21

U.N.A.M.

FACULTAD DE INGENIERIA

Esquema de Administración de Servidores Internet para la Coordinación de Servicios de Red

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
P R E S E N T A N :

SILVIA BELTRAN SANCHEZ
MARIA BETZABE ZAVALA RODRIGUEZ

DIRECTOR DE TESIS: ING. RICARDO MARTINEZGARZA FERNANDEZ

MEXICO, D. F. 1998

Agradecemos ...

Al *Ing. Ricardo Martinezgarza Fernández,* por el apoyo y la paciencia que nos ha brindado para poder realizar este trabajo.

Al *Ing. José Francisco Becerril Caballero,* por sus invaluables consejos, su gran apoyo y amistad.

Al la la *Lic. Livia Esmeralda Zavala Rodríguez* y al *Ing. Francisco Xavier Flores Vargas,* por sus excelentes consejos y apoyo.

A la *Coordinación de Servicios de Red,* por habernos brindado la oportunidad de realizar éste proyecto.

A la *Faculad de Ingeniería* por todos los conocimietos y las vivencias que nos dió.

A nuestra amada *Universidad* por la valiosa formación que nos brindó.

Doy gracias a Dios por permitirme llegar a realizar este trabajo que es una de mis grandes metas.

Dedico este trabajo a...

Mis padres Esmeralda y Arturo, con todo mi amor, respeto y una inmensa gratitud por haberme apoyado, amado y enseñado a luchar por superarme en todos los aspectos de mi vida

Mis hermanos Livia, Raymundo y Salvador por todo su amor y apoyo que siempre he sentido. A Gladys y Paco, mis cuñados, por ser también unos verdaderos hermanos.

Mi hermosa sobrina Daniela con todo mi amor.

A Luis Alberto, mi gran amor. Gracias por todo el amor, el apoyo y aliento que siempre me has brindado para seguir adelante.

A todos y cada uno de mis familiares, gracias por su apoyo.

A mis verdaderos amigos, que a lo largo de mis estudios compartimos innumerables y hermosas experiencias.

Betzy...

Este trabajo esta dedicado:

A mis padres.... Ma. Teresa y Jorge H. Por que siempre han estado conmigo brindándome todo su cariño y dándome la fortaleza para seguir adelante, porque han sido mis maestros y mis amigos al mismo tiempo y por que no existen palabras para expresar la gratitud y el cariño que siento por ellos.

A mis hermanos.... Xóchitl, Jorge y Daniel, por serlos mejores hermanos del mundo y por creer en mi.

A Lilia.... la persona más especial que nunca me abandona y a la que nunca olvido.

A mis amigos y compañeros.... de la Facultad de Ingeniería, de la Coordinación de Servicios de Red y del programa de becas de la DCAA... gracias por su valiosa amistad.

Silvia...

Introducción.

Introducción

Desde sus inicios la Universidad Nacional Autónoma de México ha sido una de las instituciones educativas mexicanas vanguardistas de mayor importancia, además de ser una de las universidades pioneras en el campo de las redes. A partir de 1989 con la inauguración de RedUNAM por parte del Dr. José Sarukhán y con la conexión a Internet de ésta, se establecieron proyectos para proporcionar servicios que brindaran a toda la comunidad universitaria un espacio para compartir información e intercambiar ideas contribuyendo a la formación de profesionistas y apoyando a la investigación.

La Dirección General de Servicios de Cómputo Académico (DGSCA) a sido el líder de estos proyectos asignándolos a sus diferentes departamentos, de entre los cuales destaca la Coordinación de Servicios de Red (CSR).

La CSR ha tenido la experiencia de proporcionar servicios en Internet durante casi cinco años, enriqueciéndose de valiosas experiencias al tener el compromiso de dar a la comunidad un servicio cada día mejor.

Debido a este compromiso la CSR ha visto que para proporcionar un servicio en Internet además de contar con la infraestructura de conexión necesaria, se requiere un buen plan de administración del servidor, de esta manera en junio de 1995 surgió la idea de establecer un esquema de administración el cual contuviera todos los aspectos necesarios para lograr un servicio de calidad, dando origen a éste trabajo de tesis.

Este trabajo está dirigido a todas aquellas personas encargadas de la administración de los sistemas que proporcionan servicios dentro de la CSR, dándoles una guía de apoyo para lograr proporcionar servicios de calidad, o bien, mejorar los servicios que actualmente se prestan. A pesar de que este trabajo está aplicado a la CSR, puede ser utilizado por otros administradores siempre y cuando cuenten con una infraestructura semejante a la de ésta, y que el fin que se persiga sea el académico.

La infraestructura de la CSR consta de servidores con una plataforma operativa UNIX y de una red local Ethernet con conexión directa a Internet proporcionada por el Departamento de Conectividad; la administración de ésta red es realizada por la Subdirección de Comunicaciones y Redes.

A continuación se describirá la estructura de ésta tesis.

Capítulo 1.

En este capítulo damos a conocer aspectos generales que ayudarán a comprender de manera breve lo que es Internet dando un panorama del crecimiento que ha tenido a lo largo de estos últimos años alrededor de todo el mundo.

Posteriormente, proponemos una clasificación de los servicios que son proporcionado en Internet de acuerdo al tipo de uso que se le da, además de las características generales que debe tener un servicio para que se considere de calidad, permitiendo que el lector se familiarice con éstos términos que serán tratados en capítulos posteriores.

Por último se realiza un estudio en el cual se lleva al lector a través de la evolución de los tipos de procesamiento hasta llegar al modelo cliente-servidor que corresponde a la arquitectura en la que están basados los servicios de Internet (UNIX).

Capítulo 2.

Este capítulo esta enfocado a la administración del servidor, por lo cual se presentan las características de hardware y software para poder prestar un servicio en Internet.

También presentamos los conceptos fundamentales para llevar a cabo la administración de un servidor basándonos en la experiencia de la CSR y de una investigación en el campo de la administración para servidores en Internet.

Cabe mencionar que es necesario que las personas sin experiencia en administración de servidores en Internet, comprendan en primer lugar este capítulo, ya que estos conceptos son los fundamentos en la administración de servicios y constituyen la base del presente trabajo.

Capítulo 3.

Aquí proponemos una serie de procedimientos a realizar en la administración de servidores para lograr que sea de calidad.

El contenido de este capítulo resulta ser uno de los más técnicos de toda la tesis, por tal motivo es necesario que se cuente con los fundamentos básicos de administración tratados en el capítulo 2. También se requiere que el administrador conozca el sistema operativo para poder llevar a cabo cada uno de los procedimientos.

Capítulo 4.

Proponemos una estrategia para la aplicación de los procedimientos establecidos en el capítulo 3. Ésta estrategia está dirigida al administrador líder y consiste en siete pasos establecidos en un orden que permite llevar a cabo la implementación de manera organizada, se recomienda que éste administrador, tenga conocimientos tanto de planeación, como de dirección para facilitar la implementación.

Consideramos que tanto el capítulo 3 como el 4 son la parte más creativa de nuestro trabajo, y se pretende que los dos sean claramente entendidos por el lector antes de su implementación.

Capítulo 5.

Este capítulo es un ejemplo de la implementación de los procedimientos de administración para uno de los servidores de la CSR mediante la estrategia descrita en el capítulo anterior. Su contenido es la documentación que se realizó en el séptimo paso de la estrategia de implementación.

Para la implementación de este trabajo, se determinó utilizar el equipo SunSITE (Sun Software Information and Technology Exchange), mismo que fue donado a la Universidad por Sun Microsystems.

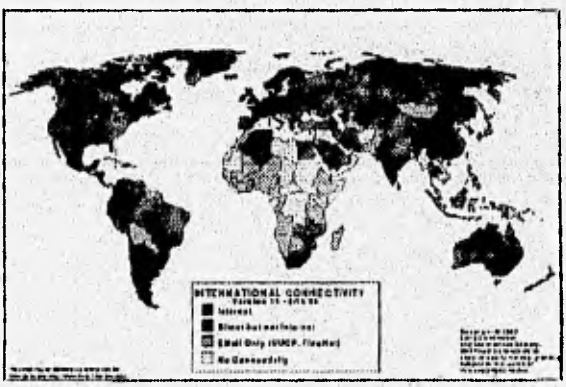
1. Antecedentes.

1.1 Internet

La interconexión de computadoras en los últimos años ha crecido notablemente, y éstas se han convertido en un campo sumamente atractivo debido al interés de satisfacer la necesidad de compartir información entre diferentes organismos. Gran parte de la tecnología en esta rama a dado pie a interconectar computadoras en áreas geográficas pequeñas o muy grandes. En este contexto existen las redes de área local (Local Area Network, LAN) que proporcionan un medio de comunicación en áreas geográficas reducidas, por ejemplo en campus universitarios y en empresas con instalaciones distribuidas en áreas pequeñas. Otros tipos de redes son las de área metropolitana (Metropolitan Area Network, MAN) que como su nombre lo dice son redes que abarcan áreas geográficas metropolitanas y por último las redes que abarcan áreas mucho más amplias que las anteriores como lo son las redes de área amplia (Wide Area Network, WAN).

Cada tecnología está disponible según las necesidades que se tengan, pero surge entonces la necesidad de formar una red que cubra todas éstas para formar una sola entidad, y aunque existan redes computacionales que no compartan la idea de integrarse a una red de este tipo y sólo quieran satisfacer necesidades de información de un grupo de personas limitado, con esta red mundial, se pueda tener diferentes ventajas como lo es el intercambiar información con diferentes universidades o centros de información en forma inmediata y directa. Es así como en Estados Unidos se realizaron investigaciones en este campo, comenzando la formación de una red en donde alrededor de 40 países se han conectado para formar una red mundial llamada "Internet" (Gráfica 1.1).

Mapa de los países conectados a Internet

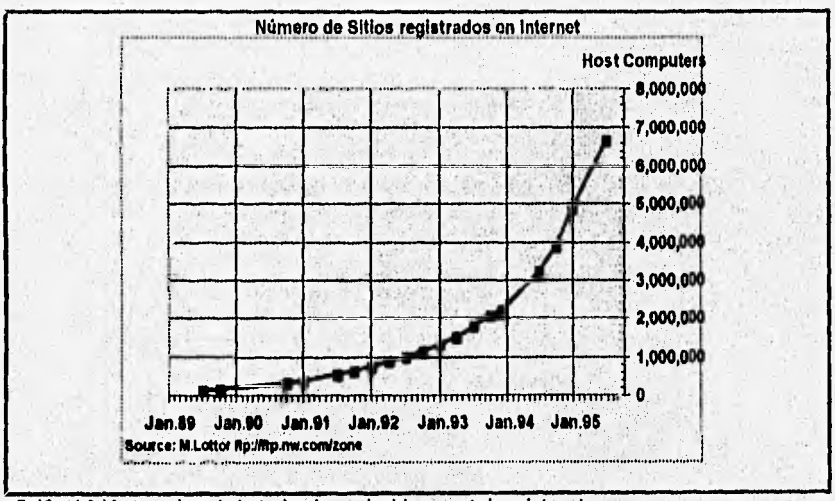


Gráfica 1.1 Mapa de los países que están conectados a Internet.

El inicio de Internet se dio a principios de los años setentas cuando la Agencia de Proyectos Avanzados de Investigación (Defense Advanced Research Proyect Agency, DARPA) desarrolló una tecnología que incluía un conjunto de estándares para comunicar computadoras e interconectar redes, formando así la red militar ARPAnet, que tuvo mucha aceptación y que fue un punto muy atractivo en varios centros de investigación.

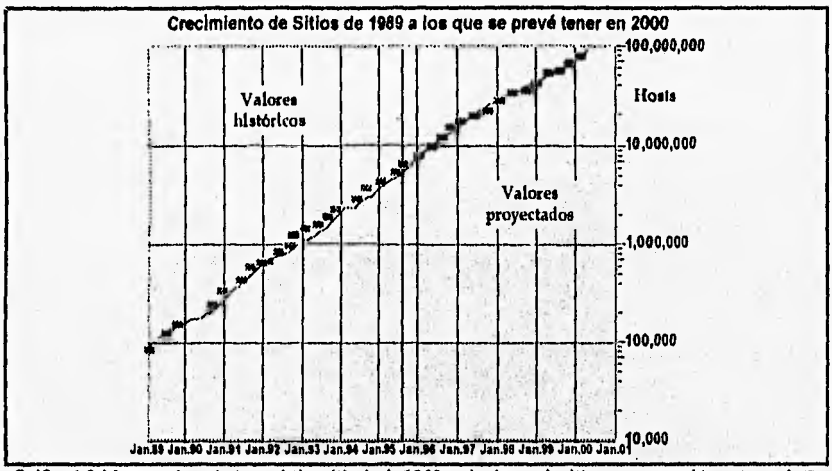
Esta red se fue desarrollando mediante reuniones entre científicos y para el año de 1979 los resultados de estas reuniones, además de valiosos experimentos e investigaciones realizadas, fueron encaminados a la especificación de un conjunto de protocolos que sería denominado TCP/IP, constituyéndose la base de protocolos en Internet.

Internet ha sido lo suficientemente flexible como para permitir la interconexión entre una gran variedad de arquitecturas de red. Actualmente la mayoría de las universidades están conectadas a ésta y se esta tratando de conectar otro tipo de escuelas de grado menor como lo son primarias y secundarias, al igual que bibliotecas locales en todo el mundo (Gráfica 1.2).



Gráfica 1.2 Muestra el crecimiento de número de sitios conectados a Internet.

La gráfica 1.3 muestra el resultado de un estudio que realizó La Organización Internacional para la Coordinación y Cooperación en Internet (Internet Society) en donde se observa el crecimiento que ha tenido desde el año 1989 al año 1995 y el estimado para el año 2000.



Gráfica 1.3 Muestra el crecimiento de los sitio desde 1989 y el número de sitios que se prevé tener para el año 2000

Como se mencionó, TCP/IP consta de varios protocolos que tienen aplicaciones específicas (estos se podrán ver con mas detalle en el apéndice TCP/IP). El propósito general de TCP/IP es permitir el desarrollo de aplicaciones a alto nivel de manera transparente, es decir ocultando las especificaciones propias de hardware al usuario final.

En Internet también existen limitantes que indican lo que se permite hacer en la red, estas limitantes están formadas por leyes, políticas y un conjunto de reglas de ética. La forma en que estas se relacionan varía de un lugar a otro ya que Internet es una red de redes en donde cada una de estas redes cuentan con sus propias reglas y políticas. Es importante indicar que estas leyes no son demasiado restrictivas y que mientras se actúe de acuerdo a estas, se podrá trabajar como se desee.

Desde el punto de vista académico, el principal propósito de Internet es compartir información, por lo que se han creado servicios públicos para facilitar esta tarea, aunque actualmente Internet ha tomado un giro comercial, lo cual a dado pauta a crear servicios privados. Conforme ha avanzado la tecnología, los servicios se han ido sofisticando haciendo que el usuario final interactúe con el servicio de una forma más amigable permitiéndole también hacer uso de más recursos computacionales, como es el caso de la multimedia.

Este tipo de servicios hacen que Internet sea más atractiva, ya que las personas que se encuentran conectadas a ella, pueden compartir información de diferentes intereses y además tener una comunicación a nivel mundial.

1.2 Servicios en Internet.

Un servicio en Internet es aquel que sirve como medio entre los usuarios para poder compartir y acceder a recursos que se encuentran dentro de esta red.

Se han creado servicios para satisfacer las necesidades de acceso, búsqueda y transferencia de información y comunicación entre usuarios, tomando como base algunos protocolos y éstándares que puedan ser utilizados en cualquier plataforma logrando una interoperabilidad entre éstos.

Podemos agrupar estos servicios, tomando como criterio su uso en Internet, de la siguiente manera:

Servicios de Información:

Estos servicios son los más importantes ya que una de las funciones principales de una red es compartir la información contenida en ella. La información organizada es presentada al usuario, quien posteriormente le da un sentido según su necesidad. Dentro de este tipo de servicios es común utilizar la transferencia de información así como herramientas de búsqueda de información.

Transferencia de Información:

Estos servicios permiten el intercambio de información realizando una copia de archivos que se encuentran en un sistema remoto al sistema local, estos archivos pueden tener cualquier longitud y tipo de formato.

En Internet existen sitios en donde se encuentra información de dominio público que puede ser transferida a cualquier lugar, cabe mencionar que en cada uno de estos sitios existen restricciones de acuerdo a las políticas determinadas por los administradores de cada uno de los servicio.

Herramientas de búsqueda:

Las herramientas de búsqueda son el medio para facilitar la localización de información en Internet. Existe una variedad de herramientas específicas para cada servicio de información, permitiendo así que el usuario elija la que mejor se adapte a sus necesidades.

Servicios de Comunicación:

La comunicación entre usuarios se vuelve un punto atractivo y es así cómo en Internet este aspecto se vuelve más importante ya que esta comunicación es a nivel mundial y por lo tanto, es uno de los servicios más utilizados.

Comunicación Interactiva y no interactiva

Actualmente, en Internet se encuentran servicios de comunicación interactiva y no interactiva entre usuarios. La interactiva consiste en que dos o más usuarios establezcan una comunicación al mismo tiempo, pudiendo interactuar entre ellos. También, de manera contraria existe un tipo de servicio que trabaja en forma no interactiva, es decir, permiten enviar información, sin esperar una respuesta

Independientemente del tipo, se considera un servicio de calidad si reúne las siguientes características:

- Disponibilidad. El servicio debe estar siempre disponible es decir, que tanto el sistema como el software servidor estén en disposición de atender cualquier petición.

- Eficiencia: En el contexto de este trabajo, es el tiempo de respuesta en que el sistema responde para ofrecer el servicio. Aclaramos que no nos corresponde la evaluación de tiempo de respuesta de la red, sino solamente del servidor.

- Estado de la Información: Si se trata de un servicio de información , su información debe de ser actual, organizada y con el formato adecuado.

Es un gran compromiso el presentar un servicio, debido a esto se debe poner atención en los aspectos arriba mencionados, para garantizar que el usuario satisfacerá sus necesidades.

En cuanto a la arquitectura de los servicios, en general, éstos están basados en un caso particular de los sistemas distribuidos. Los sistemas distribuidos se refieren a cómo se lleva acabo el procesamiento de una manera descentralizada y transparente al usuario final.

Para el interés de este trabajo a continuación mencionaremos la evolución del procesamiento en sistemas hasta llegar a lo que son los sistemas distribuidos, y especialmente a un caso particular de éste, que es el modelo cliente-servidor, el cual es la base del procesamiento de los servicios en Internet.

1.3 Tipos de Procesamiento

La evolución del procesamiento en sistemas se ha dado en dos formas: el procesamiento centralizado y el procesamiento distribuido. Estos han sido la base para todas las aplicaciones desarrolladas en un ambiente de red.

Procesos Centralizados

> En este caso, todos los usuarios comparten el poder de un procesador central y una sola copia de software de aplicación corre en la CPU central. Las terminales "tontas" enlazadas que necesiten usar la aplicación deben compartir dicho CPU. Para este tipo de procesamiento se han utilizado los mainframe y minicomputadoras.

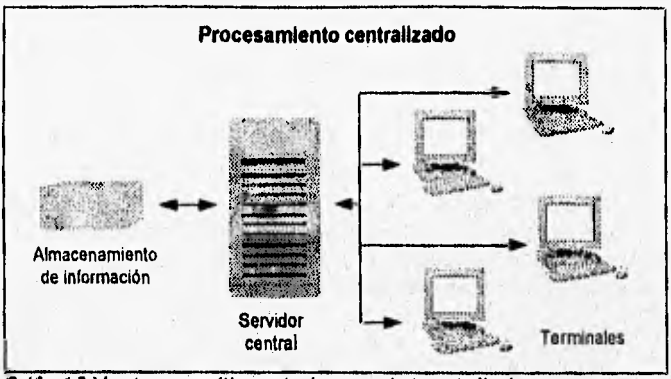
Procesos Distribuidos

> Cuando el procesamiento de la información se lleva acabo en una manera descentralizada se dice que es un proceso distribuido. Esto resulta ser la forma en cómo trabaja un conjunto de sistemas y computadoras organizadamente para proporcionar servicios en un ambiente de red.

La diferencia que hay entre estos dos tipos de procesamiento es que el centralizado requiere que todo el procesamiento ocurra de forma central en una sola máquina, y en el distribuido el trabajo es repartido entre las computadoras de la red.

La ventaja del procesamiento distribuido consiste en que cada uno de los procesos corriendo en máquinas locales, hacen uso de sus propios recursos de hardware, de esta forma las máquinas conectadas a la red corren aplicaciones sin afectar a las demás.

El procesamiento más antiguo que proveía un ambiente primitivo para dar soporte al procesamiento de aplicaciones es el *procesamiento centralizado* (Gráfica 1.5), este procesamiento es llamado también *basado-en-máquina (Host-based)*. Las aplicaciones procesadas son realizadas en una computadora de la que se tienen conectadas una serie de terminales "tontas", es común que en éste tipo de procesamientos se utilizaban arquitecturas mainframe. Desde el punto de vista de procesamiento este es totalmente no distribuido.



Gráfica 1.5 Muestra esquemáticamente al procesamiento centralizado.

El procesamiento distribuido de aplicaciones ha evolucionado en diferentes esquemas, el esquema llamado *procesamiento maestro-esclavo*, en el cual las computadoras esclavas están conectados a la computadora maestra en donde todo el desempeño de las funciones de procesamiento de aplicaciones son tomadas directamente por el maestro.

El procesamiento de aplicaciones en este ambiente maestro-esclavo es algo distribuido, ya que tiende a ser unidireccional, del maestro a los esclavos (Gráfica 1.6). Normalmente, las computadoras que hacen el papel de esclavos son capaces de realizar procesamiento de aplicaciones locales, como lo es el editar, validaciones en pantalla, o bien procesamiento y de algunas funciones.

Gráfica 1.6. Se muestra como es el procesamiento Maestro-Esclavo.

El esquema de procesamiento cliente-servidor, surgió como el nivel más alto del procesamiento de recursos compartidos utilizando un ambiente LAN. En éste se tiene un conjunto de computadoras conectadas a un sistema mediante el cual se permite compartir recursos, de tal manera que si se cuenta con una impresora o un archivo a los que se puede tener acceso, éstos son llamados servidor de impresión, o bien, servidor de archivos respectivamente.

Si una LAN crece en el número de terminales conectadas, entonces, la evolución de sistemas de dispositivos compartidos también debe crecer en capacidad y en poder; y es así como gradualmente, las máquinas que ofrecen servicios se vuelven capaces de servir a un número más grande de terminales de trabajo.

La evolución de estos procesamientos llegó a tal grado que el papel de las terminales cambió y se convirtieron en clientes de los servicios. La razón principal del cambio se debe a que en un ambiente LAN, el compartir recursos entre las terminales conectadas, representa sólo una fracción de una aplicación. Es así como el procesamiento de aplicaciones fue distribuido a servidores que son quienes reciben las peticiones de aplicaciones que se encuentran ejecutándose en estaciones de trabajo llamadas clientes (Gráfica 1.7). De esta manera el procesamiento se encuentra dividido entre el cliente y servidor es decir, de manera cooperativa entre los dos para lograr una ejecución exitosa de una aplicación.

Gráfica 1.7 En este esquema se muestra el procesamiento distribuido cliente-servidor

En general, los requerimientos que debe cumplir el modelo cliente-servidor, son los siguientes:

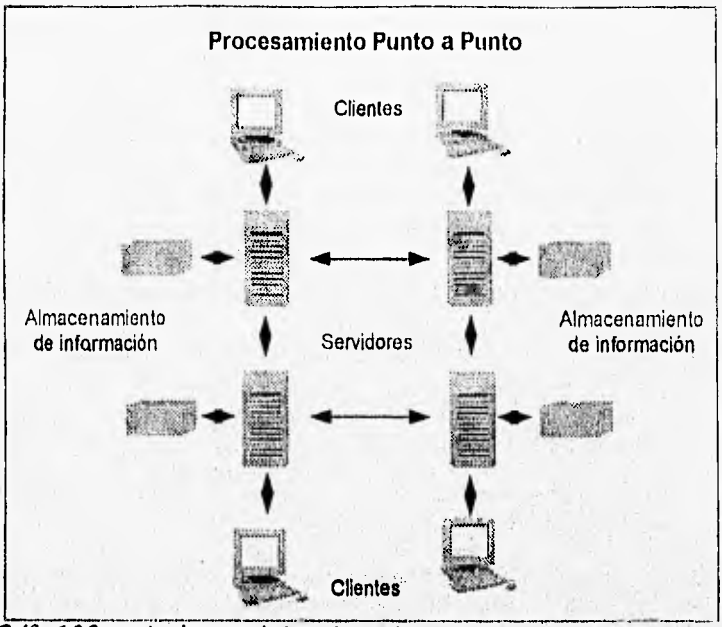
- Comunicación confiable y robusta entre el cliente y el servidor.
- Las interacciones entre el cliente y el servidor se realizan de manera cooperativa entre ambos, siendo iniciadas por el cliente.
- Distribución en el procesamiento de aplicaciones entre un cliente y su servidor.
- El servidor tiene el control sobre los servicios y los datos que un cliente puede solicitar.
- El servidor toma el arbitraje cuando se encuentra con peticiones conflictivas de clientes.
- Debe existir una coordinación del servidor cuando se tengan peticiones en procesos automáticos.

Un modelo cliente-servidor se caracteriza dado que tiene un cliente que solicita un servicio y un servidor que provee el servicio a esa petición.

Sin embargo, el siguiente nivel de procesamiento en la evolución de sistemas de procesamiento cooperativo distribuido es el procesamiento punto a punto, en éste el procesamiento de las aplicaciones es distribuido y realizado, en donde se encuentran los servicios disponibles incluyendo memoria, procesador y dispositivos compartidos (Gráfica 1.8). Todos los sistemas de procesamiento en este nivel, de cualquier manera, son iguales además de que pueden hacer peticiones y proveer servicios desde y para a todos los que están conectados a la red.

Un ambiente de punto-a-punto provee un procesamiento cooperativo distribuido entre aplicaciones que posiblemente se encuentran en una amplia variedad de plataformas de software y hardware.

El modelo cliente-servidor se encuentra alejado del procesamiento punto a punto, sin embargo debido a que su implementación es más factible y es la mejor solución en la actualidad para lo que ha desarrollo de sistemas distribuidos se refiere.



Gráfica 1.8 Se muestra el procesamiento punto a punto.

1.4 Modelo Cliente-Servidor

Actualmente no existe una definición aceptada por todos, cada quien la define de acuerdo a su contexto. Larry T, Vaughn la definió de la siguiente manera: "La arquitectura cliente-servidor es un diseño de aplicación que resulta de la descomposición de un sistema de información en un pequeño número de funciones de servidor, ejecutándose en una o más plataformas de hardware, que proveen servicios usados por un gran número de funciones clientes, ejecutadas en una o más diferentes plataformas de hardware interconectadas; este desempeño es definido por las limitaciones del trabajo que se realiza en las funciones del servidor".[1]

[1] *Larry T. Vaught, "Client/Server Systems Designg and Implementation", 1994.*

Larry T. Vaughn define el modelo Cliente-Servidor enfocándose a la forma como interactuan las funciones del cliente y del servidor. Tomando esta definición, decimos que la arquitectura Cliente-Servidor se basa en la interacción de un cliente y un servidor.

Podemos definir al cliente y al servidor de la siguiente manera:

- Un cliente es responsable de interactuar con el usuario, éste es el que va hacer una petición de algún recurso al servidor.

- Un servidor esta encargado de proporcionar información al cliente cuando este los solicite.

Este modelo se puede ver desde el punto de vista hardware o software, pero los dos enfoques parten de un mismo principio: "Que es el solicitar y proporcionar recursos". En el caso del software el cliente y el servidor pueden ejecutar en una misma computadora, pero por lo general corren en computadoras diferentes. En este caso el cliente es el programa que hará una petición al servidor, que es el programa que la proporcionara.

En el caso del hardware se trata de tener una máquina A y una máquina B en donde la máquina A cuenta con recursos que no tiene la máquina B. Entonces la máquina B necesita algún recurso que contiene la máquina A, por lo cual le hace una petición de ese recurso, y la máquina A se lo proporciona. Es así como la máquina B realiza el papel de cliente y la máquina A el de servidor.

1.4.1 Arquitectura Servidor

En el modelo cliente-servidor , el servidor es quien realiza una parte de la tarea ya que como se mencionó, es el encargado de compartir recursos de manera estable, flexible y con un desempeño aceptable para las necesidades de los clientes.

En términos de Hardware

El servidor de hardware debe ser capaz de proveer los recursos solicitados por los clientes aún cuando se tengan múltiples peticiones simultáneas en la red. Este es un aspecto que se debe considerar en la arquitectura de éste, ya que debe ser flexible y considerar que sus características van a producir efectos en el desempeño de los clientes.

Debido a esto, para que un servidor pueda realizar su tarea de manera confiable es necesario que reúna ciertas características:

- *Soporte Multiusuario.* Esta es la característica que debe tener para servir múltiples usuarios concurrentes. Sin embargo es importante considerar que el servidor soporte también el procesamiento multitarea, ya que ésta es una necesidad y un requerimiento para poder dar al soporte multiusuario un desempeño favorable. Cabe mencionar que el hecho de tener procesamiento multitarea no significa que se cuente con un sistema multiusuario, debido a que este se puede implementar también en un sistema monousuario.

- *Escalabilidad.* Un servidor debe de ser capaz de satisfacer las demandas de crecimiento de sus recursos. En este contexto escalabilidad significa que el sistema deba satisfacer los requerimientos y al mismo tiempo ser fácil de expandir (probablemente con una actualización de lo que ya se cuente). Una alternativa menos para la escalabilidad sería reemplazar el sistema cada vez que éste sobrepase sus límites de capacidad.

- *Desempeño.* Un servidor debe de prever un desempeño con un nivel satisfactorio a los intereses y necesidades que requiere un usuario en un ambiente multiusuario cliente-servidor.

- *Sistemas de Almacenamiento.* Conforme el número de usuarios y de aplicaciones corriendo en un servidor incrementa, y hay avances en las tecnologías de dispositivos de almacenamiento físico, la demanda de un almacenamiento extra y un acceso rápido se convierte en un requerimiento crítico para el sistema. La demanda del almacenamiento empieza cuando los usuarios necesitan almacenamiento adicional para nuevas implementaciones y otras aplicaciones que podrían consumir grandes cantidades de almacenamiento.

- *Trabajo en Red.* Las comunicaciones cliente-servidor se realizan en un ambiente de red. Ambas aplicaciones, cliente y servidor, deberán desarrollarse con capacidades de trabajo en red. Es importante mencionar que cualquier sistema, independientemente de su arquitectura, puede integrarse óptimamente con las interfaces para trabajo en red y protocolos.

En el caso especial en que la máquina servidor también contenga el software cliente, entonces debe considerarse que soporte un ambiente multimedia, esto es debido a que las nuevas aplicaciones y nuevas tecnologías empiezan a estar disponibles, ya que ahora se tiene aplicaciones con imagen, video y sonido, que cada vez se vuelven más populares.

También existen otros aspectos que se deben considerar como son, la habilidad de multitarea que no es una opción, sino un requerimiento, en este caso podemos distinguir dos tipos de multitarea: la multitarea preventiva que provee una gran tolerancia para fallas de programas, ya que el sistema operativo actúa como una puerta a los recursos compartidos, forzando a todas las aplicaciones a requerir el acceso a los recursos, y la multitarea cooperativa donde se ejecutan las aplicaciones que cooperan para acceder a recursos compartidos tales como RAM y CPU, entre otros.

Otro de los aspectos es la habilidad de direccionar gran cantidad de memoria, volviéndose esto un requisito más, por lo que se debe considerar un mínimo básico para garantizar la funcionalidad, además se debe tener en cuenta que la capacidad de almacenamiento se pueda extender en un momento dado.

Todos estos aspectos mencionados pueden mostrar un mejoramiento significativo en el desempeño del servidor. La misión de los servidores, es compartir recursos a muchos clientes con una gran sofisticación y funcionalidad, y va más allá de lo que es requerido por los clientes, ya que las facilidades que éste provee son parecidas a las proveídas por el sistema operativo multiusuario.

Una vez teniendo claras las características anteriores, también se debe considerar el Sistema Operativo con el que cuenta el servidor, ya que mediante éste se aprovechan los recursos de una manera organizada y óptima.

El primer propósito del sistema operativo de un servidor es acceder los recursos de hardware (memoria, almacenamiento en disco de datos, salida de video y de impresión, etc.) y administrar las interfaces entre la terminal de trabajo y los dispositivos externos (video, impresora, etc.).

Un sistema operativo que provee una administración y un manejo de sus capacidades, seguridad de acceso, archivos compartidos a clientes, impresión con cuotas y enrutada (encaminada) , y varias otras funciones, es generalmente referido como un *sistema operativo de red (NOS)*. Algunos sistemas operativos de red han sido diseñados específicamente para conocer las necesidades de compartir de recursos de red.

Los sistemas operativos de red también tiene dos formas de trabajo para compartir recursos a través de la red. La forma punto-a-punto nubla la distinción entre cliente y servidor, haciendo esencialmente esto posible para cada nodo de la red, corriendo el sistema operativo para jugar el papel tanto del cliente o del servidor. Cada nodo puede estar sirviendo a un usuario específico como una estación de trabajo cuando comparte simultáneamente su almacenamiento de datos, procesador y los recursos de impresión con una red. La forma servidor, requiere de la dedicación de una o más plataformas especificadas como la base del sistema operativo de red , y esto es sólo en esas plataformas cuyos recursos pueden ser compartidos.

En cualquiera de los dos enfoques, punto-a-punto o servidor, el sistema operativo de red debe proveer, como mínimo, las siguientes funciones:

- *Compartir Recursos-* proveer el control de acceso a él, compartir lo básico de los recursos de red.

- *Administración-* la habilidad de identificar y definir la autorización de usuarios a la red, los recursos que esos usuarios pueden acceder, la localización de esos usuarios, y otra información que ayude en el control y manejo de accesos a los recursos de la red.

- *Manejo de Recursos-* Son esas funciones que autorizan un diagnóstico y corrección de problemas tanto en la red como en el servidor, monitoreo de utilización de los recursos, la habilidad de optimizar el desempeño de los servidores en situaciones específicas, y provisionar la capacidad planeando capacidades.

- *Tolerancia de fallas-* La habilidad de un servidor para recuperarse de las fallas. Existen muchos niveles diferentes y tipos de tolerancia de fallas. En los niveles más bajos , esta la habilidad del sistema operativo para soportar la anormal terminación de un programa ejecutándose. En los niveles más altos en tolerancia de fallas se puede incluir la corrección de errores en memoria y disco, entre otros, utilizando estrategias específicas a la infraestructura con la que se cuenta.

En términos de Software.

El servidor recibe la petición del cliente, éste realiza el proceso necesario para poder enviarle al cliente la respuesta solicitada para posteriormente quedar en un estado de espera a otra petición. Un aspecto importante es que cuando el servidor está realizando los procesos adecuados para proporcionar el servicio al cliente, puede atender otras peticiones al mismo tiempo de manera confiable. Es común que el software de servidor llegue a estar limitado en cuanto al número de peticiones que puede aceptar en un momento dado, aunque en esta limitación interviene en gran medida el número de procesos que puede aceptar la plataforma en la que se encuentra el software y casi siempre, éste es un factor decisivo para delimitar cuantos clientes puede atender al mismo tiempo.

