitutos.

4.2.3 Servidores sustitutos

Una parte integral de muchos de los sistemas de seguridad es el servidor sustituto, el cual se coloca en un firewall y actúa como intermediario entre computadoras en una Intranet e Internet. Estos servidores sustituyen al acceso de muchas computadoras en la Intranet; de esta manera, se incrementa la seguridad, puesto que sólo el servidor estará expuesto a Internet.

Los administradores pueden configurar servidores sustitutos que puedan utilizarse para muchos servicios; también pueden decidir el tipo de servicios son admitidos desde Internet. Se necesita software específico del servidor sustituto para cada tipo de servicio de Internet.

Cuando una computadora en la Intranet realiza una petición a Internet, la computadora interna se pone en contacto con el servidor Internet; éste envía la página Web al servidor sustituto, que después la mandará a la computadora de la Intranet. Este proceso se muestra en la figura siguiente:



Los servidores sustitutos registran todo el tráfico entre Internet e Intranet; y pueden anotar:

- Dirección
- Fecha y hora de acceso
- URL
- Número de bytes recibidos
- Etcétera

Esta información se puede utilizar para analizar cualquier ataque iniciado en contra de la red. También puede ayudar a los administradores de las Intranet´s a construir un mejor acceso y servicios para los empleados.

Algunos servidores sustitutos tienen que trabajar con clientes sustitutos especiales. Una tendencia más popular es utilizar clientes con servidores sustitutos ya configurados (Netscape, por ejemplo). Cuando se emplea este paquete ya hecho, debe configurarse de manera especial para trabajar con servidores sustitutos desde el menú de configuración. Hecho esto, el usuario de Intranet utilizará el software como de costumbre. En este caso, el software cliente debe salir hacia un servidor sustituto para obtener datos, en vez de hacerlo hacia Internet.

Los servidores sustitutos también pueden hacer efectivos los diseños de seguridad, tales como:

- Permitir el envío de archivos desde Internet a una computadora de la Intranet.
- Impedir que se manden archivos desde la red empresarial a Internet.
- Impedir que cualquier persona externa a la corporación reciba datos corporativos vitales.
- Evitar que los usuarios de la Intranet reciban archivos que puedan contener virus.

4.2.4 Anfitriones Bastión

Un anfitrión bastión o servidor bastión, es una de las defensas principales en el firewall de una Intranet. Se trata de un servidor fuertemente fortificado que se coloca dentro del firewall, y es el punto de contacto principal entre la Internet y la Intranet. Al tener como punto de contacto principal un servidor aislado y duramente defendido, el resto de los recursos de la Intranet se pueden proteger de los ataques que se inician en Internet.

Los servidores bastión se construyen para que cada servicio posible de la red quede inutilizado una vez dentro de ellos; así, lo único que hace el servidor es permitir el acceso específico de Internet.

Al colocar este tipo de servidor en una red, si son atacados, ningún recurso de la Intranet se pone en peligro.

Los anfitriones bastión registran todas las actividades para que los administradores de Intranet´s puedan determinar si la red ha sido atacada. Normalmente, guardan dos copias de los registros del sistema por razones de seguridad: en caso de que se destruya o falsifique un registro, el otro siempre estará disponible como reserva y para cotejo.

Un modo de guardar una copia segura del registro es conectar el servidor bastión mediante un puerto de serie con una computadora especializada, cuyo único propósito es seguir la pista del registro de reserva.

Los monitores automatizados son programas incluso más sofisticados que el software de auditoría. Comprueban con regularidad los registros del sistema del servidor bastión, y envían una alarma si encuentra un patrón sospechoso.

Algunos servidores bastión incluyen programas de auditoria, que examinan activamente si se ha iniciado un ataque en su contra. Hay varias maneras de hacer una auditoría; la más común es el utilizar un programa de control que compruebe si algún software en el servidor bastión se ha modificado por una persona no autorizada.

El programa de control calcula el número basándose en el tamaño de un programa ejecutable que hay en el servidor. Después calcula con regularidad el número de control

para ver si ha cambiado desde la última vez que lo hizo; si esto sucede, significa que alguien ha alterado el software, lo que puede indicar un ataque externo.

Puede haber más de un servidor bastión en un firewall; y cada uno puede administrar, independientemente, administrar varios servicios de Internet para la Intranet.

