

27
2ej.



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

ANALISIS, DESARROLLO Y PUESTA EN MARCHA DE LOS SERVIDORES WEB BANXICO

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMPUTACION

P R E S E N T A :

MAURICIO J. GONZALEZ MARTINEZ
avila

DIRECTOR DE TESIS: M. EN C. CARLOS VILLASEÑOR AVILA



MEXICO, D.F.

1999.

TESIS CON FALLA DE ORIGEN

276379



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

GRACIAS . . .

A Dios, por dejarme ver su propósito y caminar junto a mí durante toda la vida.

A mi Madre, por que por ella y para ella existo.

A mi Hermana, por ser ejemplo y guía desde niños.

A mis primos Ricky y Chio, por enriquecer mi vida con la suya y ser dos hermanos mas.

A mis tíos Ricardo y Chela, gracias por el apoyo.

A mi princesa Yuri, por el apoyo y comprensión que siempre me ha dado.

A mi mejor amigo Hector, por ser como es y ayudarme a ser como soy.

A mi amigo y guía de esta aventura Carlos, por confiar y creer en mí desde el principio.

Un agradecimiento especial a Jose Sidaoui, por confiar en mí y dejarme aprender de él.

Mauricio

ÍNDICE

INTRODUCCIÓN	1
DEFINICIÓN DEL PROBLEMA	5
1.1.- ANTECEDENTES	5
1.1.1.- <i>Como ArpaNet se Convirtió en Internet</i>	5
1.2.- LA NECESIDAD DE LOS SERVICIOS DE WEB DENTRO Y FUERA DE LA INSTITUCIÓN.....	7
INTERNET : CONCEPTOS Y SERVICIOS	11
2.1 SISTEMAS ABIERTOS	11
2.1.1 <i>Modelo de Referencia OSI</i>	12
2.2 PROTOCOLOS	16
2.2.1 <i>OSI-TCP/IP</i>	17
2.2.2 <i>TCP/IP</i>	18
2.2.3.- <i>Direccionamiento en el protocolo IP</i>	20
2.2.4.- <i>TCP</i>	22
2.3 REDES.....	24
2.3.1 <i>Redes de Area Local (LAN)</i>	24
2.3.2. <i>Proveedor de Servicios de Internet</i>	28
2.3.3 <i>Puntos de Acceso a Internet (NAP's)</i>	29
2.4 INTERNET/INTRANET	29
2.4.1 <i>Servicios</i>	29
2.4.2 <i>Protocolo HTTP</i>	33
ANÁLISIS DE FACTIBILIDAD	37
3.1 DEFINICIÓN DE LOS SERVICIOS INSTITUCIONALES	37
3.1.1 <i>Groupware</i>	37
3.1.2 <i>Información Dirigida</i>	38
3.1.3 <i>Servicios y Comunicaciones</i>	39
3.2 DEFINICIÓN DE ALCANCES Y REQUERIMIENTOS	39
3.3 ESTRATEGIA.....	40
3.4 INFRAESTRUCTURA TECNOLÓGICA	42
3.4.1.- <i>Características: Plataformas Banxico</i>	42
3.4.2.- <i>Elección de Hardware para el Servidor</i>	44
3.4.3.- <i>Servidor</i>	45
3.4.4.- <i>Ciente</i>	50
3.5 COSTO ESTIMADO DE LA IMPLEMENTACIÓN	57
3.5.1 <i>Software - Hardware</i>	57
3.5.2 <i>Comunicaciones</i>	57
3.5.3 <i>Recursos Humanos</i>	57

DISEÑO Y DESARROLLO.....	59
4.1 ESTRUCTURA DE LOS SERVICIOS INSTITUCIONALES.....	59
4.2 PLAN DE IMPLEMENTACIÓN.....	60
4.3 SEGURIDAD.....	68
4.3.1 Sistema de filtros a través de un ruteador.....	69
4.3.2 Firewall.....	70
4.3.3 Sistema Operativo: Windows NT.....	71
4.3.4 Servidor de Web: Internet Information Server.....	73
4.3.5 Internet Security Scanners.....	75
IMPLANTACIÓN Y PRUEBAS.....	77
5.1 PREPARACIÓN DEL LUGAR FÍSICO.....	77
5.2 PLAN DE PRUEBAS.....	80
5.2.1. <i>Objetivos de la prueba</i>	80
5.2.2. <i>Diseño de casos de prueba</i>	81
5.2.3. <i>Técnica de grafos de causa - efecto</i>	81
5.3 PROCESOS DE RESPALDO.....	83
5.4 INSTALACIÓN.....	85
5.4.1 <i>Requerimientos de Instalación</i>	86
5.4.2. <i>Inicio y Configuración</i>	86
5.4.3 <i>Configuración del servidor de Internet</i>	88
5.4.4 <i>Configuración de los Servidores Internos</i>	88
5.4.5 <i>Prueba de Instalación</i>	88
5.4.6 <i>Configuración del Servidor</i>	90
5.4.7 <i>Configuración de propiedades</i>	91
5.4.8 <i>Configuración de seguridad</i>	93
5.5 OPERACIÓN Y ADMINISTRACIÓN.....	94
5.5.1 <i>Administración de los servicios</i>	95
5.5.2 <i>Operación</i>	99
TENDENCIAS A FUTURO.....	103
6.1 TENDENCIAS TECNOLÓGICAS.....	103
6.1.1 <i>HTML?</i>	103
6.1.2 <i>HTTP</i>	104
6.1.3 <i>Las aplicaciones</i>	105
6.1.4 <i>Servidor</i>	106
6.1.5 <i>I2</i>	107
6.2 TENDENCIAS INSTITUCIONALES.....	108
RESULTADOS Y CONCLUSIONES.....	109
BIBLIOGRAFÍA.....	111
APENDICE A.	
ANÁLISIS A DETALLE DE CADA SERVIDOR DE WEB	
ESTUDIADO/PROBADO.....	113
GLOSARIO.....	123

INTRODUCCIÓN

Internet se ha convertido en el fenómeno de los últimos años, y la tecnología está cada vez más cerca de todos los segmentos de la sociedad. A pesar de que la mayoría de la gente se precia de saber lo que es Internet, muy pocas personas tienen una respuesta certera del significado que ésta tiene.

Al respecto se ha dicho que es el negocio del siglo, que por su contenido disperso, no es funcional, que es malo para los niños debido al contenido pornográfico que se puede encontrar dentro y muchas cosas más. Sin embargo, estas líneas podrán servir como una guía de lo que Internet es y no es, y lo que representa para nuestra sociedad.

Internet es un medio interactivo que se utiliza para la transmisión de información, sea ésta datos, voz o imágenes, que acorta las distancias y modifica en gran forma la manera como las personas pueden obtener información o comunicarse. Físicamente no es más que una red conectada a otra red, éstas a su vez a otras redes, es decir, una red de redes con gran alcance cuyo funcionamiento está basado en el uso de estándares y convenciones.

Internet ha cambiado radicalmente la manera como la gente busca información y ha reducido de manera sustancial el costo de acceso a esa información, a grado tal que los servicios en línea se han tenido que ajustar a ésta nueva realidad.

Las formas de participación en Internet son muy amplias, pero podrían clasificarse en dos grandes grupos : el ingreso a la red como proveedor de algún servicio o producto, o como cliente activo de los beneficios que la red ofrece.

Internet no es el depositario de toda la información existente en el universo, sino un recurso adicional que existe y que continuamente se beneficia de nueva información generada no sólo por universidades, instituciones públicas y centros de investigación, sino también por empresas y hasta individuos que contribuyen a expandir los servicios de información para la comunidad global.

La revolución INTERNET/INTRANET esta cambiando el flujo tradicional de información y la base tecnológica que ésta representa se convertirá en un recurso crítico como el "mainframe" y SNA (System Network Architecture) solían ser. Un número de importantes y nuevas aplicaciones están surgiendo. Estas aplicaciones tendrán un impacto dinámico sobre la manera en que son conducidos los negocios y sus operaciones, serán de misión crítica y rápidamente adoptarán la misma importancia que aquellas que actualmente funciona sobre un "mainframe".

Este cambio en la forma de uso de las aplicaciones, tendrá un enorme efecto sobre los patrones tradicionales de tráfico en LAN (Local Area Network) y la confianza de las organizaciones sobre una infraestructura LAN. De esta manera el uso del "mainframe" esta convirtiéndose en solo otro servicio adicional de la red.

La banca mexicana así como la internacional, ven a Internet como un medio de entrega y de venta de sus servicios. El uso de este medio de entrega no solo reduce el costo de operación sino que permite además llegar a un número inmenso de clientes potenciales.

Los clientes del sistema financiero nacional están cada día más acostumbrados al uso de elementos tecnológicos que les facilite su trabajo diario, por lo que hacer banca a través de medios electrónicos no representa ya una novedad.

El principal motor de cambio del sector financiero ha sido indudablemente la tecnología de la información, ya que ha contribuido a derribar barreras, haciendo posible la entrada de nuevos competidores provenientes de los sectores comercial, industrial y de servicios; pero también ha permitido que este sector evolucione hacia nuevos conceptos de atención y servicio.

Para Banco de México, como organismo responsable de regular el Sistema Financiero Mexicano, tiene como necesidad imperiosa ofrecer canales de distribución electrónicos que agilicen la distribución de información a nivel nacional e incluso mundial. La carencia de ésta información en el momento adecuado puede originar sin duda, especulaciones respecto de la economía, con el riesgo de ocasionar una crisis a nivel nacional.

Es, debido a la importancia de la información y a la oportunidad que ésta representa, que el banco central decide incorporarse al mundo de Internet. La importancia en el desarrollo del proyecto sobre la creación de un servidor de web para Banco de México, esta por demás acentuada por el impacto en la economía Mexicana, teniendo como objetivo principal el implementar un sistema que permita la difusión de información que la Institución genera, de manera rápida y confiable para el Sector Financiero, comunidad Banxico y público en general. En resumen, el objetivo es: Oportunidad de Información.