Por lo general este servidor tiene que cumplir algunas especificaciones para poder ser instalado en cierta plataforma, por esto es necesario conocer bien las características de la plataforma con la que se cuenta, para saber cuál será el servidor adecuado y cuál va a ser el alcance del servidor.

El software servidor, como ya se mencionó, es quien se encarga de tomar la petición enviada por el software cliente y es capaz de entender el lenguaje que el cliente utiliza para hacer la petición, ya que este lenguaje está regido por protocolos que tanto el cliente como el servidor conocen.

Protocolos de Comunicación Interprocesos

Los protocolos de comunicación entre procesos (Interprocess Comunications Protocols, ICP) son el lenguaje común que permite a cualquier programa ejecutarse en el mismo ambiente o en otro diferente para enviar y recibir mensajes, comandos y respuestas. La naturaleza de la arquitectura cliente-servidor requiere de un alto desarrollo de protocolos de comunicación entre procesos para el control, sincronización y facilidad del flujo de mensajes entre aplicaciones cliente y servidor. Los ICP son responsables de:

- Coordinar una transacción entre un proceso cliente y un proceso servidor.
- Realizar la transferencia de datos entre los dos procesos para que cada uno pueda completar el procesamiento de datos viejos antes de que lleguen los datos nuevos.
- Permitir que los procesos sean transparentes entre ellos.

1.4.2 Arquitectura Cliente

En las aplicaciones cliente-servidor las funciones del cliente son generalmente las que se ejecutan en la estación de trabajo del usuario final, y tiene la función de cliente-hardware. Los componentes de la estación de trabajo son: el hardware básico, el sistema operativo, el software de conectividad a las bases de datos, las aplicaciones, y opcionalmente una interfaz gráfica al usuario (Graphical User Interface, GUI).

En términos de hardware

El hardware que sirve como plataforma para la aplicación cliente se puede dividir en:

- *Terminales inteligentes.* En este caso, los componentes básicos de hardware del cliente incluyen la CPU, la RAM, los manejadores de dispositivos, y uno o más dispositivos de entrada y salida (teclado, mouse, monitor, etc.). Las estaciones de trabajo cliente pueden ser de tecnología propietaria, semipropietaria y totalmente abierta a los estándares.

- *Sistemas de cómputo independientes.* Este concepto no se refiere a una máquina en particular, sino a un conjunto de máquinas que actúan como un sólo cliente de un servidor que también puede estar conformado por un grupos de máquinas.

Existe otro tipo de terminales denominadas terminales tontas. Estas terminales no se consideran un cliente hardware debido a que tienen recursos limitados, con esto nos referimos a que no cuentan con una unidad de almacenamiento, ni con una unidad de procesamiento central (CPU), por lo general mínimamente sólo cuenta con memoria (RAM).

Para el caso de las terminales inteligentes, estas deben de contar con un sistema operativo, ya que este proveerá de sus operaciones a la máquina dando acceso a los recursos de ésta (memoria, almacenamiento en disco, etc.) además de manejar las interfaces entre la máquina y los dispositivos externos (impresora, video, etc.).

En términos de Software

Como se ha mencionado, el cliente es quien empieza la actividad en el modelo cliente-servidor y éste es el que interactua más directamente con el usuario. El cliente va de la mano con el servidor, es decir, cuando se tiene un software servidor, se debe de contar de igual manera con el software cliente que le hará las peticiones.

Existen versiones de clientes que pueden proporcionar al usuario la interfaz necesaria al tipo de sistema con el que se cuenta, además estas pueden ser desde una interface muy rudimentaria hasta interfaces sofisticadas. Un servidor software puede entender a clientes que se encuentren en una plataforma diferente a la de él, siempre y cuando este maneje el mismo protocolo. Por lo general cuando se tiene un servidor se pueden encontrar varias versiones del cliente para que pueda ser usado en cualquier plataforma. En Internet esto es muy común ya que en esta red se encuentran conectadas máquinas con diferentes plataformas que en determinado momento desean acceder a un determinado servicio en otra máquina que no cuenta con la misma plataforma del cliente.

Aunque existen diversos tipos de clientes para un servidor, dependiendo de la plataforma, estos varían en sus características de funcionalidad, esto es, todas las versiones de software cliente realizan una función principal pero tiene variantes dependiendo de lo que se quiera obtener como resultado final de la aplicación.

Por lo general, el software cliente cuenta con las siguientes características:

- Puede encontrarse en un sistema multiusuario para facilitar el compartir e integrar la aplicación.
- El software generalmente no se encuentra en forma encapsulada y es posible modificarlo.
- Accede de una manera más directa a muchos tipos de servidores.

En términos de software el sistema operativo, en el que se encuentra interactuando el cliente con el usuario, debe soportar, incluir o proveer la ejecución de la aplicación con interfaces estándares que permitan al usuario interactuar con la aplicación de manera fácil y que sea consistente a través de aplicaciones residentes en el ambiente. También se puede tener el caso de contar con una aplicación en donde se pueda usar una GUI para comunicarse con el usuario final, proporcionándole al usuario un ambiente más amigable.

1.4.3 Ventajas y Desventajas de Modelo Cliente-Servidor

El modelo cliente-servidor por su manera de trabajar presenta tanto ventajas como desventajas, sin embargo las ventajas hacen de este uno de los modelos más utilizados en ambientes de red. A continuación se mencionaran las ventajas y desventajas del modelo cliente-servidor:

Ventajas:

- Permite aprovechar mejor tecnologías de cómputo que se encuentran disponibles. En la actualidad las estaciones de trabajo de alto desempeño mejor conocidas como workstations y computadoras personales de alta tecnología, proveen un considerable poder de cómputo, disponibles anteriormente sólo en mainframes, a solo una fracción del costo de estos.

- Facilita el uso de las interfaces gráficas de usuarios que se encuentran disponibles en las estación de trabajo. Estas son interfaces que pueden estar distribuidas a los usuarios en gran variedad de presentación visual y con un fácil manejo de la interfaz dando una consistencia al basarse en estándares.

- Acepta sistemas abiertos; gracias a esto, existe la posibilidad de que los clientes y los servidores puedan correr en diferentes plataformas tanto de hardware como de software. Esta es una de sus grandes ventajas ya que el usuario se puede olvidar hasta cierto punto de arquitecturas propietarias particulares, dando así una ventaja competitiva de economía y de mercado para los diferentes productos abiertos disponibles.

A pesar de estas ventajas que proporciona y del nuevo concepto que presenta a los servicios basados en este modelo , se presentan algunas consideraciones de riesgo.

Desventajas:

- Cuando los recursos de un servidor son limitados y si se tiene un número creciente de usuarios finales que son los consumidores de recursos, resulta esto una desventaja, ya que cada día serán más solicitados y el servidor no podrá atender todas las peticiones solicitadas en un momento dado. Esta, sin duda, es una desventaja que debe de ser resuelta por una planeación adecuada a las necesidades del sistema.

- Las aplicaciones distribuidas, especialmente aquellas diseñadas para un procesamiento cooperativo, tienen la característica de ser más complejas de diseñar que las no distribuidas. Volviéndose ésta en una desventaja con respecto a los no distribuidos, sin embargo se puede solucionar eliminando parte de esta complejidad al reducir el problema grande en un conjunto de problemas pequeños.

En Internet se sigue el modelo cliente-servidor debido a la flexibilidad con que pueden interactuar el cliente y el servidor, dado esto, los desarrolladores adoptan los protocolos y estándares que permiten crear servicios fáciles de acceder y usar en la red mundial. Como se mencionó anteriormente Internet es la red mas ulllizada, esto se ha logrado gracias a las ventajas que ofrece el uso de este modelo en los servicios.

2. Fundamentos de Administración para un Servidor en Internet.

2.1 Sistema

En este trabajo nos referimos a sistema como a la organización de la plataforma y al conjunto de aplicaciones que darán soporte al servicio establecido.

La plataforma es la parte que contempla el hardware y el sistema operativo utilizado, la cual necesita reunir determinadas características para desempeñar el papel de servidor:

2.1.1 Características de la Plataforma del Servidor.

En el modelo cliente-servidor se establecieron las características que debe reunir la plataforma para poder desempeñar la función de servidor, éstas se mencionarán a continuación:

- Contar con un soporte multiusuario
- Ser escalable
- Tener un desempeño favorable para las necesidades del servicio
- Contar con un sistema de almacenamiento
- Soportar multimedios (opcionalmente)

Es común que se cuente con una máquina más potente que una computadora personal, aunque hoy en día ya contamos en el mercado con computadoras personales que tienen las suficientes capacidades para desempeñar el papel de servidor, sin embargo se recomienda que si se pretende tener un sistema servidor con un alto grado de demanda, se utilicen máquinas con capacidades superiores diseñadas especialmente para soportar un ambiente multiusuario.

En Internet se cuenta con una gran variedad de tipos de computadoras que desempeñan el papel de servidor. Hoy en día en el mercado de computadoras, existe una gran variedad. de arquitecturas que pueden soportar un ambiente multiusuario y cualquier proveedor puede proporcionar información sobre éstas, al igual que de sus especificaciones y costos, por lo tal razón, en este trabajo no se realiza ningún análisis sobre plataformas comerciales.

Para que un sistema sea multiusuario se debe de considerar el tipo de sistema operativo, ya que éste realiza el papel primordial. Este sistema operativo debe ser dedicado para trabajo en red y depende mucho de la plataforma hardware con la que se cuente para determinar el tipo de sistema operativo de red conveniente.

Una vez contempladas las características anteriores es necesario llevar a cabo un cuidado específico del equipo. Esta tarea es conocida como administración del sistema y consta de una serie de actividades que utilizando el sistema operativo y otras herramientas de software, permiten aprovechar los recursos de la máquina y así tener un control de éstos para hacer que el sistema sea utilizado de manera óptima.

2.1.2 Administración del Sistema

La administración del sistema nunca debe faltar, ésta debe ser constante y flexible a las necesidades que se presenten día con día, por esto, las personas encargadas de la administración deben contar con los conocimientos del sistema operativo necesarios para realizar esta tarea.

Generalmente, para llevar acabo una administración organizada se recurre a elaborar un plan de administración, sin embargo hay personas que no lo consideran importante, teniendo como resultado una administración deficiente, afectando a los servicios y causando desagrado en los usuarios.

Esta tarea puede ser realizada por una sola persona, aunque si es así, puede darse el caso de que en un momento dado se encuentre con una saturación de trabajo, provocando una administración deficiente, por esta razón recomendamos que se cuente con más de una persona, dependiendo del tamaño del sistema.

Si se cuenta con un grupo de personas para la administración, el trabajo debe estar distribuido de tal manera que no se repitan las mismas acciones por personas diferentes ya que esto ocasiona perdida de tiempo y conflictos dentro del grupo, además de desperdiciar los recursos humanos pudiéndolos aprovechar en otras actividades que beneficien la administración, es por eso que se necesita organizar a todas las personas que participen, de tal manera que no se deje sin atender ningún aspecto que se determine en el plan de administración.

A continuación se propone un plan de administración que abarca los aspectos primordiales a considerar en la administración propia de la plataforma hardware junto con sistema operativo (administración del sistema).

El plan de administración de un sistema lo consideramos como un procedimiento organizado para atender las necesidades de administración de los recursos del sistema, este procedimiento debe contemplar los siguientes aspectos:

- Administración Básica.
- Análisis de rendimiento y sintonización.
- Seguridad.

2.1.2.1 Administración Básica

La administración básica reúne una serie de actividades que engloban el cuidado mínimo que el sistema debe tener, estas actividades deben ser las suficientes de tal manera que garanticen el buen funcionamiento del equipo pero también deben ser amplias en cuanto a la perspectiva de crecimiento del sistema.

Actividades de la administración básica:

a) Políticas del Sistema

El administrador debe establecer la finalidad del sistema, además de definir los permisos y privilegios para los usuarios, en forma de reglas y procedimientos para el uso de los recursos, teniendo en cuenta casos especiales (como privilegios de acceso para cierto tipo de usuarios). Una vez establecidas éstas deben ser difundidas a los usuarios mediante una serie de avisos dentro del servicio que es o será accedido.

b) Instalación de Sistema Operativo de Red y Configuración.

En la administración básica, además de los aspectos anteriores, también se contemplan aspectos de configuración del propio sistema, es decir, desde la instalación del sistema operativo, la configuración de la máquina para que pueda hacer uso de la red, hasta la configuración de las aplicaciones o herramientas que se tendrán en el sistema.

La instalación del sistema operativo es una de las actividades fundamentales dentro de la administración ya que es aquí donde se definen los parámetros de configuración del sistema y de esto depende de la operación adecuada del mismo.

No hay que perder de vista que la elección del sistema operativo debe ser resultado de un análisis de requerimientos propios del hardware y de los servicios que se planean ofrecer, además es necesario conocer las características, ventajas y desventajas que ofrecen para llevar a cabo la elección de la mejor opción.

La configuración a red de una máquina que ofrece algún servicio en Internet se considera como un punto crítico dentro de la administración, ya que no se deben permitir fallas en la configuración debido a que afectan considerablemente la disposición de un servicio. La manera específica de configurar a red una máquina depende directamente del sistema operativo que se maneje, aunque en términos generales, en Internet cualquier configuración debe cumplir con las especificaciones de TCP/IP.

c) Control de Usuarios

Si el sistema cuenta con usuarios que ocupen el servicio proporcionado por el sistema como tal, es decir, usuarios internos que ocupan el sistema de almacenamiento, altas cantidades de procesamiento de CPU u otras aplicaciones del sistema, se debe contar con un control de estos usuarios.

El control de usuarios se refiere a tener un registro de todos los usuarios con los datos personales, además de tener un registro del tipo de uso que se le está permitido dar a la cuenta, es común que éste uso sea el mismo que la mayoría de los usuarios del sistema, sin embargo es sumamente importante contar con estos datos, ya que se puede detectar si algún usuario se encuentra rebasando los límites de lo que se le es permitido o bien que este pida que se le permita hacer uso de alguna otra aplicación o recurso específico.

Además este control de usuarios involucra que el administrador registre a los usuarios del sistema, sabiendo con cuantos usuarios cuenta y bien proporcionándole a cada uno los permisos necesarios para el uso de las aplicaciones o recursos que solicitó. Lo cual significa que el administrador cada vez que quiera adicionar un usuario al sistema, tendrá que registrarlo y abrir una cuenta con un identificador único que es llamado clave del sistema (login o identificador de usuario) y una contraseña única y secreta (password), además se le debe proporcionar los permisos adecuados al acceso de las aplicaciones o recursos. La clave y la contraseña formarán parte de la seguridad básica para acceder a la cuenta del sistema (ésta es una característica propia de un sistema multiusuario).

d) Administración del Sistema de Almacenamiento de Información

El espacio en disco es un requerimiento tanto para el sistema operativo como para el servicio, por esta razón se necesita tener un especial cuidado en la organización de todos los datos que se pretendan almacenar y cuidar que se tenga espacio disponible según lo que requiera el propio sistema o el servicio.

La manera en cómo se organice depende mucho del tipo de sistema operativo con el que se cuenta ya que de acuerda a éste hay recomendaciones para tratar los datos, ya sea formando árboles organizados, o alguna otra agrupación recomendada para el sistema operativo.

e) Mantenimiento del Equipo

Es necesario que el equipo cuente con un plan de mantenimiento que contemple la máquina en producción y todos sus dispositivos, este plan de mantenimiento puede estar formado por contratos con los proveedores de hardware o por planes de mantenimiento internos.

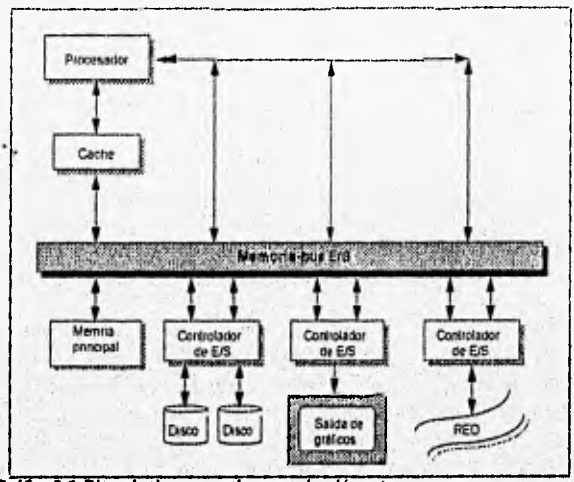
El mantenimiento se clasifica de dos formas: mantenimiento preventivo y mantenimiento correctivo. El primero se refiere a una verificación del sistema y limpieza del equipo para aminorar las posibles fallas, el segundo se refiere a que una vez acontecido un problema se deben realizar las actividades pertinentes para dejar al equipo en estado operativo. Es aconsejable que en el plan de mantenimiento se cubran ambos, ya que de esta forma se garantiza que el equipo mantendrá un buen funcionamiento el mayor tiempo posible redituando así, en la prestación de los servicios.

2.1.2.2 Análisis de Rendimiento y Sintonización

Anteriormente, "el rendimiento" se media generalmente en "tiempo de respuesta", es decir, desde que se pulsaba una tecla hasta que aparecía el carácter en la pantalla, y los dos únicos recursos implicados eran la red y la computadora central. En el mundo de los sistemas distribuidos el rendimiento general es determinado por la capacidad de todos los recursos participantes, es decir intervienen factores como la estación de trabajo del usuario, la red y el servidor.

En este caso nos enfocaremos al servidor y determinaremos en qué consiste y cuáles son los factores que intervienen en el rendimiento del sistema.

El rendimiento del sistema está limitado en gran medida por la parte más lenta del camino entre la CPU y los dispositivos de E/S, además de estar limitado también por la velocidad de cualquiera de estas partes del camino, la gráfica 2.1 muestra un ejemplo de cómo puede ser la comunicación de los recursos.

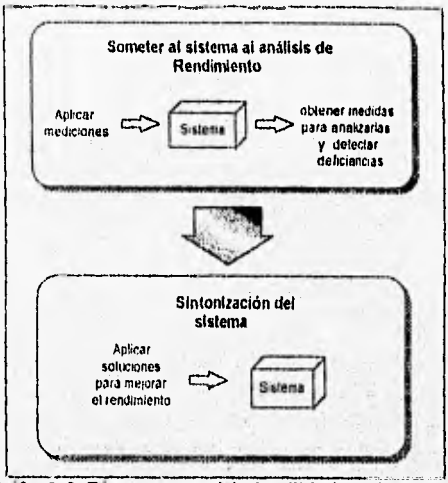


Gráfica 2.1 Ejemplo de como es la comunicación entre recursos.

Los principales factores que contribuye al rendimiento del sistema son carga de la CPU, memoria, subsistemas de entrada y salida, dispositivo(s) de almacenamiento y configuración de software, todos estos son considerados recursos del sistema.

Para poder tener un sistema con un alto rendimiento, se necesita someter a éste a un estudio de rendimiento de sus recursos, en donde se necesitará realizar las mediciones necesarias y un análisis de estas mediciones para hacer los cambios convenientes. Es así como podemos esquematizar en la gráfica 2.2 el modelo conceptual de rendimiento y sintonización.

El análisis de rendimiento y sintonización del sistema conocido como "performance and tunning" es una actividad que requiere una gran dedicación de tiempo y esfuerzo, además de una rigurosa organización para obtener éxito en su realización.



Grafica 2. 2 Diagrama general de el análisis de rendimiento y sintonización

A continuación se listarán los factores que intervienen en el rendimiento, con el fin de que sean tomados en cuenta para realizar el análisis:

- Configuración:

  Muchas veces la causa de un mal rendimiento es la configuración de aplicaciones, o bien del propio sistema, es por eso que siempre se debe tener en cuenta que: "un sistema que esta bien configurado puede dar un desempeño mucho mejor que cualquier otro que no lo este".

- CPU:

  El tener problemas de sobrecarga de trabajo en el CPU, puede significar que el CPU está gastando el mayor tiempo en realizar sus funciones y hace que el sistema sea muy lento.

- Sistema de memoria:

  La disputa empieza cuando los requerimientos de memoria en las actividades de los procesos exceden de la memoria disponible en el sistema, esto hace que el sistema baje su rendimiento o bien que no aproveche el máximo rendimiento que puede alcanzar.

- Sistemas de entrada/salida:

  Los Sistemas de entrada/salida son la fuente común de la contención de problemas en el rendimiento, por ejemplo: puede existir una cantidad finita de capacidad de entrada/salida que deberá ser compartida por todos los programas (incluyendo las del kernel del sistema operativo) que pueden estar corriendo concurrentemente.

- Unidades de almacenamiento:

  Los problemas que se pueden presentar en las unidades de almacenamiento ya sea por que esté averiado por que las características de éste son muy cortas a las requeridas repercute en el rendimiento del sistema cuando se trata de almacenar o leer datos.

Como todo, optimizar el rendimiento de un sistema es de alguna manera realizar algunos trueques en el. No se puede optimizar un aspecto del rendimiento sin que se comprometa otro aspecto, de cualquier manera, esto es importante para entender cual es el significado de la medición del desempeño y como se relacionan uno con otro.

Desde la perspectiva de los recursos del sistema, existe una solución fundamental a todos los problemas presentados: comprar más de algún recurso que hagan falta. Esto puede ser comprar más computadoras, más memoria, más disco y controladores de discos. Pero ésta resultaría muy costosa y, por lo tanto, no resultaría ser la óptima a los problemas de desempeño del sistema, en caso de no contar con los recursos económicos necesarios. Se recomienda que no hay que perder de vista que el objetivo fundamental de la sintonización, es obtener lo mejor que se pueda sacar del hardware que se tenga, pero si se decide que el escalamiento de algún recurso es la mejor solución, se debe de encontrar la mejor inversión de lo que se pague para realizar una mejora en el rendimiento, en este caso se debe mostrar exactamente lo que el sistema deberá necesitar para hacerle un escalamiento.

Cada uno de los recursos tiene sus problemas particulares, cuando se presenta un problema en algún recurso es complicado detectarlo ya que todos los recursos interactúan entre ellos. Sin duda alguna gran parte del trabajo que se debe realizar en el desempeño es conocer cuidadosamente que es lo que cada recurso del sistema hace: CPU, I/O, memoria y unidades de almacenamiento.

2.1.2.3 Seguridad del Sistema

Dentro de la administración se debe garantizar la seguridad del sistema, para que de esta manera se protejan los servicios que se proporcionan.

En el contexto de este trabajo, la seguridad la podemos entender como el conjunto de actividades que prevén o detienen las acciones no autorizadas, generalmente de usuarios externos, que afectan en forma negativa el funcionamiento de un sistema.

Hay que considerar que un sistema multiusuario cuenta con una seguridad básica implementada en el sistema operativo, la cual establece permisos y contraseñas de acceso, esta base sirve como soporte de aplicaciones más complejas de protección.

Lo anterior da lugar a niveles de seguridad, que van desde el más bajo de protección hasta el más completo para sistemas de alto riesgo. Existen diversos criterios para definir los niveles de seguridad, uno de los mas utilizados es el modelo que describe el "Libro Naranja", desarrollado por el Centro de Seguridad en Computo del Departamento de Defensa de los Estados Unidos. El Libro Naranja hace una descripción abstracta, y concisa de los requerimientos de seguridad para un sistema de computo, con lo cual provee una plataforma para construir y evaluar los sistemas y determinar su confiabilidad, esto lo logra dividendo los requerimientos de seguridad para formar niveles, en donde cada uno expresa un grado de confiabilidad del sistema, de esta manera se tienen siete niveles que describen desde el sistema con los mas elementales aspectos de seguridad hasta el sistema que contienen información secreta de estado.

Las desventajas de la utilización de este modelo se basan en que fue realizado para instituciones gubernamentales de los Estados Unidos y a pesar de cubrir el aspecto de información confidencial, trata en forma vaga los aspectos de disponibilidad y autentificación, además de no contemplar la seguridad en la comunicación. A pesar de esto, el modelo se puede utilizar como una guía en la elaboración de modelos particulares, dependiendo del nivel de seguridad que se desee alcanzar y de los objetivos que se establezcan.

Dentro de un sistema de seguridad que garantice la protección de un sistema, se deben llevar a cabo las siguientes actividades:

- Determinar la combinación adecuada de precauciones físicas y lógicas.
- Evaluar cada uno de los riesgos de seguridad.
- Realizar las funciones de monitoreo y vigilancia.
- Llevar bitácoras del sistema.
- Mantener contacto con el grupo de administración.
- Realizar procesos de selección e instalación de productos.
- Definir las acciones a tomar ante violaciones de seguridad.
- Establecer políticas de protección.

Estas funciones deben de realizarse con el fin de elaborar un plan íntegro que contemple todos los aspectos importantes del sistema.

Para generar un plan íntegro de seguridad se deben identificar en primer lugar, los recursos que se van a proteger así como las amenazas a las cuales son susceptibles, en segundo lugar se deben desarrollar sistemas que se dediquen a la verificación de la integridad del sistema y de los servicios (como son respaldos y control de accesos) y por último se debe establecer por cuanto tiempo se llevará a cabo la protección, esto con el fin de poner a prueba el sistema y verificar si los resultados obtenidos son los deseados. En el desarrollo del plan íntegro de seguridad se debe tener especial cuidado en la inversión de recursos humanos y monetarios que esto puede representar.

Las actividades mencionadas anteriormente se pueden organizar dentro de los siguientes aspectos:

a) Seguridad física.
b) Integridad de la información.
c) Accesos autorizados al sistema.
d) Políticas de protección y procedimientos en caso de violación al sistema

Es importante hacer notar que la forma de proporcionar seguridad a un equipo, depende de un análisis de las necesidades reales, ya que cada sistema tiene vulnerabilidades y objetivos específicos. Mediante este análisis se obtiene la información de cuales serán las mejores herramientas a utilizar, además de cómo y en qué momento se deben aplicar mediante la mejor estrategia de implementación.

En el caso de los sistemas que proporcionan servicios en red, la seguridad se convierte en una necesidad ya que existen muchos factores físicos y lógicos que pueden comprometer la disponibilidad de los servicios.

a) Seguridad Física

La seguridad física se refiere a los lineamientos que deben cumplir las instalaciones y el equipo de cómputo, pero también incluye el plan de protección del hardware y del software que conforman el sistema.

Todos los sistemas tiene vulnerabilidades, esto es, contienen puntos que son susceptibles de ataque. Estas vulnerabilidades pueden ser amenazadas por un posible daño al sistema, el cual puede ser realizado por una persona o un evento.

Las vulnerabilidades que podemos encontrar son las siguientes:

1. *Físicas*: Los equipos deben encontrarse en lugares seguros a los que sólo tenga acceso el grupo de administración.
2. *Hardware y software*: Se debe tener en cuenta que tanto el hardware como el software pueden tener defectos en su fabricación y desarrollo, lo que provoca que este sea un aspecto muy importante de cuidado.
3. *Medios de almacenamiento*: La parte del hardware que corre los más altos riesgos son los medios de almacenamiento: discos y cintas. Estos deben ser protegidos para que la información contenida en ellos se mantenga íntegra.
4. *Comunicaciones*: Una actividad ampliamente difundida es la intercepción de mensajes a través del canal de comunicación.

Las amenazas que se pueden encontrar y contra las cuales se deben realizar acciones realmente efectivas, son:

- *Naturales*: Este tipo de amenaza se refiere a los desastres naturales que pueden ocurrir, y también se contempla al polvo y a la excesiva humedad.

- *Físicas*: Se refiere a los daños físicos que se les puede causar a los equipos y a los medios de almacenamiento.

- *No intencionales*: Se pueden causar daños al sistema de forma no intencional, es decir, por descuido o por ignorancia.

- *Intencionales*: Son los daños causados con el fin explícito de alterar o probar de alguna forma el sistema, este tipo de amenaza puede ser explotada por los siguientes usuarios de la red:
  - *Usuarios externos*: Conocidos como crackers y hackers. Los crackers son personas que tienen metas destructivas que van desde borrar información hasta dañar al sistema físicamente. Los hackers son personas que sólo prueban al sistema sin causar daño.
  - *Usuarios internos*: Pueden ser usuarios del sistema que por alguna razón (como puede ser sabotaje y espionaje interno entre otras) desean alterar el sistema en forma negativa.

El plan de seguridad debe ser lo suficientemente robusto para que pueda abarcar todas las vulnerabilidades y sea capaz de proteger, de se posible, contra todas las amenazas. El grado de protección en el sistema depende del tipo de servicio que se desee dar y de las políticas que se establezcan para cada sistema.

b) Integridad de la Información.

La seguridad debe garantizar que la información que se encuentra en los discos (principalmente internos) del sistema sea íntegra, esto es, que la información cumpla con las siguientes características:

- La información propia del sistema no debe sufrir alteraciones sin autorización.
- La información del sistema debe estar actualizada y completa.

Si la información vital del sistema (como lo son los archivos de configuración y los archivos binarios), cumple con las características mencionadas, entonces se está cubriendo uno de los principales puntos dentro de la seguridad del equipo, ya que frecuentemente las fallas de seguridad son producto de una mala configuración o de modificaciones incorrectas en los archivos vitales.

Un aspecto importante para garantizar la integridad del sistema, es el realizar respaldos periódicos ya que estos son útiles porque hacen recuperable la información en caso de pérdida. Las causas que pueden provocar la pérdida de información son: errores de usuarios, errores de los administradores, daños intencionales de agentes externos, fallas de hardware, fallas de software, robo de equipo y desastres naturales.

Otro de los aspectos dentro la integridad de la información, es el contemplar la posibilidad de que la información que viaja a través de los canales de comunicación sea interceptada, copiada o alterada, esto hace necesario buscar mecanismos que garanticen la confidencialidad e integridad de la misma de la mejor forma posible. Para enfrentar esta situación, una de las herramientas más útiles es la criptografía.

La criptografía convencional basa su funcionamiento en la utilización de una sola "llave" para realizar el cifrado, esta llave única es utilizada el usuario que envía información utilizando un algoritmo que encripta y que debe ser también utilizada por el usuario que va a desencriptarla, este tipo de criptografía tiene las siguientes desventajas:

- Para poder ser utilizado es necesario realizar un previo intercambio de la llave mediante un canal de comunicación seguro (si existiese este canal seguro para transmitir la llave, sería innecesaria la utilización de la criptografía).
- El intercambio de llaves puede llegar a ser difícil o costoso.
- La cantidad de llaves que se requieren para intercambiar información entre un número grande de personas crece demasiado.
- Es imposible el intercambio de información entre personas que no hayan tenido un previo arreglo o contacto para un intercambio.

Estas limitaciones de los sistemas de criptografía de llave única, que los hacen imprácticos para un uso rutinario y a gran escala, llevó a la creación de un nuevo tipo de criptografía llamado criptografía de llaves públicas. Esta criptografía se basa en la utilización de dos llaves, una utilizada para encriptar el mensaje y otra distinta, utilizada para desencriptarlo, estas dos llaves se encuentran relacionadas matemáticamente entres sí, pero el conocimiento de una de ellas (llave pública), no permite deducir cual es la otra.

Actualmente el uso de la criptografía se a difundido ampliamente en Internet con el fin de proteger la información que viaja a través de la red, resguardándola de posibles alteraciones, y a sido tal el éxito de este mecanismos que muchos de los servicios ofrecidos en Internet la integran a si mismos en forma transparente para el usuario.

c) Accesos Autorizados al Sistema

Es importante tener control sobre los accesos al sistema ya que pueden existir accesos de usuarios externos que comprometan al sistema en forma grave, de hecho las acciones que un cracker puede realizar son variadas, por ejemplo, puede modificar, reemplazar o eliminar archivos binarios del sistema o del servicio y modificar archivos especiales, frecuentemente el cracker realiza estas acciones con el fin de garantizarse un acceso ilimitado a los recursos, o bien, de provocar una caída de sistema.

Otros tipos de usuarios que pueden obtener accesos no autorizados, son los hackers, los usuarios con permisos básicos o especiales y personas con claves prestadas o robadas, estos pueden llegar a causar daños considerables si utilizan herramientas especializadas o simplemente si ignoran el adecuado uso del sistema.

Los accesos no autorizados al sistema una vez realizados son difíciles de monitorear, debido a esto, es aconsejable instalar herramientas de monitoreo que permitan descubrir el acceso en el instante que se realiza, o bien, detectar fallas en el sistema antes de que sean utilizadas.

Otro aspecto ha considerar son los accesos a los servicios, ya que éstos deben ser realizados por personas consideradas como usuarios permitidos debido a que muchas veces éste sirve como puente para obtener acceso no autorizado al sistema.

Dado a que ésta es una de las principales preocupaciones de seguridad en Internet, se ve la necesidad de poder controlar las peticiones de servicios a través de la red, para esto, actualmente son utilizadas los métodos de filtración de paquetes que constituyen una manera eficaz para controlar el tráfico en la red. Tales métodos tienen la ventaja de no afectar las aplicaciones del cliente o del servidor, pues operan en las capas de transporte y de red (modelo OSI), las cuales son independientes de los niveles de aplicación. Debido a que la mayoría de los métodos de filtración no realizan el filtrado de los paquetes UDP y RPC en forma efectiva, es necesario involucrar otros métodos llamados barreras de protección o paredes de fuego.

Las barreras de protección son mecanismos que operan en las capas superiores del modelo OSI y tienen como objetivo principal proteger una red de otras aislando el tráfico a través de ellas, para esto, tienen la información completa sobre las funciones de los servidores, en la cual basan sus decisiones de control. En general, la red que se protege es responsabilidad del administrador y la red contra la que se protege es externa, en la que no puede confiarse y desde la cual puede violarse la seguridad.

Proteger la red es prevenir que los usuarios no autorizados tengan acceso a datos del sistema delicados y permitir que los usuarios legítimos tengan libre acceso a los recursos de la red. La barrera actúa como un punto que monitorea y rechaza el tráfico en la red a nivel de aplicación.

Existen dos principios en los cuales se basan todos las barreras de protección desarrolladas actualmente:

- Lo que no esta expresamente permitido esta prohibido:
  En esta caso las barreras de protección bloquean todo el tráfico y el administrador debe configurar los permisos para soportar cada servicio.

- Lo que no esta expresamente prohibido esta permitido:
  Sólo se bloquean los servicios que son potencialmente un riesgo, debido a esto los usuarios externos pueden encontrar debilidades en los sistemas remotos.

Actualmente hay tres tipos de barreras de protección más utilizados son:

1. *Rutcadores de Selección.*

Son los dispositivos que hacen sólo el ruteo de la información permitida al interior de la red, tienen la desventaja de tener un registro de las actividades muy pobre, las reglas de selección son difíciles de establecer, no contienen autentificación, no todos los servicios están soportados por lo que son un riesgo para la red interna.

2. *Anfitriones de Bastión.*

Un anfitrión de bastión es un anfitrión de barrera de protección que es determinante para la seguridad en la red ya que su configuración lo hace ser el único punto de acceso a la red interna, debido a esto, es el anfitrión central para la seguridad en la red de una organización. Esto significa que el anfitrión de bastión debe ser monitoreado con constantemente por los administradores de la red.