4.2.5 Encriptación

Un medio de asegurar una red Intranet es utilizar la encriptación; es decir, el alterar los datos para que sólo alguien con acceso a códigos específicos para descifrar, pueda comprender la información obtenida.

La encriptación se utiliza

- Para almacenar y enviar contraseñas para asegurarse de que ningún entrometido pueda entenderla.
- Cuando se envían datos entre Intranet´s en redes privadas muy seguras (VSPN).
- Para dirigir el comercio en Internet y proteger la información de la tarjeta de crédito durante la transmisión.

Las claves son el centro de la encriptación. Se trata de fórmulas matemáticas complejas (algoritmos) que se utilizan para cifrar y descifrar mensajes. Si alguien cifra un mensaje, sólo otra persona con la clave exacta, será capaz de descifrarlo. Básicamente, hay dos sistemas de claves:

- Criptografía de claves secretas
- Criptografía de claves públicas

El estándar de encriptación de datos (DES) es un sistema de claves secretas (simétrico); no existe componente de clave privada. El emisor y el receptor conocen la palabra secreta del código; sin embargo, este método no es factible para dirigir negocios por Internet.

RSA es un sistema de claves públicas (asimétrico), que utiliza pares de claves para cifrar y descifrar mensajes, cada persona tiene una clave pública, disponible para cualquiera en un anillo de claves públicas; y una clave privada, guardada sólo en la computadora. Los datos cifrados con la clave privada de alguien sólo pueden descifrarse con su clave pública; y los datos cifrados con su clave pública sólo pueden descifrarse con su clave privada; es decir, se complementan.

Por lo tanto, RSA necesita un intercambio de claves públicas; esto se puede realizar sin necesidad de secretos ya que la clave pública es inútil sin la privada.

PGP, privacidad de las buenas, es un programa inventado por Philip Zimmermann, y es un método popular empleado para cifrar datos. Utiliza MD5 (resumen de mensaje 5) y los sistemas cifrados de RSA para generar los pares de claves. Es un programa sumamente extendido que se puede ejecutar en diversas plataformas. También ofrece algunas variaciones de funcionalidad, como la comprensión, que otros sistemas cifrados no brindan. Los pares de claves múltiples se pueden generar y ubicar en anillos de claves públicas y privadas.

4.2.6 Contraseñas y sistemas de autenticación

Una de las primeras líneas de defensa de una Intranet es usar la protección de las contraseñas. Varias técnicas, incluyendo la encriptación, ayudan a asegurarse de que las contraseñas se mantengan a salvo.

También es necesario exigir que las contraseñas se cambien frecuentemente, que no sean fáciles de adivinar o palabras comunes del diccionario, y que no se revelen simplemente. La autenticación es el paso adicional para verificar que la persona que ofrece la contraseña sea la autorizada para hacerlo.

El servidor cifra la contraseña que recibe del usuario, utilizando la misma técnica de encriptación empleada para cifrar la tabla de contraseñas del servidor. Compara la contraseña cifrada del usuario con la contraseña cifrada en la tabla. Si los resultados encajan, el usuario tiene permiso para entrar en el sistema. Si los resultados no encajan, el usuario no tiene permiso.

Las contraseñas de la gente y los nombres de usuario en una Intranet se almacenan dentro de un formulario de tablas de un archivo que se encuentra en un servidor que verifica las contraseñas. A menudo, el nombre del archivo es “password” y el directorio en el que se encuentra es “etc”. Dependiendo de la técnica de autenticación de contraseñas que se use, el archivo puede estar cifrado o no.

Un método para reconocer a un usuario es a través del Protocolo de Autenticación de contraseñas (PAP). PAP no asigna la encriptación, pero la tabla de contraseñas en el servidor está normalmente cifrada. Cuando alguien quiere entrar a la red o a un recurso de la red protegido con una contraseña, se le pide el nombre de usuario y la contraseña. El nombre de usuario y la contraseña se envía después al servidor.

El sistema del Protocolo de Autenticación para Cuestionar el Handshake (CHAP) es un sistema de respuesta. El CHAP requiere una tabla de contraseñas no cifrada. Cuando alguien entra en un sistema con CHAP, el servidor genera una clave al azar que se envía al usuario para que cifre su contraseña.