Sin embargo, no basta dar la información como series impresionantes de datos, es aquí donde las herramientas de web cobran importancia para una institución como Banco de México, así como los medios visuales que podrían llegar a ser utilizados. Una página de web tiene como un objetivo principal proporcionar información de forma oportuna, y al hablar de una institución como Banco de México, esta información debe ser útil no solo a nivel nacional sino también internacional.

En los capítulos siguientes se realizará un análisis que va desde la selección del software y hardware básico necesario para la puesta en marcha de un servidor de web, pasando también por el análisis de sistemas involucrados en el mismo entorno, hasta terminar con la administración y mantenimiento del mismo.

Los capítulos uno y dos serán de análisis, definiendo los principios básicos de conocimiento, los cuales establecerán las bases para la posterior etapa de diseño; así también, quedarán establecidas las necesidades y limitaciones de la propia Institución en materia de tecnología y de servicios a nivel general.

Los capítulos tres y cuatro conformarán la sección medular del presente proyecto, definiendo los alcances y requerimientos del mismo, estableciendo toda la infraestructura tecnológica sobre la cual funcionará el web Banxico, dando lugar a la etapa final de desarrollo e implantación en el capítulo 5.

El penúltimo capítulo tratará de dar una perspectiva a futuro de la Institución en materia de tecnología, basado en el principio de Internet. Así también, de cómo se presenta ésta última, en el futuro cercano, para el sector financiero y México en general; para finalizar con las conclusiones obtenidas como resultado del presente trabajo.

DEFINICIÓN DEL PROBLEMA

El presente capítulo tiene por objetivo el establecer las bases que para Banco de México dan origen al análisis, desarrollo y puesta en marcha de los servidores de web, así como dar a conocer de forma breve los hechos que antecedieron a Internet en Banco de México y en el mundo en general.

1.1.- ANTECEDENTES

La red que dio origen a Internet comenzó hace aproximadamente 25 años, a fines de la década de los 60's. Fue creada por un equipo de científicos de "Advanced Research Projects Agency" (ARPA), parte del Departamento de Defensa del Gobierno Federal de Estados Unidos. Esta red fue denominada ARPANET y fue originalmente utilizada con propósitos militares como un vehículo de comunicación para grupos de investigación. Una red que podía ser capaz de resistir eventos inesperados y dar a E.U. un liderazgo tecnológico. La utilidad de las comunicaciones electrónicas cobró importancia y denotó su utilidad para otras áreas. Se buscaba compartir información y recursos que se tenían almacenados en las computadoras. Así, más y más gente se fue adhiriendo a los servicios de ARPANET.

1.1.1.- Como ArpaNet se Convirtió en Internet

Internet esta cambiando muy rápidamente, pero esto es producto de su historia, con todas las leyes, acuerdos y estándares, denominados estos últimos como protocolos.

Los protocolos permiten a computadoras de sistemas diferentes comunicarse una con otra, y rastrear datos a través de múltiples caminos de comunicación usando grupos de datos o paquetes con su propia dirección de destino. Estos métodos fueron tan

exitosos que los grupos civiles fuera del gobierno norteamericano adoptaron estos estándares creando sus propias redes: "User Network" (USENET), utilizada en Universidades y expandida poco después a servicios comerciales, "Computer Sciences Network" y "Because It's Time Network" (BITNET) se vieron involucradas alrededor de 1981. Siendo estas las principales redes de información.

A fines de los 80's, "National Science Foundation" (NSF), otra agencia federal, crea NFSNET utilizando la tecnología utilizada por ARPANET con canales de alta velocidad, usualmente referidos como "Internet Backbone". ARPANET desaparece en 1989.

Mientras, NSFNET establece el ritmo de avances tecnológicos, conjuntamente al avance en las computadoras y las comunicaciones de alta velocidad, 1986, 1988 y 1990 marcan los años cuando algunos de los cambios comienzan a tomar efecto. De esta manera lo que inicialmente empezó a una velocidad de 56 Kbps, en una red de seis centros de computadoras de NSF, eventualmente comenzó a operar a 45 Mbps.

El avance de NSF permite a las universidades y centros de investigación usar las supercomputadoras del propio NSF, sin embargo el fenómeno más interesante fue el incremento en el uso de conexiones utilizadas para correo electrónico y transferencia de datos. Este crecimiento de la red de redes se conoce actualmente como Internet.

Para el Banco de México la red mundial Internet empezó a ser estudiada desde los primeros años de la década de los 90's. En esos años, como se menciona, dicha red empezaba a crecer en forma exponencial gracias a la construcción de canales digitales de fibra óptica en muchos países del mundo, así como el uso extendido de las computadoras personales. Las aplicaciones de la red estaban orientadas a usuarios expertos en computación algo muy distinto en comparación a las facilidades de uso que existen en la actualidad. Hacia 1994, dos factores principales impulsaron el ingreso del Banco de México al mundo de Internet:

1. El interés por utilizar los servicios de consulta de información existentes en la red, el cual surgió primero en los campos de informática y telecomunicaciones y, posteriormente, en áreas sustancialmente financieras. Pronto surgió el interés de distribuir información generada por el Banco a través de este medio.
2. La construcción de la red del Sistema Financiero, basada en sistemas abiertos. El diseño lógico de esta red requería que se contara con un esquema de direcciones para las computadoras y subredes lo suficientemente flexible y amplio, que permitiera la interconexión de los mayores intermediarios financieros del país (principalmente bancos y casas de bolsa).

En abril de 1994, se negoció con el Network Information Center en Estados Unidos, la obtención de las direcciones IP (de las cuales hablaremos en capítulos posteriores) para Banco de México. Gracias a la justificación de que se encontraba en construcción la Red del Sistema Financiero, fue otorgado un conjunto de direcciones que permiten potencialmente la conexión de cerca 65,000 computadoras. La obtención de las direcciones IP permitió, por una parte, un diseño lógico muy limpio de la red del Sistema Financiero, por otra, este hecho representó el primer paso importante para el ingreso de Banco de México a Internet.

Un segundo paso en este sentido se dió en el mes de agosto de 1994, al establecerse el primer canal de comunicación hacia Internet, a través de la Universidad Nacional Autónoma de México (U.N.A.M.) La U.N.A.M. fue de las instituciones pioneras en México en formar parte de Internet y también en establecer uno de los primeros mecanismos para proveer servicios de conexión a dicha red. El canal utilizado por el Banco tenía una capacidad de transmisión de 64,000 bits por segundo y fue utilizado inicialmente con propósitos de experimentación dentro de la Dirección de Sistemas del Banco.

En el mes de Octubre del mismo año, se registró ante la comunidad internacional el nombre de la red del Banco de México (Nombre de Dominio): banxico.org.mx.

Durante 1995, el Banco de México realizó esfuerzos importantes para mejorar la oportunidad, frecuencia y los canales de difusión de los diversos indicadores económicos que produce, así como la información sobre sus principales acciones en materia de política monetaria. Con estos esfuerzos, el instituto central mantiene su convicción y compromiso, mediante una diseminación transparente y oportuna de la información, proviendo a los mercados financieros de los elementos necesarios para una mejor toma de decisiones en materia de economía y finanzas.

Congruente con el principio anteriormente mencionado, Banco de México dió a conocer en marzo, y en forma revisada en julio de 1995, un calendario al cual se sujeta la difusión y publicación de su información.

Es en 1995 cuando se constituye un hecho trascendente para la publicación de información a través de Internet, estando disponible a través de un servidor FTP, una parte importante de la base de datos elaborados por Banco de México, así como sus boletines de prensa y otra información relevante.

Estando todo establecido y gracias al avance tecnológico en las áreas de cómputo y telecomunicaciones se inicia el proyecto para la implantación de un Servidor de web a nivel institucional, con el objetivo de brindar al sector financiero del país, comunidad Banxico y público en general una de las herramientas más importantes para la toma de decisiones: La oportunidad de Información.

1.2.- LA NECESIDAD DE LOS SERVICIOS DE WEB DENTRO Y FUERA DE LA INSTITUCIÓN

Actualmente, muchas organizaciones se encuentran en la tarea de investigación sobre el uso comercial de aplicaciones para Internet debido básicamente al bajo costo en las transacciones y al gran alcance que estas representan. Grandes, medianas y pequeñas instituciones realizan actualmente intercambio de información, transmiten órdenes y especificaciones y dan a sus clientes un acceso potencial a sus catálogos electrónicos.

Recientemente la revista CIO condujo una investigación sobre aproximadamente 200 Servicios de Información y empresas ejecutivas para descubrir como se han ido involucrando organizaciones dentro de Internet.

Las conclusiones obtenidas muestran que el 74% de las instituciones encuestadas se encuentran ya dando un servicio sobre Internet, usando FTP, e-mail, Gopher entre otros tipos de servicios. El 6% no fueron capaces de responder sobre el tema. (Figura 1.1)

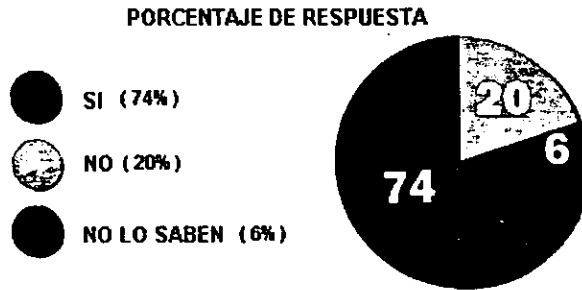


Figura 1.1 Porcentaje de uso de los servicios de Internet
Fuente : Revista CIO. <http://www.cio.com/WebMaster/webciosurv.html>

En vista de los actuales requerimientos en el mercado para capacidades orientadas a negocios específicos, no es de sorprender que la mercadotecnia, administración, líneas de negocio, y negocios de estrategia de grupo (flujo de trabajo) estén todos requiriendo las actividades de Internet. La figura 1.2 indica los departamentos que están comenzando a adoptar programas de web. En la mayoría de los casos la Tecnología de Información (TI) y comunicaciones/relaciones públicas son divisiones que conforman el centro de las aplicaciones creadas para Internet.