3. *Anfitriones de Dos Bases.*

El término anfitrión de bases múltiples se refiere a una máquina que tiene múltiples interfaces de red, es decir, contiene mas de una tarjeta de red donde cada una se conecta a una red diferente. La función de enrutamiento en el anfitrión de bases múltiples esta inhabilitada, debido a esto el anfitrión puede aislar el tráfico en la red, donde cada red procesará las aplicaciones en los anfitriones de bases múltiples.

El anfitrión de dos bases puede aislar una red interna de una red externa no confiable, como el anfitrión no envía tráfico TCP/IP, bloquea por completo cualquier tráfico IP entre las redes no confiables interna y externa.

Si los servicios en Internet se ejecutan en el anfitrión de dos bases, pueden configurarse para transmitir servicios de aplicación desde una red hacia la otra, si los datos de aplicaciones deben cruzar la barrera de protección, es factible configurar los agentes emisores de aplicación para hacer la ejecución en el anfitrión de dos bases. Estos agentes son programas especiales, utilizados para enviar solicitudes de aplicación entre dos redes. Otro método es permitir que los usuarios se conecten al anfitrión de dos bases y después tengan acceso a los servicios externos desde una interface de la red externa del anfitrión.

Si se mantienen los registros adecuados de las conexiones de usuarios, es posible rastrear las conexiones no autorizadas a la barrera de protección, en el momento en que se descubra una brecha de seguridad.

d) Políticas de Protección y Procedimientos en Caso de Violación.

Se deben establecer las políticas a seguir por los administradores y los usuarios con la finalidad de asignar derechos y responsabilidades para ambos y proteger los recursos del sistema.

También se deben establecer las acciones a tomar en caso de detectarse una violación al sistema así como determinar cuáles son los pasos a seguir para la recuperación del mismo, estos procedimientos deben definirse a lo largo de cada uno de los aspectos contemplados anteriormente ya que es necesario establecerlos para los casos específicos que se encuentren.

2.2 Servicio

Dado el objetivo de este trabajo de tesis, ésta resulta ser la sección más importante, debido a que se plantea la forma en cómo se puede proporcionar un servicio de calidad en Internet.

Al referirnos a software estamos contemplando la parte lógica que realizará la tarea del servidor según el tipo de servicio que se ofrece, sin embargo no hay que descartar la importancia que tiene la administración del sistema ya que sin ésta el servicio no podrá lograr su fin.

Entonces podemos decir que una vez establecida la administración del sistema, el siguiente paso es la administración del servicio. La administración del servicio consta de las tareas necesarias para mantener un servicio actualizado, que esté siempre funcionando y además que se logre en forma eficiente.

2.2.1 Características del Servicio

Los servicios desarrollados para Internet cumplen con las siguientes características:

- Base el protocolo TCP/IP:

  Como estos servicios se presentan en Internet, deben tomar como base el conjunto de protocolos TCP/IP. Para esto, es necesario que se sepa cómo es que trabaja este conjunto de protocolos en Internet (ver apéndice Conjunto de protocolos TCP/IP).

- Se basan en el modelo Cliente-Servidor en términos de software.

  Los servicios en Internet se estructuran bajo la arquitectura cliente-servidor, es por eso que deben cumplir con las especificaciones determinadas en términos de software del modelo

Siendo el software servidor objeto principal, se deben establecer la características con las que debe contar implícitamente para tener una visión clara de los requerimientos que se necesitan.

2.2.2 Administración de Servicios

La administración del servicio consiste en una serie de lineamientos que permiten que éste se mantenga utilizable.

Como ya se mencionó la administración del servicio se refiere a la administración del software servidor como tal, ésta es particularizada según el tipo de servicio y por tal razón es necesario establecer los puntos generales y particulares que podemos contemplar en dicha administración.

Los recursos humanos con los que se cuenten para realizar esta tarea, es otro aspecto a considerar, el grupo de personas que se dedique a realizarla debe estar en constante comunicación con el personal que se encarga de la administración del sistema.

Dentro de la administración de servicios se puede considerar la administración básica especializada dependiendo del tipo de servicio. Sin embargo, se deben contemplar las actividades de contabilidad de uso, monitoreo y seguridad como actividades generales independientemente del tipo de servicio.

Estas actividades se tratan en forma amplia a continuación.

2.2.2.1 Administración Básica

La administración básica de los servicios consiste en un conjunto de tareas que involucran el cuidado básico del servicio, es necesario que ésta se realice constantemente y de manera correcta ya que si se llegan a cometer errores en esta administración repercutirá en la calidad del servicio que se este prestando.

a) Establecimiento de Políticas de Uso

Se deben establecer las políticas de uso del servicio que sirvan para que los usuarios no cometan abusos que vayan en contra del objetivo principal del servicio.

El establecimiento de políticas es una actividad necesaria cuando se presta un servicio, ya que de esta manera se podrá determinar lo que es permitido y lo que no en el uso del servicio, dando como resultado que el servicio tendrá el fin determinado por los que proporcionan el servicio y de esta manera se podrá delimitar las actividades del usuario dentro del servicio para proteger de cierto modo al propio servicio.

b) Estudio de Crecimiento

Consiste en realizar un estudio del crecimiento futuro del servicio ya que éste debe ser conocido por los administradores del sistema para que ellos planteen soluciones ante posibles saturación de algún recurso del sistema y así prevenir algún problema en la disponibilidad del servicio por falta de recursos.

c) Actualizaciones del Servidor.

Cuando se tiene un servicio funcionando, es necesario que el administrador esté actualizado respecto a los avances que se realicen en dicho servicio, es decir, el administrador debe buscar nuevas versiones de éste, ya que es común que conforme pasa el tiempo se liberen otras versiones, en donde se atacan algunas vulnerabilidades que se hayan tenido en versiones anteriores, o bien, que se hayan realizado algunas mejoras en sus funciones o inclusive tener más funciones para dar un mejor servicio.

Cuando se encuentre una versión nueva del servidor, antes de sustituir a la que se encuentra operando, se deberán realizar una serie de actividades, ya que de esta manera se podrá conocer antes todas las nuevas facilidades y funciones del servidor así como las fallas y puntos vulnerables que pueda tener.

d) Estudio de Nuevos Servicios

No hay que descartar la idea de que conforme la tecnología avanza se están desarrollando nuevos servicios, por lo que es necesario que el administrador sepa de la existencia de estos y realice su evaluación para determinar si es factible que se pueda proporcionar dicho servicio y tener así servicios de punta en Internet.

e) Desarrollo de Servicios.

En caso de requerirlo, se debe considerar el poder desarrollar interfaces para que algunos servicios operen entren si, obteniendo como resultado un servicio más robusto. Esto no descarta la posibilidad de realizar cambios del código fuente de servidor atacando algunos errores encontrados, o bien, para adecuar el servicio de manera correcta a la plataforma en donde operará, por cuestiones de derechos de autor, esta actividad generalmente sólo se puede realizar en servidores de dominio público en donde se autoricen la modificación del código fuente.

f) Administración Básica para Servicios de Información

La administración de un servicio de información resulta ser una tarea muy comprometedora, ya que se necesitan cuidar muchos aspectos para que la información se este presentado de una manera agradable al usuario y éste se encuentre satisfecho de accederla y encontrar lo deseado.

Información organizada

En este tipo de servicios se debe contar con la información agrupada en un lugar del sistema de manera organizada para que al usuario le sea fácil encontrarla y accederla.

La organización de la información debe seguir cierto criterio establecido por los propios administradores dependiendo el tipo de información a manejar, además, este criterio debe darse a conocer mediante el mismo servicio a los usuarios antes de que empiecen a navegar por el servicio.

Actualización de la información

La actualización de la información es un aspecto estratégico para que el servicio sea popular ya que mientras más actual sea la información, será mas atractivo y por lo tanto más accedido.

Cuando se tiene un servicio que consta de una herramienta de búsqueda de información, generalmente se cuenta con un conjunto de información concentrada en archivos (con el formato correspondiente según las especificaciones del servidor), al igual de contar con sus archivos generados al momento de indezarlos, estos últimos archivos contienen los índices que servirán para que el servidor encuentre la información requerida por el usuario. Es sumamente importante no descuidar la actualización de la información de los archivos, así como su nueva indización para que la búsqueda que se realice contemple la nueva información.

Formato de la información

El formato de la información es un aspecto que no se debe descuidar el administrador del servicio, dado a que la presentación de la información debe de cumplir con los requisitos de formato propios del servidor para que ésta sea legible por los usuarios. Por esta razón toda la información presentada en el servicio debe de cumplir ese formato.

g) Administración Básica para Servicios de Comunicación

Cuando se cuenta con un servicio de comunicación la administración de éste es propia de la administración del sistema, dado a que éstos necesitan hacer uso de recursos del sistema directamente.

Existe algunos de estos servicios que utilizan más recursos que otros, por lo general todos los recursos ocupan memoria, procesador y un gran uso del sistema de entrada y salida a red, sin embargo hay algunos que requieren del sistema de almacenamiento, para lo cual se necesita del establecimiento de políticas de su uso además de un estricto control de usuarios ya que podrían afectar en la disponibilidad del servicio.

2.2.2.2 Contabilidad de Uso

La contabilidad es uno de los aspectos que no deben olvidarse ya que con este se puede dar cuenta el administrador si el servicio es realmente accedido y que tanto lo es. Estos datos pueden ser indicativos para detectar fallas tanto del sistema como del servicio, o bien si el servicio ha sido exitosamente accedido.

2.2.2.3 Monitoreo del Servicio

El monitoreo del servicio consiste en la revisión periódica de su disponibilidad y del estado en que se encuentra, esta revisión se realiza con el fin de detectar problemas en el momento en que se generen para así encontrar una solución con la cual el servicio se pueda recuperar rápidamente.

Los aspectos principales que se deben monitorear son:

- Que el servidor esté siempre disponible
- Verificar que estén funcionando adecuadamente los programas servidores.
- Estado de los recursos requeridos por los servicios.

2.2.2.4 Seguridad del Servidor

El aspecto de la seguridad del servicio está muy relacionado con la seguridad del sistema, ya que en ésta se contemplan todos lo puntos necesarios que garanticen la integridad del servicio.

Cuando sea instalado el servidor, se debe realizar de una manera confiable para el sistema implementando la seguridad máxima de acuerdo al tipo de uso que tendrá, dado a que si no se implementa su seguridad es posible que algún usuario mediante una sesión en el servicio logre corromperlo y tener acceso directo a los recursos del sistema pudiendo realizar actividades ilícitas.

Generalmente los servicios cuentan con seguridad implícita que permite limitar al servicio en su uso si se detectan actividades ilícitas por parte de alguno usuario o grupo de usuarios. Esta limitación del servicio debe estar sujeta a las políticas establecidas por el grupo de seguridad de la administración del sistema.

En caso de que el servicio no contenga seguridad implícita, o bien, si se desea que la seguridad sea más estricta, se pueden instalar o desarrollar herramientas que la proporcionen.

2.2.2.5 Atención a Usuarios

Una de las principales razones de la existencia del servicio son los usuarios, por lo que el administrador siempre debe tomar en cuenta las opiniones o necesidades que pueden presentar, ya que ellos son los primeros que resienten la calidad de éste.

Existen varias formas de estar en contacto con los usuario atendiendo sus necesidades, sin embargo es necesario considerar los recursos y el servicio que se proporcionan para determinar de que manera se le dará atención.

3. Procedimientos de Administración para un Servidor en Internet.

3.1 Plan para la Puesta en Operación de un Servidor

Si se desea implementar un servicio es necesario llevar a cabo un estudio de la plataforma necesaria (es decir, hardware, sistema operativo, versión del software servidor), esto con el fin de seleccionar la adecuada. La puesta en operación comprende los siguientes aspectos:

1. Selección de la plataforma del servidor

Antes de elegir la plataforma del servidor es necesario saber cual servicio en Internet se desea poner a disposición (*ver apéndice de Servicios en Internet*).

Sabiendo cuál es el servicio o servicios que se desea prestar se debe contactar con proveedores de diferentes marcas y arquitecturas que proporcionen características de propias de hardware, como CPU, memoria principal (RAM), memoria secundaria (capacidad de almacenamiento en disco) y subsistema de entrada-salida. De esta manera se podrán plantear varias alternativas y elegir la que mejor se adecue a las necesidades y al presupuesto.

2. Configuración

Una vez seleccionando el hardware necesario se debe dar paso a la configuración del sistema y del servicio. La configuración del sistema consta de la instalación del sistema operativo y de la configuración a red, a continuación se describirán las actividades propias de cada aspecto.

Instalación del sistema operativo

Se debe seleccionar el sistema operativo más adecuado de acuerdo a las características de la plataforma hardware y a su marca.

La instalación del sistema operativo de red debe realizarse según las indicaciones propias del producto adquirido, frecuentemente se necesita realizar una distribución organizada del sistema de almacenamiento, en caso de contar con discos duros, estos se debe particionar.

Para realizar la partición se necesita previamente hacer un estudio de capacidades y asignar los tamaños a cada partición, se consideran dos grupos de particiones:

- *Almacenamiento para el servicio:*

  Se debe de tomar en cuenta el análisis que se realizó cuando se selecciono el hardware y de esta manera definir el tamaño que tendrá la partición, se recomienda que si se van a tener grandes volúmenes de datos, se tenga un distribuya la información en diferentes particiones, de tal manera que la información no se concentre en una única partición demasiado grande, o bien considerar algún sistema tolerante a fallas con el fin de proteger la información.

- *Almacenamiento para el sistema operativo*:

  El espacio requerido por el sistema operativo depende de las especificaciones propias de éste, aunque en general se puede realizar una instalación básica, completa o completa con utilerias especiales. Para esto se recomienda que se ayude de la documentación del sistema operativo adquirido.

Configuración a Red

Debido a que el servicio se pondrá a disposición de los usuarios de Internet, se debe asegurarse de que el sistema operativo de red utilizado cuenta con el conjunto de protocolos TCP/IP, en caso de no contar con estos es necesario realizar la instalación, una vez teniendo estos protocolos se deben determinar los siguientes aspectos en la configuración interna del sistema:

- La clase de red al que pertenecerá la máquina (*)
- Dirección IP y dominio (*).
- Determinar el nombre de la máquina
- Mascara de red, tomando en cuenta si existen subredes (*)
- Ruteador por omisión (Default gateway) (*)
- El servidor de nombres (*)

***NOTA:** (*) Todos estos aspectos deben ser determinados por el administrador de red correspondiente al dominio.*

Una vez determinados los datos anteriores, estos deben ser incluidos en los archivos de configuración propios del sistema, aunque dependiendo de la versión de NOS, estos pueden ser configurados desde la instalación del sistema operativo.

3.- *Instalación del Servicio*

En cuanto a la configuración del servicio se deben contemplar las actividades necesarias que forman parte de la instalación del software servidor, como son:

Búsqueda del software servidor

Existen dos fuentes para la adquisición de un software servidor, estas son: con un proveedor de software comercial, o bien, que este sea un software de dominio público (que no incluye ningún tipo de garantías ni soporte), con la ventaja de que el costo de adquisición es nulo.

Independientemente de la fuente de adquisición se debe cuidar que el software del servicio que se desea proveer sea la versión mas actualizada, para que funcione con las características deseadas, como son funciones de seguridad y contabilidad mejoradas. (Ver apéndice Servicios Internet).

Instalación del Software servidor

En el caso de que el servidor se adquiera comercialmente deben de seguirse las indicaciones de la documentación de éste.

Es común que si el software es de dominio público, para su instalación es necesario contar con un compilador, en caso de no contar con alguno puede adquirirse, también, de manera comercial o de dominio público. El punto de partida para la instalación del servicio es que ya se cuenta con compilador y que éste funciona adecuadamente, ya que muchas veces el éxito de la instalación depende del compilador.

Antes de la compilación del servicio es necesario configurar los archivos indicados en la documentación, ya que por lo regular se requieren las especificaciones de las características de la plataforma operativa, también no se debe olvidar habilitar la opción de poder registrar accesos, actividades de los usuarios y la seguridad que contiene en forma implícita.

Una vez teniendo el servidor compilado, se deben realizar las pruebas suficientes para garantizar que el servicio funcionará adecuadamente, los resultados de las pruebas deben ser cotejados con los objetivos o resultados que se esperan obtener de ellas.

Las pruebas deben constar de las siguientes actividades:

- En el caso de ser un servicio de información se deben poner a disposición datos para la prueba
- Habilitar un puerto lógico
- Simular accesos
- Utilizar todas las funciones posibles del servicio
- Verificar los registros de la contabilidad
- Verifica Seguridad

Si los resultados obtenidos son satisfactorios se debe proceder a la liberación del servicio.

4. Liberación del Servicio.

Para la liberación del servicio, en el caso de los servicios de información, se requiere colocar la información en las particiones planeadas en forma organizada (Seguir procedimiento de Organización de Datos en el Plan de Administración de Servicios). Para los dos tipos de servicios, de información y de comunicación, es necesario habilitar un puerto lógico de acceso al servicio público, esto se debe hacer dependiendo de los puertos que se tengan disponibles, por lo general para cada servicio es sugerido un puerto específico, el cual se puede consultar en la documentación de dicho servicio.

El último paso en la liberación del servicio es el darlo a conocer, es decir, se le debe de dar difusión dentro de Internet mediante la publicación de la existencia de este en los diferentes servicios de información, además realizar publicaciones por otros medios de comunicación.

3.2 Plan de Administración del Sistema

A continuación se mencionaran los procedimientos que corresponden a la administración propia del sistema.

3.2.1 *Recursos Humanos*

La asignacion de los recursos humanos para poder llevar acabo la implementación del plan de administración, consiste en dividir el trabajo en tres áreas, en estas se realizarán las actividades planteadas en cada uno de los procedimientos correspondientes. Las áreas son las siguientes:

1. Administración básica
2. Análisis de desempeño y sintonización
3. Seguridad

El número personal asignado en cada área depende del tamaño del sistema, de la infraestructura del personal con el que ya se cuenta y del que se pretende integrar, pudiendo ser una sola persona, si el sistema no es muy grande.

3.2.2 *Administración Básica*

Políticas del Sistema

Para establecer las políticas del uso sistema se debe:

- En caso del servicio de comunicación, determinar los tipos de usuario y cuáles son los recursos que les será permitido utilizar del sistema.
- Determinar el uso correcto de los recursos, esto es, delimitar la manera y en que cantidades será ocupado determinado recurso.
- Dar a conocer a los usuarios las políticas establecidas.
- Determinar las responsabilidades del administrador.

Control de Usuarios

Dentro del control de usuarios se necesita llevar a cabo una revisión del seguimiento de las políticas, esto es, verificar cómo se utilizan los recursos mediante diversas formas como pueden ser:

- Si se tiene la facilidad de asignar permisos por tipos de usuarios, se debe de verificar que la asignación de los permisos sea de manera correcta según lo que es permitido para cada tipo de usuario.

O bien,

- El realizar un monitor, en caso de contar con archivos que registran la actividad de cada usuario (estos archivos son llamados log), se puede realizar verificando estos archivos.

En el caso de servicios de comunicación, el control de usuarios también involucra el registro de datos y de uso de recursos por usuario. Este registro debe llevarse a cabo en forma organizada, la forma de auxiliarse en este registro es mediante formas, estas pueden administrarse en forma electrónica o manual. La hoja de registro que proponemos para datos personales y para asignación de recursos es la siguiente:

Datos Personales				Identificador de usuario	Tipo de usuario	Recursos asignados	
Nombre	Ocupación	Dirección	Teléfono			CPU	Almacenamiento Utilerías del sistema

Es recomendable realizar una base de datos en la que se registren estos datos, sobre todo en el caso de contar con un número de usuarios tal que el manejo de formas en papel sea una tarea impráctica.

Administración del Sistema de Almacenamiento de Información.

El procedimiento de administración del sistema de almacenamiento de información consiste en:

1. Verificar que la información correspondiente al sistema operativo se encuentre en donde se determinó que estaría.
2. Cerciorarse que la información del sistema operativo no esté corrupta.
3. Que la información que se tenga a disposición por medio de un servicio de información se encuentre realmente en la parte del sistema de almacenamiento en donde se planteo que estaría.
4. Realizar una constante revisión del estado físico del sistema de almacenamiento y en caso de que se encuentre alguna falla seguir el procedimiento de mantenimiento correctivo.
5. Realizar un monitoreo periódico de espacio libre en el sistema de almacenamiento, con el fin de prevenir saturaciones en este sistema. Se debe realizar una depuración de archivos temporales y de los archivos que no sean autorizados dependiendo de las políticas establecidas para los usuarios.
6. Se deben asignar permisos de accesos, lectura o escritura a áreas de información sensible (como lo son archivos de configuración o archivos binarios). Esto se hace con fin de proteger información que es esenciat para el sistema (archivos de configuración tanto del sistema operativo como del propio software servidor).

Mantenimiento del Equipo

Los aspectos pertenecientes al mantenimiento preventivo deben seguir un calendario de las siguientes actividades:

1. Verificar la configuración del sistema, para poder detectar posibles fallas que repercutirán en el estado operativo del servidor.
2. Realizar periódicamente una limpieza física del equipo y dispositivos.

Una vez acontecida una falla en el equipo se debe proseguir a realizar el mantenimiento correctivo, el cual consisten en lo siguiente:

1. Detectar el problema principal, esto es, localizar qué parte del sistema está fallando, ya que muchas veres una falla se ve reflejada en otros aspectos del sistema.
2. Establecer cuál es la causa de dicha falla. Este consiste en verificar si realmente es un problema físico o es un problema de configuración, para esto se puede apoyar en la contabilidad del sistema y en herramienta de monitoreo del análisis de rendimiento.
3. Plantear soluciones. Una vez detectando si la falla fue física, se requiere verificar el estado del dispositivo averiado, para esto se puede solicitar ayuda de un experto de dicha arquitectura con el soporte técnico del proveedor. Si fue falla de configuración se debe consultar a los manuales para reconfigurar el dispositivo de manera correcta.

Para los dos tipos de mantenimiento puede establecerse un contrato con el proveedor que se contactó para adquirir el equipo o con alguno otro que se considere que tenga experiencia en el área, es importante que se establezcan garantías posteriores al mantenimiento.

Monitoreo del Sistema

El monitoreo del sistema consiste en verificar si el equipo se encuentra en modo operativo, para poder realizar esto se puede hacer lo siguiente:

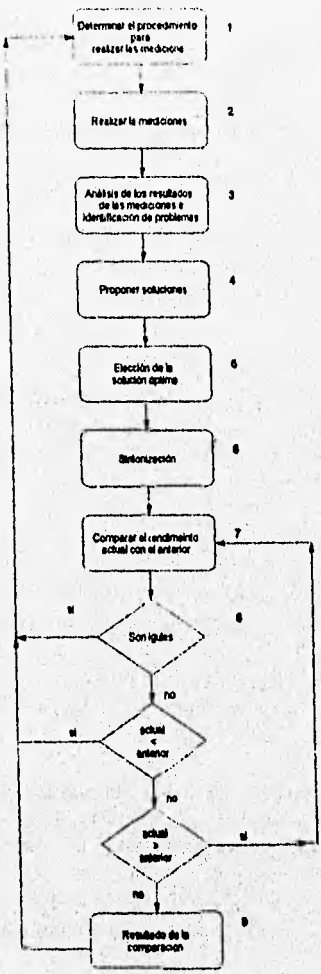
- Monitoreo manual por parte de los administradores del sistema:
  Este monitoreo se debe realizar en forma periódica realizando una conexión remota al servidor.

- Monitoreo automático utilizando un software específico:
  Este monitoreo debe ser realizado desde una máquina que no este proveyendo algún servicio, sino que sea un equipo dedicado a vigilar si esta en modo operativo el servidor, dado a que en caso de que el sistema no este operando la máquina encargado de vigilar pueda avisar de alguna manera al administrador sin que ésta se encuentre con trabajo pesado como lo estaría algún sistema que presta un servicio en Internet.

Se deben realizar los dos tipos de monitoreo, para tener un control en la disponibilidad del servidor.

3.2.3 Análisis de Rendimiento y Sintonización.

Se recomienda que antes de empezar se busque y se estudie información acerca de este tema enfocado a la plataforma con la que se cuenta e inclusive conocer claramente la arquitectura hardware.
Una manera organizada en realizar este análisis, es seguir el procedimiento que a continuación ilustramos:



Como se observa el procedimiento se divide en nueve pasos:

1. *Determinar la Manera en Cómo Realizar las Mediciones.*

Para determinar el procedimiento que se llevará acabo para realizar las mediciones se requiere conocer las utilerías que se tienen en el sistema operativo de plataforma, una vez identificadas y elegidas las que se emplearán en la medición, se debe conocer las especificaciones propias del hardware con el que cuenta. Con ayuda de las utilerías del sistema operativo se necesita medir los recursos susceptibles a tener un bajo rendimiento como : sistemas e entrada y salida, subsistema de almacenamiento, CPU, memoria y otros recursos que son utilizados por aplicaciones.

Hoy en día existen algunas herramientas que fueron desarrolladas especialmente para medir el desempeño de un sistema, estas se pueden adquirir por distintos proveedores de hardware y sòftware, o bien, se pueden adquirir algunos que sean de dominio público. El hecho de contar con una herramientas de estas, facilitará el trabajo de realizar las mediciones, por lo que se recomienda que se adquieran.

Si se cuenta con la contabilidad propia del sistema, ésta puede ayudar para dar una idea de lo que puede estar sucediendo en el sistema y detectar algunos problemas.

Se debe de tomar en cuenta que la principal medición que se debe realizar es el tiempo de ejecución de tareas. Por lo cual recomendamos que se elijan algunas tareas y propiciar un estado en el sistema que posteriormente se pueda volver a generar para realizar las mismas mediciones después de la sintonización.

2. *Realizar las Mediciones.*

Independientemente de la manera como se realicen las mediciones del rendimiento, éstas se deben llevar acabo cuidadosamente, ya que de ello dependerá el éxito de la sintonización.

3. *Análisis de los Resultados de Mediciones e Identificación de Problemas de Desempeño.*

Para identificar los problemas que pueden tener los recursos del sistema es necesario realizar un análisis de las mediciones ayudándose de las especificaciones propias del hardware.

Los problemas identificados deben de tratarse con cuidado, ya que es necesario realizar un estudio de estos para ver las causas que lo están generando.

4. Proponer Soluciones

Una vez identificados los problemas y las causas, se debe realizar una lista de posibles soluciones, para esto se debe empezar con una lluvia de ideas.

Existen algunas teorías y leyes que pueden ayudar a obtener una solución, esta leyes y teorías son utilizadas en el diseño de computadoras y son aplicables de igual manera cuando se determina cómo emplear los recursos.

Uno de los principios más utilizados para determinar el empleo de los recursos es el de "Incrementar el caso común", el cual menciona que: "Al realizar un diseño, favorece el caso frecuente sobre el infrecuente ". Este principio se aplica cuando se determina el empleo de recursos, ya que el impacto de hacer alguna ocurrencia más rápida es mucho mayor si la ocurrencia es frecuente. Mejorar el evento frecuente en lugar del evento raro, evidentemente esto ayudará a incrementar el rendimiento. Además el caso frecuente es por lo regular, más sencillo y puede realizarse de forma más rápida que el caso infrecuente" [1].

Entonces podemos decir que al aplicar este principio se debe proponer las soluciones partiendo del problema más frecuente hasta el problema menos frecuente.

5. Elección de la Solución Óptima.

En este paso se debe evaluar cada una de las soluciones respondiendo dos preguntas:

1. *"¿Qué va a pasar si ....?"*
2. *"¿Qué pasa si se incrementa el número de usuarios?"*

Para esto se recomienda que se realice otra lista en donde se respondan estas preguntas para cada una de las soluciones propuestas en el paso anterior. Para responder estas preguntas es conveniente que se consulten las especificaciones del hardware para determinar las limitantes en las soluciones, además de aplicar intuición y sentido común.

De esta manera con la lista que se obtenga servirá como apoyo para tomar la solución que ofrece mayores ventajas, esto permitirá determinar el primer impacto del sistema después de la sintonización.

[1] *Hennesy john, Pattersom David. "Computer Architecture, A Quantitative Approch".*

No hay que olvidar que la solución elegida debe ser la más apegada al concepto de sintonización que se mencionó en el capítulo anterior, ya que el principal propósito de ésta es lograr subir el nivel de rendimiento procurando realizar los mínimos cambios posibles en el hardware. En caso de elegir una solución en donde se requiera invertir se debe de tomar en cuenta el presupuesto con el que se cuente y el costo total de la inversión para ver si la solución es viable o si se requiere elegir otra solución en donde no se tenga que invertir más del presupuesto.

Si se considera que la plataforma es obsoleta porque se detectó un gran número de deficiencias de capacidad en la misma, o bien que el equipo no es el indicado para realizar las tareas asignadas, se debe de pensar en migrar a otro hardware servidor.

6. Sintonización

La sintonización consiste en aplicar la solución que se eligió en el paso anterior, pero antes de aplicarla, se debe de realizar un plan de actividades:

Si se requiere realizar una inversión:

- Se debe de contactar a proveedores de productos.
- Hacer la elección del producto
- Solicitarlo al proveedor
- Instalar el producto y configurar lo necesario para que funcione, las configuraciones deben ser cuidadosamente determinadas ya que el rendimiento dependerá en gran medida de éstas.

Si se requiere migrar a otro equipo:

- Hacer un respaldo de la información del sistema y del servicio que se tenga en producción.
- Empezar la aplicación del esquema desde la puesta de operación de un servidor.
- La información del servicio debe ser restaurada del respaldo hecho.

Si no es ninguna de las soluciones anteriores, se requiere listar una a una las actividades necesarias para aplicar la soluciones elegidas y llevarlas a cabo.

7. Mediciones del Nuevo Rendimiento.

Después de realizar la sintonización se requiere volver a evaluar al sistema, para esto se deben hacer las mismas mediciones y con el mismo procedimiento que se efectuó en los pasos 1 y 2.

8. Comparar los Dos Rendimientos, Antes y Después de la Sintonización.

Las mediciones que se realizaron deben evaluarse para poder comparar el rendimiento del sistema, para eso llamaremos al rendimiento anterior " A " y al rendimiento actual "B".

El rendimiento lo mediremos como el tiempo de respuesta (el tiempo transcurrido entre el comienzo y el final de una tarea, denominado también tiempo de latencia o de ejecución).

La comparación se realizará mediante el cumplimiento de la siguiente frase " el rendimiento B es mejor que el rendimiento A", es decir, el tiempo de ejecución con un rendimiento B es inferior al tiempo de ejecución con un rendimiento A para un tarea dada, o bien, B es *n* por ciento más rápida que A , lo que significa que :

$$\frac{\text{Tiempo de ejecución}_A}{\text{Tiempo de ejecución}_B} = (1 + n)/100$$

Como el tiempo de ejecución es el recíproco del rendimiento, se mantiene la siguiente relación:

$$(1+n)/100 = \frac{\text{Tiempo de ejecución}_A}{\text{Tiempo de ejecución}_B} = \frac{\frac{1}{\text{Rendimiento}_A}}{\frac{1}{\text{Rendimiento}_B}} = \frac{\text{Rendimiento}_B}{\text{Rendimiento}_A}$$

De esta manera *n* se puede considerar un incremento en el rendimiento.

Al aplicar el principio de " Incrementar el caso común" , se tiene como resultado la Ley Amadahl, con la cual se puede cuantificar la ganancia de rendimiento mediante, esta ley establece que: "La mejora obtenida en el rendimiento al utilizar algún modo de ejecución más rápido esta limitada por la fracción de tiempo que se puede utilizar en ese modo de ejecución más rápido".

Esta ley define la ganancia de rendimiento que es vista como una aceleración (speedup) que puede lograrse al obtener una mejora en sistema de manera que cuando se utilice aumente su rendimiento. Entonces la ganancia de rendimiento está definida por la siguiente relación:

$$\text{Ganancia de rendimiento} = \frac{\text{Rendimiento de la tarea completa utilizando la mejora cuando sea posible}_B}{\text{Rendimiento de la tarea completa sin utilizar la mejora}_A}$$

Alternativamente se puede tener que :

$$\text{Ganancia de rendimiento} = \frac{\text{Tiempo de ejecución de la tarea sin utilizar la mejora A}}{\text{Tiempo de ejecución de la tarea utilizando la mejora cuando sea posible n}}$$

Esta ganancia nos indicará la rapidez con que se realizará una tarea utilizando el rendimiento A con respecto al rendimiento B

NOTA: Las fórmulas utilizadas fueron obtenidas del libro Computer Architecture. A quantitative Approach de John L. Y David A. Pettersen.

9. Resultado de la Comparación:

a) Si el rendimiento actual es mayor que el rendimiento anterior

Si la *ganancia de rendimiento* es mayor que 1 y *n* es mayor que cero, entonces se ha logrado una mejora considerable en el rendimiento, sin embargo se debe realizar un monitoreo del rendimiento por medio de las mediciones y realizando comparaciones, es decir , se debe realizar el procedimiento a partir del paso 7.

Este monitoreo tiene que ser periódico, se recomienda que se realice cada 15 días, o bien, en caso de darse cuenta de alguna falla en el sistema.

b) Si el rendimiento anterior es igual que el rendimiento actual.

Si la *ganancia de rendimiento* es igual a 1 y *n* es igual a cero, se debe realizara una revisión de todo lo que se realizó para así identificar porque no se produjo mejora del desempeño.
Si el problema fue que no se siguió el plan para aplicar la solución adecuadamente, se debe de proceder la realización del método, en caso de que esta no sea la causa, se debe aplicar el proceso de nuevo desde el primer paso.

Cabe considerar que si el rendimiento medido de A y de B son iguales debido a que no se tenían muchos problemas que solucionar (se debieron solucionar todos los problemas detectados), ésta se considera aceptable y se debe proceder al monitoreo constante del sistema y partir del paso 7. El monitoreo se debe realizar de la misma manera en la que se describió en el inciso a).

c) Si el rendimiento anterior es mayor que el rendimiento actual.

Si la *ganancia de rendimiento* fue menor que 1 y *n* menor que cero, se debe proceder a la aplicación del proceso desde el primer paso, ya que seguramente el análisis y la sintonía no fue realizados correctamente.

3.2.4 Seguridad

Los pasos para garantizar la seguridad en un sistema que proporciona servicios en red son lo siguientes:

1. *Seguridad física.* Realizar un plan de protección física para el hardware y el software que conforman el sistema, este plan necesita de un análisis de riesgos de todos los recursos.
2. *Integridad de la información.* Garantizar que la información contenida en el sistema no está corrupta.
3. *Accesos autorizados al sistema.* Verificar todos los accesos al sistema para prevenir cualquier modificación no autorizada en el mismo.
4. *Establecimiento de políticas de protección.* Determinar políticas que regulen el comportamiento de los usuarios, así como generar lineamientos específicos que los administradores deben tener en cuenta y determinar las acciones a tomar en caso de violación de una política. También se deben establecer los procedimientos en caso de detectarse una violación en el sistema para que de esta forma se asegure la recuperación del sistema.