La computadora del usuario emplea esta clave para cifrar su contraseña. Después la contraseña cifrada se devuelve al servidor. El servidor se remite a la tabla de contraseñas para la clave al azar, y cifra la contraseña con la misma clave que se envió al usuario. El servidor compara después la contraseña cifrada con la del usuario con la contraseña cifrada que creó. Si encajan, el usuario tiene permiso de entrada.

La clave de diferencia de CHAP en que el servidor continúa preguntando a la computadora del usuario a lo largo de la sesión. Además, se envía distintas preguntas que deben ser cifradas y devueltas por la computadora, sin intervención humana. De este modo CHAP limita tu ventana de vulnerabilidad. Una sesión no puede piratearse, puesto que el pirata no sería admitido una vez que la computadora no respondiera correctamente a los desafíos que se suceden periódicamente.

Sin importar qué tipo de sistemas de contraseñas se utilice, ni la tabla de contraseñas está cifrada o no, lo importante es proteger la tabla de contraseñas. El archivo debe protegerse contra el acceso FTP y debería haber acceso restringido al archivo para que sólo el administrador o alguien bajo el control del administrador pueda acceder a él.

4.2.7 Software para examinar virus

Los virus son el mayor riesgo en la seguridad de las Intranet´s. Pueden dañar datos, ocupar y consumir recursos, e interrumpir operaciones. Los archivos de programas eran la principal fuente de problemas en el pasado, pero los nuevos virus de "macro" se pueden esconder en archivos de datos e iniciarse, por ejemplo, cuando se ejecutan una macro en un programa de procesamiento de texto. El software para examinar virus basado en el servidor y el basado en el cliente poseen dispositivos que ayudan a proteger a la Intranet.

Un virus se esconde dentro de un programa. Hasta que se ejecute el programa infectado, el virus, que permanecía inactivo, entonces entra en acción. Algunas veces, lo primero que hará es infectar otros programas del disco duro copiándose en ellos.

Algunos virus colocan mensajes denominados V-marcadores o marcadores de virus dentro de programas que están infectados y ayudan a manejar las actividades víricas. Cada virus tiene un marcador de virus específico asociado con él. Si un virus se encuentra con uno de estos marcadores en otro programa, sabe que el programa ya está infectado y de ese modo no se reproduce allí.

Cuando un virus no encuentra ningún archivo sin marcar en una computadora, eso puede indicar al virus que no hay que infectar más archivos. En este momento, el virus empieza a estropear la computadora y sus datos. Los virus no pueden corromper los archivos de programas o de datos ya que cuando se ejecutan funcionan extrañamente, no funcionan o causan daños. Pueden destruir todos los archivos que la computadora necesita cuando se conecta y provocar otro tipo de averías.

El software para examinar virus se ejecuta en un servidor dentro del firewall de una Intranet. El software no comprueba la posible existencia de virus en cada paquete que entra en la Intranet, ya que eso sería imposible.

En su lugar, sólo comprueba aquellos paquetes enviados con los tipos de servicios y protocolos Internet que indican que un archivo puede encontrarse en el proceso de transferencia desde Internet, comúnmente, e-mail (que se envía mediante SMTP, (Protocolo Simple de Transferencia de Correo), el Protocolo de Transferencia de Archivos (FTP) y la World Wide Web (http; Protocolo Transferencia de Hipertexto). El

software emplea la tecnología de filtrado de paquetes para determinar qué paquetes se están enviando con estos protocolos.

Cuando el software encuentra paquetes que se envían con SMTP, FTP o HTTP, sabe que debe examinarlos más a fondo, para ver si tienen virus. El software para examinar virus funciona de varias maneras. Un método de detección es comprobar archivos para revelar marcadores de virus que indican la presencia de un virus. Los paquetes que no están utilizando SMTP, FTP o http (como TNP) se admiten y el software no realiza ninguna acción en ellos.

Si se encuentra que el archivo está libre de virus, se le permite pasar. Si se encuentra que tiene virus, no se le permitirá entrar en la Intranet.

El software antivirus también debería ejecutarse en computadoras individuales dentro de la Intranet porque es posible que se pueda introducir un virus en la Intranet por disquetes, por ejemplo. Además de la protección contra virus, puede detectar virus y extirpar cualquier virus que encuentre.