Internet puede ser una poderosa herramienta de promoción de bienes y servicios de las empresas.

La emergente industria relacionada con Internet ha creado una demanda especializada de recursos humanos multidisciplinarios, que no solo dominen y administren el nuevo medio interactivo y sus potencialidades de interconectividad, sino que además puedan desarrollar contenidos de acuerdo con sus características.

Desde enero de 1995, el crecimiento de Internet en México ha sido acelerado no sólo en cuanto al número de usuarios conectados a la red y servidores web mexicanos, sino en cuanto al número de empresas dedicadas a los servicios de desarrollo de contenido web. En los últimos meses, los web empresariales y comerciales también han proliferado, debido al rápido impacto de sus beneficios.

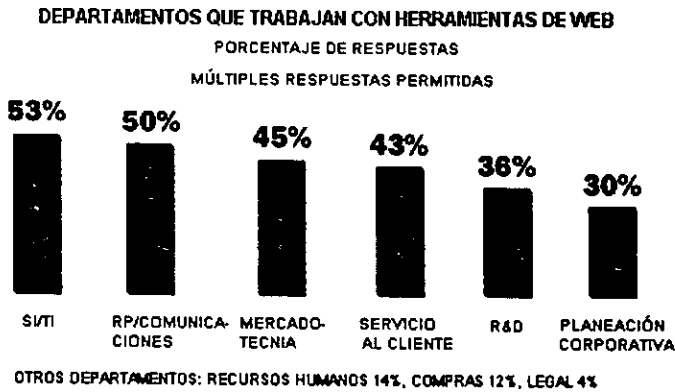


Figura 1.2 Departamentos que trabajan con herramientas de Web.
Fuente : Revista CIO. <http://www.cio.com/WebMaster/webdosurv.html>

Es importante hacer notar que el acelerado crecimiento de Internet en México es en gran parte debido a la liberación en 1991 de los servicios de valor agregado y a la política liberal en la importación de equipo de cómputo y telecomunicaciones, que ha generado hasta la fecha más de 40 proveedores de acceso a Internet en el país y el número sigue en aumento.

El hecho de que Internet sea una red que reúne a redes de todo el mundo para conformar un verdadero mundo virtual, en donde se puede encontrar información sumamente variada y especializada, permitiendo que millones de personas estén constantemente accediendo a toda esta información, situación que en sí misma constituye gran parte del éxito de cualquier persona que desee hacer negocios y que se enfoque hacia un cliente cualquiera que sea su tipo.

Los avances en la comunicación interactiva sin duda alterarán las estructuras de difusión que actualmente existen en las distintas economías mundiales que cada día se globalizan más. Hoy en día se ha establecido una nueva relación cliente-vendedor y en los próximos años los avances en las computadoras conectadas en red y el software trasformarán radicalmente la estructura de los canales de distribución.

El comercio electrónico creará una reestructuración masiva del actual sistema de distribución, los elementos clave de esta reestructuración serán las barreras para entrar, el costo de estructura y la reducción de precios, entre otras cosas.

La trascendencia de las funciones que realiza el Banco de México se deriva de la responsabilidad que el Estado mexicano le ha conferido, en cuanto a su carácter de Banco Central autónomo. Estas funciones están referidas al ámbito monetario y crediticio en que se desenvuelve la actividad económica del país.

Uno de los elementos más poderosos en la toma de decisiones es la información, y la importancia que tiene ésta en el sector financiero es por demás relevante, la ausencia de información oportuna es causa primordial de especulaciones en los mercados, pudiendo ocasionar una crisis financiera inclusive, a nivel nacional.

De esta manera, el brindar al sector financiero y público en general un medio donde se presente la información de manera oportuna es tarea fundamental para la Institución.

Brindarle al usuario la información en medios magnéticos es de gran ayuda, sin embargo, el tiempo que es requerido para que la Institución obtenga dicha información en medios magnéticos y el tiempo que tarda en llegar ésta al usuario podría ser crítico.

Tomando en consideración los postulados antes mencionados, la necesidad de un medio que brinde información casi en tiempo real es imperativo, convirtiendo la necesidad de un servidor de web es una realidad.

Información tal como el Tipo de Cambio, Saldos Promedio del PIB, Cetes, etc, podrían llegar a variar de un día a otro o incluso de un momento a otro. Poder acceder a ésta información dado el último valor de la fuente oficial resulta, para la mayoría del Sector Financiero de una importancia vital, la información dentro de la toma de decisiones juega el papel principal, la mejor decisión no puede ser tomada sin la información necesaria.

Conjuntamente, no basta darle al usuario la información en crudo, de poco serviría brindar series impresionantes de información si la persona que consulta en realidad solo necesita una dato, es por esto que aprovechando las herramientas de Internet (como son los servicios de WWW o FTP, los cuales serán analizados en capítulos posteriores), se planea dar la facilidad para la personalización de la información en la forma en que esta es presentada. Los medios visuales para la presentación de monedas y billetes juegan un papel más que importante ya que estos van encaminados a la información y conocimiento a detalle de nuestra moneda.

Una página web tendrá la misión de proporcionar la información oportunamente no solo a las instituciones nacionales, sino también a organizaciones de carácter internacional, proporcionando una mejor imagen de la perspectiva económica y financiera de nuestro país.

Las razones para ser parte de Internet son obvias. Si se desea hablar a una audiencia global, no hay mejor vehículo que Internet. Un web site – corporativo, personal o incluso interno - es la mejor entrada para los hogares y oficinas en el mundo.

INTERNET : CONCEPTOS Y SERVICIOS

Internet: Servicios y Conceptos, establece las bases de conocimiento necesarias en lo referente a un servidor de web. Abarcando los campos de cómputo y comunicaciones, estableciendo desde la estructura (protocolos), hasta llegar a la plataforma de servicios proporcionados por servidor.

2.1 Sistemas Abiertos

En el campo tecnológico un sistema cerrado significa que una vez que una empresa adquiere computadoras de un determinado fabricante, se ve obligada a continuar adquiriendo productos de ese fabricante por la imposibilidad de conectar su equipo a aparatos diseñados y fabricados por otra compañía. Este proceso está cambiando, la tendencia apunta a los sistemas abiertos, es decir, equipos que pueden ser conectados y son capaces de intercambiar información con cualquier otro, sin importar la empresa o país de procedencia. Para lograr esto, las compañías fabricantes deben ajustarse a los estándares que se fijan en organismos nacionales e internacionales, para hacer posible la comunicación de unos con otros.

En resumen, en un sistema cerrado, las computadoras de un fabricante no pueden intercambiar información con las computadoras de otro. En cambio, en un sistema abierto, un equipo que respete el conjunto de estándares internacionales, puede intercambiar información con el equipo de otro fabricante que se rija por esos mismos estándares.

El objetivo final de un sistema abierto es que un proceso (programa) siendo ejecutado en una computadora se puede comunicar con otro proceso ejecutándose en otra computadora.

Los sistemas abiertos estimulan un medio ambiente de real competitividad. El equipo que una empresa construya puede tener un diseño propio, pero los puntos de acceso para comunicarse con el mundo exterior, deben estar contruidos sobre la base de reglas acordadas internacionalmente.

No existe en la actualidad un medio ambiente abierto ideal, pero la tecnología avanza en esa dirección. Hoy en día un usuario de equipo de cómputo debe tratar muchas veces con sistemas operativos diversos, con lenguajes de programación diferentes, con protocolos particulares o con interfaces propietarias. Sin embargo, pronto será común un ambiente de cómputo y comunicación donde el usuario posea una sola vista de su sistema, es decir, manejará un solo lenguaje de comandos para correr cualquier proceso en un sistema de cómputo. Esta es la promesa de los sistemas abiertos.

2.1.1 Modelo de Referencia OSI¹

El modelo utilizado para desarrollar y administrar sistemas en red es denominado Modelo de Referencia OSI. El propósito de este modelo es permitir a aplicaciones heterogéneas, datos, hardware, etc. ser capaces de funcionar en un ambiente de red. De esta manera, la conexión lógica entre las computadoras es dividida en capas que, en conjunto, forman una Arquitectura de Red.

Cada capa del modelo OSI tiene una función específica y cuando necesita llevar a cabo una tarea, utiliza los servicios de la capa o módulo inferior. Cuando este módulo termina su función, pasa el control y los datos a la capa superior. Cada capa realiza su propio trabajo, sin consideración al desarrollado internamente en las otras capas.

La función de cada capa o nivel en una computadora es formalmente especificada como un protocolo que define el conjunto de reglas y convenciones utilizadas por esa capa para comunicarse con una capa lógicamente igual de una computadora remota. De este modo, cada nivel opera de acuerdo al protocolo definido, intercambiando mensajes tanto de control como de información.

El modelo OSI divide las funciones de una red de computadoras en las siete capas que se ilustran en la figura 2.1.

Cada capa se comunica con su igual (peer) en otro sistema remoto por medio de un protocolo. Sin embargo, la comunicación tiene lugar utilizando los servicios de la capa inferior. La comunicación entre la capa n y n-1 se conoce como una interfaz. De esta manera, cada capa presta servicios a la capa inmediatamente superior y utiliza los servicios de la capa inmediatamente inferior. La información fluye en forma lógica, horizontalmente mediante el uso de protocolos y en forma real verticalmente sobre interfaces.

Solo es en la capa 1 (Física) donde ocurre una comunicación real entre las máquinas.