Seguridad Física

La serie de pasos que definen este procedimiento son los siguientes:

1. Determinar los recursos vulnerables que se requieren proteger, estos pueden ser identificados de la siguiente manera:

- Hardware: procesadores, tarjetas, unidades de disco y medios de almacenamiento secundario como lo son las cintas y discos con información grabada.
- Software: programas auxiliares a la administración, utilerías, sistema operativo y programas de comunicación.
- Datos: datos almacenados, datos en tránsito sobre medios de comunicación y registro de bitácoras.
- Documentación: sobre programas, manuales de hardware y documentos auxiliares en la administración.

De acuerdo a la finalidad del servicio que se presta se deben identificar los recursos más importantes a proteger, ya que de no hacer esta selección se corre el riesgo de sobrevalorar un recurso innecesario y saturar el sistema de seguridad.

2. Determinar contra que amenazas se va a proteger .

Se debe comprender que tan reales son las amenazas para los recursos, para esto es necesario identificar en cada tipo de recurso cuáles son la vulnerabilidades por las que puede ser atacado. Para dar un mejor panorama se describe la siguiente tabla:

	AMENAZAS		PRINCIPALES CAUSANTES DE LAS AMENAZAS	
Recurso vulnerable	Daño físico	Alteraciones lógicas	Usuarios Internos	Usuarios Externos
Hardware	✓		✓	
Software		✓	✓	
Datos	✓	✓	✓	✓
Documentación	✓		✓	

3. Análisis de riesgos. Una vez identificadas las vulnerabilidades y las amenazas, el siguiente paso es realizar un análisis de riesgos que permita evaluar al sistema en forma íntegra.

Los riesgos se clasifican por el nivel de importancia del recurso y por la severidad de la pérdida que éste representa, debido a esto es necesario tener en cuenta que no se debe llegar a la situación de gastar mas para proteger lo menos valioso. De acuerdo a Karanjit Siyan y Chris Hare (Internet Firewalls and Network Security) [2], en el análisis de riesgos es necesario determinar los siguientes factores:

- Estimación del riesgo de pérdida del recurso (Ri)
- Estimación de la importancia del recurso (Wi)

Es posible cuantificar estos valores al asignarles un valor numérico (0 - no existe riesgo, 10 - riesgo mas alto), en donde la evaluación general del riesgo será entonces el producto numérico del valor del riesgo y su importancia (peso del recurso).

$$WRi = Ri * Wi$$

con las siguiente notación:

i es el recurso,
W.Ri es el peso del riesgo del recurso,
Ri es el riesgo del recurso,
Wi significa la importancia del recurso.

[2] *Karanjit Sryan Ph.D. Chis Hare "Internet y Seguridad en Redes", 1995*

De esta manera se puede tener una forma de registro que contenga el peso del riesgo de todos los recursos en forma organizada para facilitar el análisis de riesgo.

Nombre del recurso	Riesgo de pérdida del recurso Ri	Importancia del recurso Wi	Peso de riesgo WRi

Con esto se logra una jerarquía en los recursos, de los cuales los que tengan el mayor peso de riesgo deben ser protegidos en forma estricta y se les deben aplicar los métodos de protección antes que a los otros recursos.

4. Determinar cómo se va a proteger, este aspecto debe determinar el nivel de seguridad física que se requiere, además de la instalación o desarrollo de software de seguridad.

En primer lugar se deben detectar las formas en que se puede dañar el equipo:

- Pérdida total, como puede ser robo, o si se ocasionó un daño que pueda ser considerado como pérdida total del equipo.
- Pérdida parcial, el equipo se daño por alguna causa sin que esto provoque pérdida total.

La forma de proteger el hardware contra estos dos tipos de daños varía mucho dependiendo de lo estricto que se desee planear la protección y del costo que esto represente, por lo que se debe elegir la mejor manera de proteger los recursos de una manera económica y oportuna.

En segundo lugar se debe realizar un estudio del software requerido para proteger el sistema, esta estudio consiste en determinar cuales programas proveen una mejor protección. Es aconsejable contar con programas que al menos cubran con las funciones de encriptamiento, control de acceso a los servicios y a los sistemas y programas de monitoreo en general.

5. Por cuanto tiempo se va a proteger

Determinar si la protección del sistema requiere de:

- Planeación de protección a corto plazo, esto es con el fin de realizar pruebas para verificar la efectividad del plan de protección.
- Planeación de protección a largo plazo, si ya se cuenta con un plan de protección que resultó exitoso en sus pruebas, se pueden establecer las actividades específicas para llevarlo a cabo en un plazo de tiempo largo.

Integridad de la Información

Un factor importante para garantizar la integridad de la información es el realizar respaldos, estos garantizan que aunque se lleve a cabo una modificación o alteración grave del sistema, éste se pueda recuperar su estado correcto en corto tiempo.

Para esto es recomendable generar un calendario de respaldos para cada sistema que preste servicios en Internet, éste dependerá del valor de la información a proteger y de la frecuencia de modificación de la información. Una vez estableciendo un calendario de respaldos, el siguiente paso es realizar un *sistema íntegro de respaldos*. A continuación se presentan las características principales con que debe cumplir un sistema de respaldos para un sistema que proporciona servicios en red:

1. Los respaldos deben realizarse en forma constante dependiendo del calendario establecido, además no deben existir rompimientos drásticos en la secuencia del calendario.
2. Se deben tener más de un dispositivo con las mismas características para realizar los respaldos, esto trae diversas ventajas como son: realizar respaldos en forma paralela, garantizar que se tiene una unidad funcionando en caso de emergencias y realizar pruebas sin afectar a los sistemas en producción.
3. Tener medios de almacenamiento disponibles, ya sean cintas o discos; una forma de lograrlo es reutilizar las unidades después de un tiempo razonable, el cual depende de la frecuencia de los respaldos, por ejemplo, se pueden tener hasta un juego de cintas por seis meses y reutilizarlas al término de este si la información que contiene ya no es útil.
4. Determinar qué parte de la información se va a respaldar, esto es necesario debido a que no toda la información del sistema es vital o necesaria.
5. Se deben realizar respaldos en forma separada para el sistema y para el servicio, con el fin de mantener la información organizada. Por lo que es recomendable generar calendarios de respaldos para los dos tipos de información.
6. Si se tiene más de un sistema en producción, es factible establecer un sistema más completo que realice respaldos automáticamente. Este tipo de sistemas consta de un análisis previo para determinar cuál será la unidad de almacenamiento y como se manejarán los diversos calendarios de respaldos.

Para establecer el calendario se puede utilizar la siguiente forma:

Fecha	Sistema Directorio a respaldar	Servicio Directorio a respaldar	Comentarios

Accesos Autorizados al Sistema

Sólo se debe permitir el acceso a los recursos del sistema a usuarios autorizados, esto es, usuarios con permiso previo cuyo comportamiento esté regido por las políticas que se establezcan para el uso del servicio.

Dentro de el control de los accesos del sistema se deben cubrir los siguientes aspectos:

Primero, es necesaria una verificación constante de los accesos al sistema con el propósito de detectar cualquier anomalía, esta verificación debe de cubrir los siguientes aspectos:

- Verificar que los recursos hayan sido utilizados por usuarios permitidos.
- De ser el caso de detectar un acceso no autorizado, es necesario determinar el origen del usuario que lo realizó para restringir de manera estricta el acceso a los recursos.
- Las acciones a tomar en contra del usuario infractor dependen de las políticas que se establezcan, las cuales se describirán a detalle más adelante en éste capítulo.
- Si el sistema sufrió alteraciones debido al acceso no autorizado, se debe proceder a determinar que modificaciones existen en el sistema o en algún recurso, para que posteriormente se realice su restauración.

Ya que los accesos no autorizados se realizaron generalmente a través de la red, es necesario determinar algún tipo de protección para los puertos lógicos por los cuales se accede al sistema, esta protección de incluir las siguientes tareas:

- Utilizar encriptamiento en los puertos necesarios.
- Restringir el uso de puertos, esto es, cancelar los puertos del sistema que son innecesarios o que no se utilizan.
- Monitorear una contabilidad mas estricta del acceso a los puertos.
- Instalación una barrera de protección.

Por último, se debe realizar una verificación de las claves de acceso de las cuentas del sistema, ya que éstas pueden ser violadas por personas ajenas al sistema, con lo cual pueden disponer de los recursos que la propias clave les permita. Por esto se hace indispensable establecer políticas en cuanto a la forma de asignación de la clave, para establecer esta política, se debe determinar lo siguiente:

- Establecer periodos de tiempo para realizar una renovación de claves de acceso.
- Establecer las características de la clave de acceso.
- Revisar periódicamente las claves de acceso, mediante algún método específica, con la finalidad de prever los accesos no autorizados.

Debe procurarse que el proceso anterior se realice en forma automática con herramientas ya sean de origen público, comercial o desarrolladas en forma exclusiva, esto con la finalidad de agilizar la detección accesos no autorizados.

Establecimientos de Políticas de Protección.

Definir una política de seguridad del sistema significa desarrollar procedimientos y planes que salvaguarden los recursos contra pérdidas y daños, para esto se debe examinar con frecuencia si los objetivos o circunstancias no han cambiado dentro del sistema.

Las políticas de seguridad se definen al determinar los siguientes aspectos:

1. Definir a qué tipo de usuarios se les permiten utilizar los recursos

   La forma de llevar a cabo esta tarea es hacer un listado de usuarios permitidos, indicando el recurso que pueden acceder. La política debe establecer qué tipo de uso es aceptable e inaceptable y qué tipo de uso será restringido. Estas políticas pueden definirse junto con las políticas de uso del sistema mencionadas anteriormente.

2. Dentro del grupo de administración se debe definir qué personas están autorizadas para garantizar el acceso y aprobar el uso de los recursos.

   Si hay un gran número de administradores de sistemas, es difícil mantener el control de los permisos que han sido otorgados para los recursos, por lo que es necesaria una organización del personal y una división de funciones en el mismo.

3. Definir cuáles son los derechos y las responsabilidades del usuario.

   El usuario puede hacer uso de los recursos que le son otorgados según los lineamientos del sistema, además de que no se le puede negar el acceso sin una justificación.
   Se debe mantener confidencialidad en la información personal de los usuarios, por lo que no debe ser permitido ningún tipo de violación. El usuario es responsable de administrar su cuenta en el sistema y de no permitir el uso de la misma a personas ajenas al sistema.

4. Determinar los derechos y responsabilidades del administrador del sistema frente a los del usuario.

   Una de las funciones de el administrador es el proporcionar en forma adecuada los recursos que le fueron asignados a cada uno de los usuarios, además de determinar si la información sensible (o vital de la máquina) debe estar a disposición de los mismos o debe estar completamente oculta. También debe garantizar la confidencialidad de todo tipo de información contenida en el sistema.

Todas las funciones del administrador deben estar orientadas a dar un buen servicio a los usuarios.

5. Deben definirse las sanciones tanto para administradores como para usuarios en caso de que estos no cumplan con lo establecido en las políticas de administración y uso del sistema.

   En caso de detectar accesos no autorizados al sistema, se debe determinar a quien le corresponde tener una notificación del hecho, dependiendo de las acciones que se quieran llevar a cabo en contra del intruso y de la necesidad de ayuda para rastrearlo. Además es necesario definir un procedimiento de recuperación del sistema para garantizar que el servicio estará disponible en el menor lapso de tiempo posible.

En cuanto a los procedimientos en caso de violación al sistema, estos deben ser definidos dentro de cada uno de los aspectos mencionados arriba, ya que estos son procedimientos muy específicos que dependiendo del tipo de sistema y de los daños encontrados en el mismo.

3.3 Plan de Administración de Servicio

Una vez que es liberado el servicio se deben seguir los procedimientos referentes a su administración.

3.3.1 Administración Básica para los Dos Tipos de Servicios:

Recursos Humanos

La asignación de recursos humanos consiste en determinar el grupo de personas que se va a encargar de la administración del servicio.

a) *Servicios de información:*

Para las actividades como: organización de Datos, actualización de datos y cuidado del formato de los datos; resulta ser trabajo un poco pesado según las cantidades de información periódica a actualizar, además del cuidado excesivo que se debe de tener en el formato que deberá tener la información para que el servidor pueda mostrar al usuario correctamente. Si se está en el caso de contar con grandes volúmenes de información y con un corto periodo de actualización, es recomendable que un grupo de personas se encarguen exclusivamente a esta tarea. Estas personas deberán estar capacitadas respecto a las características del formato de la información requerida por el servidor.

En caso de que la fuente de información sea externa, es recomendable que a la persona encargada de proporcionarla se capacite para que la entregue lo más acercado al formato requerido por el servidor. Este debe ser un acuerdo entre la persona que proporciona la información y el administrador del servicio que se encarga de las actualizaciones de los datos, en caso de llegar a este acuerdo, el administrador debe tener los datos de la persona que es responsable.

Las demás actividades como lo son: establecimiento de políticas de uso del servicio, estudio de crecimiento, actualizaciones del servidor, estudio de nuevos servicios, desarrollo de servicios deben ser realizadas por personas dedicadas exclusivamente a dichas actividades.

b) Servicios de comunicación:

En el caso de un servicio de comunicación, las personas que se pueden dedicar a su administración, pueden ser las mismas que se dedican a la administración del sistema, ya que las actividades de ambos están relacionadas.

Establecimiento de Políticas de Uso del Servicio:

El procedimiento para establecer la políticas resulta ser subjetivo, ya que depende de la finalidad de la existencia del servicio, a continuación mencionaremos algunos de los giros que un servicio en Internet puede tener:

- Académico
- Investigación
- Comercial
- Asuntos Gubernamentales

Para establecer las políticas no se deben de perder de vista los siguientes aspectos:

- Se deben prohibir actividades ilícitas (por ejemplo propagar noticias que puedan afectar a la sociedad en los aspectos económicos, políticos y sociales).
- El uso debe ser exclusivamente el determinado según la finalidad del servicio.
- Los usuarios no deberán tomar al servicio como un medio para provocar terrorismos (por ejemplo la propagación de virus informáticos).
- No se deben realizar actividades que puedan afectar en la disponibilidad del servicio, ni que puedan perturbar el uso de éste a los demás usuarios.

Estudio de Crecimiento

a) Servicios de comunicación:

Para el sistema de almacenamiento es necesario establecer:

1. La capacidad total de almacenamiento disponible para todos los usuarios, para esto es recomendable descontar un 20% del total disponible con la finalidad de poder tener un espacio de holgura.

2. El máximo número de usuarios, se debe de realizar la siguiente operación: Máximo número de usuarios = capacidad total de almacenamiento / Cuota establecida para cada usuario.

Una vez teniendo el número máximo de usuarios, se debe considerar el número de procesos promedio que puede soportar el sistema, al igual que el número de conexiones, esto con el objetivo de establecer si el sistema es adecuado para soportar ese número de usuarios.

En caso de que se establezca que no puede soportar ese número usuarios el sistema se recomienda que se disminuya el número de usuarios de tal manera que pueda ser soportado por todo el sistema. No hay que perder de vista que es necesario saber el número máximo de usuarios que el sistema puede soportar ya que sobrepasar este límite puede afectar a la calidad de servicio.

b) *Servicios de información*:

El estudio de crecimiento referente a los servicios de información se debe determinar sólo para el sistema de almacenamiento, ya que los demás aspectos del sistema serán atacados en el análisis de rendimiento y sintonización del servidor.

El procedimiento referente a este tipo de servicios solo involucra determinar la cantidad de información promedio que se adiciona en cierto periodo de tiempo, es decir, realizar un cálculo para determinar en el crecimiento del servicio y saber hasta cuanto el sistema puede crecer.

1. Determinar el espacio total disponible para almacenar información menos un 20% que se considera de holgura.

2. Establecer la cantidad promedio de información que se adiciona al mes para realizar esto se necesita hacer un estudio mínimo de 3 meses.

3. Promedio del numero máximo de mes que se podrán almacenar = espacio disponible / contada de información promedio a actualizar en un mes.

En caso de que la capacidad del sistema de almacenamiento no sea la suficiente para toda la información que se planea almacenar, se puede considerar la posibilidad de adicionar medios de almacenamiento externos.

Actualizaciones del Servidor

La actualización del software consiste en lo siguiente:

1. Estar en contacto directo con las novedades en Internet.

2. Buscar de manera constante si hay versiones recientes del software servidor con el que se cuenta.

3. En caso de encontrar una nueva versión se requiere hacer un análisis de las especificaciones de requerimientos, de tal manera que se pueda asegurar que esa versión tenga mejoras que beneficien. Para esto se recomienda que se revise la documentación que se encuentra acerca de esa versión.

4. Si es atractiva, se debe recurrir a una Instalación del software (ver procedimiento de instalación de software en el plan de puesta en operación de un servidor).

Estudio de Nuevos Servicios

El estudio de nuevos servicios consiste en lo siguiente:

1. Para estar informado de los nuevos servicios que se encuentran en Internet es recomendable que de alguna manera se esté navegando constantemente mediante algún servicio de información dentro de Internet y así poder saber de las novedades en cuanto a servicios.

2. En caso de encontrar algún nuevo servicio, se recomienda que se considere la posibilidad de poder prestar este. Para esto no se debe de perder de vista la razón por la cual se esta prestando un servicio en Internet y si se cuenta con los recursos para poder proveerlo.

3. Si pretende proveer este nuevo servicio, entonces debe referirse al procedimiento de instalación del servicio en el plan de puesta en operación de un servidor.

Desarrollo de Servicios

El desarrollo de servicios debe considerarse solamente en caso de tener alguna necesidad específica o si la finalidad al prestar el servicio en Internet es el de Investigación. Para esto se recomienda seguir los siguientes paso:

1. Plantear los objetivos del desarrollo del servicio, para que de esta manera se puedan establecer las políticas de uso.

2. Tener en cuenta el modelo cliente-servidor para el desarrollo de un nuevo servicio, ya que de esta forma se podrá proveer a través de Internet (ver especificaciones del software servidor, capítulo dos).

3. Considerar el poder modificar un servicio existente, en este caso también se debe mantener el modelo cliente-servidor, sin perder de vista la existencia de los derechos del autor.
4. Antes de la liberación del servicio se deben realizar pruebas sobre su funcionamiento y verificar que no existan fallas en el software que impliquen problemas al utilizarlo.

5. Debe considerarse que el nuevo servicio tenga funciones que ayuden a la administración, como son la contabilidad del mismo.

6. Dar a conocer el nuevo servicio para que éste sea utilizado por la comunidad de Internet.

Procedimientos a Considerar en la Administración Básica para Servicios de Información

Organización de Datos:

1. La información puede organizarse de acuerdo a un criterio, como puede ser, por tema en un orden alfabético, realmente el criterio a seguir es subjetivo, ya que depende del tipo de información que se este manejando.

2. En la organización se debe mostrar al usuario un índice de cómo se encuentra estructurada la información.

3. Realizar un documento en donde se de el panorama general de lo que trata dicha información, quién la proporciona y a dónde se puede dirigir en caso de dudas y comentarios, para proporcionarlo a los usuarios dentro del servicio de información.

4.Una vez teniendo esto es importante que nunca se descuide la actualización de estos índices y documentos de referencia.

5.Realizar una constante verificación de que la información este en el lugar que le corresponde.

6.La información que no es reciente y/o poco accedida puede colocarse en otro medio de almacenamiento externo.

Actualización de datos:

1.La presentación de la información debe cumplir con los requisitos de formato propios del servidor. En caso de que la información que es proporcionada ya tenga un formato, el administrador del servicio deberá verificar que el formato sea el adecuado.

2.Si la información no es proporcionada con el formato, el administrador del servicio deberá darle a la información el formato requerido.

3.Poner la información en la estructura organizada.

Es recomendable que se realicen programas que lleven a cabo las actualizaciones de manera automática, ya que muchas veces, los pasos que se siguen resultan ser generalizados para cualquier tipo de información. Una vez automatizada esta tarea el administrador sólo tendrá que supervisar que la información se encuentre disponible en el servicio. Al finalizar la actualización se debe verificar que el servicio se vea correctamente o identificar posibles errores, esto solo se puede realizar manualmente accediendo al servicio como cualquier usuario final.

En caso de que la información sea proporcionada con el formato adecuado, los administradores del servicio deben revisar esta información antes de presentarla en el servidor para poder identificar posibles errores en el formato.

3.3.2 Contabilidad de Uso

1. Obtener los archivos en donde se registran los accesos y/o actividades que se tienen en el servicio.
2. Contabilizar el número total de accesos y las actividades realizadas en el servicio.
3. Teniendo los datos anteriores se deben generar reportes estadísticos.
4. Realizar una automatización de esta tarea con la elaboración de programas que se ejecuten automáticamente cada determinado tiempo.

3.3.3 Monitoreo del Servicio

1. Verificar que se esté ejecutando el software servidor, esto puede realizarse

   - Ya sea accediendo el servicio
   - Confirmando que el programa residente servidor esté ejecutándose.

   En caso de que se detecte que el programa del servidor no esté de manera residente es necesario registrar su estado en una bitácora y hacer que el programa se ejecute de manera residente.

   Se recomienda que ésta tarea se automatice ya que el procedimiento para realizar el monitoreo requiere un tiempo considerable por parte de los administradores, además de que esta tarea es un procedimiento que no cambia.

2. Las funciones del software servidor deben realizarse correctamente, esto se puede determinar realizando accesos al servicio y probando las funciones del software servidor.

Si el servicio no responde se debe verificar si la falla fue del sistema o del servicio, en caso de ser falla del sistema se debe recurrir al grupo de administración del sistema y analizar el problema ya que éste puede ser causado por limitantes propias de la plataforma, en caso de ser falla del servicio se debe detectar si:

- La versión del software servidor contiene un error propio de su desarrollo, en este caso se debe seguir el procedimiento de actualización del servicio, o bien, el procedimiento de desarrollo de servicios con el fin de corregir el error detectado.
- Los archivos de configuración del servicio contienen los datos correctos.

3.3.4 Seguridad del Servicio

1. Si el servicio no cuenta con seguridad que se pueda activar en su configuración, entonces se debe recurrir a la instalación de herramientas auxiliares de seguridad.
2. Se requiere un monitoreo constante de las actividades realizadas por los usuarios del servicio para poder detectar cualquier acción que no esté de acuerdo con las políticas establecidas en las políticas de uso del servicio. Este monitoreo debe ser muy estricto ya que un acceso no autorizado puede comprometer en forma grave tanto al servicio como al sistema.
3. En caso de detectar alguna acción ilícita dentro del servicio se debe denegar acceso al servicio por violación de las políticas.

Las actividades que involucran este procedimiento se pueden automatizar de tal manera que sólo se tengan reportes de sucesos o alarmas en caso de peligro en el sistema.

3.3.5 Atención a Usuarios

Una de las principales razones de la existencia del servicio son los usuarios, por lo que el administrador siempre debe tomar en cuenta las opiniones o necesidades que pueden presentar, ya que ellos son los primeros que resienten la calidad de éste.

La manera en como se realiza la comunicación entre el administrador y el usuarios puede variar dependiendo de las políticas establecidas, las principales formas de comunicación son:

- Vía telefónica.
- Vía correo electrónico.
- Mediante formas.
- Proporcionando cuestionarios de las preguntas más frecuentes.

La atención vía telefónica es la más personalizada y se recomienda que sólo sea utilizada en caso de emergencia, o bien, que se establezcan grupos dedicados especialmente a la atención de dudas y comentarios, ya que es preferible que el administrador se dedique exclusivamente a sus tareas.

La atención vía correo electrónico es de uso fácil, lo recomendable en este caso es que el personal encargado de la contestación realice una lectura mínima de cuatro veces al día.

La atención mediante formas se puede realizar por medio de una interfaz de servicio estableciendo una base de datos que almacenará toda la información proporcionada, también se puede utilizar el correo electrónico para que las formas sean enviadas a un dirección electrónica especial.

Es recomendable que de alguna manera se concentren en un cuestionario las preguntas más frecuentes de los usuarios junto con su repuestas, para que éste sea dado a conocer al usuario cuando solicite ayuda. En caso de contar con un servicio de información, se recomienda tener aun sección en donde se pueda localizar este tipo de información como ayuda al usuario.

4. Estrategia para la Aplicación de los Procedimientos de Administración

La estrategia de Aplicación está compuesta por una serie de pasos que permitirán implementar los procedimientos de administración de manera ordenada y así poder tener mejor control del servidor ofreciendo un servicio de calidad.

Para la aplicación de ésta estrategia se da por hecho que ya se cuenta con la infraestructura necesaria para estar conectados a Internet. En caso de la CSR, la infraestructura es proporcionada por la Subdirección de Redes y Comunicaciones y el Departamento de Conectividad

Antes de empezar la aplicación de ésta estrategia, es necesario que se defina la situación dentro de uno de los casos que se plantean a continuación, dependiendo del estado actual:

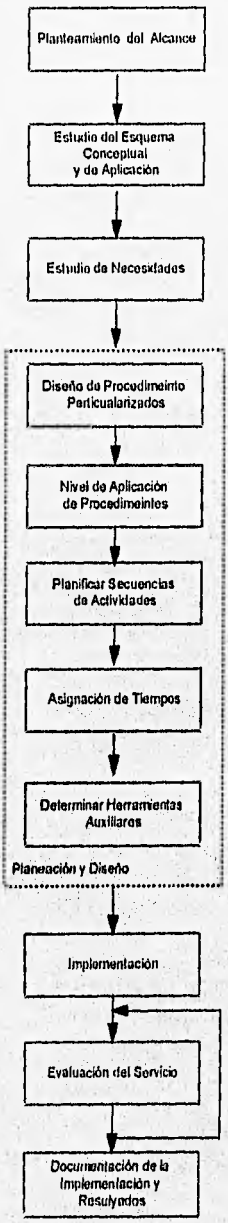
CASO	DESCRIPCIÓN
1	Sólo se cuenta con la infraestructura de conectividad hacia Internet, pero no se tiene ningún recurso de hardware para proveer servicios en Internet.
2	Se cuenta con la infraestructura de conectividad hacia Internet y con algún servidor hardware que provee determinado tipo de servicio en Internet.

Una vez que se establece el caso correspondiente a la situación, se debe seguir la estrategia de acuerdo a éste. A continuación se describirá la estrategia propuesta en forma general, además de realizar una subdivisión dependiendo del caso que se haya determinado, y cada una de las etapas que comprende:

1. *Planteamiento del Alcance.*
2. *Estudio de los Fundamentos y Procedimientos de Administración de un Servidor en Internet (capítulos 2 y 3).*
3. *Estudio de Necesidades.*
4. *Planeación y Diseño.*
5. *Implementación.*
6. *Evaluación de los Resultados.*
7. *Documentación de la Implementación y Resultados.*

El siguiente diagrama muestra la secuencia de la estrategia :

Diagrama de Procedimientos de la estrategia de Aplicación



4.1 Planteamiento del Alcance.

En esta etapa se define el objetivo por el cual se pretende realizar la implementación de los procedimientos descritos en el capítulo anterior, es decir definir hasta dónde se pretende llegar.

Especificaciones de acuerdo a los casos:

Caso 1 - El alcance consiste en definir el tipo de servicio que se desea proveer (*como referencia consulte el apéndice de Servicios de Internet*) y hacer que este servicio logre el punto máximo de calidad posible.

Caso 2 - El alcance para este caso define al objetivo como el mejoramiento del servicio hasta alcanzar el punto máximo de calidad posible.

4.2 Estudio de los Fundamentos y Procedimientos de Administración de un Servidor en Internet (capítulos 2 y 3).

a) Estudio de los Fundamentos de Administración

Como primer paso del análisis es necesario conocer claramente los fundamentos de administración (*capítulo 2*) para que de esta manera se comprendan los aspectos que se deben tomar en cuenta durante la etapa de diseño del Esquema de Aplicación.

b) Estudio del Esquema de Aplicación

Antes de empezar a diseñar se recomienda que se lean todos los procedimientos de aplicación (*capítulo 3*), comprendiendo cada uno de estos, ya que esto facilitará el diseño, además de que el tiempo dedicado a éste será más productivo.

4.3 Estudio de Necesidades

Es posible que con la lectura previa del esquema, se pueda determinar la situación actual y así poder detectar algunas deficiencias, además de determinar los recursos (dinero y humanos), con los va ser necesario contar para alcanzar el objetivo propuesto.

4.4 Planeación y Diseño.

Para llevar acabo esta etapa se debe de realizar lo siguiente:

4.4.1.- Diseño de Procedimientos Particularizados

Se debe llevar a cabo el desarrollo de una estrategia de implementación de los procedimientos que se proponen, la cual está ampliamente relacionada con la planificación cronológica, de tal forma que mediante el establecimiento de ambas y su riguroso seguimiento se asegura el logro del objetivo establecido en el alcance.

El diseño de procedimientos particularizados y asignación de tiempos para la implementación en cada uno de los casos, es el siguiente:

Caso 1:

- Planeación de la puesta en operación
- Elaboración del plan de administración del sistema
- Elaboración del plan de administración del servicio

Caso 2:

- Elaboración plan de administración del sistema
- Elaboración plan de administración del servicio

Consideraciones al elaborar el diseño de los planes

- Nivel de aplicación de procedimientos para el diseño:

Para el diseño de los procedimientos particularizados se propone una jerarquización de los aspectos del Esquema Conceptual. Esta jerarquización esta realizada bajo niveles en donde se plantean desde los aspectos críticos a tratar, hasta los aspectos que de alguna manera su diseño resulta ser subjetivo según los intereses que muestre la organización. De cualquier manera todos los aspectos que se contemplan en los planes de administración se deben diseñar.

En la jerarquización la notación utilizada es la siguiente:

NIVEL	NOMBRE	DESCRIPCIÓN
1	Crítico	Su aplicación se debe seguir estrictamente según el procedimiento descrito.
2	Subjetivo	Su proceso de aplicación puede variar según el tipo de sistema o situación en la que se encuentre, sin embargo no debe dejarse de considerar su aplicación.

Jerarquización para el Plan de Puesta en Operación

Actividad	N1	N2
Selección de la Plataforma del servidor.		✓
Configuración del sistema	✓	
Instalación del servicio.	✓	
Instalación: Liberación del servicio.	✓	

Jerarquización para el Plan de Administración del Sistema

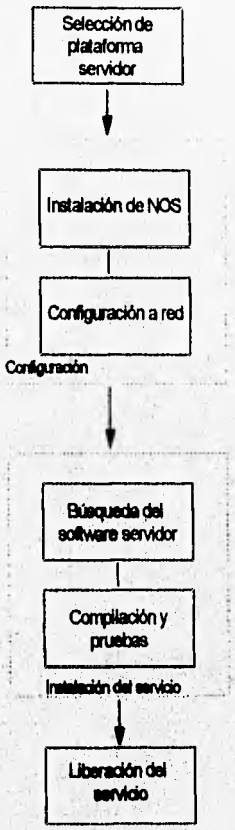
Actividad	N1	N2
Políticas del sistema	✓	
Instalación de NOS y configuración de equipo		✓
Control de usuarios		✓
Atención a usuarios		✓
Organización del sistema	✓	
Mantenimiento del equipo		✓
Análisis de rendimiento y sintonización	✓	
Seguridad: Administración de herramientas de protección	✓	
Seguridad física	✓	
Seguridad: Integridad de la información	✓	
Seguridad: Accesos autorizados al sistema	✓	

Jerarquización para el Plan de Administración del Servicio

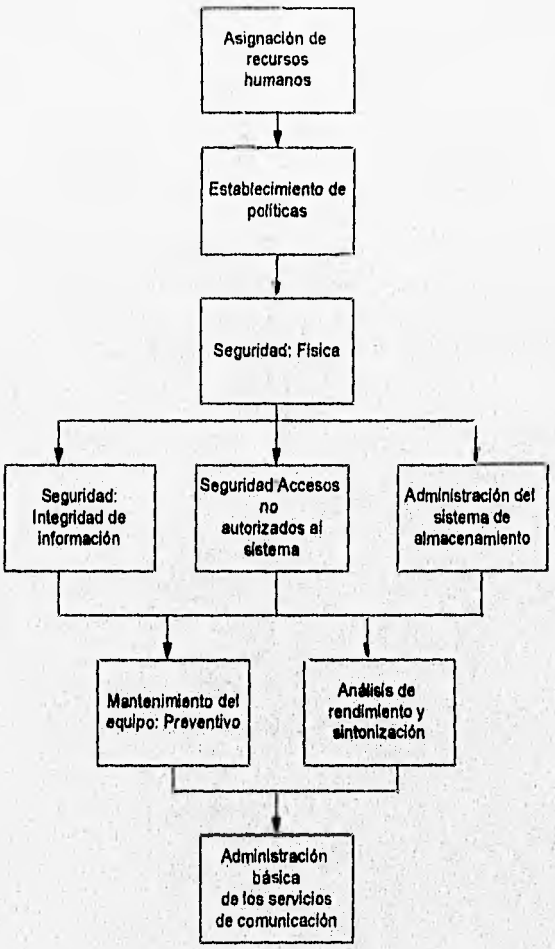
Actividad	N1	N2
Estudio de crecimiento	✓	
Actualización de servidor	✓	
Estudio de nuevos servicios		✓
Desarrollo de nuevos servicios		✓
Mantenimiento a la información	✓	
Contabilidad de uso		✓
Monitoreo	✓	
Seguridad	✓	

- Planificar secuencia de actividades en cada plan de administración

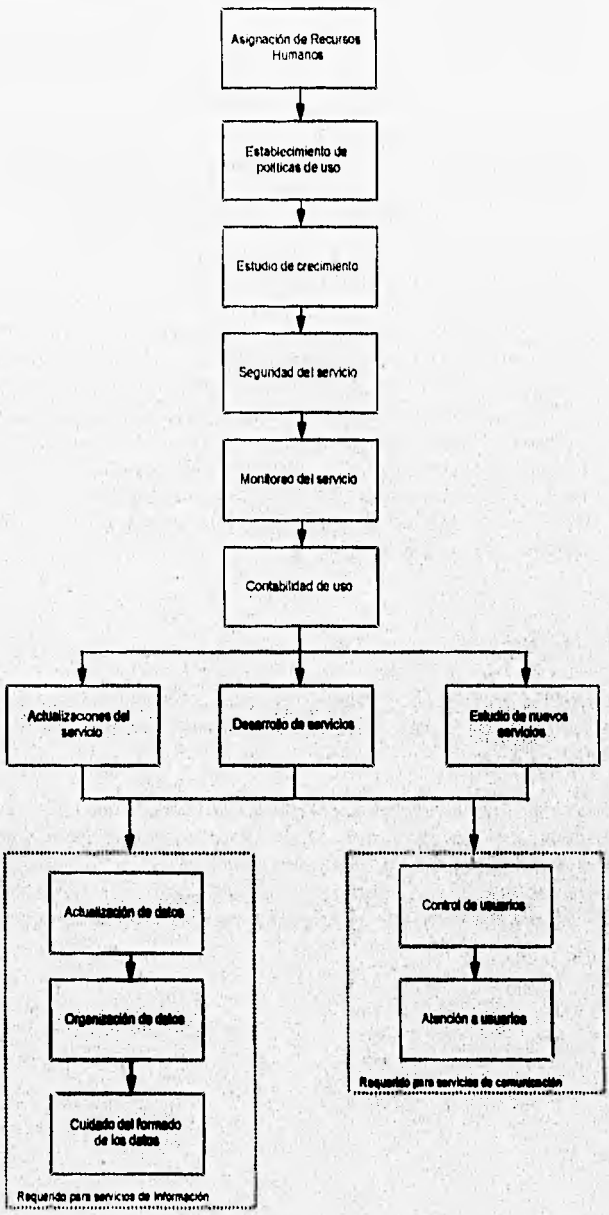
Puesta en Operación:



Administración del Sistema:



Administración del Servicio:



El seguimiento dela implementación pueden llevarse a cabo en forma simultánea, lo cual mejora el tiempo de implementación del esquema.