4.2.8 Bloqueo de sitios indeseables

El software para el bloqueo de sitios examina el URL de cada petición que sale de la Intranet. Los URL más propensos a no ser aceptados accederán a:

- La Web (http)
- Grupos de noticias (ntp), ftp (ftp)
- Gopher (gopher)
- Conversaciones de Internet (irc).

El software toma cada uno de estos tipos de URL y los pone en sus propias "cajas" separadas. El resto de la información de la Intranet que sale tiene permiso para pasar.

Cada URL en cada caja se comprueba en una base de datos de los URL de los sitios censurables. Si el software de bloqueo encuentra que algunos de los URL provienen de sitios desagradables, no permitirá que la información pase a la Intranet. Los productos como SurfWatch como prueban miles de sitios y enumeran varios miles en sus bases de datos que se han encontrado molestos.

El software para bloquear sitios comprueba después el URL con una base de datos de palabras que puede indicar que el material que se solicita puede ser censurable. Si el software de bloqueo encuentra un patrón que encaje, no permitirá que la información pase a la Intranet.

El software para bloquear sitios puede entonces emplear un tercer método para comprobar los sitios desagradables; un sistema de clasificación llamado PICS

(Plataforma para la Selección de Contenido en Internet). Si el software para el bloqueo de sitios encuentra, basándose en el sistema de clasificación, que el URL es para un sitio que puede contener material censurable, no permitirá el acceso a ese sitio.

Debido a que Internet está creciendo tan rápido, las bases de datos de sitios censurables podrían llegar a ser anticuados. Para resolver el problema, la base de datos se actualiza cada mes. El software para el bloqueo de sitios conectará automáticamente con un sitio en Internet, y recibirá la base de datos de sitios desagradables más nueva a través de ftp.

Los administradores de Intranet´s pueden encontrar sitios no enumerados en la base de datos y no filtrados por el software para bloquear sitios que ellos quieren bloquear. Para bloquear manualmente el acceso a esos sitios, pueden añadirlos simplemente a la base de datos.

4.3 Software de supervisión de Intranet´s

El software utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar. Ambos observan los datos en la cabecera de cada paquete IP que entra y sale de la Intranet. Sin embargo, se diferencian en que los enrutadores para filtrar deciden si admiten o no a los paquetes.

El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes además delos datos como la dirección del emisor y destino, el tamaño del paquete, el tipo de servicio de Internet implicado (como la WEB o FTP) y la hora del día en la que se recogen en una base de datos.

Mientras que todos los paquetes deben pasar a través del servidor, el software no introduce necesariamente la información de cada paquete en la base de datos.

Por ejemplo, la información acerca de los paquetes http (World Wide Web), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes e-mail (SMTP), los paquetes delos grupos de noticias (TNP) y los paquetes Telnet pueden seguirse, mientras que los paquetes de sonido fluido pueden ignorarse.

El software incluido con el programa del servidor permite a los administradores de redes examinar y analizar el tráfico de la Intranet y de Internet en un grado extraordinario.

Puede mostrar la cantidad total del tráfico de la red por día y por horas, por ejemplo, y mostrar a cualquier hora a qué sitios de Internet se estaban transfiriendo. Puede incluso mostrar qué sitios estaban visitando los usuarios individuales en la Intranet, y los sitios más populares visitados en forma gráfica.

Algún software va más allá del análisis y permite a los administradores de Intranet´s cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores. El software permitirá también a los administradores de Intranet´s prohibir que se visiten ciertos sitios de la Intranet.

4.4 Redes virtuales seguras

Una Red Privada Virtual Segura (VSPN) o Red Privada Virtual (VPN) permite a los empresarios, siempre y cuando cada uno posea una Intranet, enviarse comunicaciones seguras por Internet y saber que nadie más será capaz de leer los datos.

Esencialmente, crea un canal privado y seguro entre sus respectivas Intranet´s, incluso aunque los datos enviados entre ellas viajen por la Internet pública.

Esto significa que las compañías no tienen que alquilar líneas caras entre ellas para mandar datos a través de un enlace seguro. Esta tecnología también se puede emplear para permitir a una compañía enlazar sucursales sin tener que alquilar líneas caras y saber que los datos se pueden leer por la gente de la VSPN.

CONCLUSIÓN

Toda empresa, para su funcionamiento, requiere de herramientas útiles, eficientes y fáciles de manejar; una combinación cuyo proceso de conciliación requiere de un arduo trabajo.