¹Fuentes: Local Networks, Stallings William, ed. Macmillan
Redes de Computadoras, Robledo Cornelio, ed Foc

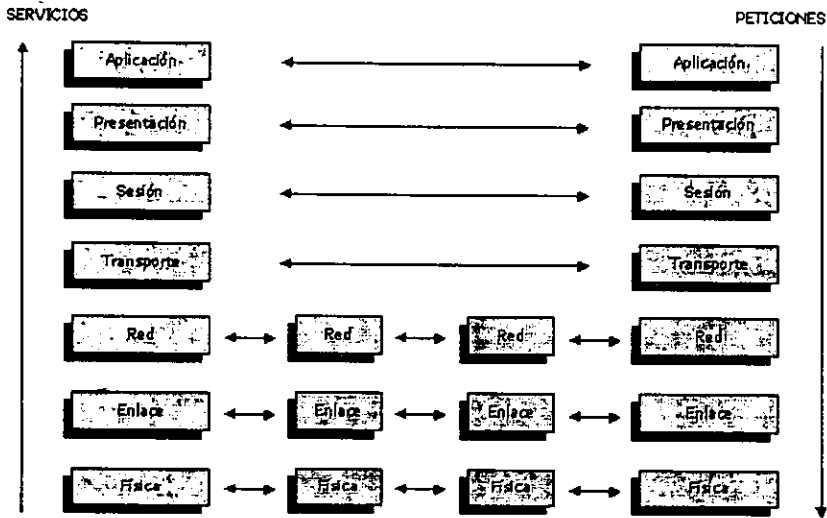


Figura 2.1 Capas del Modelo OSI

Un protocolo siempre conecta dos entidades al mismo nivel mientras que una interfaz acopla capas de una misma entidad, por ejemplo la capa n con la capa $n-1$. Un protocolo tiene los siguientes elementos claves:

- **Forma:** Comprende el formateo de los datos y los niveles eléctricos de las señales.
- **Semántica:** Incluye información de control para la coordinación y manejo de errores.
- **Base de Tiempo:** Incluye sincronización del receptor y el transmisor para la detección adecuada de bits. También comprende el acoplamiento de velocidades y la secuencia de paquetes de datos.

Funciones de las capas del modelo OSI.

Capa Física.

En esta capa se especifican los requerimientos eléctricos, mecánicos y de procedimiento para activar, mantener y desactivar el enlace físico por medio de un canal de comunicación así como la transmisión de datos a través de este medio. A continuación se incluyen ejemplos de requerimientos de cada tipo:

- **Requerimientos Eléctricos.**
 - Niveles de voltaje
 - Base de tiempo para las señales
 - Duración de cada pulso
 - Impedancia

- **Requerimientos Físicos**
 - Tipos de conectores (BNC, RJ11, RJ45, etc.)
 - Forma de conectores
 - Conexión física al medio (fibra óptica, cable coaxial, par de hilos)

- **Requerimientos de procedimiento**
 - Transmisión síncrona o asíncrona
 - Transmisión full duplex o half duplex
 - Uso de cada pin en un conector
 - Códigos de línea.

La unidad de transmisión en la capa física es el bit. Para ella, la trama que recibe de la capa de enlace de datos solo es una secuencia de bits en forma de impulsos eléctricos. La capa física opera punto a punto, es decir, sirve a la capa de enlace de datos como un vehículo para transportar una secuencia de bits de un nodo a otro.

Capa de enlace de datos

Es responsable de que el medio de transmisión se convierta en una línea sin errores de comunicación para la capa de red. Esta tarea la realiza a partir de transformar el flujo de datos entre las computadoras en tramas de datos, realizando las siguientes funciones específicas:

- Organiza los datos (paquetes) que recibe de la capa superior (red) en tramas.
- Agrega información redundante a la trama, para permitir al receptor detectar si existió o no error en la comunicación.
- Regula el tráfico usando buffers, para que un transmisor rápido no sature a un receptor lento.
- Agrega banderas para indicar comienzo y fin de mensajes.
- Provee métodos para que las estaciones conectadas puedan acceder el canal de comunicación.
- Establece un número de folio a cada mensaje que transmite
- Empaqueta los bits que recibe de la capa física en tramas
- Asegura que las dos computadoras que se comunican estén sincronizadas
- Provee esquemas de direccionamiento entre múltiples nodos

En la capa de enlace de datos la unidad de transmisión es la trama. Esta capa opera punto a punto y presta servicios sin conexión a la capa de red.

Capa de red

Establece una trayectoria física y lógica entre dos nodos que se comunican, enruta los mensajes a través de nodos intermedios a su destino y controla el flujo de mensajes entre nodos. Implementa las siguientes funciones:

- Establece rutas de un nodo fuente a un nodo destino para transmitir los paquetes.
- Direcciona los nodos intermedios en la ruta que siguen los paquetes.
- Ensambla los paquetes que recibe de la capa de transporte en paquetes y los desensambla en el otro extremo.
- Realiza control de flujo y control de error.
- Reconoce prioridad en los mensajes y los envía con la prioridad establecida
- Ofrece servicios de interconectividad para enlazar redes por medio de ruteadores

En la capa de red la unidad de transmisión es el paquete.

Capa de transporte

Esta capa actúa como una interfaz entre las tres capas inferiores orientadas a comunicaciones (capas de interconectividad) y las tres capas superiores orientadas a cómputo (capas de interoperatividad). La capa de transporte ofrece a la capa de sesión un servicio de transferencia de mensajes ocultando los detalles de operación de las capas de comunicaciones. Con este fin, esta capa provee a la de sesión los servicios siguientes:

- Asegura la integridad de los mensajes.
- Control de flujo y control de error.
- Poleo o sondeo de los mensajes.
- Mapeo de direcciones a nombres.
- Multiplexa conexiones de transporte a conexiones de red.

Capa de Sesión

Esta capa ofrece a la de transporte el servicio de establecimiento, mantenimiento y terminación de una sesión entre un proceso funcionando en una computadora A y un proceso funcionando en una computadora B. Las funciones que realiza son las siguientes:

- Controla el diálogo entre procesos: quién transmite, cuándo, durante que tiempo, que tipo de enlace, etc.
- Sincronización. Restablece la comunicación si ocurre una ruptura del enlace sin perder los datos.
- Transmite la información del usuario (capa de presentación) en una forma ordenada.

Capa de presentación

Esta capa proporciona a la de aplicación mecanismos para traducir los formatos de datos del transmisor de modo que sean adecuados para el receptor. Es decir, la capa de presentación maneja la información para que sea desplegada físicamente en la forma correcta para el receptor. De este modo asegura al proceso de aplicación la solución de cualquier problema de sintaxis. La capa de presentación realiza las siguientes funciones:

- Compresión de datos
- Encriptación de datos.
- Transformación sintáctica del conjunto de caracteres, formato del desplegado de datos, organización de archivos, etc.

Capa de aplicación

Esta capa provee los siguientes servicios directamente al usuario:

- Tránsito, administración y acceso de archivos
- Correo electrónico
- Emulación de terminales de computadoras
- Servicios de directorio.
- Comunicación entre programas.

2.2 PROTOCOLOS²

¿Qué es en realidad el conjunto de protocolos que permite a todas las redes que conforman Internet comunicarse entre sí?. El grupo de protocolos que hace esto posible es denominado TCP/IP, siglas de Transmission Control Protocol / Internet Protocol, los cuales son actualmente los nombres de los dos protocolos mayormente utilizados dentro del grupo. Cada computadora sobre Internet soporta TCP/IP. Si una computadora A en Sydney permite comunicación utilizando los protocolos de TCP/IP, y una computadora B en Buenos Aires también lo permite, y ambas están direccionadas a redes interconectadas capaces de soportar TCP/IP, entonces, dichos equipos de cómputo podrían ser capaces de enviar y recibir información uno del otro.

No debe confundirse el servicio con el protocolo. El servicio es un conjunto de operaciones que una capa n ofrece a la capa inmediatamente superior ($n + 1$), mientras que el protocolo es el conjunto de reglas que rigen la forma (formato de los datos y niveles de señales), la semántica (significado de mensajes y control de errores) y la base de tiempo (velocidad y secuencia) de los mensajes, que son intercambiados por dos entidades iguales en las capas correspondientes de las computadoras.

La entidad de una capa usa protocolos para implementar la definición de sus servicios y es libre de cambiar sus protocolos, siempre que no cambie el servicio visible a sus usuarios. El servicio define que operaciones puede desarrollar una capa en nombre de sus usuarios, pero no establece nada acerca de la implementación de estas operaciones.

² Fuentes: Local Networks, Stallings William, ed. Macmillan
Redes de Computadoras, Robledo Cornelio, ed Foc

2.2.1 OSI-TCP/IP

TCP/IP es una familia de protocolos cuya arquitectura comprende principalmente las capas de red, de transporte, de presentación y de aplicación del modelo OSI. Las dos últimas se agrupan en una sola capa llamada de aplicación. TCP/IP no incluye una capa de sesión debido a que ésta es propia de los sistemas de tiempo compartido que no se emplean en un medio ambiente como el de TCP/IP caracterizado por un esquema cliente-servidor.

El modelo OSI describe un protocolo de comunicación idealizado y a pesar que TCP/IP no corresponde directamente a este modelo se puede hacer una referencia de semejanza entre ambos.

Un protocolo de comunicación de datos se compone de una serie de reglas que describen como el software y el hardware deben interactuar en una red. Para que una red funcione correctamente, la información debe ir de un punto a otro de una forma estandarizada, es para esto, por lo cual se definieron protocolos de comunicación.

La mayoría de los protocolos de comunicación están estructurados en capas. Cada capa esta diseñada para alguna actividad en específico y existen tanto en el transmisor como en el receptor.

La figura 2.2 ilustra la correspondencia entre las capas del modelo OSI y las capas de TCP/IP.