•Asignación de tiempos.

Se debe determinar una planificación de actividades en cuanto a tiempos, utilizando algún método de organización (como Diagramas de Gantt o Programación de proyectos con PERT-CMP, etc.), o bien, auxiliarse con algún software de planeación de proyectos, con esto se pretenden establecer fechas límites que disminuyan el tiempo ocioso en la implementación.

•Determinar herramientas auxiliares

No hay que descartar la idea de considerar herramientas que auxilien a la implementación de los procedimientos, se recomienda que primero se haga una búsqueda y análisis de las herramientas de dominio público que se encuentran en Internet con el objetivo de cubrir las necesidades planteadas en el Esquema de Aplicación, ya que esto reducirá costos y tiempo de desarrollo; si no se encuentra ninguna herramienta pública adecuada a las necesidades, se procede a buscar una herramienta comercial, o bien, desarrollarla, en ambos casos se debe considerar el presupuesto disponible, capacitación y tiempo requerido tanto de búsqueda como de desarrollo.

4.5 Implementación.

En esta etapa se llevan a cabo las actividades para la implementación real del Esquema de Aplicación, esta implementación se realiza de acuerdo a la planeación que se determinó en la etapa de diseño.

Cabe mencionar que la implementación debe ser llevada con disciplina respetando la planificación cronológica para no ocasionar retrasos considerables en la misma. En caso de que surjan circunstancias que no permitan su total aplicación, se debe tener consciencia de que el servicio proporcionado tendrá deficiencias que serán reflejadas en su uso, sin embargo recomendamos que se apliquen de ser posible los aspectos jerarquizados como nivel 1.

4.6 Evaluación de los Resultados.

Se debe llevar un estudio posterior a la implementación mediante el cual se determine si los objetivos fueron alcanzados en forma satisfactoria, o de lo contrario si se necesita regresar a cualquiera de las etapas anteriores o volver a aplicar los procedimientos.

Para evaluar si se cumplió el objetivo se debe realizar una revisión de todos los procedimientos implementados, es decir, se debe determinar si la implementación realmente se llevó a cabo como se había planeado. La revisión se realiza cotejando cada paso del plan particularizado del servidor contra su implementación.

Una vez que se obtienen los resultados de la revisión y siendo estos satisfactorios, se debe realizar una evaluación por medio de un método para obtener un porcentaje que determine la calidad del servicio.

Esta estratrategia consiste en realizar una estimación de cada uno de los aspectos involucrados en la calidad del servicio. Para esto se debe hacer un estricto registro de las causas que afectan los factores determinantes de la calidad, como lo es la disponibilidad, la eficiencia y el estado de la información . Posteriormente se asignará una puntuación dependiendo del resultado registrado y del criterio propuesto para cada aspecto. De esta manera, la puntuación será la forma como se asignarán porcentajes y así saber en que grado se cumplió el objetivo.

A continuación se plantean una serie de formas con las cuales ser puede llevar acabo la evaluación de :

- La disponibilidad
- La eficiencia
- El estado de Información (en caso de tener un servicio de información).

4.6.1 Evaluación de la Disponibilidad

La evaluación consta de realizar lo siguiente:

1.*Accesos*, se deben realizar diariamente diez accesos simultáneos en tres horarios aleatorios durante un periodo de una semana, dependiendo del número de accesos exitosos se asigna una puntuación.

Se considera que fue un acceso exitoso si se cumplen los siguientes aspectos:

Para los Servicios de Información:

- Lograr la conexión al servidor (*).
- Lograr navegar por el servicio accediendo aleatoriamente información.
- Transferir al sitio local dos documentos elegidos aleatoriamente en el servicio.

Para los Servicios de comunicación:

- •Lograr conexión y respuesta (en casos requeridos) (*)
- •Enviar y recibir correos de prueba (en caso de correo electrónico)

NOTA: (*) Sin considerar el tiempo de respuesta de la conexión, dado que esto depende del tiempo de respuesta de la red y puede estar afectado por diferentes factores como lo es el exceso de tráfico.

Para evaluar se requiere asignar una puntuación de acuerdo a los accesos exitosos durante los siete días tomando como referencia que el 210 accesos exitosos corresponden a un total de 100 puntos, y dependiendo del número accesos, se asigna una puntuación utilizando la siguiente relación:

Puntuación = No. total de accesos exitosos X 0.4762

Ejemplo:

Total de accesos exitosos	Puntuación
210	100
209	97,61
208	95,23

2.*Sistema de almacenamiento*, para asignar la puntuación correspondiente a lo registrado en el monitor de saturación del sistema durante una semana, dependiendo del número de saturaciones alcanzadas, se tiene el siguiente criterio:

Total de saturaciones alcanzadas	Puntuación
0	100
1 a 2	80
3 a 4	60
más de 5	10

3.*Monitoreo del sistema*, de acuerdo a los resultados obtenidos del monitoreo del sistema (descrito en los procedimientos de administración básica) durante el periodo de una semana, se tiene el siguiente criterio para la asignación de puntos:

Total de caídas del sistema	Puntuación
0	100
1	50
más de 1	0

4.*Monitoreo del servicio*, dependiendo de los resultados del monitor del servicio durante el periodo de una semana, el criterio de asignación de puntuación es el siguiente:

Total de caídas del software servidor	Puntuación
0	100
1	50
más de 1	0

Para obtener la evaluación final se requiere sumar la puntuación obtenida para cada uno de los aspectos evaluados:

Puntuación total obtenida para la disponibilidad = (Accesos + Sistema de almacenamiento + Monitoreo del sistema + Monitoreo del servicio)

4.5.2 Evaluación de la Eficiencia:

La evaluación de este aspecto corresponde directamente a los resultados obtenidos en el análisis de desempeño y sintonía realizados de acuerdo a lo descrito el los procedimientos de administración, por lo que la asignación de puntos se puede establecer de la siguiente manera:

Resultado de la comparación de la ganancia y el incremento del rendimiento (*)	Puntuación final de Eficiencia
Si el rendimiento actual es mayor que el rendimiento anterior (a*)	100
Si el rendimiento anterior es igual que el rendimiento actual (b*)	70

Nota: (*) El resultado de la comparación de la ganancia y el incremento del rendimiento, es definido por el caso en el cual se detecto el sistema al finalizar el procedimiento de análisis de desempeño y sintonización, (ver Capítulo 3, Resultado de la comparación del Análisis de desempeño y sintonía. pag52)

4.5.3 Evaluación del Estado de la Información:

Este es un aspecto que sólo se debe evaluar en caso de contar con un servicio de información.
Para verificar el estado de la información se necesitan monitorear los siguientes aspectos:

1.*Actualización*, para este caso, se requiere hacer referencia de las formas de registro de los datos del procedimiento de actualización de datos que se realizó en el plan de administración del servicio. Se deben realizar diez accesos aleatorios desde el servicio a la información para verificar que se llevo a cabo la actualización y detectar si existen retrasos. La asignación de puntos debe seguir el siguiente criterio:

Número de casos de retrasos	Puntos
0	100
1-4	50
más de 5	0

2.*Organización*, de acuerdo a la estructura que se definió en el procedimiento de organización de datos en el plan de administración de servicios, se debe monitorear la existencia de los archivos índices y verificar si la referencia ésta de acuerdo con la estructura real. Para esto se tiene la siguiente forma en donde se cotejan los números de casos en que se encuentran índices incorrectos o no se encuentran para asignar la puntuación correspondiente :

		No. de índices con referencias incorrectas			
		0	1	2	3
No se encontró índice	0	100	90	80	70
	1	90	80	70	60
	2	80	70	60	50
	3	70	60	50	40

Para obtener el número de puntos, es necesario saber el total de índices no encontrados y el número total de índices incorrectos encontrados. Para los casos no contemplados en la tabla anterior el porcentaje a asignar es cero puntos (0) dado a que se considera que el usuario no podrá encontrar la información de manera oportuna.

3.*Formato,* los documentos que pertenecen al servicio de información obedecen a un formato establecido por el propio servicio, el monitoreo del formato consisten en realizar diez accesos a documentos aleatorios y verificar que la información es legible. De tal manera que del registro de los resultado de los accesos, se asignará la siguiente puntuación para la evaluación de este aspecto:

Número de documentos con el formato inadecuado	Puntuación
0	100
1	66.66
2	33.34
más de 2	0

Para evaluar la disponibilidad se requiere sacar el porcentaje promedio de los aspectos evaluados:

Puntuación total para el estado de la información = Actualización + Organización + Formato

4.5.4 Evaluación Final de la Calidad del Servicio

Para evaluar la calidad se tomará la suma total de la puntuación total obtenidos en la evaluación de eficiencia, disponibilidad y del estado de la información (en caso de contar con un servicio de información).

Dado que se considera que los aspectos sometidos a evaluación son de igual importancia en la calidad, se propone que esta se evalúe mediante la siguiente relación:

Puntuación Final = No. total de puntos de Disponibilidad + No. Total de puntos para la Eficiencia + No. Total de puntos obtenidos para el estado de Información (*)

NOTA: (*)En caso de estar evaluando un servicio de Información

Calidad = Puntuación Final X 0.125

NOTA: Esta relación es resultado de asignarle al máximo número posible de obtener en la evaluación un 100% de calidad y de realizar el calculo necesario para asignar el porcentaje de acuerdo a la puntuación final obtenida

El rango de porcentaje que se considera satisfactorio en la evaluación final de calidad está entre el 100% y el 95 %, en este rango de porcentajes se considera que el servicio esta en optimas condiciones para ser proveído, en el caso de que cualquiera de los resultados o el resultado global no sea satisfactorio, se debe determinar cuál es el factor que disminuye en gran medida el promedio y proceder a aplicar de nuevo el procesamiento correspondiente (ayúdese de la siguiente tabla).

Aspecto	Procedimientos correspondientes
Disponibilidad	Sistema: Administración de almacenamiento de datos. Mantenimiento de equipo: preventivo y correctivo. Seguridad: física. Seguridad: integridad de la información. Seguridad: accesos no autorizados. Servicio: Estudio de crecimiento. Monitoreo del servicio.
Eficiencia	Sistema: Análisis de rendimiento y sintonización
Estado de la información	Servicio: Administración básica: Organización de datos Actualización de datos Cuidado del formato de datos

Una vez teniendo un servicio de calidad es necesario evaluar periódicamente el estado de los servicios llevando acabo el mismo método propuesto para asegurar que el servicio continúe siendo de calidad.

4.7 Documentación de la Implementación y Resultados

Una vez terminado la evaluación de debe documentase formalmente todo el trabajo de la implementación, es decir en realizar una descripción escrita de los planes implementados junto con todas las formas utilizadas.

Esta documentación debe de ser clara y concisa para ser guardada como una bitácora formal de lo implementado.

5. Implementación de Procedimientos para la Administración de un servidor en Internet

Este capítulo es la recopilación de todos los datos generados en la implementación del esquema de aplicación utilizando el método propuesto.

La implementación se realizó en un equipo que fue donado a la UNAM por Sun Microsystems (Software Information and Technology Exchange, SunSITE), este es uno de los más grandes proyectos de parte de SunMicrosystems para dar apoyo a instituciones educacionales y de Investigación. Dadas estas circunstancias se determinó que nos encontrábamos en el primer caso descrito en el esquema de aplicación.

A continuación describiremos lo que se realizo en la implementación de los procedimientos de administración, utilizando la estrategia propuesta en el capítulo anterior.

5.1 Alcance

Proporcionar los servicios World Wide Web, Ftp y Listas de Discusión en un nuevo servidor en la Coordinación de Servicios de Red con el máximo grado de calidad posible, utilizando la metodología propuesta en este proyecto de tesis.

5.2 Estudio de Necesidades

De acuerdo a las características del equipo donado y a los servicios que se proporcionarían, se asignaron por parte de la CSR a cuatro personas para realizar la implementación y la administración de estos.

Dado a que fue una donación hecha por Sun Microsystems hacia la Universidad, no se requiere de una inversión económica.

5.3 Planeación y Diseño

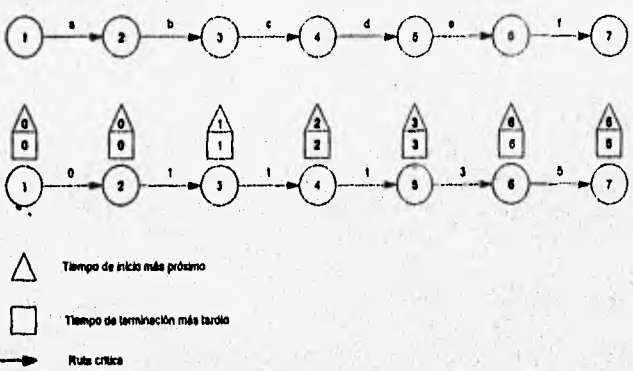
Se realizó un estudio para determinar la duración de las actividades para la implementación de cada uno de lo planes, utilizando diagramas de flechas, determinación de ruta crítica, determinación de las holguras y construcción de diagramas de tiempos.

5.3.1 Planeación y Diseño para el Plan para la Puesta en Operación

De acuerdo a los procedimientos de administración, las actividades que se planearon fueron las siguientes:

Actividad	Descripción
a	Selección de Plataforma
b	Instalación de Sistema Operativo
c	Configuración a Red
d	Búsqueda de software (ftp, majordomo)
e	Compilación, instalación y pruebas (ftp, www y majordomo)
f	Liberación del servicio (ftp, www y majordomo)

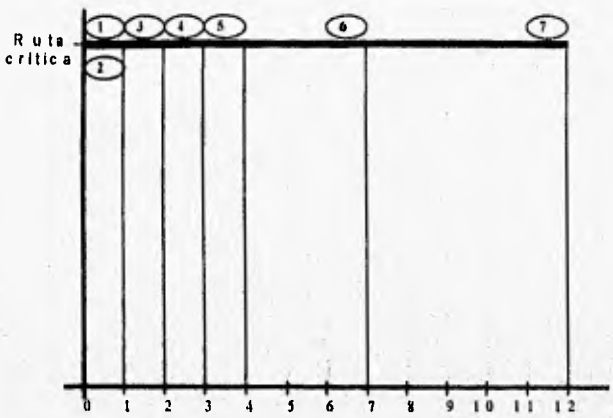
El diagrama de flechas y ruta crítica:



Los tiempos calculados son:

Actividad (i,j)	Duración Dij (días)	Inicio TIPj (días)	Terminación TTIj (días)	Inicio ITIj (días)	Terminación TTTj (días)	Holgura Total HTIj (días)	Holgura Libre HLIj (días)
(1,2)	0	0	0	0	0	0	0
(2,3)	1	0	1	1	1	1	0
(3,4)	1	1	2	1	2	0	0
(4,5)	1	2	3	2	3	0	0
(5,6)	3	3	6	3	6	0	0
(6,7)	5	6	11	6	11	0	0

El diagrama de tiempos es el siguiente:

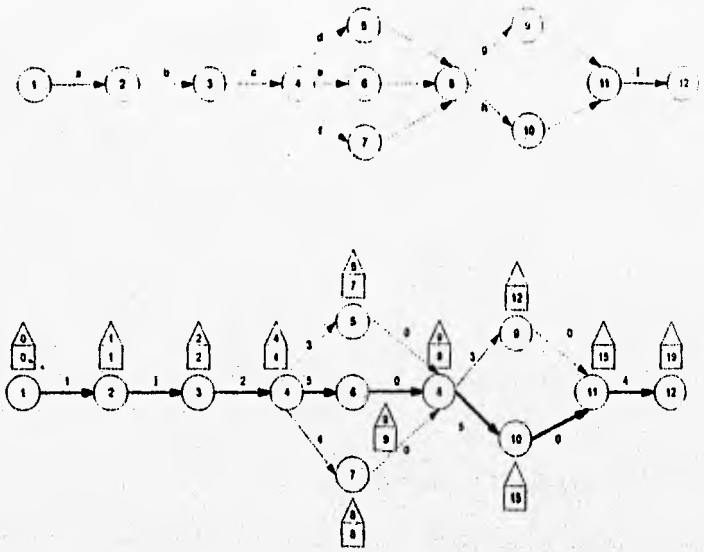


5.3.2 Planeación y Diseño de el Plan de Administración del Sistema

Las actividades que se planeo realizar para la administración del sistema son las siguientes:

Actividad	Descripción
a	Asignación de Recursos Humanos
b	Establecimiento de Políticas
c	Seguridad Física
d	Seguridad :Integración de Información
e	Seguridad: Accesos no autorizados
f	Administración del sistema de almacenamiento
g	Mantenimiento del Equipo Preventivo y Correctivo
h	Análisis de Rendimiento y Sintonía
i	Administración básica de los servicios de comunicación

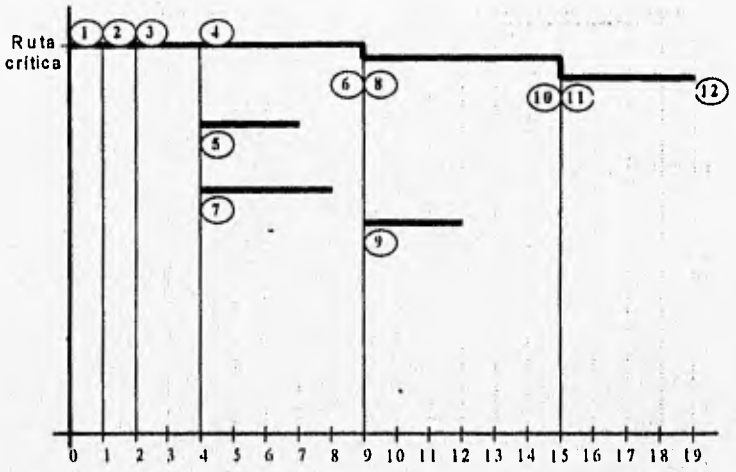
El diagrama de flechas y ruta crítica son:



Los tiempos calculados para las actividades de administración del sistema son:

Actividad (i,j)	Duración Dij (días)	Inicio Tlij (días)	Terminación Tfij (días)	Inicio Tlij (días)	Terminación Tfij (días)	Holgura Total Htij (días)	Holgura Libre Hlij (días)
(1,2)	1	0	1	1	1	1	0
(2,3)	1	1	2	1	2	0	0
(3,4)	2	2	4	2	4	0	0
(4,5)	3	4	7	6	9	2	0
(4,6)	5	4	9	4	9	0	0
(4,7)	4	4	8	5	9	1	0
(5,8)	0	7	3	9	9	6	2
(6,8)	0	9	9	9	9	0	0
(7,8)	0	8	8	9	9	1	1
(8,9)	3	9	11	12	15	3	0
(8,10)	6	9	15	9	15	0	0
(9,11)	0	12	12	15	15	3	3
(10,11)	0	15	15	15	15	0	0
(11,12)	4	15	19	15	19	0	0

El diagrama de tiempos correspondiente es:

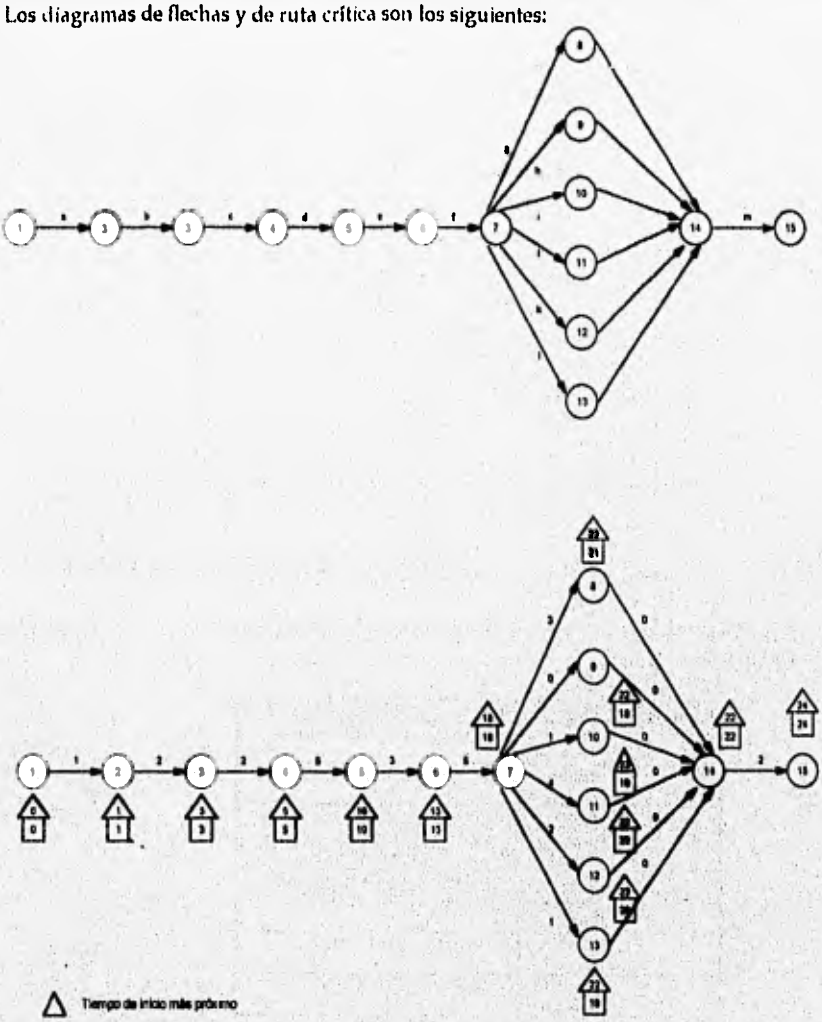


5.3.3 Planeacion y Diseño para el Plan de Administración del Servicio

Las actividades que se planearon realizar para los servicios FTP, World Wide Web (WWW) y majordomo son:

Actividad	Descripción
a	Asignación de recursos humanos (FTP , WWW y majordomo)
b	Establecimiento de políticas (FTP , WWW y majordomo)
c	Estudio de crecimiento (FTP , WWW y majordomo)
d	Seguridad del Servicio (FTP , WWW y majordomo)
e	Monitoreo del servicio (FTP , WWW y majordomo)
f	Contabilidad de uso (FTP , WWW y majordomo)
g	Actualizaciones del servicio (FTP , WWW y majordomo)
h	Desarrollo de servicios (No se aplico en ningún servicio)
i	Estudio de nuevos servicios (FTP , WWW y majordomo)
j	Actualización de datos (FTP y WWW)
k	Organización de datos (FTP y WWW)
l	Cuidado del formato de datos (FTP y WWW)
m	Atención a usuarios (FTP , WWW y majordomo)

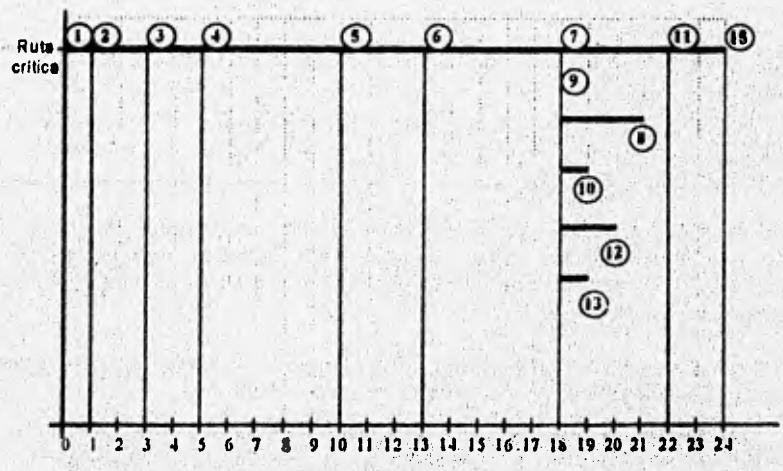
Los diagramas de flechas y de ruta crítica son los siguientes:



Los tiempos calculados son:

Actividad (i,j)	Duración Dij (días)	Inicio TIPi (días)	Terminación TTIj (días)	Inicio TTIj (días)	Terminación TTTj (días)	Holgura Total HTij (días)	Holgura Libre HLij (días)
(1,2)	1	0	1	0	1	1	0
(2,3)	2	1	3	1	3	0	0
(3,4)	2	3	5	3	5	0	0
(4,5)	5	5	10	5	10	0	0
(5,6)	3	10	13	10	13	0	0
(6,7)	5	13	18	13	18	0	0
(7,8)	3	18	21	18	22	0	0
(7,9)	0	18	18	22	22	4	0
(7,10)	1	18	19	21	22	3	0
(7,11)	4	18	22	18	22	3	0
(7,12)	2	18	20	20	22	3	0
(7,13)	1	18	19	21	22	3	0
(8,14)	0	21	21	22	22	1	1
(9,14)	0	18	18	22	22	4	4
(10,14)	0	19	19	22	22	3	3
(11,14)	0	22	22	22	22	0	2
(12,14)	0	20	20	22	22	2	2
(13,14)	0	19	19	22	22	3	3
(14,15)	2	22	24	22	24	0	0

El diagrama de tiempos es el siguiente:



5.4 Implementación

5.4.1 Plan para la Puesta en Operación.

5.4.1.1. Selección de Plataforma.

No se siguió este procedimiento ya que no estaba a nuestro alcance hacer la selección, lo cual se considero permitido debido a que en la jerarquización es un procedimiento subjetivo (N2).

La selección la hizo Sun Microsystems bajo el criterio que diseño para los requerimientos de un SunSITE, este criterio fue establecido pur su experiencia de los últimos dos años y de estimar que serán más de un millón de accesos que tendrá el servidor. Este criterio consiste en definir al hardware en tres categorías para un SunSITE: pequeño, mediano y grande.

Las características de cada una de estas categorías se describen en la siguiente tabla. Cabe mencionar que esta tabla no debe ser usada como propósito general para la selección de hardware de un servidor en Internet:

TIPO	PEQUEÑO	MEDIANO	GRANDE
SPARC Sistema Solaris	SPARC server 20	SPARC server 1000	SPARC server 2000
MEMORIA	64 Mb	128-256 Mb	512Mb-1.2 Gb
ESPACIO EN DISCO	5 Gb	10-30 Gb	30 -100 Gb
CPUs	1	2-7	8-20
PERIFERICOS	CD-ROM, Unidad de cinta de 4 mm	CD-ROM, Unidad de cinta 4mm	CD-ROM, Unidad de cinta 4mm

La elección de cualquiera de estas categorías es determinada por SunMicrosystems y depende del propósito que tendrá el servidor, es decir, si tendrán uno o mas servicios de información, además de definir que tan grande será la cantidad de información que se tendrá en cada uno de estos servicios.

Dado lo anterior Sun Microsystems proporcionó a la UNAM a través la Coordinación de Servicios de Red el hardware con las siguientes características:

MÁQUINA	SISTEMA OPERATIVO	RAM (MB)	ALMACENAMIENTO (GB)	NO. DE CPUs	VEL. CPU (MHz)
SPARC Server 1000 E	Solaris 2.4 3/95	64	6 (Arreglo de discos Externo)	2	60

Se estableció que el SunSITE tendrá los siguientes servicios de información:

- ♦ World Wide Web
- ♦ FTP

Servicios de comunicación:

- ♦ Correo electrónico para ser usado con los servicios de información.
- ♦ Listas de discusión.

5.4.1.2 Configuración

a) Instalación del Sistema Operativo.

Instalación de sistema operativo

El equipo con el que se cuenta sólo soporta versiones del sistema operativo Solaris, la versión proporcionada por Sun Microsystems fue Solaris 2.4.

Planeación del sistema de almacenamiento.

Se cuenta con un SPARC Storage Array Disks que contiene 6 discos con una capacidad total de 6GB, de este arreglo se tendrá un disco en donde se alojará al sistema operativo, de esta manera nos quedarán 5 discos como un arreglo que estará configurado como RAID-5.

Este tipo de configuración se eligió debido a las ventajas que presenta en cuanto a la protección de la información. Las ventajas de utilizar un RAID de nivel 5 son:

- Presentar la capacidad de almacenamiento del arreglo al host como uno o más discos virtuales con el deseado balance de disponibilidad de los datos y desempeño I/O.
- Cubrir la complejidad interna del arreglo de discos al host.
- Alta tolerancia a fallas y proveer servicio continuo.

El RAID utiliza una verificación de datos, la cual puede ser usada para regenerar bloques individuales de datos desde un disco con fallas, dependiendo del momento en que las aplicaciones lo requieran, o bien, para reconstruir completamente el contenido de un disco y restaurar la información.

Uno de los discos del arreglo será utilizado como disco independiente en donde se tendrá la información concerniente al sistema operativo.

La distribución del disco independiente es la siguiente:

No. De Partición	Directorio	Cantidad asignada (MB)	Tipo
d0s0	/	16	Sistema Operativo
d0s3	/usr	300	Sistema Operativo
d0s4	/var	320	Sistema Operativo y logs tanto de servicios como de sistema operativo
d0s5	/export/home	264	Listas de correo y Cuentas especiales: ♦ Administración básica ♦ Seguridad ♦ Rendimiento
d0s6	/opt	150	Sistema de Operativo
	swap	200	Memoria

Los otros 5 discos están configurado como RAID-5 y dado a esta configuración se tendrán sólo 4 GB de capacidad para los servicios, debido a que el RAID-5 consume internamente 1 GB en la verificación de datos.

Directorio	Tipo
/wwwadm	WWW
/ftpadm	Ftp

b) Configuración a red.

Se tiene los siguientes datos de configuración:

Nombre: sunsito
Dominio: dgsca.unam.mx
Mascara: 255.255.255.0
Subred:
IP: 132.248.10.21
Ruteador: 132.248.10.254
Servidor de nombres: 132.248.10.2

Espacio de almacenamiento interno: 0 GB
Espacio de almacenamiento externo: 6 GB
TOTAL: 6 GB

5.4.1.3 Instalación del Servicio

a) Búsqueda de software

SERVICIO	VERSIÓN	LUGAR EN DONDE SE ENCONTRÓ
WWW	Netscape Commerce Server 1.1	Producto comercial de Netscape Co.
Ftp	wu-ftp	wuarchive.wustl.edu
Listas de discusión	majordomo 1.93	ftp.greatcircle.com

b) Instalación del software servidor

Para la instalación de los servicios se utilizó un compilador público que se obtuvo mediante ftp anónimo en infoys.advuni-mainz.edu, el compilador es GNU CC.

Se instaló cada servicio bajo una cuenta de administración:

SERVICIO	login	Directorio home
WWW	wwwadm	/wwwadm
FTP	ftpadm	/ftpadm
Listas de discusión	listadm	/export/listadm

La contabilidad de los servicios se activó en los siguientes directorios:

	RUTA
www	/var/servicios/wtvw
FTP	/var/servicios/ftp
Listas de discusión	/var/servicios/majordomo

Los servicios se levantaron bajo los siguientes puertos lógicos para realizar las pruebas correspondientes:

www	8000
FTP	7000

Las pruebas que se llevaron a cabo para los servicios son las siguientes:

- .Se puso información de prueba.
- Se simularon accesos simultáneos.
- Se revisó que se realizara la contabilidad de los accesos realizados.
- Se realizaron accesos a los servicios con el fin de atacar los puntos "débiles" y detectar si era posible violar la seguridad.

5.4.1.4 Liberación del Servicio

Una vez realizadas las pruebas se levantó el servicio bajo el puerto elegido:

SERVICIO	PUERTO
WWW	80
FTP	21

La difusión de estos servicios se realizó por parte de Sun Microsystems mediante ligas en otros SunSITEs y por parte de la UNAM para difundir a toda la comunidad tanto de Internet como de la UNAM la existencia de este SunSITE.

En lo que se refiere a la difusión de estos servicios por parte de la UNAM se realizó una campaña de difusión de la manera siguiente:

- Se dio a conocer por medio de otros servicios en Internet que se tiene a disposición por medio de la CSR.
- Se realizó una liga del World Wide Web de la UNAM (http://www.unam.mx) al World Wide Web del Sun SITE.
- Se activó el comando finger a sunsite.unam.mx en donde se desplegara información acerca de los servicios que se ofrecen en este.
- Se presentó públicamente, a nivel nacional y con presencia del Rector de la Universidad, en el mes de Junio de 1996.

5.4.2 Plan de Administración del Sistema.

5.4.2.1 Administración Básica:

Recursos Humanos.

Se cuenta con un equipo de administración formado por tres personas, la distribución de actividades es la siguiente:

No. De Personas	Actividad
1	Administración básica
1	Desempeño y sintonización
1	Seguridad

Políticas del Sistema.

El servidor SunSITE no alojará a usuarios dado los servicios que proporcionará, por tal razón no se establecerán políticas de usuarios, cabe mencionar que sólo se tendrán alojados en el sistema cuentas para la administración de este.

Sabiendo ésto, las políticas de administración que se establecieron son:

1. No se abrirán cuentas personales a los administradores ni a personas externas.
2. No se deberán usar las cuentas de administración para uso personal.
3. Las únicas personas que pueden modificar la configuración del sistema son las personas de administración del sistema.
4. Las cuentas de administración deberán ser utilizadas organizadamente.
5. Los permisos deben estar asignados de forma que solo se permita el acceso a la cuenta propietaria del directorio.
6. Se debe establecer entre todos los administradores un trato de confidencialidad de toda la información que se maneje.

Control de Usuarios y Atención a Usuarios.

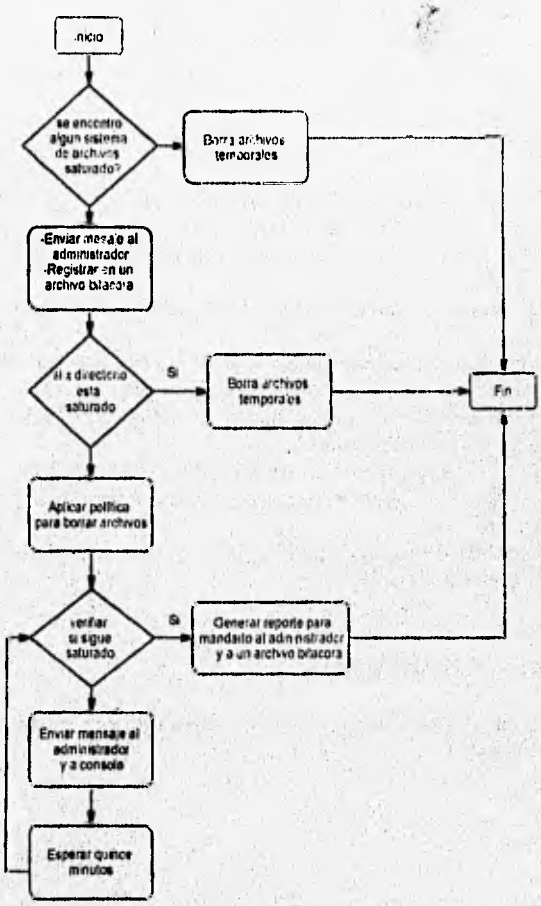
Dado a que no se encuentran usuarios, no se tiene un control y no proporcionará atención a usuarios del sistema.