Esto se hace posible a través del uso y manejo de aplicaciones por parte de los especialistas en ellas.

Los ámbitos de comunicación y transacciones a nivel empresarial son muy amplios y muy variados. Por ello, se necesita de un medio que permita a las organizaciones manejar de manera eficaz su información y ofrezca una garantía de minimización de riesgos.

Como una respuesta a esta necesidad, surgen diversos sistemas para cubrirlos; entre ellos, las redes informáticas de computadoras.

Las redes se clasifican en grandes grupos; cada uno de ellos con sus propias características, ventajas y costos.

Las red más utilizada es la Internet, también conocida como “la gran red”, que tiene la ventaja de ofrecer una alcance enorme y a nivel mundial; de llegar a todos los rincones del plantea en cualquier lugar en donde exista una computadora.

Sin embargo, el uso de la Internet es muy difundido, por lo que, a pesar de ser sumamente útil, también resulta muy inseguro para las empresas, puesto que el acceso por este medio es más abierto y la seguridad es más fácil de franquear.

La Internet se puede dividir en varias subredes que, si bien dependen de ella, son independientes en cuanto a su funcionamiento. De entre ellas, se destaca a la red organizativa privada, conocida como Intranet.

La Intranet es una red inevitablemente subordinada a la gran red: Internet. No obstante, tiene características propias que representan ventajas notables para los usuarios de la Intranet.

Entre los beneficios que ofrece esta red privada, destaca la seguridad en el manejo de la información, ya que esta se restringe a los miembros de la organización en particular.

En este punto, cabe hacer énfasis en que cada empresa es diferente y, por lo tanto, sus necesidades son también distintas. La Intranet tiene la capacidad de adaptarse a cada organización; es la razón por la que resulta una herramienta muy útil, práctica y segura para quienes la usan.

Se destaca que no existe un sistema 100% eficiente, confiable y seguro. Para cada usuario, empresa y/u organización, deben analizarse las necesidades particulares y dar mayor importancia a aquellos factores in dispensables; y menos énfasis a las características que, si bien son necesarias, no tienen tanto peso para la organización.

Se hace notar, en este punto, como el gran alcance de las redes informáticas pueda ser tan fácilmente sacrificable en pro de la seguridad de la información y de la transmisión de datos, lo que provee de tranquilidad, también, a la organización en general.

GLOSARIO

2B+D Codificación de línea: 2B1Q. 2B+D.- Canales B, By D.

AC Control de Acceso, (Access Control)

ACF Campo de Control de Acceso, (Access Control Field).

ACK Acuse de Recibo, (Acknowledgement).

ADM Multiplexor de Agregar-Soltar, (Add-Drop Multiplexer).

ADPCM Modulación Adaptativa por Código de Pulso Diferencial (Adaptive Differential Pulse Code Modulation).

ARP Protocolo de Resolución de Dirección, (Address Resolution Protocol).

ARPA Agencia de Investigación de Proyectos Avanzados, (Advanced Research Projects Agency).

ARQ Requerimiento de Repetición Automático, (Automatic Repeat Request).

ASCII Código Estándar Americano para el Intercambio de Información, (American Standard Code for Information Interchange).

ATM Model de Transferencia Asíncrono, (Asynchronous Trabsfer Mode).

SER Tasa de Errores de Bit (Bit Error Rate). BOOTP.- Bootstrap Protocol.

BRI Interfaz de Tasa Básica, (Basic Rate Interface).

CSR Tasa de Bit Constante, (Constant Bit Rate).

CCS Señalización de Canal Común, (Common Channel Signaling).

CCITT Comité Consultivo Internacional de Telegrafía y Telefonía, (Committee Consultative Internacional for Telegraphy and Telephony).

CDMA Acceso Múltiple por División de Código, (Code Oivision Multiple Access).

CIB Bit Indicador de CRC 32, (CRC 32 Indicator Bit).

CIR Tasa de Información Comprometida, (Commited Information Rate)

CNM Gestión de Red de Cliente, (Customer Network Management).

COCF Función de Convergencia Orientada a Conexiones, (Connection-Oriented Convergente Function).

BIBLIOGRAFÍA

- GRALLA, P.(1996). Como Funcionan las Intranets. (1ra ed.). Maylands: Prentice Hall.

- Desarrollo y Aplicaciones.(1999). Disponible en: http://vobo.com.mx/intranet.html.