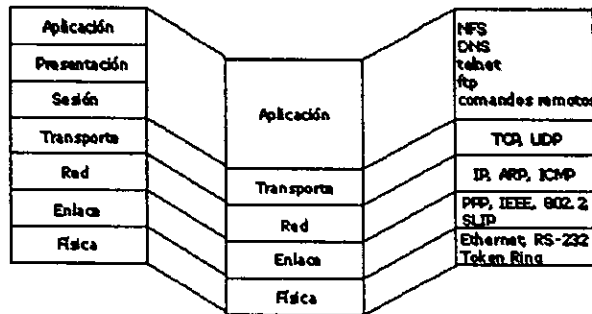


Figura 2.2 Correspondencia entre las capas ISO-OSI y TCP/IP

2.2.2 TCP/IP

La familia de TCP/IP comprende los siguientes protocolos:

- **FTP** File Transfer Protocol.
Permite la transferencia de archivos de un programa de aplicación funcionando en una computadora a otra funcionando en otra computadora remota.
- **SMTP** Simple Mail Transfer Protocol
Permite la transferencia de correo electrónico entre dos sistemas TCP/IP.
- **TELNET** Permite a un sistema TCP/IP emular una terminal de otro sistema.
- **SNMP** Simple Network Management Protocol.
Este protocolo se utiliza para administrar, monitorear y controlar una red de comunicaciones.
- **TCP** Transport control Protocol
Protocolo de transporte orientado a conexión.
- **UDP** User Datagram Protocol
Protocolo de transporte no orientado a conexión.
- **IP** Internet Protocol
Protocolo de ruteo de paquetes de la capa de red. Conjuntamente con TCP/IP da nombre a esta familia de protocolos.
- **ICMP** Internet Control Message Protocol
Protocolo utilizado para diagnóstico y prueba de redes TCP/IP.
- **ARP** Adress Resolution Protocol
Protocolo utilizado para traducir direcciones IP en direcciones MAC de una red LAN
- **RARP** Reverse Adress Resolution Protocol
Protocolo utilizado para traducir direcciones físicas en la LAN a direcciones IP.
- **NFS** Network File System
Sistema de manejo de archivos

Protocolos TCP/IP

A continuación se describen cada una de las capas de TCP/IP

Aplicación

Esta capa se refiere al programa ejecutado en el equipo del usuario el cual esta por utilizar las funciones de comunicación en TCP/IP. A pesar de que la aplicación no es parte de TCP/IP, ésta invocará alguno de los servicios de las siguientes capas. Es decir, se definen las aplicaciones y servicios de red de alto nivel, tales como telnet, ftp, tftp, comandos remotos de UNIX, servicios de archivos como NFS.

Transporte

Los datos serán ensamblados dentro de paquetes denominados unidades de transferencia de mensaje (MTU- Message Transfer Units). La capa de transporte verificará y contará la transmisión de cada MTU a través de la red. Así también, esta capa es responsable de proveer una conexión virtual entre las dos computadoras involucradas en la transferencia.

Red

Se encarga de recibir y entregar paquetes a través de la red. La capa de transporte envía los datos a la capa red para el desplazamiento y ruteo de los mismos entre los nodos de la propia red o las computadoras que intervienen. Como ejemplos de protocolos de esta podríamos mencionar: ACP, ICMP e IP, este último, cuya implicación es directa para el desarrollo de un servidor de web, es explicado en el punto 2.2.3

Interfase de red

Especifica el tipo de paquete que se utilizará para la transmisión.

Física

La capa física es la interfaz actual del circuito de comunicaciones, LAN o módem que desarrolla la transmisión. Esta capa esta compuesta de funciones como Ethernet 802.3, Interfaces de módem, paquetes de red, etc.

No es necesario entender todas las características de TCP/IP para crear servicios de información sobre Internet, pero es necesario tener los fundamentos de los dos protocolos más importantes dentro del conjunto. A continuación se describe los dos protocolos de mayor uso dentro del conjunto: IP, Internet Protocol y TCP: Transmission Control Protocol.

Antes de realizar una descripción mas a detalle de los protocolos TCP e IP se documentan las funciones que realizan

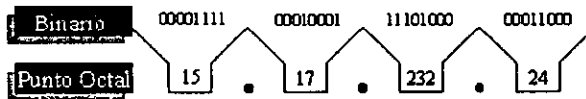
a) El software del protocolo IP corre en las computadoras que se comunican y en los ruteadores que las enlazan, mientras que el software del protocolo TCP solo corre en las computadoras donde están las aplicaciones.

b) IP es un protocolo de la capa de red no orientado a conexión que enruta paquetes (datagramas) a través de Internet pero no garantiza que lleguen a su destino sin error, sin pérdida y sin duplicación. TCP es un protocolo full duplex, orientado a conexión que envía mensajes (segmentos), de extremos a extremo entre las computadoras que se comunican y asegura que los segmentos serán entregados al programa de aplicación destino en secuencia, sin pérdida, sin error y sin duplicación.

2.2.3.- Direccionamiento en el protocolo IP.³

El protocolo IP utiliza direcciones para identificar a las computadoras que están conectados a una red. Así mismo, un ruteador en una red toma como base la dirección destino en un datagrama para decidir a que nodo debe transferirlo en la red. Más específicamente una dirección IP se asigna a la tarjeta NIC⁴ la cual, conecta la computadora a la red.

Las direcciones sobre los paquetes IP son una secuencia de números. La dirección es un número de 32 bits, el cual va desde cero hasta cerca de 4.3 billones. No es necesario recordar una secuencia enorme de valores binarios, dichas direcciones son comúnmente representadas bajo la notación punto octal, la cual agrupa la dirección de 32 bits en cuatro conjuntos de 8 bits cada uno (8 bits forman un octeto). Entonces cada uno de los conjuntos de 8 bits es convertido en números decimales, siendo los cuatro números resultantes concatenados y separados por puntos. La figura 2.3 ilustra lo anterior.



Fuente : Managing Internet Information Services
Figura 2.3 Notación Punto Octal

El formato de una dirección IP esta constituido por las dos partes siguientes:

- Dirección de red
- Dirección local o host

La parte de la red identifica a la red física a la cual esta conectado la computadora y es única a nivel internacional, siendo asignada por el International Network Information Center (InterNIC). La parte de la dirección local identifica a una computadora de manera individual en la red y es asignada localmente por el administrador de la misma.

Las direcciones IP están asignadas a las computadoras acordes a la red en Internet a la cual pertenecen. Por ejemplo, Banco de México trabaja sobre una red privada que esta conectada a Internet. Las computadoras sobre esta red todas tienen direcciones IP que inician con el mismo octeto. Banco de México divide su red en subredes. Cada subred es identificada por los primeros tres octetos de la dirección IP.

³ Fuente: Managing Internet Information Services, Liu - Peek, ed. O'reilly

⁴ Network Interface Card

Existen un par de razones por las cuales las direcciones IP están asignadas de esta manera. Primera, el usar una jerarquía de asignación (Red-Subred-Computador) permite a las personas sobre Internet asignar direcciones relativamente autónomas.

Cuando se creó la red de Banco de México (y hasta la fecha) las direcciones IP iniciaron con los primeros dos octetos fijos, garantizando la posibilidad de asignar a la red Banxico cualquier dirección IP con variantes en los dos últimos octetos (Clase B). Por otro lado el uso de direcciones jerárquicas simplifica el ruteo de los paquetes IP entre las computadoras emisoras y receptoras. Desde que Internet es un lugar enorme con cientos o miles de ligas entre las redes, esto ha dejado de ser una tarea trivial. Debido a que las direcciones son jerárquicas, los ruteadores en Internet solo necesitan mantener una lista de las redes sobre la propia Internet y la manera de accederlas. Sería imposible mantener una lista con cada computadora individual, ya que ésta podría alcanzar un tamaño de 4.3 billones de registros. Una vez que el paquete IP es elaborado en una red, los ruteadores de esa red tendrán la misión de enviarlo a subred adecuada para finalmente llegar a la computadora indicada.

Existen cinco clases de direcciones IP A,B,C,D y E. ⁵

Clase A

Las direcciones clase A comienzan con un número entre 1 y 127, usan 7 bits para identificar la red y 24 bits para identificar la computadora dentro de la red (host), por lo que esta clase puede emplearse para direccionar hasta 127 redes ($2^7 - 1$, ya que la dirección 00000000 no se emplea) y 16, 777, 216 computadoras (2^{24}) en cada red.

Clase B

Estas direcciones comienzan con un número comprendido entre 128 y 191. Específicamente usan 14 bits para identificar redes y 16 bits para identificar computadoras dentro de cada red, por lo que pueden tener 16,384 redes con 65,536 computadoras en cada una. Esta clase de direcciones se encuentran prácticamente agotadas en Internet.

Clase C

Esta clase de direcciones comienzan con un número comprendido entre 192 y 223 y dejan 21 bits para identificar la red y 8 bits para identificar las computadoras dentro de la red, por lo cual se pueden direccionar 2,097,152 redes (2^{21}) y 256 computadoras en cada red. Aún hay disponibilidad de este tipo de direcciones en Internet.

Clase D

Las direcciones de clase D se emplean para multicast, es decir, para que un conjunto de computadoras puedan compartir una misma dirección, lo cual permite que una copia de un mensaje con una dirección de multicast, sea entregado a cada uno de los equipos que comparten esa dirección.

Clase E

Las direcciones clase E son reservadas para uso futuro.

Es necesario mencionar que una dirección que contiene solo bits 1, representa una dirección de broadcast, es decir, una dirección que todas las computadoras de la red

⁵ Fuente: Redes de Computadoras, Robledo Cornelio, ed. FOC

conocen como suya. Así mismo, una dirección en la cual todos los bits son 0, se utiliza para referirse a la red en sí misma.