Administración del Sistema de Almacenamiento de Información.

Se realizó un algoritmo que nos ayudara a monitorear que no exista una saturación del sistema de almacenamiento.

Este monitoreo se realiza diariamente de manera automática a las 12:00 pm, en donde se verifica, mediante utilerías del sistema operativo, si el disco independiente se encuentra saturado en alguna de sus particiones. En caso de encontrar alguna de estas saturada, se envía un mensaje al administrador del sistema para que detecte la causa por la cual se saturo y proceda a depurar, de tal manera que ya no exista la saturación.

Diagrama de flujo para el monitor de Saturacion del Sistema de Archivos



Mantenimiento del equipo

- Correctivo

En caso de detectar alguna falla de hardware se recurre al servicio directo de Sun Microsystems, debido a que el equipo cuenta con dos años de garantía. Las fallas pueden ser detectadas por los diferentes monitores del sistema.

- Preventivo

El equipo cuenta con dos años de garantía con la cual se pueden realizar peticiones de limpieza al equipo, además se pretende establecer un contrato con Sun Microsystems para que se realice este tipo de mantenimiento al final de la garantía.

Monitoreo del Sistema

Se desarrollo un monitor que permite verificar si el SunSITE puede ser accedido a través de la red. Para esto el monitor debe ejecutarse en un sistema remoto que detecte si el SunSITE:

- Puede ser alcanzado a través de la red, en este caso la solución del problema no corresponde a la CSR.
- Puede ser alcanzado a través de la red pero no se detecta en modo operativo, en este caso se debe determinar la causa de la baja del sistema.

Dentro del monitoreo del sistema también se incluye la verificación de la carga del CPU, la cual es un factor que puede afectar a la disponibilidad del servicio.

Para cumplir con las actividades mencionadas anteriormente se utilizará la herramienta SunNetManager proporcionada por Sun.

5.4.2.2 Análisis de Rendimiento y Sintonización

El procedimiento que se llevo acabo de la manera siguiente:

1.-Conocer todas las características de hardware

Procesador

Característica	Descripción
Número de procesadores	Dos
Arquitectura	Superescular SPARC Versión 8

Memoria Principal:

Característica	Descripción
Capacidad de memoria	64 MB por sistema
Capacidad de memoria de expansión	32 MB a 128 MB

Interfaces estándares:

Característica	Descripción
Serial	Puertos RS-232/423 por cada tarjeta del sistema
SBus	Tres slots de expansión por cada tarjeta de expansión
Puertos de Teclado y mouse	Uno por sistema
Ethernet	10 MB/seg estándar par trenzado por cada tarjeta de sistema
Canales de I/O	10 MB/seg, simple-salida estándar SCSI-2 por tarjeta de sistema

Sistemas de almacenamiento:

Característica	Descripción
Disco duro interno	No tiene
Disco duro externo	SPARCstorage Array 6 MB
Cinta	Sistema SPARCstorage library 140-GB 4 mm

Monitor de consola:

Característica	Descripción
Monitor Sun	17- pulgadas a color.

Opciones de Sbus:

Característica	Descripción
Trabajo de Red	Controlador Ethernet, adaptador de SunFastEthernet (TM) y de SunATM (TM) Interfaz FDDI y Token Ring.
Comunicaciones	Interfaces serial de alta-velocidad, serial / paralela.
Adaptador de Host	Canal de fibra, Diferencial Fast/Wide intel Singe-ended Fast/Wide inteligente SCSI-2, F.Diferencial SCSI-2/Buffered Ethernet, Fast SCSI-2/Buffered Ethernet

2.-Determinar la manera en como se realizarían las mediciones

Se busco en Internet la existencia de algún programa que monitoreara el desempeño del sistema, se tomaron en cuenta el sistema operativo y la plataforma hardware.

Se encontró una herramienta que fue elaborada para plataforma Sun con Sistema Operativo Solaris 2.3 en adelante, SE toolkit (SE [Symbol Engine] Performance Toolkit) fue desarrollada por Rich Pettit y Adrian Cockroft como un conjunto de programas formados de diferentes comandos del sistema operativo bajo condiciones que son determinadas como reglas para clasificar el rendimiento de cada recurso.

Con esta herramienta se realizaron las mediciones del rendimiento en:

- Cpu
- Memoria, paginación , swapeo y memoria principal
- Actividad de la Red
- Controladores
- Sistema de almacenamiento

3.- *Realizar las mediciones:*

Las mediciones obtenidas por la herramienta instalada SeeToolKit fueron las siguientes:

Sistema de almacenamiento:

Aspecto	Estado
Evaluación general del sistema de almacenamiento	Sin demasiada actividad
Controladores	Sin demasiada actividad

Actividad de red:

Aspecto	Estado
Actividad en interfaces de red	Sin demasiada actividad.

Memoria:

Aspecto	Estado
SWAP	Se detecto que se tenia memoria para swap asignada sin utilizar.

CPU:

Aspecto	Estado promedio
CPU No. 1	USR 3% SYS 2% WAIT 0% IDLE 95%
CPU No. 2	USR 4% SYS 4% WAIT 0% IDLE 92%

4.- Análisis de Resultados de mediciones e identificación de problemas

La herramienta proporciona un análisis de las medidas del sistema a base de reglas que son específicas de la plataforma, estas son evaluadas por rangos determinados para un desempeño favorable del sistema, y detecta cualquier problema que se puede presentar, ya sea en configuración o en capacidades (si es ocioso, si esta muy ocupado o bien este esta en conflicto). A continuación se listaran los problemas detectados o los resultados del análisis de las mediciones que se obtuvieron.

Sistema de almacenamiento:

Dado a que este es un servicio es nuevo y se encuentra sin demasiada demanda y a que las mediciones indican que no hay mucha actividad, se determinó que este sistema se encuentra en perfectas condiciones de rendimiento. Sin embargo se prevé que con forme vaya pasando el tiempo, el SunSITE sea mas accedido y se haga necesario crecer en capacidad.

Actividad de red:
Este aspecto se encuentra en el mismo caso que el sistema de almacenamiento, ya que se cuenta con mayor capacidad para soportar la actividad que tiene en la actualidad, pero se prevé que el servidor tendrá cientos de accesos diarios.

Memoria:
La memoria tanto física como la que se configuro para SWAP esta en un estado sin problemas, aunque se indica que la cantidad asignada al SWAP es demasiada a lo que se esta requiriendo para la actividad actual.

CPU:
El procesamiento del servidor es favorable para cualquier persona que acceda al servidor, dado a que en estos momento no se encuentra saturado, e inclusive se ocupa un 5 % en promedio de su capacidad para el primer CPU y un 8% de su capacidad para el segundo CPU. SunMicrosystems prevé que la actividad que tendrá el servidor, serán suficientes para soportar la carga de trabajo.

5 y 6 .- Soluciones y elección de la solución óptima

Realmente no existe ningún problema que sea critico para que afecte en el rendimiento y la eficiencia de los servicios. Se determino que el sistema no requiere de sintonización dado a que la actividad de sus servicios no han creado problemas en el funcionamiento de manera que afecte su eficiencia a los usuarios.

Se planea utilizar el monitor para detectar en un futuro problemas presentados por el incremento en la utilización de los servicio. Y en cuanto se detecte algún problema se someterá a otro análisis de rendimiento y sintonización utilizando el mismo sistema de mediciones planteadas anteriormente.

7.- Mediciones del nuevo rendimiento

Dado a que el rendimiento fue aceptable y no se requirió una sintonización, no se realizaron mediciones posteriores.

8.- Resultado del análisis

Se considera que este análisis será más robusto cuando sea más accedidos los servicios y de este manera incremente el consumo de recursos. Dado a que no se encontraron problemas que resolver de rendimiento y que se detecto un rendimiento aceptable para la actividad actual, el resultado se encuentra en el caso de que el rendimiento anterior es igual al rendimiento actual.

Monitoreo

Para el monitoreo del desempeño del sistema se utiliza la misma herramienta SeToolKit, dado a que incluye un monitor que mediante su conjunto de reglas y evaluaciones detectan los problema que se puedan presentar en el sistema.

Esta herramienta se implementa utilizando un calendario que incluye el sistema operativo el cual registra el día y el estado critico de que fue monitoreado permitiendo que se verifique constantemente si se ha encontrado algún problema.

También registra cada cierto tiempo un en archivo el estado de todos los aspectos evaluados y el resumen de las mediciones realizadas en el monitoreo.

Esta herramienta utiliza un código para clasificar el estado de rendimiento del sistema y registrarlo en los archivos de monitoreo y en el calendario:

Blanco	Completamente ocioso
Azul	Desbalanceado, ocioso mientras otro recurso esta sobrecargado
Verde	No hay problema, estado de operación normal
Ámbar	Precaución (warning)
Rojo	Sobrecargado o con problemas
Negro	Problema critico, este puede causar que el sistema baje a un estado de no operante.

Se revisará constantemente en la red para buscar nuevas versiones de esta herramienta que permita realizar mejor esta tarea.

5.4.2.3 Seguridad

Seguridad Física.

1. Identificación de los recursos vulnerables:

Los recursos con los que se cuenta en el SunSITE para la prestación de servicios son:

- Hardware:

  CPU, accesorios (tarjetas, monitor, teclado, mouse), arreglo de discos y cintas de respaldo

- Software:

  Sistema operativo, programas servidores y aplicaciones en general.

- Datos:

  Datos almacenados en el arreglo de discos y datos en tránsito sobre las vías de comunicación.

- Documentación:

  Formas elaboradas en la administración, manuales de hardware y manuales de aplicaciones en general.

2. Identificar contra que amenazas se van a proteger los recursos:

Los recursos son afectados, principalmente, por alteraciones físicas y alteraciones lógicas, las cuales pueden ser causadas por usuarios internos y usuarios externos. Es importante hacer notar que los usuarios externos (o personas externas) siempre son una amenaza para todos lo tipos de recursos, por lo que se debe establecer una plan seguridad que contemple la forma de proteger totalmente al sistema contra hackers.

3. Análisis de riesgos.

El análisis de riesgos comprende una evaluación de los recursos que contribuyen a la prestación del servicio, esta evaluación consisten en determinar cual es el impacto de la pérdida de un recurso. De esta forma podemos establecer las acciones de protección para los recursos con mas alto riesgo de daño.

A continuación se presenta la tabla de evaluación de riesgos, donde la notación es la siguiente:

- *Riesgo de pérdida del recurso* - Se refiere a que tan susceptible es el recurso, o bien, que tan propenso es a dañarse o alterarse.
- *Importancia del recurso* - Se refiere a que tan importante es el recursos en la prestación del servicio.
- *Peso de riesgo* - Es el valor final asignado a un recurso dado, la cual nos permite determinar que recurso requiere de mayor protección.

El criterio de evaluación de cada uno de los aspectos anteriores es:

- Riesgo de pérdida: 10 muy susceptible
  8 susceptible
  5 difícilmente se daña

- Importancia del recurso: 10 vital para los servicios
  5 preferible
  0 no afecta el no tenerlo

Nombre del Recurso	Riesgo de pérdida del recurso (RI)	Importancia del recurso (WI)	Peso de riesgo (WRI)
CPU	5	10	50
Accesorios	10	5	50
Arreglo de discos	8	10	80
Cintas de respaldo	10	10	100
Sistema operativo	8	10	80
Programas servidores	10	10	100
Aplicaciones desarrolladas	5	10	50
Datos almacenados (proveídos por fuentes externas y proveídos por el mirror)	8	10	80
Datos en tránsito (no se maneja información confidencial)	8	10	80
Formas de administración	8	5	40
Manuales de hardware	8	5	40
Manuales de software	8	5	40

De la tabla anterior se determina que los recursos a los cuales se les deben aplicar en primer lugar los métodos de protección para cada uno de los tipos de recursos, son :

- Hardware: Arreglo de discos y cintas de respaldos.
- Software: Sistema operativo y programas servidores.
- Datos: datos en tránsito y datos almacenados tienen el mismo peso.
- Documentación: Toda la documentación tiene el mismo peso.

4. Determinar como se va a proteger

Se protege al equipo contra pérdida total, para lo cual se cuenta con un sistema de seguridad que restringe el acceso al equipo. El sistema consiste en tarjetas de acceso al área donde se encuentra el equipo físicamente manteniendo un control estricto, de esta forma se garantiza que el equipo no representará pérdida total por robo.

En cuanto al software, se tiene una selección de programas (de dominio público), que han pasado por una etapa de prueba en diversos equipos (con características similares al SunSITE) por lo que se ha determinó instalar en SunSITE para la protección de éste, los cuales son:

Cops:
Es un sistema que consisten en múltiples programas, cada uno de los cuales revisa aspectos específicos de la seguridad de la máquina, reportando los posibles problemas encontrados.

Tcp-wrapper:
Es una herramienta que permite monitorear y controlar el acceso a los puertos que contienen servicios de red en un sistema Unix.

Crack:
Es un programa que verifica si las contraseñas son débiles haciendo uso de utilerías llamadas librerías, las cuales le dan mas poder al programa para realizar la verificación.

Passwd+:
Es un programa que reemplaza al programa passwd de Unix, y que permite a los usuarios modificar su contraseña de acceso, pero vigilando que la nueva contraseña no sea fácil de adivinar.

De acuerdo al resultado del análisis de riesgos, existen tres recursos que necesitan una especial protección protección debido a su alto riesgo de daño, para cada uno de estos, el método de protección es descrito a continuación:

Arreglo de discos	La forma de proteger el arreglo de discos es recurrir a la protección física del lugar donde se encuentra el equipo, también se debe atender al mantenimiento tanto preventivo como correctivo y en caso de que el equipo sufra algún daño hacer uso de la garantía del proveedor.
Cintas de respaldos	Se determinó tener un lugar específico que contenga las cintas de respaldos, diferente al sitio donde se encuentra el equipo. Solo el administrador del sistema tendrá al acceso a las cintas para evitar posibles daños
Sistema operativo	Para proteger todas las utilerías y programas que contiene el sistema operativo, se determino el uso de herramientas de protección. Estas herramientas tienen como finalidad proteger contra accesos no autorizados que dañen el sistema y examinar el estado del mismo en forma periódica.
Programas servidores	Los programas servidores son uno de los principales puntos de ataque de los usuarios externos, por lo que se debe cuidar que estos no sufran modificaciones no autorizadas, o bien, garantizar que el programa servidor siempre esta atendiendo adecuadamente las peticiones.
Datos en tránsito	La información proporcionada a través del WWW, ftp y Listas de correo, no es totalmente confidencial debido a que no se maneja información personal, debido a esto sólo se propone utilizar algún método de criptografía para la información de las listas de correo si el usuario lo desea.

5. Por cuanto tiempo se va a proteger

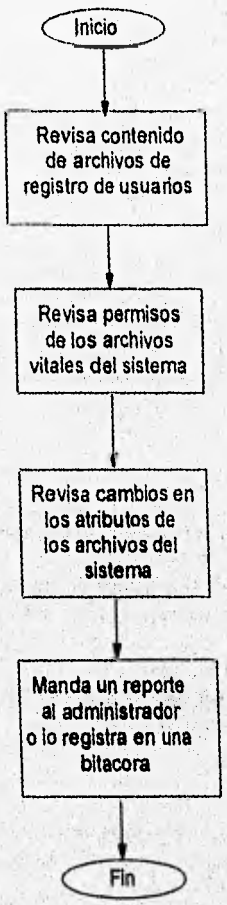
Se eligió un plan que permite la protección del SunSITE que cubre un plazo de 3 meses como prueba para verificar su eficacia, en caso de que el plan demuestre tener buenos resultados se adoptara con un plazo de un año agregando funciones dependiendo de las necesidades.

Integridad de la Información.

Es necesario verificar constantemente los atributos (permisos y modificaciones) de:

- los archivos de configuración,
- programas en general (binarios y scripts),
- bitácoras,
- directorios .

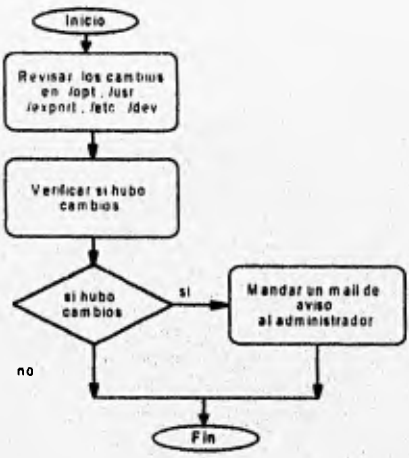
Esto se realiza con el fin de prevenir y detectar alteraciones en el sistema. Para llevar a cabo ésta tarea se utiliza la herramienta de dominio público Cops, la cual es descrita es el siguiente diagrama de flujo:



Se cuenta con dos módulos para llevar a cabo la verificación de la integridad de la información, basándose estos en la herramienta Cops anteriormente descrita.

Módulo I

Verificar que la información propia del sistema operativo este en las particiones correctas.



a) Revisar los cambios en /opt , /usr , /export , /etc , /dev.

Se compara la estructura árbol almacenada en un archivo que sea la original contra otro archivo que contenga la estructura árbol del estado actual del los directorios puestos a revisión.

La manipulación de los archivos se realiza desde la cuenta de administración básica bajo el directorio de /admin_almacen.

b) Verificar si hubo cambios.

El resultado de la verificación se guarda como un reporte en un archivo que es reemplazado cada mes por uno nuevo. Estos reportes se almacenan bajo /var/reportes/admin_almacen.
En este modulo se prende una bandera en caso de detectar algún cambio en la estructura.

c) Mandar aviso al administrador del sistema en caso de haber cambios.

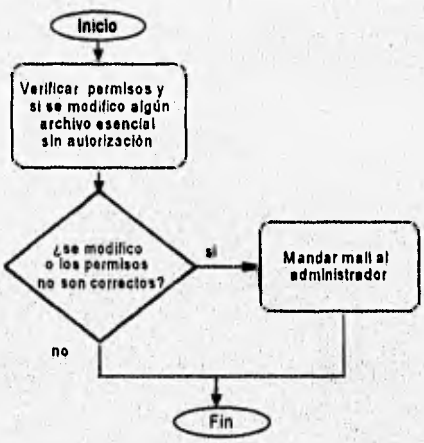
En caso de que la bandera se encuentre prendida se manda un aviso por correo electrónico al administrador del sistema.

Módulo II

Cerciorarse que la información del sistema operativo y de los servicios no este corrupta y revisión de sus permisos.

La verificación se realiza solamente para aquellos archivos que son esenciales para que el servidor se encuentre operando correctamente.

Esta verificación consiste en verificar que los archivos no hayan sido modificados sin autorización o que sus permisos no sean los correctos, para esto se debe ejecutar un script que haga uso de la utilería find con las opciones que permiten detectar si un archivo ha sido modificado en determinado tiempo, dando como resultado un reporte que será enviado al administrador.



En cuanto al sistema de respaldos que sirve como protección en caso de detectar alteraciones a la información, se estableció lo siguiente:

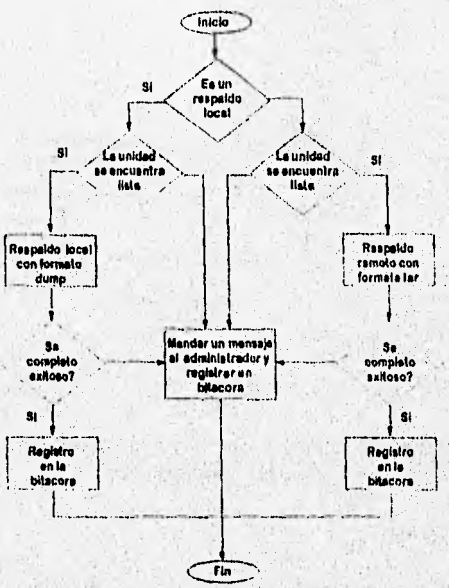
- Calendario de respaldos

  Con el fin de proteger la información en la forma mas estricta posible, sin llegar a la saturación en los medios, se planea realizar respaldos en un periodo de quince idas de la información del disco con el sistema operativo, y un respaldo con periodo de 30 dias de la información que contienen los servicios. Estos respaldos se realizaran en cintas magnéticas debido a su flexibilidad de manejo y su alta eficiencia.

Fecha	Sistema Directorio a respaldar	Servicio Directorio a respaldar	Comentarios
Primer sábado del mes		/wwwadm /ftpadm /export/home	Respaldo completo
Segundo sábado del mes	/, /usr, /var, /opt		Respaldo incremental
Tercer sábado del mes			Respaldo incremental
Cuarto sábado del mes	/, /usr, /var, /opt		Respaldo incremental

- Programa que realiza respaldos automáticos

Para realizar lo anterior se cuenta con un programa llamado Networker que realiza los respaldos automáticamente, con la característica de poder utilizar unidades de cinta a través de la red, a continuación se muestra el diagrama de flujo del programa:



Accesos Autorizados al Sistema.

La detección de accesos autorizados al sistema se realiza mediante tres módulos que contemplan las funciones de monitoreo del sistema y alerta en caso de posibles infiltraciones. Estos módulos se describirán a continuación.

Módulo I

En éste módulo se verifica que los recursos hayan sido utilizados por usuarios permitidos de acuerdo a las políticas de uso de sistema, para ésto se cuenta con la contabilidad propia del sistema la cual consiste en una serie archivos que contienen información sobre las utilerías ejecutadas por cada usuario (utmpx, wtmpx, utmp y wtmp).

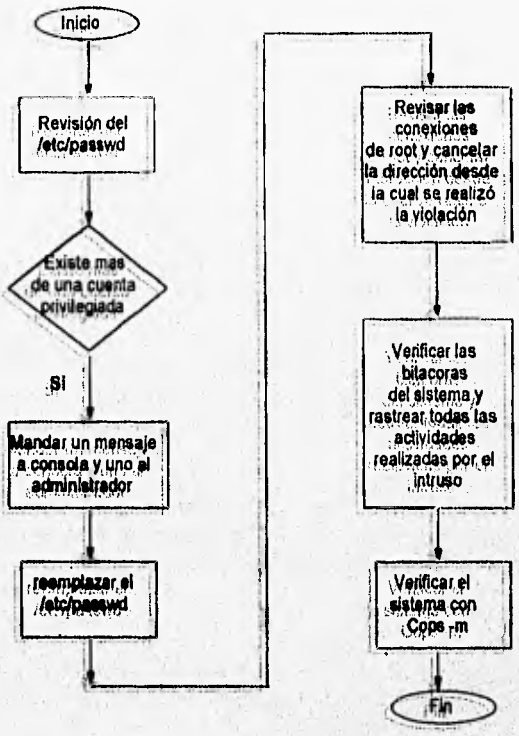
Este modulo también cuenta con un procedimiento de alarma, el cual consisten en verificar si los mensajes que envía el propio sistema indican un atentado contra la seguridad.

Si se detecta que existe un acceso no autorizado el primer paso es encontrar quien y desde donde realizó ese acceso, para lo cual se pueden utilizar utilerías especificas del sistema operativo, como son: lastcomm, last, who, finger, etc.

En segundo lugar deben detectarse los cambios que sufrió el sistema, para esto se cuenta con la herramienta Cops (descrita anteriormente), la cual general el reporte de las últimas modificaciones detectadas en el sistema.

Si se determina que el sistema sufrió modificaciones que no fueron autorizadas se debe restaurar el sistema a su forma original, para lo cual se cuenta con el apoyo de los respaldos, ya que es mejor reemplazar completamente lo que se tiene.

El siguiente diagrama muestra el procedimiento a realizarse en caso de la detección de un acceso no autorizado.

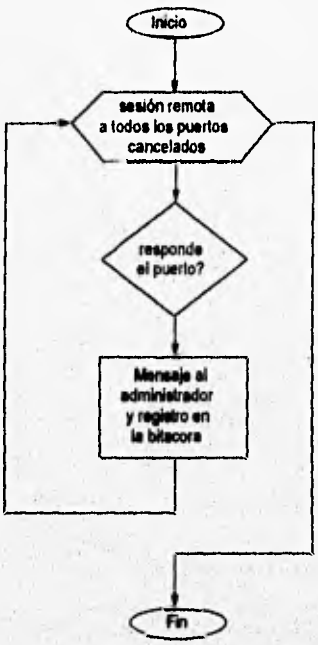


Módulo II

Los sistemas Unix cuenta con un número determinado de puertos, mediante los cuales se accede a los diversos servicios del sistema. Estos puertos son punto de frecuente ataque por parte de los usuarios externos que desean obtener información específica del sistema por lo que es necesario determinar cuales son los puertos vitales para el sistema y cancelar los que no lo sean, además de monitorearlos constantemente.

Servicio	Puerto	Necesario	No necesario	Descripción
ftp	21	■		Transferencia de archivos
telnet	23	■		Sesión remota
name	42		■	Servidor que soporta el protocolo DARPA.
shell	514	■		Provee ejecución remota del shell basado en autentificación.
login	513	■		Provee ejecución remota del login basado en autentificación.
exec	512	■		Provee ejecución remota de procesos basados en autentificación.
comsat (biff)	512		■	Escucha los reportes del correo que llega y notifica a los usuarios.
talk	517	■		Servicio de comunicación interactiva.
uucp	540		■	Permite el uso de líneas conmutadas
tftp	20		■	Transferencia de archivos de maquina a maquina.
finger	79	■		Se obtiene información sobre las sesiones activas en el sistema.
systat	11		■	Provee información sobre los procesos activos en el sistema
netstat	15		■	Provee información sobre la actividad de red del sistema
time	37	■		Servicio usado para la sincronización del reloj
echo	7	■		Usado para pruebas de los puertos
discard	9		■	Usado para pruebas de los puertos
daytime	13		■	Usado para pruebas de los puertos
chargen	19		■	Usado para pruebas de los puertos
100087/10			■	Utilizado para la instalación inicial del sistema
rquotad/1			■	Provee información de quota sobre sistemas de archivos montados a través de la red.
rusersd/2-3			■	Provee un listado de los usuarios en una maquina.
sprayd/1			■	Usado para pruebas de los puertos
walld/1			■	Permite enviar mensajes a los usuarios del sistema.
rstatd/2-4			■	Usado como monitor del estado del sistema.
rexd/1			■	Provee la ejecución de programas remotos en forma no interactiva.
100083/1			■	Herramienta para comunicarse con servidores de bases de datos.
smtp	25	■		Protocolo del correo electrónico.
pop-2	109		■	Protocolo de correo electrónico para líneas de comunicación conmutada.
who	513	■		Provee información sobre los usuarios del sistema.
syslog	514	■		Filtra los mensajes al programa syslogd, el cual abre el archivo de bitácora, escribe a consola o redirecciona los mensajes a otra maquina en la red, dependiendo de la configuración.
route	520	■		Utilizado en la tablas de ruteo de la maquina
kerberos	750		■	Autentificacion de los usuarios de la red.
listen	2766		■	Proceso que escucha las peticiones e invoca los servidores correspondientes, usado en redes orientadas a conexión.
nfsd	2049		■	Permite montar sistemas de archivos remotos.

Este módulo realiza pruebas de acceso a los puertos para verificar que sólo los puertos necesarios están disponibles, en caso de detectarse que un puerto no autorizado esta respondiendo se procede a cancelarlo, detectar quien lo habilitó y que tipo de acceso proporcionaba dicho puerto. También se cuenta con una contabilidad de acceso a los puertos mediante el programa Tcp-wrapper.



Módulo III

Para mantener la confiabilidad en los accesos al sistema es necesario asignar claves de acceso que no sean fácilmente violables, debido a esto, se determinó que el tiempo para renovar las claves de acceso en las cuentas de administración será de tres meses y para clave de superusuario es de un mes, las características con las que debe cumplir cada una de las claves de acceso son:

- Debe contener siete caracteres alfabéticos, tres letras mayúsculas y tres minúsculas
- Debe contener un caracter numérico o especial

Después de cada renovación de claves de acceso se deben verificar mediante un programa que trate de accederlas aleatoreamente, en este caso se utilizó el programa Crack.

Políticas de Seguridad.

De acuerdo al método de definición de políticas de seguridad, a continuación se definen los aspectos necesarios:

- Tipos de usuarios a los que se les permiten utilizar los recursos

  Se les permite utilizar los servicios a cualquier tipo de usuarios siempre y cuando su comportamiento este de acuerdo con las políticas de uso del sistema determinadas en el plan de administración del sistema.

- Personas que están autorizadas para garantizar el acceso y aprobar el uso de los recursos.

  Existe un equipo de 3 personas que colabora en la administración del sistema y otro equipo de tres personas que colabora en administración del servicio, de estos, sólo el equipo de administración del sistema esta autorizado para garantizar acceso y aprobar el uso de recursos de los usuarios o de los mismos administradores del servicio.

- Derechos y las responsabilidades del usuario.

  Como se mencionó anteriormente en el capítulo tres en el establecimiento de políticas, el usuario puede hacer uso de los recursos que le son otorgados según los lineamientos del sistema, además de que no se le puede negar el acceso sin una justificación. Debido a que no existirán usuarios con información residente en el sistema no se debe permitir el uso del mismo a personas ajenas a el.

- Derechos y responsabilidades del administrador del sistema frente a los del usuario.

  La función primordial de el administrador es el proporcionar en forma adecuada los servicios a los usuarios, además debe mantener la información sensible (o vital de la máquina) oculta a los mismos. Todas las funciones del administrador deben estar orientadas a dar un buen servicio a los usuarios.

- Sanciones tanto para administradores como para usuarios en caso de que estos no cumplan con lo establecido en las políticas de administración y uso del sistema.

  En caso de que los administradores cometa una falta grave en cuanto a: garantizar la confidencialidad de la información, restringir el acceso a recursos en forma sin autorización o cualquier acción que repercuta negativamente en el uso de el servicio por parte de los usuarios, es necesario cancelar los permisos de superusuario a dicho administrador para evitar posteriores conflictos.

- En caso de detectar accesos no autorizados al sistema, se debe establecer el procedimiento a seguir en el sistema para lograr la recuperación del servicio, además de determinar a que organismos especializados nacionales e internacionales les corresponde tener una notificación del hecho, dependiendo de las acciones que se quieran llevar a cabo en contra del intruso y de la necesidad de ayuda para rastrearlo.

  Algunos organismos encargados de asesoría en caso de accesos no autorizados y a los cuales se puede recurrir en caso de emergencia son:

  CERT (Computer Emergency Response Team Coordination Center): este organismo genera documentos de ayuda en caso de encontrar fallas en los servicios y en el sistema, estos documentos son llamados Cert Advisories.
  CIAC (Computer Incident Advisory Capability), este organismo genera boletines de ayuda, similares a los Cert Advisories.
  ASC (Area de Seguridad en Cómputo), grupo de la DGSCA que brinda ayuda y asesoría.

Barreras de Protección.

Actualmente se esta llevando un estudio sobre el tipo de barrera de protección que se necesario instalar para proteger los servicios que proporciona el SunSITE, así como todos los que se proporcionan dentro de la CSR.

En este trabajo se propone que se instale un Barrera de protección del tipo anfitrión de dos bases debido a las ventajas que representa este.

5.4.3 Plan de Administración de los Servicios

5.4.3.1 Administración Básica

Recursos Humanos

La asignación de personal para administración de los servicios es la siguiente:

Servicio	No. personas para la administración
World Wide Web	1
FTP	1
Listas de Discusión	1

Políticas de Uso de los Servicios

FTP y WWW

- **La información** y software que se encuentra en estos servicios es **completamente público**, todos lo pueden obtener para fines lícitos.
- **No se podrán realizar** accesos con fines de destrucción del servicio ni con fines **de quebrantar al servicio** para hacer uso de los recursos del servidor.
- **No se debe modificar la** información.
- **No se deben realizar** tareas que afecten a la disponibilidad del servicio.

Listas de Discusión

- **No utilizarlas con fines** de propagación de información para comercialización, **terrorismo, o diferentes** al tema de la lista de discusión.
- **No se deben realizar** tareas que afecten a la disponibilidad del servicio.
- **No se podrán realizar** accesos con fines de destrucción del servicio ni con fines **de quebrantar al servicio** para hacer uso de los recursos del servidor.

Estudio de Crecimiento.

Dado a que se tiene una configuración de RAID 5, no se tiene una cantidad de espacio de **almacenamiento independiente** para cada servicio. De esta manera se tomó en cuenta a **los dos tipos de servicio como uno solo** y se realizó el estudio sumando las dos cantidades **para realizar los cálculos.**

Servicio	FTP	WWW	Total
Cantidad de información inicial en el servicio	1,800 MB	58 MB + 19(25MB)	535,617 MB
Cantidad de información promedio a almacenar por mes (estimado)	10 MB	5 MB	15 MB
Cantidad de información promedio a actualizar	200 MB	25 MB	225 MB

De acuerdo a esta información el máximo crecimiento en meses del sistema de almacenamiento esta dado por la siguiente fórmula:

$$\text{Meses para lograr el máximo crecimiento} = \frac{\text{Total de espacio disponible - Cantidad de información inicial del servicio}}{\text{Información promedio a almacenar mensualmente}}$$

Lo cual da como resultado:

$$\frac{3,800\ \text{MB} - 535,617\ \text{MB}}{15\ \text{MB/mes}} = 67\ \text{meses para alcanzar el máximo crecimiento posible (5 años)}$$

Listas de discusión.

Para este servicio no se considero realizar un estudio de crecimiento dado a que no se utiliza el sistema de almacenamiento.

Actualizaciones del Servidor

- Para estar en contacto con las novedades, los administradores de los servicios deben acceder a los servidores de News constantemente.
- Para saber las actualizaciones, cambios de versiones y parches de los servidores, los administradores se inscribieron a listas de discusión y revisan constantemente los siguientes servidores de ftp para ver nuevas versiones:

Servicio	Servidores anónimos de FTP
WWW	hoohoo.ncsa.uiuc.edu
Ftp	wuarchive.wustl.edu
majordomo	ftp.greatcircle.com

Estudio de Nuevos Servicios

Se navega constantemente en varios sitios de Internet, principalmente en universidades, las cuales son una de las principales fuentes de creación de servicios, además se consultan revistas y periódicos que contienen temas relacionados a Internet.

Desarrollo de Servicios

Actualmente no se requieren desarrollar servicios adicionales, debido al enfoque que se tiene en la prestación de servicios a través del SunSITE.

5.4.3.2 Administración Básica para los Servicios de Información

Organización de Datos

Servicio de World Wide Web

El servidor de WWW mostrara información que estará alojada físicamente en el sistema de almacenamiento del servidor, y ligas a otros servidores de WWW. La información que se almacenara localmente deberá cumplir con el siguiente criterio para su organización:

- Cada sección estará determinada por un icono ilustrativo del tema de acuerdo al tipo de información que contendrá.
- Se establecerán documentos que indique una descripción del tipo de información que contiene.
- En cada página principal de cada una de las secciones se establecerán iconos que mediante selección harán referencia a las secciones que se presentan en la página principal del SunSITE.
- Se buscara que no se tenga ocupado espacio duplicado en caso de que se refiera a cierta información en diferentes secciones, sino que sólo se haga una liga a lugar donde se encuentra físicamente.