- Intranet.(1996).Disponible en: http://www.wntmag.com/atrasados/1996/02_oct96/intranet.html.

- Intranets.(1999). Disponible en: http://www.geocities.com/SiliconValley/2208/Insituacion.html.

- Wagner, William P., Chung, Q.B., Baratz, Todd. (2002). Implementing corporate intranets: lessons learned from two high-tech firms. Industrial Management & Data Systems. pp. 140-145.

- Blanc, Gerard. The intranet: first, answer the questions. (Technology Information). Feb 23, 1998. http://www.findarticles.com (Accesado Mayo 8, 2004)

- Guenther, Kim. (Jan/Feb 2003). Ten steps to intranet success. Online. pag. 66.

- McGovern, Gerry. Intranet communication versus traditional communication. November 25, 2002. http://www.gerrymcgovern.com (Accesado Mayo 8, 2004)

- Weaver, Beth . (Jun 2003). Corporate intranet paving the way. Hoosier Banker. pag. 26.

- CONESA, Alícia-RULL, Imma. " L'evolució dels sistemes documentals al departament de Documentació de TVC: el canvi de Mistral a Airs i el repte d'Intranet". En: 6es. Jornades Catalanes de Documentació. Barcelona: Socadi , Col.legi Oficial de Bibliotecaris-Documentalistes de Catalunya, 1997. 225-235pp.

- FUENTES i PUJOL, Mª Eulàlia. La información en Internet. Barcelona: Cims, 1997. 240p

- HOLTZ, Shel. INTRANET como ventaja competitiva. Madrid: Anaya Multimedia, 1997. 354p.+CD.

- ”L’Intranet s’impose dans l’enterprise”. En: Archimag, nº 105, juin 1997.25-29pp.

- MARTIN, Philippe. “Intranet. Présentations technique et perspectives”. En: Documentaliste-Sciences de l’Information, vol. 33, nº 4-5, 1996. 207-213pp.

- SANCHEZ MONTERO, José Antonio. “Hacia una optimización de los recursos Internet en la empresa”. En: Revista Española de Documentación Científica, nº 20, 1, 1997. 52-59pp..

OBJETIVOS

- Mostrar un panorama general de las intranets y su importancia dentro de las empresas y organizaciones

- Marcar la utilidad de la red Intranet para la comunicación y la seguridad en la transferencia de información

JUSTIFICACIÓN

Con la evolución que cada día sufre los sistemas de computación, su fácil manejo e innumerables funciones que nos ofrece, su puede decir que igualmente se ha incrementado el numero de usuarios que trabajan con computadoras, no sin antes destacar él Internet; una vía de comunicación efectiva y eficaz, donde nos une a todos por medio de una computadora.

Utilizando la Red de Area Local en una estructura interna y privada en una organización, seguidamente se construye usando los protocolos TCP/IP. Permite a los usuarios trabajar de una forma sencilla y efectiva, al mismo tiempo brinda seguridad en cuanto a la información ya que esta protegida por firewall: combinaciones de hardware y software que solo permite a ciertas personas acceder a ella para propósitos específicos.

Por otra parte el Intranet nos permite trabajar en grupo en proyectos, compartir información, llevar a cabo conferencias visuales y establecer procedimientos seguros para el trabajo de producción.

La Intranet es una red privada, aquellos usuarios dentro de una empresa que trabajan con Intranet pueden acceder a Internet, pero aquellos en Internet no pueden entrar en la Intranet de dicha empresa. El software que se utilizan en los Intranets es estándar: software de Internet como él Netscape, Navigator y los Navegadores Explorer para Web de Microsoft, facilitan en intercambios de información entre varios departamentos para poder llevar a cabo sus objetivos. Los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el guión de C.P.I. (Interfaz Común de Pasarela) permitiendo hacer negocios en línea, la información enviada a través de una Intranets alcanza su lugar exacto mediante los enrutadores.

Para proteger la información corporativa delicada las barreras de seguridad llamadas firewall (esta tecnología usa una combinación de enrutadores, que permite a los usuarios de Intranet utilizan los recursos de Internet, para evitar que los intrusos se introduzcan en ella).