Consideremos a continuación cada una de las clases:

Nombre de la clase	Bits iniciales en la dirección	Comienzo de la dirección
A	0	1 - 127
B	10	128 - 191
C	110	192 - 223
D	1110	224 - 239
E	11110	240 - 255

Teniendo el formato mostrado en la figura 2.4

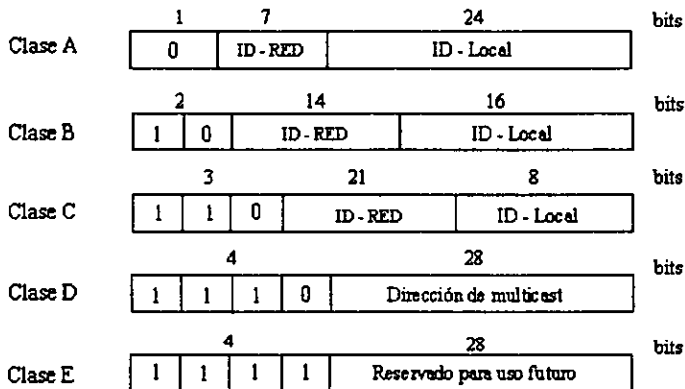


Figura 2.4 Formato de direcciones IP

2.2.4.- TCP

Después de IP el protocolo más usado es TCP/ IP opera en la capa de red y su función principal es la de rutear paquetes (datagramas) de un nodo a otro, en cambio, TCP opera en la capa de transporte y su función principal es de establecer una conexión confiable para la transferencia de datos de una aplicación corriendo en un computador a otra aplicación corriendo en un computador remoto. Según analizamos los atributos principales de IP son:

- Protocolo sin conexión
- Direccionamiento vía direcciones IP de 32 bits
- Tamaño máximo del paquete: 65,535 bytes y tamaño por omisión de 576 bytes
- Fragmenta los paquetes si es necesario
- Hace checksum sólo del encabezado del paquete IP, no de los datos.

- El tiempo de vida del paquete en la red es finito
- No garantiza la entrega de paquetes en secuencia, sin error y sin duplicación
- Opera en la capa de red
- Su diseño es simple para que solo se enfoque al ruteo de paquetes de nodo a nodo (de host a ruteador, de ruteador a ruteador o de ruteador a host).

TCP tiene la tarea de hacer confiables los servicios proporcionados por IP, en base a los atributos siguientes:

- Es un protocolo orientado a conexión, ya que antes de que dos aplicaciones corriendo en computadoras remotas comiencen a intercambiar datos, es necesario que establezcan una conexión entre ellos.
- Asegura la entrega de los datos a la aplicación destino en la secuencia correcta y sin error. Para ello el receptor envía un mensaje de reconocimiento (ACK) por cada secuencia de bytes recibida. Para implementar este mecanismo, cuando el extremo transmisor envía un mensaje, el módulo TCP arranca un temporizador. Si el temporizador expira antes que el transmisor reciba un reconocimiento, TCP retransmite automáticamente los datos no reconocidos.
- Sin embargo, TCP no envía un mensaje y espera hasta que se recibe un reconocimiento antes de enviar el siguiente mensaje, sino que utiliza la técnica llamada de "ventanas deslizantes" (sliding windows), que permite enviar varios mensajes sin esperar por un reconocimiento.
- Implementa control de flujo, es decir, si en buffer de datos en el extremo receptor de la conexión comienza a saturarse, TCP le indica al extremo transmisor que reduzca la velocidad de transmisión.
- Implementa checksum no solo en el encabezado TCP sino en todo el segmento (encabezado y datos), a modo de permitir al receptor detectar si ha ocurrido un error en la comunicación.
- TCP entrega datos como una secuencia de bytes al protocolo IP, el cual los encapsula en datagramas IP.
- TCP provee un servicio full duplex, mediante el cual maneja simultáneamente dos secuencias de datos, lo que significa que actúa al mismo tiempo como un transmisor y como un receptor.
- Una aplicación pasa datos al módulo TCP el cual los acumula en un buffer transmisor. Periódicamente, TCP forma un conjunto de bytes agregando un encabezado para formar así un segmento, el cual es la unidad de transmisión de TCP.

TCP provee otra importante característica: números de puertos. Los números de puertos resultan como otra capa de direcciones debajo de la dirección IP. La dirección IP únicamente identifica computadoras. Los números de puertos son utilizados para identificar servicios dentro de una computadora.

El número de puerto es un número de 16 bits (de 0 a 65 000 aproximadamente). Existen puertos reservados para servicios específicos, el puerto 25 por ejemplo, esta reservado para el uso del correo, SMTP en la mayoría de las computadoras. Similarmente, el puerto 23 es reservado para servidores que entienden el protocolo de TELNET, esto hace fácil a otros clientes de correo y TELNET encontrar el destino adecuado. Los números de puerto inferiores a 1024 son llamados "puertos privilegiados" sobre UNIX.

2.3 REDES

El concepto de redes aplicado al uso de Internet lo podríamos esquematizar en tres secciones (fig. 2.5) . La primera de ellas definida por la red local (Local Area Network -LAN) o el usuario final del servicio, la segunda sección esta conformada por el proveedor de servicio de Internet (Internet Service Provider -ISP) y la última de ellas por el punto de acceso a Internet (Network Access Point -NAP). La velocidad de acceso a la información va a depender básicamente del ancho de banda que se tenga (BW).

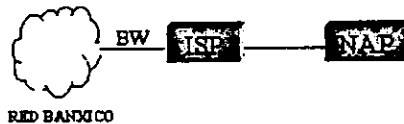


Figura 2.5 Esquema de conexión a Internet

La topología utilizada por el Banco de México es una combinación de LAN y WAN, esta última destinada a los servicios en las sucursales ubicadas en el interior de la República.

2.3.1 Redes de Area Local (LAN).⁶

Una red de área local es una red de computadoras confinada a un espacio, edificio o grupo de edificios adyacentes. Una red similar pero a mayor escala es referida como WAN (Wide Area Network) o en algunos casos mas específicamente MAN (Metropolitan Area Network).

Un equipo destinado a una LAN realiza una transmisión en promedio más rápida que el equipo destinado a una WAN, el equipo toma ventaja de la transmisión a corta distancia para implementar una transmisión rápida relativamente a bajo costo.

El uso típico de una LAN es la comunicación entre computadoras personales en una oficina así como el compartir los recursos dentro de la misma. Así también para el envío y recepción de correo o lograr la conexión de las computadoras a una WAN o a INTERNET.

⁶ Fuente: Local Networks, Sallings William, ed. Macmillan

Las operaciones necesarias para el trabajo de una red local, corresponden a las capas 1 y 2 del modelo OSI.

Las funciones para el establecimiento, mantenimiento y desactivación de un enlace físico para transferir la secuencia de bits de una estación a otra se llevan a cabo en la capa física, mientras que en la capa de enlace de datos, se implementan las funciones de:

- Encapsulado.
Organización de los paquetes en tramas
- Direccionamiento:
Indicación del origen y destino de las tramas
- Secuencia:
Etiqueta de la trama con un número de folio
- Control de flujo:
Mecanismo para evitar que el transmisor sature al receptor con tramas de información.
- Control de error:
Implementación de protocolos para la detección de errores que pudieran ocurrir en la transmisión.
- Codificación / Decodificación de Señales.
Representación de la secuencia de bits con señales eléctricas que son transmitidas en el canal de comunicación.
- Sincronización
Generación y remoción de secuencias de bits para sincronización entre las dos estaciones que intercambian información.

En una red local, se tienen varias computadoras conectadas, pero en ellas no se implementan todas las funciones de la capa de red, aún cuando se debe asegurar que un mensaje de una computadora fuente sea entregado a otro destinatario. La razón de lo anterior es la siguiente:

- a) En una red local no hay enrutamiento intermedio para llevar el mensaje de una red a otra.
- b) Algunas funciones de la capa de red son implementadas en la capa de enlace de datos.

La capa de enlace de datos en una red local tiene la particularidad de que debe soportar el acceso a un sistema que tiene múltiples computadoras fuente y destino, por lo que es necesario implementar algunas funciones de la capa de red. Para realizar lo anterior, la capa de enlace de datos se divide en las siguientes subcapas:

- Control de enlace lógico (LLC: Logical Link Control)
- Control de Acceso al Medio (MAC: Medium Access Control)

La subcapa de LLC desarrolla las funciones de:

- Control de flujo extremo a extremo para regular la transferencia de mensajes entre transmisor y receptor.
- Control de error para garantizar la entrega de un mensaje de la fuente al destino sin error.

La subcapa LLC agrega un encabezado a los datos que recibe del usuario de la capa superior. Este encabezado administra el enlace entre la entidad local LLC y la entidad remota LLC. La combinación de los datos de usuario y el encabezado LLC es denominado Unidad de Datos del Protocolo o PDU (Protocol Data Unit). El PDU preparado por la subcapa LLC de la estación fuente se transmite a su igual en la estación destino usando los servicios de la subcapa MAC. Esta subcapa agrega un encabezado y una cola, denominando la unidad resultante como trama. (Figura 2.6)

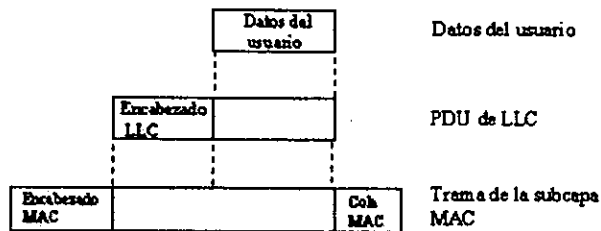


Figura 2.6 Trama y PDU en las subcapas MAC y LLC respectivamente

En la subcapa de MAC se implementan las funciones siguientes:

- Encapsulado de los datos en las tramas de transmisión y desencapsulado en las de recepción.
- Implementación del algoritmo CRC para la detección de errores en la transmisión.