Servidor de FTP

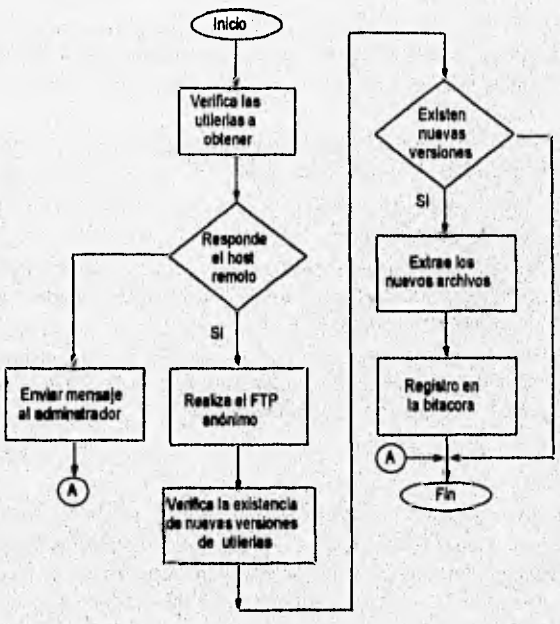
El servidor de FTP debe ser un espejo del SunSITE de la Universidad del Norte de Carolina tomado en cuenta que éste se mantendrá actualizado en el servidor local de la UNAM. Se determinó que este servidor contendrá índices y archivos en cada directorio, de tal manera que permitan dar una visión general del software que se en cuentra en cada sitio en que se sitúen.

La información en este servicio estará organizada en forma de árbol, es decir cada directorio tendrá un titulo dependiendo del tipo de información que contenga y mientras mas profunda sea la ramificación contendrá un nombre especifico de software. En cada uno de los niveles del árbol se tendrá un archivo en formato texto (ASCII 7 bits) en el cual se tendrá una referencia breve del tipo de archivos y un listado de lo que se puede encontrar en esa rama.

Actualizaciones de Datos

Para realizar las actualizaciones, se desarrolló un programa que obtiene la información del SunSITE de Carolina del Norte con la cual se crea el espejo en el servicio de FTP de el SunSITE de la UNAM, esta actividad se lleva a cabo en forma automática para agilizar el proceso.

La creación del espejo se realiza para actualizar, o bien reemplazar, las utilerías proporcionadas como software público. A continuación se muestra el diagrama de flujo que corresponde al programa de actualización de información.



5.4.3.3 Contabilidad de Uso

Se realizó un sistema de contabilidad, el cual tiene como función contabilizar el usos de cada uno de los servicios. Este sistema se basa en los registros de accesos, teniendo como resultado la generación de reportes y gráficas.

Diagrama de flujo del sistema de contabilidad para el servicio FTP

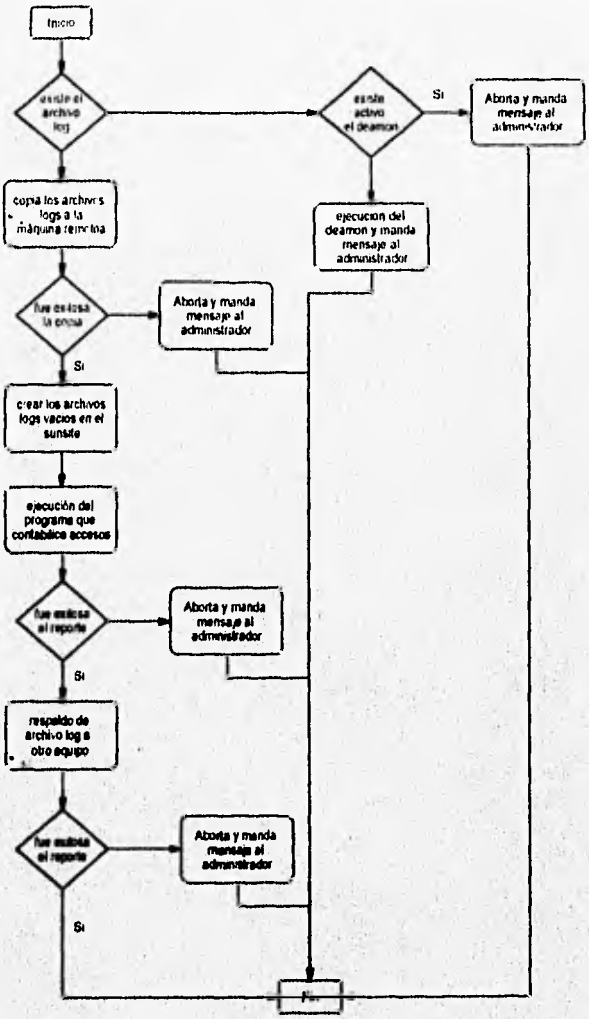


Diagrama de flujo del sistema de contabilidad para el servicios de World Wide Web

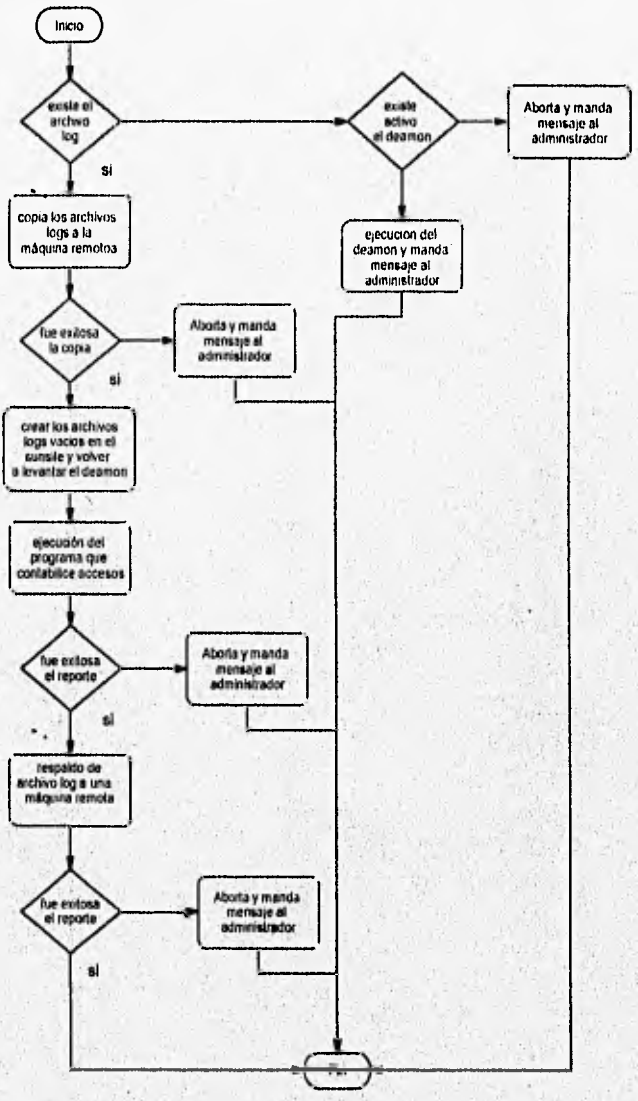
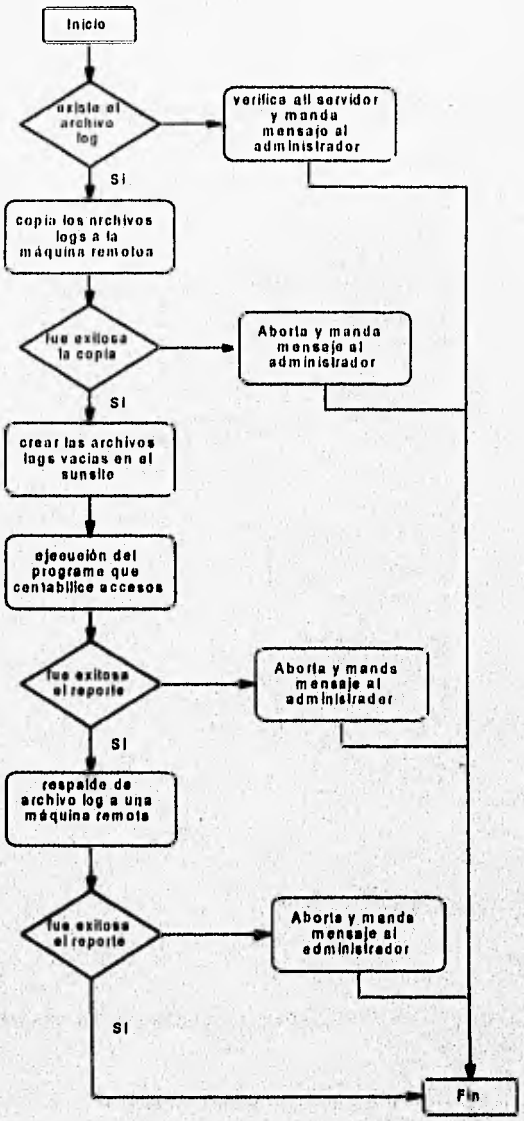


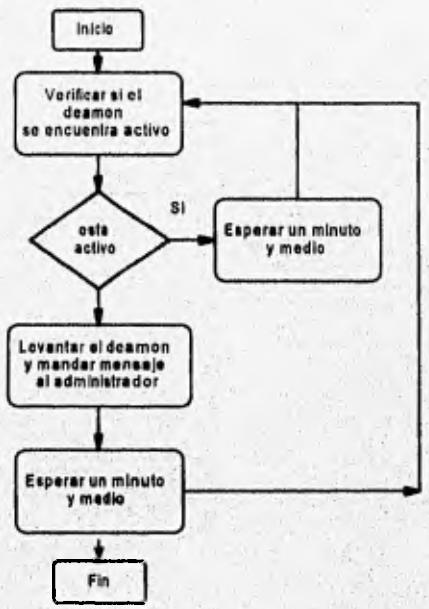
Diagrama de flujo del sistema de contabilidad para el servicio de listas de discusión "Majordomo"



5.4.3.4 Monitoreo del Servicio

El monitoreo se lleva acabo mediante un programa que fue realizado por los administradores, en el cual se verifica mediante utilerías de Unix que el servidor esté activo para atender las peticiones.

Diagrama de flujo del monitor para los servicios World Wide Web y FTP



5.4.3.5 Seguridad de los Servicios

Servidor de FTP

Se aseguró que el servidor FTP anónimo cumpliera con los siguientes aspectos que determinan su seguridad:

1. **Se verificó que el servidor no pueda utilizar el comando SITE EXEC en un telnet al puerto 21. Se instaló la versión más reciente que contiene la corrección de muchos errores de seguridad (wu-FTP 2.4).**

2. Se verificó que nadie pudiera acceder ni crear directorios en el directorio principal. Ya que se considera intruso al que pueda acceder y crear archivos como .forward y .rhosts.

3. Se verificó que el dueño del directorio principal no sea ftp, ya que si no cualquier usuario puede crear archivos (con el comando para UNIX chmod 777)que puedan ayudar a tener acceso al sistema con privilegios para realizar actividades ilícitas y afecten al servicio y al sistema.

4. Se verificó que ningún directorio o archivo lenga como dueño ftp, ya que en el caso de contar con esto es posible que algún intruso pueda reemplazarlos con versiones modificadas y causar daño en el sistema.

Para determinar el servidor FTP anónimo que se instalaría, se buscó a través de Internet documentación que describiera la implementación del mismo.

Servidor de World Wide Web.

Dado a que se instalo un servidor de WWW comercial (Netscape Commerce Sever), se implemento la seguridad tal y como fue planteada en su manual de instalación. De este manual se obtuvo la información de seguridad del servicio WWW y describe lo siguiente:

El servidor Comercial de Netscape, trabaja con un protocolo llamado SSL (Secure Sockets Layer) para la transferencia de datos por toda Internet. SSL es un criptosistema (sistema que encripta) que trabaja a nivel de protocolo.

Este protocolo provee una seguridad al servidor con autentificación, encriptamiento e integración de datos.

Autentificación. Permite que el cliente se conecte realmente con el servidor correcto. Esto previene que cualquier computadora trate de atacar la seguridad del servidor. El procedimiento de autentificación consta de los siguientes pasos:

1. El cliente envía una petición para conectarse a el servidor con seguridad.

2. El servidor envía un certificado digital asignado al cliente. El servidor usa el Certificado adquirido por CA (Certification Autorites). El certificado asignado contiene dos grupos de información. El primero es información propia certificada, incluyendo el nombre del servidor, esta es una llave pública, el certificado de la validación de datos, y el nombre de el CA. El segundo es una firma digital. Est firma no puede ser olvidada.
   Este es el encriptamiento que usa la llave privada CA.

3. El cliente autentifica al servidor encriptando la firma digital y acepta la información del certificado. Si el certificado no fue válido durante la transacción, la firma digital no es

aceptada. En este caso, el cliente termina la conexión con el servidor. Si el certificado es válido, el servidor es autentificado.

4. El cliente genera una sesión llave y encripta a este usando la llave pública del servidor dada por el certificado (de ésta manera, solo la llave privada del servidor puede desencriptarla). La sesión llave es usada posteriormente. Para encriptar los datos y asegurarse de la integridad de los datos. El cliente envía la llave de sesión encriptada al servidor.

5. El servidor recibe la llave de la sesión, la cual es usada para encriptar y desencriptar los datos, entonces, esto puede enviar y recibir de manera segura desde el cliente.

Encriptación: resuelve la transferencia de datos de tal manera que cualquiera que trate de realice copias de la información o la interfiera ilícitamente, no pueda entenderla.

Después de que el cliente autentifica un servidor, genera una llave que le permite al cliente y al servidor encriptar y desencriptar los datos, previniendo la tercera parte de la tarea de descifrar sus comunicaciones. Una tercera parte pueden corromper los datos removiendo o adicionando datos desconocidos en la transacción, lo cual hace que la función que realiza SSL mediante la integridad de los datos, ofrezca una seguridad más completa.

Integridad de los datos: verifica que los datos enviados entre el cliente y el servidor no sean alterados durante la transferencia. Es decir, este indica cuando son adicionados o borrados los datos. SSL usa mensajes de códigos de autentificación (MAC, Message Authentication Codes) para asegurar que los datos enviados entre el cliente y el servidor sean saboteados. Si se corrompió la integridad de los datos, el cliente o el servidor terminan la conexión.

Servidor de Correo Electrónico para ser Utilizado con Listas de Discusión y WWW.

El correo electrónico es uno de los servicios con problemas en su lógica interna y por lo tanto uno de los principales puntos de ataque en un sistema, debido a esto es necesario mantener herramientas auxiliares para no permitir accesos no autorizados al sistema a través de el correo electrónico. Por lo que se estableció en la CSR contar con la versión Sendmail-8.7.5, la cual garantiza que los errores que hasta ahora se habían utilizado por los usuarios externos se bloqueen.

Las principales características de esta versión de correo electrónico son:

- Elimina los bugs conocidos en las versiones anteriores, como son el uso de opciones que permitían acceso a la cuenta de superusuario.
- Mantiene un registro mas estricto en su bitácora.
- La configuración es fácil de llevar a cabo y no causa conflictos en la comunicación con otras versiones de correo electrónico.

Servidor de Listas de Discusión "Majordomo".

Majordomo es un software servidor con el cual automáticamente se administran las listas de correo electrónico en Internet, su funcionamiento es mediante comandos que son enviados al servidor vía correo electrónico, por lo que, virtualmente todas las operaciones pueden ser realizadas remotamente sin requerir la intervención del administrador del servicio.

Las principales características de majordomo son:

- Soporta varios tipos de listas, (moderadas y abiertas entre otras)
- Puede ser configurado fácilmente
- Está escrito en un lenguaje que es fácilmente personalizado.
- Se basa en el diseño modular
- Incluye soporte para FTP-mail

El modelo de seguridad para majordomo se basa en los permisos y atributos de los archivos y los directorios. Majordomo trabaja usando un programa llamado wrapper el cual permite a Majordomo correr sin permisos especiales, sino, bajo el usuario y grupo majordomo. Los archivos que utiliza Majordomo deben tener los permisos de lectura y escritura para el dueño y el grupo, y los directorios deben tener, además, los permisos de ejecución.

Majordomo utiliza tres diferentes claves de acceso para mantener separadas todo tipo de actividades:

1. Una clave de acceso maestra. Esto permite que alguien que pertenece a varias listas pueda usar la misma clave de acceso.
2. Una clave de acceso para el administrador de una sola lista.
3. Una clave de acceso para lo concerniente al contenido de la lista. De esta manera las funciones de administración y moderación pueden ser separadas.

A pesar de que el modelo de seguridad de Majordomo es lo suficientemente amplio, se han recibido reportes de vulnerabilidades en todas las versiones de Majordomo, mediante estas vulnerabilidades usuarios externos e internos pueden correr programas sin autorización en la maquina local sin que las Paredes de fuego, u otros programas de seguridad como TCP-wrapper, puedan detectarlo. La solución de este tipo de problemas se encuentra en las nuevas versiones de Majordomo ya que muchos de los parches o cambios en la configuración pueden no ser útiles para todas las plataformas operativas.

5.4.3.6 Atención a Usuarios

La atención a usuarios esta dada en cada servicio mediante un correo electrónico al cual se puede dirigir en caso de dudas y comentarios. Además, mediante la Coordinación de Servicios de Red y el Departamento de Comunicaciones y Redes se proporciona un "Laboratorio de atención a usuarios " para atender a todos los que lo deseen.

5.5 Evaluación de los Resultados.

Se realizó una revisión de todos los procedimientos implementados. Esta revisión se llevo a cabo cotejando cada paso de los planes de administración con su implementación, por lo que se determinó que los resultados de la revisión son satisfactorios.

Posteriormente se llevo a cabo un método con el cual se asegura que los servicios ofrecidos son de calidad, mediante dicho método se realizó una estimación de cada uno de los aspectos involucrados en la calidad de los servicios.

La evaluación se realizo desde máquinas que se encontraban directamente conectadas en el mismo segmento en que se encontraba el servidor SunSITE de la UNAM, los horarios establecidos para los diferentes actividades de evaluación fueron aleatorios durante el tiempo determinado en el método de evaluación descrito en el capitulo 3.

- Disponibilidad:

Accesos

Día	Total de accesos exitosos por día
1	30
2	30
3	30
4	30
5	30
6	30
7	30

De acuerdo a los resultados obtenidos se tienen 210 accesos, por lo tanto se asignaron 100 puntos

Sistema de Almacenamiento

En el resultado de la evaluación del sistema de almacenamiento se asignaron 100 puntos, dado a que no se registro ninguna saturación.

Monitoreo del Sistema

Siguiendo el criterio establecido para el monitoreo del sistema, nunca se registro una baja del sistema, por lo cual se asignaron 100 puntos a este aspecto.

Monitoreo del servicio

La puntuación correspondiente a este aspecto es de 100, dado a que el monitor del servicio nunca registro que el servidor estuviera inoperante.

La puntuación total obtenida en la evaluación de disponibilidad es:

Disponibilidad = Accesos + Sistema de almacenamiento + Monitoreo del sistema + Monitoreo del servicio

Disponibilidad = 100 + 100 + 100 + 100

Disponibilidad = 400

- Eficiencia:

Dado a que se obtuvo en el resultado del anállsis de rendimiento y sintonización que el sistema se encontró en el caso b) (ver análisis de rendimiento y sintonía de este capítulo 3, pag52), la puntuación que corresponde a la eficiencia es de 70.

Eficiencia = 70

- Estado de la Información:

Para verificar el estado de la información se necesitan monitorear los siguientes aspectos:

Actualización

Debido a que el servidor se puso en operación por primera vez se y a que información que se presenta en el servicio fue recientemente puesta a disposición, en los accesos realizados aleatoriamente al servicio, no se registro que algún documento estuviera atrasado de acuerdo a su fechas de actualización, por lo cual se asigno una puntuación de 100 en su evaluación. Cabe mencionar que sólo se evalúo para la información que se encuentra alojada localmente en el servidor.

Organización

Se accedio aleatoriamente a los servicio y se encontró que la organización de la información que se tenía estaba de manera correcta, por lo tanto se le asigno de acuerdo al criterio establecido una puntuación de 100.

Formato

Dados los resultados de los accesos aleatorios se determinó una puntuación de 100 en la evaluación, ya que no se encontró algún documento que no tuviera el formato adecuado para que se pudiera leer la información.

El resultado final de la evaluación del estado de la información es el siguiente:

Estado de la información = Actualización + Organización + Formato

Estado de la información = 100 + 100 + 100

Estado de la información = 300

Resultado Final

El resultado final de la evaluación es el siguiente:

$$Calidad = (Disponibilidad + Eficiencia + Estado\ información)\ X\ 0.125$$

$$Calidad = (400 + 70 + 300)\ X\ 0.125$$

Calidad = 96.25%

De acuerdo a los resultados obtenidos se considera que el resultado de la implementación fue satisfactoria ya que se encuentra entre el rango establecido (100 %- 95%). Además se establecio que se atacará el aspecto que se evalúo con la puntuación menor a 100 para poder alcanzar posteriormente un 100% de calidad.

Conclusiones

El contenido de este trabajo, los conocimientos obtenidos a lo largo de el desarrollo y la aportación que deriva de él, podemos concluir en lo siguiente:

Conocimientos Adquiridos

Con el surgimiento de Internet se ha abierto una puerta en la cual los ingenieros en computación pueden aplicar sus conocimientos y hacer uso de la formación adquirida en los diversos campos computacionales de desarrollo, investigación y administración.

De esta manera, éste trabajo nos ha permitido incrementar nuestros conocimientos, aplicarlos y aprender acerca de la arquitectura y el funcionamiento de los servicios que se ofrecen a través de Internet, además de que hemos podido valorar la importancia de esta red, con la cual se pueden cubrir las necesidades de compartir información, recursos y sobre todo ideas a nivel mundial.

También nos ha permitido incursionar en el área de la administración de los servidores en Internet, la cual nos parece que es un campo interesante, extenso y con muchas expectativas de desarrollo en el futuro.

Contenido del Trabajo

Valoramos la gran oportunidad que tuvimos de poder recopilar las experiencias adquiridas en la CSR y de investigaciones realizadas en el área de administración de servidores, la cual fue nuestro apoyo para desarrollar este documento que indudablemente ayudara a los administradores que deseen mejorar sus servicios.

Consideramos que el diseñar los planes de administración, tomando en cuenta todos los aspectos necesarios para lograr un administración efectiva de los equipos y de los servicios, ha sido un trabajo que requiere de organización y dedicación para lograr un resultado positivo.

Una de las principales aportaciones de la tesis para nosotras fue la estructuración de una estrategia, la cual se propuso a lo largo de este trabajo, siendo un método que diseñamos con el fin de facilitar la implementación de los procedimientos de administración, permitiendo realizar una evaluación completa de los resultados obtenidos al final de ésta. El objetivo de esta estrategia es el permitir llevar un orden de todas las actividades involucradas en la administración, proporcionando un mayor control de estas actividades.

En nuestro caso de aplicación la estrategia propuesta resultó exitosa, permitiéndonos llevar los servicios que contiene el SunSITE a un nivel que consideramos de calidad, ya que se cubrieron los aspectos de disponibilidad, eficiencia y presentación de la información en la forma esperada. Por tal motivo consideramos que el objetivo de este trabajo se cumplió y puede ser aplicado para cualquier servidor de la CSR que cumpla con las características planteadas.

Comentarios Finales.

Creemos que este trabajo es de gran utilidad para el grupo de administración de la CSR, sin embargo consideramos que además de tomar en cuenta la base que ofrece este trabajo, se debe mantener una constante investigación en el área de administración de servidores en Internet con el fin de estar actualizados en los avances de la tecnología. En general podemos decir que éste trabajo puede ser un apoyo para todas aquellas personas que están relacionadas con el área de administración de los servidores en el ámbito académico.

Debido a que hasta nuestros días no había existido un documento que tuviera la función de guía para los administradores, sentimos que con este trabajo estamos contribuyendo a que los servicios que proporciona la UNAM, sean de calidad y puedan llegar a ser considerados un ejemplo por las instituciones educativas de México.

1. Apéndice "Conjunto de Protocolos TCP/IP"

Inicio de TCP/IP

DARPA en 1969, creó una red experimental de conmutación de paquetes llamada ARPANET. Su fin era proporcionar un medio para la transferencia de información seguro e independiente del tipo de tecnología.

En 1975 la Agencia de Comunicaciones de la Defensa de Estados Unidos (DCA) toma la administración de ARPANET debido a que su utilización la convierte en una red ampliamente utilizada por importantes compañías y deja de ser una red experimental para convertirse en una red operacional.

A causa de su popularidad surge la estandarización de comunicación, agrupando protocolos que en el futuro serían la base fundamental de los servicios, transferencia de información, envío de mensajes, administración de la red y seguridad, surgiendo así el conjunto de protocolos TCP/IP.

En 1983 ARPANET se divide en una parte militar, llamada MILNET y otra en una pequeña porción que continuaba con la misma filosofía de la red original. Y hasta 1990 ARPANET deja de llamarse así para convertirse en INTERNET, que sería desde entonces conocida como la red internacional más grande.

Definición

TCP/IP es un conjunto de protocolos de comunicación. Un protocolo de comunicaciones de red es un conjunto formal de reglas que describen cómo el software y el hardware internacional con la red proporcionando una forma de comunicación homogénea a través de ella.

Características

Las principales características de TCP/IP son las siguientes:

- Independencia del hardware o software de un equipo específico. Debido a que es ampliamente soportado, TCP/IP es el ideal para comunicar computadoras de diferentes plataformas .

- Independencia de la tecnología de red que se utilice. Permitiendo integrar redes diferentes, tales como Ethernet, Token Ring, X.25 y prácticamente cualquier tipo de red.

- Tiene un esquema de direccionamiento común. Permitiendo identificar inequívocamente un host dentro de la red.

- Contiene protocolos de alto nivel estándar para poder implementar servicios de manera consistente y de alta disponibilidad para los usuarios.

Muchos conjuntos de protocolos están estructurados en capas, en ocasiones se refieren a ellos como un *stack de protocolos*. Cada capa está diseñada para un propósito particular y es independiente de lo que pase en las demás capas.

Cómo trabaja TCP/IP

TCP/IP maneja a los paquetes como unidad básica de transferencia sobre la red. Los paquetes contienen en el formato un encabezado con información del transmisor y receptor además la manera en cómo se va a manejar en las capas de protocolos. Debido a que los paquetes contienen un número finito de bytes frecuentemente se recurre a la fragmentación de paquetes para su transmisión.

TCP/IP sólo reconoce dos tipos de entidades que son enruteadores y hosts. Los ruteadores son máquinas que se dedican a enviar paquetes de una red a otra, por lo cuál este debera tener dos interfaces de red. Un hosts es una máquina que sólo contienen una interfaz de red por lo que no puede enviar paquetes a través de redes.

A un host lo identifican las tres siguientes características del conjunto de la red:

- Su nombre (hostname). Este es el nombre del host (por ejemplo *servidor*), que también es el nombre de su primer interfaz. El hostname junto con el dominio forma el nombre completo de host (*servidor.dgsca.unam.mx*)

- Su dirección IP (IP address). Esta es la dirección que tiene una red TCP/IP e identifica a la máquina entre todas las demás. Esta dirección también puede servir para saber o darse una idea de en donde se encuentra ese host en la red.

- Su dirección de Hardware (Ethernet Address). Esta dirección es única y todo host debe de tener esta dirección que es asignada *físicamente* a la interfaz de red.

El Modelo OSI y TCP/IP

MODELO OSI (Open System Interconection)

En los sistemas abiertos se utilizan los protocolos estatificados debido a que los organismos de normalización más importantes como OSI, CCITT, ECMA y ANSI entre otros, apoyaron la utilización de estas , además que los principales fabricantes como Hewlelt Packard, XEROX, DEC, IBM y Nothern Telecom han instalado protocolos estatificados, pero lo principal era basarse en el sentido común, estar respaldados por la teoría para que de esta manera:

- Se pudiera descomponer lógicamente una red en partes (niveles o estratos) más pequeñas y fáciles de entender,
- Proporcionar interfaces normalizadas entre distintas funciones de la red,
- Conseguir simetrías en las funciones que se realizan en cada nodo de la red,
- Ofrecer un método que permita predecir y controlar posibles cambios en la lógica de la red,
- Establecer un lenguaje normalizado que permita clarificar la comunicación entre los distintos diseñadores, fabricantes, distribuidores y usuarios de redes, a la hora de discutir las funciones de una red.

De esta manèra ISO y CCITT crearon un modelo para interconexiones de sistemas abiertos llamado Open System Interconection (OSI) cuyos objetivos principales son:

- Proporcionar normas para la comunicación de sistemas.
- Abstraer el funcionamiento interno de los sistemas individuales.
- Eliminar todos los impedimentos técnicos que pudieran existir para la comunicación de sistemas.
- Definir los puntos de interconexión para el intercambio de información entre los sistemas.
- Ofrecer un punto de partida válido desde comenzar en caso de que las normas del estándar no satisfagan todas las necesidades.
- Limitar el número de opciones, para incrementar las posibilidades de comunicación sin necesidad de muchas conversiones y traducciones entre diferentes productos.

Este Modelo consiste en siete niveles, cada uno de los cuales especifica funciones particulares de la red, tales como direccionamineto, control de flujo, control de errores, encapsulamiento, transferencias confiables de mensajes y muchas otras. El nivel más alto es el más cercano al usuario y el nivel más bajo es el más cercano a la tecnología del medio físico. El modelo OSI es universalmente usado como método para enseñar y entender la funcionalidad de las redes.

A continuación describiremos brevemente cada una de las siete capas del Modelo OSI:

1 *La capa física* es la más baja del modelo. Provee las características mecánicas, eléctricas, funcionales y de procedimiento, necesarias para establecer, mantener y liberar conexiones físicas entre el dispositivo terminal DTE y el punto de conexión a la red DCE, o entre dos DTEs. Para el nivel físico se han publicado bastantes estándares.

2 *La capa de enlace* de datos provee la conexión lógica a través de la línea, el direccionamiento, la secuencia y la recuperación de errores. Existe una dirección de enlace que identifica una conexión de enlace en este nivel. Aquí se determina el uso de una disciplina de comunicaciones conocida como HDLC (High Level Data Link Control). HDLC es el protocolo de líneas considerado como un estándar universal, al cual muchos toman como modelo. Los datos en HDLC se organizan en tramas.

La trama es un encuadre de los datos según un formato:

BANDERA	DIRECCION	CONTROL	INFORMACIÓN	SECUENCIA DE CHEQUEO	BANDERA
8 BITS	8 BITS	8 BITS	N/8 BITS	1 BG BITS	8 BITS

Por lo tanto, juntando las capas 1 y 2, ya tenemos la forma de conectar físicamente dos nodos adyacentes y de transferir un mensaje de datos entre ellos, manejando direccionamiento, control de errores, etc., según se especifica en HDLC.

3 *La capa de red* provee el control entre dos nodos adyacentes. Dos conexiones se proveen: punto a punto o en red. Una o más conexiones de red pueden ser ubicadas en la misma conexión de enlace y se distingue por sus direcciones.

Las funciones proporcionadas por este estrato incluyen el ruteo de los mensajes, las notificaciones de errores y opcionalmente la segmentación y el bloqueo. La utilidad de esta capa puède ser vista como de "dirección del control entre los puntos de comunicación", más que como proveedora de ayuda para la transferencia de datos entre estos puntos.

En este estrato se determina el formato del campo de información de la trama HDLC. A esto se le llama Paquete y es un término cuya popularización es muy grande a raíz de la difusión del uso de redes X.25 o de Conmutación de paquetes (Packet switching). Estos tres primeros niveles recomiendan procedimientos para solucionar los requerimientos de conexión entre DTE y un DCE, para efectos de realizar la transmisión de mensajes con propósitos prácticos y con un buen grado de confiabilidad.

4 *La capa de Transporte* proporciona el control entre nodos de usuarios a través de la red. Para ir de un nodo a otro es necesario pasar por otro(s), por lo tanto, es necesario llevar "en memoria" dos direcciones: el destino final y el destino inmediato.

Solamente en el último tramo, ambos destinos coincidirán. En cada nodo intermedio, es necesario tomar la dirección correcta y saber que desde un nodo se llega a otro nodo fácilmente. De la misma forma que un viajero debe elegir adecuadamente (con conocimiento) el próximo destino inmediato, cada nodo de la red debe enviar el mensaje hacia un punto perteneciente a la ruta más conveniente para llegar al destino final. Los criterios de selección de ruta dependen de diversos factores (existencia de costos, ocupación, etc).

De la capa 1 a la capa 4 de OSI, conforman el subsistema de transporte. La capa 4 releva a las sesiones de cualquier consideración de detalle referente a la forma en la cual se realiza la transferencia de los datos.

Una conexión de transporte utiliza un "identificador de punto final de transporte" y una o más conexiones de transporte puede ubicarse dentro de la misma conexión de red.

5 *La capa de sesión* provee el soporte para interacciones entre entidades que cooperan en la capa de presentación (siguiente nivel). Las funciones de la capa de sesión se puede dividir en dos categorías:

Determinación y cancelación de contrato entre dos entidades de la capa de presentación (esto se llama Servicio de Administración de Sesión).

Control del intercambio de datos, entre esas dos entidades, comprendiendo sincronización, delimitación y recuperación de operaciones con los datos (esto se llama Servicios de Dialogo de Sesión).

Una sesión utiliza "identificadores de destino final". Se han definido tres tipos de interacciones:

* Dos vías simultáneas.
* Dos vías alternadas.
* Una vía.

6 *La capa de presentación* proporciona un conjunto de servicios de conversiones y descifrado que la capa de aplicaciones (nivel siete) puede seleccionar para poder interpretar el significado de los datos intercambiados.

El modelo identifica tres tipos de protocolos en la capa 6:

* Protocolos de terminal virtual (VTP).
* Protocolos de archivo virtual.
* Protocolos de transferencia de trabajos y manipulación.

Otra de las cosas que pueden incluirse en esta capa es la conversión de código.

7 *La capa de aplicación.* Todas las otras capas existen en función de brindar soporte a esta. Una aplicación se compone de procesos cooperativos que se intercomunican mediante el uso de protocolos definidos en esta capa. Estos procesos de aplicación son la fuente y el destino último de los datos intercambiados.

A continuación mencionaremos la relación que hay entre el modelo OSI y TCP/IP.

TCP/IP trabaja directamente con cada una de las capas del modelo OSI, este proporciona diferentes protocolos para hacer una implementación real de este modelo.

Capa de Enlace

En esta capa se identifica el tipo de protocolo de red que tiene el paquete. Es decir, identifica a TCP/IP el cual proveerá el control de errores.

Capa de Red

Aquí se aceptan y se disminuyen paquetes através de la red, interviniendo protocolos como IP, ARP e ICMP

PROTOCOLO IP

El protocolo IP se encarga de

- El direccionamiento IP
- Las comunicaciones de un Host a otro Host. Decide el path que el paquete tomará en base a la dirección del host que ha recibido.
- El formato del Paquete. Ensambla paquetes en unidades llamadas datagramas IP.
- La fragmentación. En caso de que un paquete sea demasiado largo para una transmisión por la red, los divide en paquetes más pequeños. En el host receptor, IP esta encargado de reconstruir el paquete original.