Construyendo los protocolos TCP/IP (son los que diferencian a la Intranet de cualquier otra red privada) las cuales trabajan juntos para transmitir datos. (TCP: Protocolo de Control de Transmisión y el I.P: Protocolo de Internet), estos protocolos manejan el encadenamiento de los datos y asegura que se envían al destino exacto, funciona conjuntamente y se sitúan uno encima de otro en lo que se conoce comúnmente Peta de Protocolo, esta formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir.

Cuando hay una gran cantidad de trafico en una Red de Area Local, los paquetes de datos pueden chocar entre ellos, reduciendo en eficacia de la Red. Por tal motivo se utilizan combinaciones de Hardware y Software denominados Puentes que conectan con enrutadores en un solo producto llamado brouter, que ejecuta la tarea de ambos. Los

enrutadores son los que aseguran que todos los datos se envíen donde se supone tienen que ir y de que lo hacen por la ruta más eficaz, desviando él trafico y ofreciendo rutas, cuentan con dos más puertos físicos. Los de recepción (de entrada) y los de envío (de salida), cada puerto es bidireccional y puede recibir o enviar datos.

Saliendo un poco en cuanto a Procesamiento de Datos podemos destacar dentro del Intranet el Uso de Correo Electrónico, utilizando a la vez el Protocolo Simple de Transmisión de Correo (CMTP), emplea una arquitectura cliente / servidor; el receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo. Frecuentemente el e-mail generado por Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, en otra Intranet. El mensaje deja la Intranet y se envía a un enrutador Internet. EL enrutador examina la diversión, determina donde debería mandarse el mensaje, y después lo pone en camino.

El motivo por el cual una Intranet es porque a Web facilita la publicación de la información y formularios usando el Lenguaje de Hipertexto (HTML), permite también la creación de páginas iniciales multimedia, que están compuestas por textos, video, animación, sonido e imagen.

Los programadores pueden vincular datos corporativos desde una Intranet, permitiendo el uso de sistemas patrimoniales como base de datos en el Java, el cual es similar al lenguaje informático C++, es compilado, lo que significa que después de que el programa Java se escribe, debe ejecutarse a través de un compilador para transformar el programa en el lenguaje que pueda entender la computadora.

La Intranet se puede subdividir en varios niveles al momento de sobrepasar su tamaño y al ser difícil de manejar, para resolver el problema se crea subsecciones de una Intranet que las hacen más fáciles de hoslid: los bits que se usan para distinguir sub – redes se llaman números de sub – red.

Al mismo tiempo la Intranet cuenta con firewall que es la combinación de hardware / software que controla el tipo de servidores permitidos hacia o desde la Intranet, esta línea de defensa es por los ataques de aquellas personas que tengan el propósito de destruir o robar datos en una empresa ya que la Internet se expone a este tipo de ataques.

Otra manera de emitirlos es usando un enrutador para filtrar, encaminar la dirección IP, y la información de cabecera de cada paquete que entra con la Intranet y solo permite el acceso aquellos paquetes que tengan direcciones u otros datos, que el administrador del sistema ha decidido previamente que puedan acceder a la Intranet.

Seguidamente para asegurar una Intranet se debe usar la encriptación el cual se utiliza para almacenar y enviar contraseñas o códigos específicos para asegurase que ninguna persona pueda entenderla. Las claves son el centro de la encriptación. Las contraseñas deben cambiar frecuentemente, que no sean adivinadas fácilmente y tienen que ser elaboradas por personas autorizadas.

Por otra parte tenemos los vienes en la Intranet, son el mayor riesgo en la seguridad, pueden dañar datos, ocupar y consumir recursos e interrumpir operaciones. Estos virus se esconden dentro de un programa, hasta que no se ejecute ese programa el virus es inactivo, al ejecutarse entra en acción infectando en el disco duro copiándose de ellas.

El software se ejecuta en un servidor de firewall para examinar al virus, también utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar.

El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes. Igualmente incluidos con el programa del servidor permite a los administradores de redes examinar y analizar él trafico de la Intranet y de Internet en un grado extraordinario. Algún software va más allá del análisis y permite a los administradores de Intranets cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores.

Finalmente podemos decir que las Intranets permiten a los empresarios que a sus empleados trabajen en grupo, tal motivo se debe al extenso aportado de programas para trabajo en grupo y admite que los usuarios empleen la conferencia visual, compartan documentos, participen en discusiones y trabajen juntos de otro modo, no solo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlo – recibir y rellenar pedidos de bienes y servicios.