Para la subcapa LLC de una red local existen las siguientes opciones de la subcapa MAC:

- CSMA/CD (Ethernet)
- Token Bus
- Token Ring

La subcapa MAC en redes locales se implementa en la tarjeta NIC que se inserta en la PC para que esta pueda ser conectada a una LAN. El tipo de tarjeta NIC determina lo siguiente:

- El método usado para enviar y recibir datos
- La velocidad de transmisión de datos
- El tamaño y forma de la trama de los datos.
- El método de acceso al medio de transmisión
- La topología de red.

Las tarjetas NIC se construyen en base a estándares desarrollados por organizaciones internacionales como el IEEE. Los estándares especifican aspectos como:

- Estructura de la trama
- Método de acceso al medio
- Fuerza de la señal
- Tipo de cable
- Distancia permitida del cable.

Banco de México posee una red LAN de tipo Ethernet, dicha red utiliza el método de acceso CSMA/CD (Carrier Sense Multiple Access/Colission Detection) en el cual, las computadoras compiten por el uso del medio de comunicación. En este método, cuando una PC desea transmitir un paquete de datos, sensa el canal de comunicación para verificar si existe una señal portadora. Si la hay, significa que el canal esta ocupado y la PC espera antes de sensarlo nuevamente. Si la PC no detecta portadora alguna, significa que el canal esta libre y procede a enviar su información.

Por la forma de sensar la portadora el método se llama Carrier Sense (sensor de portadora) y como el medio puede ser accedido por múltiples PC, se le agrega la terminación Multiple Access (acceso múltiple). Dando el nombre de CSMA.

Con esta técnica existe el problema de que cuando dos computadoras desean transmitir un paquete, sensan el canal y no detectan portadora, ambas trasmiten su paquete al mismo tiempo dando origen a una colisión, como se ilustra en la figura 2.7.

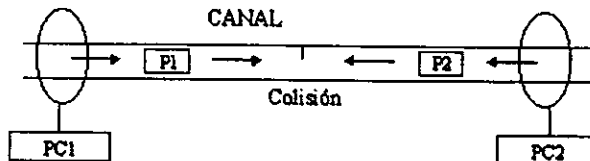


Figura 2.7 Colisión de paquetes en una red local Ethernet

Para solucionar este problema Ethernet utiliza la técnica de Detección de colisión (Collision Detection), mediante la cual una computadora trasmite su paquete tan pronto como ve el canal libre, posterior monitorea la transmisión. Si detecta colisión, trasmite una señal de alarma alertando al resto de las computadoras para que estas eviten la transmisión de paquetes.

Después de un tiempo aleatorio, la computadora intenta de nuevo la transmisión, detectando primero si existe portadora y procediendo a trasmir una trama si no la detecta.

Con el método CSMA/CD el acceso a la red es aleatorio, lo cual significa que una computadora tiene la probabilidad de acceder la red en cualquier momento, sin embargo, dicho acceso no esta garantizado.

2.3.2. Proveedor de Servicios de Internet.⁷

El ISP (por sus siglas en inglés -Internet Service Provider) es elemento sustancial dentro del esquema de conexión a Internet ya que es la conexión física al NAP⁸, punto final para la información en Internet. Para la selección del ISP para Banco de México fueron tomados aspectos tales como:

a) *Topología de red*

La topología de red es uno de los criterios mas importantes a considerar cuando se va a seleccionar un proveedor. A través de la topología se puede conocer que tan vulnerable es la red, que capacidad de servicio es disponible cuando la red presenta su mayor carga y que tan bien el proveedor entiende Ingeniería de Software.

b) *Velocidad de conexiones en red*

La velocidad en las conexiones en el "backbone" (medio de comunicación principal en una red) operacional.

c) *Conexiones externas en la red*

Se debe determinar si existe una sola conexión por parte del ISP al resto del mundo, esto es un punto único de falla potencial. Por lo cual es recomendable un tipo de conexión múltiple.

d) *Backbone de alta velocidad.*

Es necesario verificar sin el Backbone es de alta velocidad y donde se encuentra localizado.

e) *La tecnología*

La tecnología utilizada para la operación de la red es de importancia crítica. Actualmente existen ruteadores, switch y modems de calidad, siendo necesario que el ISP tenga disponible esta clase de tecnología.

f) *Seguridad*

Es necesario determinar si se cuentan con un sistema de respaldos entre sus instalaciones y el backbone de Internet, así como sistemas de monitoreo que indiquen la calidad de servicio y el porcentaje de utilización del ancho de banda.

g) *Soporte Técnico*

Uno de los aspectos mas importantes a considerar es el soporte técnico, ya que de él dependerá el buen funcionamiento de la conexión inicial y que ésta se mantenga funcionando en el futuro, se deben considerar detalles como horario de servicio y el número de personas asignadas para ello.

h) *Costos*

Se debe conocer al menos cual es el costo del servicio por un canal de hasta 256 Kbps (en múltiplos de 64 Kbps) para servicios digitales, así como los anchos de banda y costos respectivos para enlaces vía conmutada.

⁷ Basado en el estudio realizado por Banco de México en su área de cómputo y telecomunicaciones, con apoyo en http://www.cnam.fr/Network/Internet-access/how_to_select.html

⁸ Network Access Point

l) Centro de Operaciones.

El centro de operaciones del ISP debe ser seguro, con un servicio 24x7 y con la capacidad de resolver una posible contingencia.

j) Organización

La experiencia de la organización en el negocio y la estabilidad financiera son aspectos importantes, ya que es necesario estar seguro si la compañía estará en función el año siguiente.

k) Completo rango de servicios.

Que tan fácil será responder para el ISP si' es necesario aumentar el nivel de servicios proporcionado por el Banco.

l) Base de clientes.

Cuantos y quienes son los clientes actuales del ISP.

Destacando puntos técnicos tales como:

- El Ancho de Banda disponible y el medio de transmisión utilizado entre sus instalaciones y el backbone de Internet al que se conectan.
- El número exacto de ruteadores para lograr la conexión al usuario final.
- Diagramas de red e interconexiones.

2.3.3 Puntos de Acceso a Internet (NAP's)

Los puntos de acceso a Internet (NAP's) son lugares de intercambio de tráfico en Internet. Los proveedores del servicio en Internet (Internet Service Provider -ISP) conectan sus redes al NAP para propósitos de intercambio con otros ISP's. Esto permite a los ISP's regionales conectarse al backbone de los grandes proveedores, ruteo, resolución de direcciones y asistencia. Los proveedores del backbone nacional conectados al NAP obtienen los beneficios de la base de clientes del ISP regional.

2.4 INTERNET/INTRANET

Internet no solo provee una infraestructura de comunicaciones, sino también un sistema de información la cual es provista a través del uso de diferentes servicios. Los tradicionales servidores de información sobre Internet -FTP, Gopher- dejan de ser ya funcionales. Los servidores de web introducen gráficas e hipertexto y una forma de navegar accionando solo un "click" del ratón.

2.4.1 Servicios⁹

Existen tres clases definidas por su uso de servidores de web (descritos posteriormente en este mismo capítulo), su implantación dependerá del tipo de información a manejar:

⁹ Fuente: Internet Information Services, Liu- Peek, ed. O'Reilly

- Intranet.
- Internet
- Extranet

Los servicios de información de Internet son la forma en que el usuario accede a la información. Cuando se instala un servidor de web, cualquiera que sea su tipo, se debe decidir que servicios o combinación de éstos serán utilizados durante el desarrollo.

A continuación se describen los servicios de información mas comúnmente utilizados, cabe mencionar que se planea la implantación de todos estos en el servidor de web de Banco de México, con excepción del servicio de gopher.

Servicios de Correo

El correo electrónico es la forma predominante de comunicación en Internet, las listas de correo son una buena manera de distribuir información de alta prioridad.

Existen dos clases básicas de servicios de correo: listas de correo (y los servidores que manejan estas listas) y servidores de archivos. Una lista de correo es básicamente una lista de direcciones de correo de personas que podrían ser accedidas enviando un correo a una dirección individual. Mantener una lista actualizada podría resultar un trabajo tedioso, es por ello que existen programas que realizan esta labor de manera automática (majordomo, listserv, etc.). Los servidores de archivos reciben peticiones de usuarios y envían archivos a través de correo electrónico.

FTP

FTP es el servicio a través del cual la mayoría de los usuarios envían y reciben documentos o archivos en Internet. Es similar a establecer una conexión (registro) a un servidor, pero restringiendo a los usuarios a un limitado conjunto de comandos y, para usuarios de FTP anónimo, a un limitado conjunto de archivos. Los clientes de FTP son disponibles para la mayoría de las computadoras del mercado.

FTP soporta todos los formatos y con una configuración extra y un servidor especial de FTP, es posible definir clases de usuarios quienes poseen acceso privilegiado a secciones del servidor, es decir, es posible establecer un completo control de acceso para el servidor a través de FTP.

Gopher

Los clientes gopher solo despliegan un menú de opciones de texto, y el usuario simplemente selecciona una, la cual puede dar como resultado el despliegue de otro menú. Un servidor gopher es relativamente sencillo de administrar, los subdirectorios que se crean se convierten en menús, y los archivos en esos directorios se vuelven disponibles para clientes gopher.

La limitación de gopher radica en los tipos de datos que soporta y en la variedad de servicios a los cuales puede hacer referencia. Gopher solo soporta texto ASCII, pudiendo transferir datos binarios y desplegando estos con la ayuda de otro software.

Word Wide Web

El word wide web (www o web) es el más poderoso servicio de información sobre Internet. El servicio de web posee grandes características por sí mismo, integrando otros servicios de una forma más simple de utilizar. No es necesario tener un cliente FTP para acceder un servidor de FTP o un cliente gopher para acceder un servidor gopher, a través de un browser, utilizando el servicio de web se provee acceso a todos estos servicios.