PROTOCOLO ARP

Este llamado protocolo de resolución de dirección (Address Resolution Protocol) existe entre la capa de enlace y la de red. Se encarga de ayudar a IP dirigiendo datagramas apropiados hacia el host receptor, al mismo tiempo que coteja la dirección Ethernet (48 Bits) con su dirección IP conocida (32 Bits).

PROTOCOLO ICMP

El protocolo Internet de control de mensajes ICMP (Internet Control Message Protocol) es el que se encarga de detectar errores en la red y reportarlos. Los estados de error pueden ser los siguientes:

- Cuando los paquetes llegan demasiado rápido para ser procesados (Dropped Packets)
- Cuando existen fallas de conectividad; es decir, un host no puede ser alcanzado.
- En el redireccionamiento. Indica cuándo se debe de utilizar una ruta alternativa para enviar la información.

Capa de transporte

Los protocolos que son utilizados en esta capa son el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol).En esta capa se asegura de que los paquetes sean recibidos secuencialmente y sin errores.

PROTOCOLO TCP

Este protocolo se encarga de enviar los datos . Esta transmisión consiste en un inicio de conexión, la transmisión de datos y un fin de conexión, Entonces este protocolo hace posible que las aplicaciones se comuniquen.

TCP se considera un protocolo seguro orientado a conexión ya que por cada paquete enviado espera una indicación que le dice que puede continuar con la transmisión, esto es, por cada paquete recibe un acknowledge que le permite saber si el receptor ha recibido el paquete sin errores. Y se le llama end-of-end connection.

PROTOCOLO UDP

Este protocolo provee el servicio de repartición de datagramas. Este no verifica que el datagrama ha sido recibido sin errores. Las aplicaciones que envían pequeñas porciones de información y este protocolo es utilizado en lugar de TCP ya que elimina los procesos que establecen y verifican conexiones.

Capa de Aplicación

En esta capa se definen los servicios estándar de Internet y las aplicaciones de red que se pueden utilizar. En esta capa los servicios no trabajan solos, sino con la capa de transporte para enviar y recibir datos. Los protocolos que se usan son muy variados, entre algunos están:

Servicios TCP/IP estándar:

- *telnet*. Este protocolo permite procesos orientados a-terminal para poder comunicarse en una red corriendo TCP/IP. Provee una interfaz a través de la cual dos hosts pueden comunicarse. Para esto se implementa el comando telnet (local) y el daemon in.telnet (remoto).

- *ftp* Este es el protocolo de transferencia de archivos (File Transfer Protocol) se implementa con el comando ftp y el daemon in.ftpd (remoto). Permitiendo la transferencia de archivos a través de la red.

- tftp. El protocolo de transferencia de archivos trivial (Trivial FTP) provee funciones similares a FTP con la diferencia de que no establece sesiones interactivas, ya que es usado entre máquinas y no entre usuarios.

Comandos UNIX "r":

Estos comandos permiten que el usuario pueda ralizar accesos remotos hacia un host ; estos pueden ser rcp (remote copy) , rlogin(remote login), rsh (remote shell).

Servicios de Resolución de Nombres:

DNS (Domain Name Service). Servicio de Nomenclatura de Dominios. Resuelve los nombres de host, esto es que asocia a cada dirección una dirección IP única.

Servicios de Archivos:

- NFS(Network File System) . Sistema de Archivos por Red provee la facilidad de compartir archivos a través de la red.

Protocolos de Ruteo:

- *RIP* (Routing Information Protocol). Protocolo de Información de Ruteo.
- *RDISC* (Router Discovery Protocol). Protocolo para descubrir enrutadores Estos dos protocolos se utilizan para obtener información sobre el ruteo en un red.
- *TCP/IP*.

PROTOCOLOS DE ADMINISTRACIÓN PARA TCP/IP

Cuando se trata de una red internacional como Internet resulta difícil las interconexiones y comunicación entre diferentes arquitectura de computadoras, ruteadores, etc., cuando la conversión difiere en las alarmas de direccionamiento, en los indicadores ejecutados , en el tráfico estático y otros elementos importantes.

Debido a esto en los años de 1990s, el IAB asume la guía en estándares para la base de TCP/IP para redes internacionales y patrocina dos protocolos de administración. Uno de estos protocolo es destinado para direccionar soluciones short-terms y es llamado *simple network management protocol (SNMP).* El otro protocolo es destinado a direccionar soluciones longe-range y es llamado *common management information service and protocio over* TCP/IP *(CMOT).*

SNMP

SNMP es conceptual , de contexto virtual de ejecución que su operación esta restringida (por seguridad u otros propósitos) a una definición administrativa.

Implícitamente en el modelo de arquitectura de SNMP es una colección de estaciones administradoras de redes y elementos de red. Las estaciones que administran una red ejecutan aplicaciones de administración con su monitor y sus elementos de control para la red. Los elementos de red son dispositivos como hosts,getways y terminales entre otros , que tienen agentes administradores encargados de ejecutar funciones de petición de administración de la red a través de las estaciones administradoras. Entonces SNMP es usado para comunicar información de administración entre estaciones de administración y agentes en los elementos de red.

El SNMP explícitamente, minimiza el número y la complexión de las funciones de administración realizadas por el agente de administración. Esto es mostrado en los siguientes puntos:

- El costo del desarrollo de el software de agentes de administración para soportar el protocolo es, por consiguiente, reducido.
- El grado de administración de las funciones que es soportado remotamente es, por consiguiente, incrementado, por medio de esto admite el uso de un numero muy alto de recursos de Internet para la tarea de administración.
- El grado de administración de las funciones que es soportado remotamente es, por consiguiente, incrementado, por medio de la imposición de un menor número de herramientas sofisticadas para la administración.
- Los pasos simplificados de las funciones de administración son más fáciles de entender y usar para desarrolladores de herramientas de administración.

Otra de las metas de este protocolo es que el paradigma funcional de monitoreo y control sea suficientemente extensible para acomodar adiciones, posiblemente aspectos anticipados de la operación de redes y de administración.

También otra de las metas es que la arquitectura sea, lo mas que se pueda, independiente de la arquitectura de mecanismos de hosts o getway particulares.

La arquitectura de SNMP proporciona una solución de problemas de administración en términos de:

- El ámbito de la información de administración comunicada por el protocolo.
- La representación de la información de administración comunicada por el protocolo.
- Operaciones soportadas en la administración por el protocolo.
- La forma y significado de las relaciones administrativas entre entidades de administración.
- La forma y significado de referencias de información de administración.

2. Apéndice "Servicios en Internet"

GOPHER

El nombre de "Gopher" es juego de vocablos. Este fue desarrollado originalmente en Abril de 1991 por el University of Minnesota Microcomputer, Workstation, Networks Center para ayudar a encontrar algunas respuestas en campo de la computación, puede decirse que la Universidad de Minnesota es la casa de los " Gophers".

Mucha gente a contribuido al proyecto, demasiados para mencionarlos. Las personas detrás de la mayoría de software de Gopher puede ser conectada vía e-mail en gopher@boombox.micro.umn.edu, o vía correo:

Gopher, o más adecuado "El Gopher Internet " le permite acceder recursos usando menús, es decir es un servicio de búsqueda y recuperación de información distribuida a lo largo de Internet y que se considera de dominio público. Este servicio fué designado para tener cierto control tanto de servidores como de información.

Se le llama Gopher tanto a el programa mismo que se ejecuta, como a el protocolo que permite la transferencia de información.

Características Principales:

La principal característica de Gopher es que esta basado en el modelo cliente servidor es decir existen quien solicita información y Gopher la proporciona.

En forma general podemos mencionar que Gopher tiene las siguientes características:

- Se torna en un medio de comunicación e intercambio de información de tipo académico entre Universidades y Centros de Estudio.
- Existen clientes de Gopher prácticamente para cualquier plataforma y son de dominio publico.
- Es un modelo de cliente/servidor distribuido.

- Se puede organizar la información para atender las necesidades locales de los usuarios de una institución.
- La mayor parte de los servicios de Internet son compatibles con Gopher, lo que amplía el horizonte de información y de servicios disponibles para el usuario.
- La información puede residir en servidores diferentes y completamente autónomos.
- El enlace de un servidor a otro es completamente transparente para el usuario.

JUGHEAD.

Jughead es un acrónimo de:

***J**onzy's*
***U**niversal*
***G**opher*
***H**ierarchy*
***E**xcavation*
***A**nd*
***D**isplay*

Jughead es una herramienta que realiza búsquedas sobre menús de Gopher presentando al usuario opciones que concuerdan con una palabra indicada como necesaria. Jughead restringe su búsqueda a menús de Gopher que se encuentran en un mismo dominio, vgr.

Gopher.micro.umn.edu
cecac.umn.edu
boombox.micro.umn.edu

No se podrá identificarlo muy fácil ya que rara vez aparecerá con el nombre de Jughead, pero sí se podrá accesar con otro tipo de búsqueda en el menú de Gopher, por ejemplo:

5.-Search Gopher menu at the University of Minnesota <?>

En Jughead podremos se pueden búsquedas sobre los menús Gopher de los servidores antes mencionados indicando el dominio .umn.edu. De otro modo se puede restringir únicamente a búsquedas en un host en particular.

Características Principales

La importancia de Jughead radica en que en un servidor de Gopher se actualizan constantemente los archivos y directorios, es decir, cada vez se va haciendo mas extenso el árbol que contiene la información disponible vía Gopher, así que, se hace imperioso el utilizar una herramienta que nos permita llegar en forma inmediata a la información que deseamos consultar evitando el estar navegando a través de el árbol en busca de ella.

Jughead es capaz de reconocer los operadores lógicos AND, OR y NOT en sus búsquedas y es una herramienta que permite a los usuarios un acceso directo a los tópicos que desean consultar de el Servidor en el que se encuentran conectados.

Jughead puede ejecutarse desde el shell utilizando diversas opciones para el procesamiento de búsquedas, en este caso, la liga se puede establecer a distintos servidores. Otra forma de ejecutar el Jughead es el modo de servidor que habilita un puerto para " escuchar " las peticiones de los usuarios y procesarlas, estas búsquedas sólo se pueden realizar a traves de un cliente de Gopher donde se encuentre disponible una opción de búsquedas utilizando Jughead, de este modo se habilita un puerto para brindar el servicio de procesar búsquedas de cadenas dentro de los menús de el servidor de Gopher al que se haga referencia en la opción de búsqueda de el cliente, el resultado de la búsqueda será un menú tipo Gopher cuyas opciones contienen la cadena indicada por el usuario al realizar la conexión, en caso de no haber nada disponible, el programa lo reportara como tal. Es necesario aclarar ciertos puntos sobre Jughead:

- Las búsquedas solo se realizan sobre nombres de opciones de los menús de Gopher, nunca sobre los archivos a que se refieren esas opciones.

- Las búsquedas de Jughead no son sensitivas, es decir, no se difiere entre mayúsculas y minúsculas.

  El orden de las palabras no altera el resultado de la búsqueda, por ejemplo: una búsqueda por "UNIX and mail" equivale a una búsqueda por "mail and UNIX".

- La concordancia de las palabras debe ser exacta, si se pide buscar por " Math ", no se incluye " Mathematics " en el resultado de la búsqueda.

- Existe un operador lógico default, por lo general es AND, pero este se puede modificar, si se requiere, al momento de la compilación.

- Para abortar una búsqueda solo es necesario teclear enter.

Los derechos sobre Jughead pertenecen al Centro de Computo de la Universidad de Utah, con su primera fecha de liberación de 25 de marzo de 1993. Los autores permiten la libre distribución de el código fuente de Jughead, con la condición de que se sigan respetando los derechos reservados, y que la distribución no sea con un fin monetario para ninguna institución o persona.

El código de Jughead se escribió en ANSI C, y fue diseñado para una IBM RS6000 y para una SUN spark-10, y es portable para cualquier ambiente ANSI C. Es claro que este programa será una herramienta para administradores en Gopher, el autor pide que se le envíe copia de los archivos fuente en caso de ser modificados.

VERONICA

Podemos ver que es claramente fácil moverse dentro de un servidor Gopher y moverse de un servidor Gopher a otro servidor Gopher pero llega un momento en que navegar por todos los menús de Gopher en busca de información puede ser algo tedioso y convertirse en un problema, nos podemos preguntar: ¿Como podemos accesar información en Gopher de manera rápida y sencilla?. En la Universidad de Nevada Reno, dos personas trabajaron sobre esa pregunta y lograron construir el Gopher equivalente a Archie y lo llamaron con un poco de comicidad VERONICA.

El acrónimo VERONICA tiene el significado siguiente:

VERY
EASY
RODENT
ORIENTED
NET - WIDE
INDEX TO
COMPUTARIZED
ARCHIVES

Veronica es un servicio de Internet que se construye bajo Gopher. Este mantiene un índice de títulos tomados de opciones de menús de Gopher, y permite realizar búsquedas de palabras 'clave' en ese índice de títulos.

Como ya se menciono anteriormente, y es muy importante hacer hincapié de que actualmente no existen clientes de VERONICA por si mismos; el servicio es accedido a traves de clientes de Gopher.

Características Principales

El servicio de VERONICA reúne dos funciones básicas, la primera es recopilación de datos y la segunda búsquedas de información. Estas dos funciones no necesariamente deben estar en un mismo host, ya que la mayoría de los usuarios no necesitan preocuparse por cumplir con la primera fase de las antes mencionadas.

VERONICA ofrece búsquedas sobre esas bases de datos a los clientes de Gopher, en una forma transparente, es decir, si se establece una conexión con un host remoto el usuario no necesita hacer nada adicional a la petición inicial. Esta búsqueda se origina con un requerimiento de el usuario y esta se realiza a traves de un cliente de Gopher.

El resultado de una búsqueda con VERONICA es un conjunto de opciones tipo Gopher, que se pueden consultar por medio de el mismo cliente de Gopher utilizado para la búsqueda, en forma de un menú de Gopher. Finalmente el usuario puede acceder a cualquiera de las opciones en la forma natural de un menú tipo Gopher.

ARCHIE

Con el crecimiento de computadoras que se conectan a Internet el acceso a la información de Internet se ha complicado cada vez más, esto dio lugar a pequeños problemas para encontrar información y extraer lo deseado, es por eso que surgió Archie que es un sistema en el que se pueden realizar búsquedas indezadas para localizar archivos que pueden ser accedidos en un servidor público. Cuando usted desea obtener ciertos archivos , programas ,etc. y no sabe en que parte de Internet se encuentra lo mejor que puede hacer es empezar por Archie; este le mostrara una lista de direcciones junto con directorio en el que se encuentra el archivo o programa interesado. Pero no se podrá preguntar acerca del nombre del archivo que contenga cierta palabra o cadena. Solamente se podrá buscar acerca de archivos que usted ya conoce o por el nombre exacto o aproximado del programas, archivo, utilería, etc. que desea obtener. Archie indeza como 1200 servicios y 2.5 millones de archivos.

Antes de la existencia de Archie, encontrar estos programas requería de horas y horas de navegación a través de la red. Afortunadamente Peter Deutsh en la Universidad McGill Scool of Computer Science en Canadá desarrolló el sistema Archie, que facilita la localización de estos programas menos tiempo (minutos), esto es permite localizar la dirección de la computadora donde está almacenado ese programa, archivo o utileria, que estamos buscando.

FTP anónimo trabaja dándole un servicio de extraer de la red algunos archivos, pero la existencia de esos archivos fue largamente comunicados por una red inertpersonal.

Este servicio es muy sencillo de manejar pero es importante que se sepa que algunas veces el nombre de archivos o programas a buscar tiene que ser conocido, o bien debe proporcionar la palabra esencial del nombre del programa o archivo. Esto empieza a ser obvio cuando alguna persona escoja extraños nombres que no son intuitivos para sus archivos, como es el caso del nombre de IMacPOPclient del correo de Macintosh llamado Eudora; entonces Archie pregunta a las persona que especifique mejor el nombre del archivo (esto es que no ponga un cadena muy complicada). Archie le permite hacer búsquedas en la base de datos de Archie sin usar ningún proceso interactivo en una máquina servidor remota (ejemplo: Archie.ans.net), resultando en un mejor tiempo.

Características Principales

La forma en que trabaja la explicaremos de manera sencilla. Primeramente para tener un servidor es necesario correr un programa una vez al mes con contactos a estos servidores vía ftp. Cuando se localiza el contacto con cada uno de los servidores este crea un directorio listando todos los archivos en el servidor, usando comandos estándares de ftp (ls -lR para ser exactos). Cuando se tenga una petición de que encuentre los archivos relacionados con 'eudora'(por ejemplo). Archie sólo busca todos los directorios y manda los nombres de los archivos junto con el nombre de los servidores en donde se encuentra (ósea manda la dirección en donde se encuentran).

WAIS

WAIS es el acrónimo de:

Wide
Area
Information
Servers

WAIS es principalmente un protocolo, y por tanto otro sistema designado a acceder información. Es decir es un servicio de información de amplia área , este es otro servicio que ofrece Internet, es muy útil para buscar material indezado continuo y encontrar artículos basados en lo que contienen. Esto es WAIS, le permite buscar en archivos continuos en Internet artículos que contienen cierta cadena o grupo de palabras.

Características Principales

Este servicio es realmente una herramienta para trabajar con colecciones de datos o bases de datos. En pocas palabras WAIS ayuda a realizar búsqueda de artículos con determinado tema indicado por el usuario. Pero este realmente no busca el dato en el proceso sino que busca un índice. Si se llegaran a tener problemas para construir un índice, WAIS puede seleccionar información y presentarla para que usted pueda observar el formato. Es muy común ver índices de varios tipos de texto, pero usted puede construir índices de cualquier tipo.

Existen muchas formas de indezar algún dato que se quiera accesar (como en los índices de Archive o whois) . Algunos de ellos son usados y otros no, pero usted puede buscarlos tan frecuentemente como quiera.

Al igual que Gopher, WAIS le permite encontrar y acceder recursos en la red de trabajo sin consideraciones en donde realmente se encuentran. En Gopher se puede encontrar los recursos bajo un búsqueda continua en una secuencia de menús hasta que encontró lo apropiado. WAIS hace lo mismo, pero este hace la búsqueda, el usuario le dice los que quiere encontrar y éste trata de encantar el material que necesita, un comando de WAIS es esencialmente: "Encuéntrame los ítems acerca de esto... en tal biblioteca". WAIS entonces ve todos los documentos en la biblioteca (o bibliotecas) en donde tengo esa información y nos dice que documento es el más exacto que contiene lo que nosotros queremos.

Existen más de 500 bibliotecas libres en la red de trabajo. Realmente existe una cobertura muy amplia de bibliotecas esta pueden tratar acerca de varios temas como podría ser ciencia naturales, ciencia sociales, entretenimiento, cuestiones administrativas, etc.

WAIS es un sistema distribuido de búsqueda de información cuya arquitectura se basa en el modelo cliente-servidor y en el estándar llamado Z39.50 (es un protocolo computadora-a -computadora y es un estándar de ANSI para peticiones bibliográficas de información). WAIS es un de los primeros sistemas basados en este tipo de estándar, y en éste es el más común.

Para hacer un documento capaz de aprovechar un servidor de WAIS, es necesario crear un índice para ese servidor para y así poder realizar búsquedas. Para textual información, cada palabra en el documento es usualmente indezada. Cuando se realiza una búsqueda desde el cliente de WAIS, este contacta el servidor que tenga las bibliotecas que se necesita. Si se pregunta cada servidor, en cambio, la búsqueda es establecer en las palabras índices. Entonces el servidor le manda una lista de los documentos que tal vez sean apropiados, y una cuenta (score) diciendo como es apropiada cada una de ellas. Esta lista de cuentas es normalizada, así es que el documento podría tener una lista de diferentes criterios.

World-Wide Web ("WWW")

El World-Wide Web (WWW, W3) se empieza a desarrollar en Marzo de 1989, cuando Tim Berners-Lee de El European Particle Physics Laboratory (conocido como CERN, una colección de investigaciones de European high-energy physics) propusieron el proyecto par ser usado como medio de transportación de investigaciones e ideas efectivamente encaminadas a la organización. Efectivamente comunicarse era un objetivo de muchos años en muchos de los países.

El inicial propósito del proyecto era obtener un simple sistema de hipertexto para redes y transmitir documentos y comunicarse una cantidad de miembros de la comunidad de high-energy physics. En ese momento no había intensión de adicionarle audio ni video , al igual que la capacidad de transmisión de imágenes tampoco fue considerada.

A finales de 1990, la primera pieza de el software de Web fue introducido en maquinas NeXT. Esta tenía la capacidad de ver y transmitir documentos hipertextos a otra persona en Internet, y vino con la capacidad de editar documentos hipertextos en la pantalla. Fueron dadas demostraciones para comités y seminarios además de una demostración especial para la conferencia de Hypertext '91.

Para 1992 Tim continuo con la difusión de proyecto, pocos emprendedores empezaron a desarrollar pequeñas piezas de World-Wide Web voluntariamente.

Desde entonces mucha gente en el mundo ha contribuido creando software para Web, escribiendo documentos o dándole difusión. Pero nunca fue tomado por el original grupo de proyecto, ahora, el proyecto ha alcanzado una proporción global. En los primeros cuatro meses de 1994 sólo, el World Wide Web ha sido mencionado por CNN, El Wall Street Journal, economistas, revistas famosas como : El New York Time y otras más.

Características principales

El software de Web es desarrollado tomando en cuenta el modelo distribuido de cliente-servidor. Un cliente de Web es un programa que puede mandar peticiones de documentos a cualquier servidor de Web. Un servidor de Web es un programa que recibe la petición y manda el documento pedido (o bien un mensaje de error en el caso apropiado) al cliente que lo solicito. Utiliza una arquitectura distribuida cliente servidor, este es que el programa de cliente es posible correr en una máquina completamente separada de el servidor. Ya que la tarea de almacenamiento del documento es tarea del servidor y la presentación del documento es tarea del cliente, cada uno de ésto programa o se puede concentrar en sus obligaciones y progresar independientes uno del otro.

Por lo tanto, los servidores operan generalmente sólo cuando los documentos son pedidos, ellos ponen una mínima cantidad de trabajo en las computadoras en que están corriendo.

A continuación mencionaremos algunos ejemplos de como trabaja el proceso:

- Corriendo un cliente de Web, los usuarios seleccionan un hiperliga de un documento hipertexto conectándose a otro documento.
- El cliente de Web usa la ubicación asociada con el hiperliga para conectar el servidor de Web en una dirección específica de la red y pregunta por otro documento asociado con la palabra de liga.
- El servidor responde mandando el texto y cualquier otro medio en el texto (fotografías, sonidos o video) al cliente, donde el cliente le da la presentación en pantalla al usuario.

El World Wide Web es compuesto por miles de esos procesos en cada lugar del mundo creando una membrana de información.

Algunos servidores y clientes de Web incluyen el encriptamiento y el cliente autentificara la información, dando así una mejora en comunicaciones entre usuarios y sostener la seguridad de los datos, que son privados. Es así se tiene un compromiso mayor en la seguridad de los servidores comerciales y educacionales que desean obtener información.

FTP

El servicio más utilizado para transferir archivos en Internet entre un servidor y otro es el FTP, no importando el lugar en donde se enuentren estos servidores podran establecer una comunicación e intercambiar archivos sinnecesidad de tener que verlos para obtenerlos. El significado de éste es:

File
Transfer
Protocol

Dada a su gran aceptación y la necesidad de intercambiar información, se han creado centros de información públicos, llamados FTPs anónimos en donde cualquier persona pora acceder a ese seridor y obtener cualquier información o software público que se encuentre en ese lugar.

MAJORDOMO

Una lista de correo electrónico es un mecanismo mediante el cual se pueden mantener comuniación entre usuarios que se encuentran en Internet, no existen restricciones a este tipo de comunicación excepto las determinadas por las políticas de cada servidor.

Majordomo es un programa con el cual automáticamente se administran listas de correo electrónico, los usuarios y administradores envían comandos al servidor de Majordomo sobre algún tipo de petición vía correo electrónico, y este la resuelve sin requerir la intervención del administrador del servidor o del administrador de las listas.

Majordomo fue desarrollado con el lenguaje Perl y bajo sistemas basados en Unix, su funcionamiento se basa en el formato de mensajes y múltiple envío, no maneja ningún protocolo para la trasmisión de los mensajes sólo los prepara para ser tomados por los programas servidores de correo.

Características principales

Las características de este servidor de listas de correo son:

- Soporta varios tipos de listas, incluyendo moderadas.
- La configuración puede ser realizada fácilmente a través de archivos editables.
- Esta esta escrito en Perl, el cual es un lenguaje muy flexible.
- Tiene un diseno modular.
- Soporta el servicio de FtpMail, esto es, realizar transferencias a través de correo electrónico.
- El almacenamiento de los mensajes se lleva a cabo en cada una de las máquinas a donde pertenecen los usuarios.

Glosario

A

Acceder
Se refiere a la acción de poder hacer uso de una entidad o recurso.

Actualización
En lo referente a la información, es la actividad que permite renovar la misma para mantenerla con los datos mas recientes.

Administración
Es la actividad mediante la cual se dirige y organiza una entidad.

Amenaza
Persona o evento que tiene la capacidad de causar un daño a una entidad.

Aplicación
Es un programa (o conjunto programas) que esta en funcionamiento realizando una tarea especifica.

B

Barrera de protección
Mecanismo que es utilizado para filtrar o bloquear el trafico de una red externa hacia una red local. Las barreras de protección también son conocidas como paredes de fuego, su implementación puede ser llevada en dispositivos físicos (hardware) o como leyes lógicas (software).

Base de datos
Conjunto de datos manejables y renovables con características en común y características limitadas pero suficientes para una aplicación especifica (no necesariamente en computadora).

C

Calidad
Se refiere a la satisfacción de las necesidades o de los servicios apreciada por el usuario, contemplando los aspectos de confiabilidad (aptitud de un servicio a funcionar sin fallos), conservación (aptitud de un servicio a ser reparado rápidamente) y la disponibilidad (aptitud de un servicio a encontrarse en estado de buen funcionamiento).
También se entiende como un conjunto de esfuerzos efectivos de los diferentes grupos de una organización para la integración del desarrollo, mantenimiento y superación de un producto con el fin de hacer posible el servicio a satisfacción completa del consumidor y al nivel mas económico.

Cliente (client)
Computadora o programa que requiere de un servicio especifico de otra computadora o programa.

Cliente-servidor modelo (client-server model)
Relación estrecha de componentes, tanto de software como de hardware, con la finalidad de realizar un proceso de manera distribuida, en donde se deben cumplir determinados requerimientos de esta arquitectura.

Comunicación
Proceso por el cual se transfiere información de una fuente a un destino a través de un canal.

Configuración
Actividad que consiste en establecer los parámetros que serán utilizados para el funcionamiento de un mecanismo.

Cracker
Son Usuarios de redes que tiene como finalidad acceder a los sistemas para provocar fallas en los mismos.

Criptografía
Se refiere a las técnicas utilizadas para ocultar información mediante el uso de claves secretas.

CSO (Central Services Organization)
Es un servicio que facilita el acceso y uso de bases de datos.

D

Daemon
Programas residentes que trabajan en el sistema operativo Unix, trabajan bajo el esquema de responder a las peticiones hechas por otros programas o aplicaciones.

DARPA (Defense Advanced Research Proyect Agency)
Es la agencia norteamericana que desarrollo un conjunto de estándares para interconectar computadoras, formando así la red militar ARPAnet.

Desempeño
Es el comportamiento de un sistema, el cual es resultado del estado y uso del CPU, subsistema de entrada/salida y memoria. El tiempo de ejecución de los procesos es resultado del desempeño del sistema.

Disponibilidad
Es la capacidad de atender peticiones o de permitir el acceso a entidades en el momento que se requiera.

Doug Engelbart
Inventor de dispositivos usados en la computación, entre ellos el mouse.

E

Eficaz
Característica que se da si una tarea cumple con el efecto deseado.

Eficiente
Característica relacionada al tiempo de respuesta y resultados obtenidos de una tarea.

Escalable
En el ámbito computacional es la característica que permite a un sistema crecer en poder al adicionarle nuevos dispositivos o bien reemplazándolos.

Estrategia
Es la habilidad para dirigir un asunto y conseguir un objetivo propuesto, mediante un método.

F

Finger
Servicio que mediante el cual es posible realizar consultas sobre información de usuarios en sistemas remotos.
Firewall
Referirse a barrera de protección.
FTP (File Transfer Protocol)
Es un protocolo que permite transferir archivos entre sistemas en Internet, también es utilizado como un servicio.

H

Hacker
Son usuarios de redes que acceden a los sistemas para probar su seguridad sin causar ningún daño en ellos.
Hiperligas (Hyperlinks)
Conexiones entre documentos los cuales son llamados hipertexto.
Hipermedia (Hypermedia)
Hipertexto que incluye o ligas otros medios.
Host
Sinónimo de equipo y de hardware.
Html (HyperText Markup Language)
Es el lenguaje de programación en el cual se basa el servicio World Wide Web y que consiste en generar conexiones entre sistemas.
Http (HyperText Transmission Protocol)
Lenguaje estándar que World Wide Web usa para comunicar clientes y servidores.

I

ICP (Interprocess Comunications Protocols)
Protocolos que permiten la ejecución de tareas en ambientes remotos. Cada plataforma contiene un conjunto específico de estos protocolos.
Información
Conjunto de datos presentados de manera tal que tienen un sentido y un valor para el que los recibe, permitiendo acrecentar los conocimientos sobre un ente.
Integridad
Estado de una entidad que mantiene todas sus partes sin alteración.
Interactivo
Característica de los sistemas de permitir acciones recíprocas.

Intercambio de procesos (Swap)
Técnica que el kernel del sistema operativo utiliza para limpiar la memoria física. El kernel mueve procesos enteros de la memoria al disco para reasignar otras funciones a la memoria. Este intercambio es usado para administrar al uso poca memoria.

Internet
Es la red mas grande a nivel mundial que permite el compartir recursos e información.

K

Kernel
Es la parte del sistema operativo que provee administración de memoria, de subsistemas de Entrada/salida y de todos los servicios de bajo nivel. El kernel es el núcleo del sistema operativo.

L

Log
Archivos que registran la actividad de un servicio o un sistema.

Login
Es el identificador de cada uno de los usuarios en un sistema multiusuario, éste identificador es único y puede ser conocido por todos los usuarios del sistema.

M

Memoria cache
Memoria volátil utilizada para que el manejo interno de los datos sea realice rápidamente.

Memoria principal
Memoria física contenida en microcircuitos y que forman la parte principal de almacenamiento en una computadora, se caracteriza por ser volátil.

Memoria secundaria
Esta contenida en dispositivos externos a la computadora que forman el almacenamiento secundario, se caracteriza por ser no volátil.

Método
Conjunto de operaciones ordenadas con el que se desea obtener un resultado.

Multiusuario
Característica de los sistemas que permite que mas de un usuario este activo en el sistema al mismo tiempo.

N

Navegador
Software que realiza la función de cliente, proporcionando una interface con el servicio de World Wide Web.

P

Paginación
Técnica que utiliza el kernel de Unix para usar la memoria física libre. El kernel busca paginas de memoria que no tenga acceso reciente y las copia al área de disco. Un sistema pagina cuando tiene poca memoria. El rendimiento comienza a decrecer cuando la paginación comienza.

Password
Clave secreta que utiliza cada uno de los usuarios de un sistema multiusuario para poder hacer uso del sistema.

Plataforma
Es la parte que contempla el hardware y el sistema operativo utilizado en un sistema, en donde se hace distinción de proveedores.

Política
Lineamientos que determinan el modo de actuar de una persona, o conjunto de personas, en un evento para conseguir un determinado fin.

Procedimiento
Conjunto de pasos que se utilizan para realizar una tarea especifica.

Proceso
Desarrollo de fases sucesivas usadas para llegar a un fin. En el contexto de sistemas operativos, un proceso es un conjunto de instrucciones que hacen uso de los recursos del sistema operativo.

Programa
Es un conjunto de instrucciones que permite ejecutar una serie de operaciones determinadas.

Protocolo
Conjunto de reglas establecidas que permiten la comunicación entre sistemas.

R

Raid (Redundant array of inexpensive disk)
Es una técnica tolerante a fallas que impide el cese de operaciones en caso de fallar un disco. Una de sus principales ventajas es que permite lecturas y escrituras independientes y múltiples de entrada y salida.

Recurso
Es cualquier parte del sistema que pueda ser utilizado con un propósito específico, por ejemplo los discos sólidos externos tiene como propósito el almacenar grandes cantidades de información.

Rendimiento
Es utilizado como sinónimo de desempeño. El rendimiento esta relacionado a la ganancia que se obtiene en un sistema dependiendo de su comportamiento inicial (entrada), de la acciones que se le apliquen al mismo de y su comportamiento final (salida).

S

Seguridad
Conjunto de actividades que prevén o detienen las acciones negativas no autorizadas en un sistema .

Servicio
Un servicio en Internet ese aquel que sirve como medio entre los usuarios para poder compartir y acceder recursos que se encuentran dentro de esta red.

Servicio de calidad
Se considera que un servicio es de calidad cuando reúne las características de disponibilidad, eficiencia y se verifica el estado de la información.

Servidor (Hardware y software)
Es la parte que se encarga de procesar la información requerida y enviar una respuesta a un cliente.

Sintonización
Es la acción de aplicar soluciones para mejorar el rendimiento de un sistema, esto se logra realizando un estudio de las causas del comportamiento del mismo.

Sistema
Es la plataforma y el conjunto de aplicaciones que dan soporte a un servicio.

SunSite
Servidores en Internet proporcionados por la compañía Sun Microsystems a través de los cuales dan a conocer su empresa y proporcionan apoyo a determinadas instituciones educativas.

Swap
Referirse a "Intercambio de procesos".

T

TCP/IP
Es un conjunto de protocolos que permiten la comunicación en Internet, estos protocolos trabajan en las capas de transporte y de red del modelo OSI.

Tecnología
Estudio de los medios, las técnicas y los procesos empleados en las diferentes ramas de la industria.

Telnet
Protocolo utilizado para acceder a sistemas remotos en una red de trabajo.

Tim Berners-Lee
Desarrollador de El World Wide Web.

U

URLs (Uniform Resource Locators)
Son propiamente las conexiones entre los documentos estandarizados con formato HTML.

V

Vannevar Bush
: Creador del concepto de hipertexto.

Vulnerabilidad
: Punto susceptible de ataque de un sistema, también llamado zona débil.

W

World Wide Web
: Servicio basado en hipertextos, creado con el principio de que el usuario pueda utilizar un método intuitivo para crear accesos a información.

Bibliografía

Alex berson y Jay Ranade
Client/Server Architecture
Mc Graw Hill
USA, 1992

Cricket Liv, Jerry Peek, Russ Jones, Bryan buus Y Adrian Nye
Managing Internet Information Services
O'Reilly & Asociates, Inc.
USA, 1994

Larry T. Vaughn
Client/Server Sysem Design and Implementation
McGraw-Hill
USA, 1994

Hennesy John y Patterson David
Computer Architecture, a Quantitative Approach
Prentice Hall
USA, 1995

Karanjit Sryan D. Y Chis Hare
Internet y Seguridad en Redes
McGraw-Hill,
1995

Hamdy A.Taha
Investigación de Operaciones
Alfa Omega.
México 1987