Los documentos a ser utilizados por el servidor de web son escritos en el lenguaje denominado HTML (HyperText Markup Lenguaje). Un archivo HTML es un archivo ASCII con comandos de formatos, los cuales son interpretados por el browser para obtener la página que se muestra al usuario, indicando la presencia de hiperligas (conexiones a otras páginas u otros servidores) dentro del propio documento HTML. Dichas hiperligas podrían llegar a ser a otro documento HTML o el acceso a un servidor gopher o FTP. Los documentos son transferidos a través del protocolo HTTP (descrito en el punto 2.4.2).

El browser puede desplegar gráficos, ejecutar un programa independiente, desplegar imágenes de alta resolución, audio, video, etc. todo con el uso del servicio de web.

Debido a los estándares de desarrollo y lo simple de éste, el número de servidores sobre Internet se estima que crece en un 100% cada seis meses¹⁰. Actualmente, es posible adquirir una herramienta para la creación de páginas web por menos de 100 usd. Microsoft ha incorporado las características de servidor de web dentro de Windows NT e incluso Lotus Notes V. 4.5 tiene interconstruido un navegador de web. El concepto de servidor de web se ha provisto por sí mismo como una herramienta poderosa de distribución de información.

Con la gran variedad de herramientas para la implementación de un servidor de web y la consecuente construcción de sus páginas, los beneficios de esta tecnología no necesitan ser restringidos al uso de Internet. En un gran campo de organizaciones, redes de sitios web internos comienzan a proliferar. Para adaptarse a este cambio, las redes están rápidamente adoptando el protocolo TCP/IP. Al colocar la información corporativa sobre servidores de web permite a cualquier empleado, con el equipo adecuado, acceder las bases de la información rápida y de forma sencilla.

En palabras simples, Intranet es el término utilizado para la implementación de las tecnologías Internet dentro de una organización corporativa.

Intranet facilita el uso común de la información empresarial y dinamiza la toma de decisiones en todos los niveles. Aún más, obliga a adoptar formas concurrentes de trabajo entre los empleados y entre estos y los directivos, con el fin de reducir drásticamente el tiempo del ciclo de procesos. Por ello es también capaz de correr aplicaciones para el manejo y la transformación de datos. Proporciona finalmente una forma universal de comunicación interna. Es decir, la información puede consultarse sin que importe el lugar en donde se encuentre almacenada y sin que importe tampoco el tipo de terminal desde donde se accede.

¹⁰ Fuente: Corporate Internet Strategy, Nostrand Reinhold, ed International Thomson

Intranet es capaz de procesar las siguientes capacidades:

- Redes corporativas para interconectar físicamente usuarios y recursos computacionales geográficamente dispersos.
- Servicios de información de procesos, para que los recursos informáticos se incorporen a flujos de trabajo del negocio ("workflow").
- Intercambio electrónico de información.
- Servicios de información disponible para crear un perfil de recursos informáticos que se puedan intercambiar, compartir o procesar fácilmente en forma transparente.
- Seguridad corporativa.

Otro impacto previsto con el uso de Intranet es la agilización en la toma de decisiones internas, al difundir información almacenada y la que se genera diariamente ampliando la base para la toma de decisiones.

Los beneficios de la tecnología de web dentro de ambientes corporativos se incrementan rápidamente debido al crecimiento de Intranet como un medio privado y una red segura para la intercomunicación del personal. Los estándares abiertos basados en correo electrónico y "groupware" extenderán la promesa de la tecnología Intranet y traerán consigo una nueva era en el intercambio de información.

Muchas organizaciones se encuentran actualmente en un cuestionamiento: Deben implementar una Intranet, expandir su red actual dentro de Internet, o desarrollar un sistema que combine estas dos aproximaciones. La decisión depende realmente de las características propias de la organización.

Con Intranet, la mayor parte de las conexiones y actividades están enfocadas a la comunicación entre usuarios dentro de la misma institución o departamento. Estando los objetivos enfocados sobre la transmisión de datos y aplicaciones de "groupware".

En una Extranet, la cual es una red conectada a Internet, los esfuerzos se canalizan a la comunicación entre usuarios fuera de la organización y usuarios o recursos dentro de esta (o viceversa). El énfasis es sobre comunicaciones y aplicaciones de publicación.

Una red híbrida es la combinación entre Intranet y Extranet. La mayoría de las redes basadas en IP eventualmente involucrarán esta estructura híbrida. Principalmente utilizada en organizaciones cuyas aplicaciones -principalmente "groupware"- residen en Intranet, pero aquellos esfuerzos de mercadotecnia y publicación son enfocados en su mayoría a Internet.

Cada red posee un conjunto de elementos internos o externos que la moldean como una entidad única. Algunas redes tienen mayor influencia externa que interna, no existiendo una red como entidad aislada. Estos elementos determinarán en parte si el resultado final es una Intranet, Extranet o una red Híbrida.

Un elemento externo de importancia es el denominado "outsourcing", el cual es virtualmente inevitable en las redes de hoy en día. El simple hecho de mantener una conexión a Internet, involucra "outsourcing" al involucrar un ISP (Internet Service

Provider), aun cuando la institución pueda ser un DNS¹¹ primario, es decir que por si misma tenga acceso a un NAP, es necesario establecer un contacto con InterNIC¹².

Es importante destacar que en el uso de "outsourcing" parte del control es delegado, sin embargo es importante mantener el control global de los cambios realizados en la red, ya que de no ser así se corre el riesgo de que la página hogar no represente la imagen y personalidad de la institución.

Como comentamos al hablar de Sistemas Abiertos, los estándares representan un punto importante tanto a niveles externos como internos. Cuando se extiende la red al exterior se necesita algo más que solo "gateways". La falta en el uso de estándares podría provocar que el soporte, seguridad y administración cobrarán un precio demasiado alto al implementar una Extranet. Esto también significa que una organización podrá convertirse en dependiente de un distribuidor, sin posibilidad de expansión alguna.

En la determinación si una Intranet, Extranet o red híbrida es mejor para los propósitos de la institución, es importante determinar los aspectos propios. Los dos principales aspectos para este enfoque son la administración de ancho de banda y la estructura de la red.

La amplitud de ancho de banda tiene un efecto dramático sobre el enfoque de la red. No solamente debe tener suficiente capacidad para satisfacer las necesidades actuales de los usuarios, debe también, poder soportar actualizaciones cuando nuevas necesidades sean requeridas.

Banco de México tiene contemplada la implantación de tres diferentes servidores de web en funcionamiento, pero iguales en sus características. Esta distinción es debido a los tres campos diferentes de trabajo que se pretende abarcar. Por una lado, la información al público en general será difundida a través del servidor de Internet, por otro, las relaciones a nivel exclusivo entre Banco de México y el Sistema Financiero serán efectuadas a través de la Extranet, y por último, todo el manejo de información interna como institución será explotada por medio de una Intranet.

El análisis y puesta en marcha de los tres servidores en esencia serán iguales, con las características propias de su ubicación física.

2.4.2 Protocolo HTTP¹³

No importa del tipo de red del cual se trate, al hablar de estándares para Internet es básico el análisis del protocolo que hace esto posible: HTTP.

HyperText Transfer Protocol (HTTP) es una aplicación a nivel protocolo con la velocidad necesaria para sistemas de información distribuidos. Es un protocolo orientado a objetos el cual puede ser utilizado para muchas tareas, tales como nombres de

¹¹ Domain Name Server

¹² Internet Network Information Center, organismo mundial que tiene entre sus funciones la asignación de direcciones IP homologadas.

¹³ Fuente: <http://www.stars.com/Internet/Protocols/HTTP/>

servidores y sistemas de administración de objetos distribuidos, a través de la extensión de sus comandos (métodos de respuesta). Una característica de HTTP es la forma y manejo de la representación de datos, permitiendo a los sistemas ser construidos independientemente de la forma de transferencia de los mismos.

Como propiedades básicas de HTTP podemos mencionar:

- **Esquema de direccionamiento**
HTTP utiliza el concepto de referencia provista a través del identificador universal de recursos (URI - Universal Resource Identifier) bien a manera de una localidad (URL - Uniform Resource Locator) o nombre (URN - Uniform Resource Name), indicando de esta manera el recurso al cual un método va a ser aplicado. URL se refiere a: *servicio://host:puerto/archivo.extension/ruta*, HTTP puede contener la mayoría de los servicios básicos de Internet.
- **Arquitectura Cliente Servidor**
HTTP es basado en el paradigma petición/respuesta. La comunicación generalmente toma lugar sobre una conexión TCP/IP sobre Internet. El puerto estándar es 80, sin embargo otros puertos pueden llegar a ser utilizados.
- **Protocolo no orientado a conexión**
Después de que el servidor ha respondido a la petición del cliente, la conexión entre estos es terminada. No existe "memoria" de esta conexión. La implementación de un servidor HTTP maneja cada petición como si fuera una nueva.
- **Representación abierta de datos.**
HTTP utiliza "Internet Media Types" (formalmente referidos como MIME Content-Types) (Multipart Internet Mail Extension) para proveer un abierta y extensiva representación de datos. Cuando el servidor de HTTP transfiere información al cliente, incluye un encabezado MIME para informar al cliente que tipo de dato le sigue. La traducción entonces depende de que el cliente procese la utilería apropiada correspondiente al tipo de dato.

Encabezados de HTTP

Una transacción HTTP consiste de un encabezado seguido opcionalmente por una línea vacía y datos. El encabezado especificará cosas como la acción requerida del servidor o el tipo de dato a ser retornado o un código de estado.

Las líneas de encabezado recibidas desde el cliente, si existen, son remplazadas por el servidor dentro del ambiente de variables CGI con el prefijo *HTTP_* seguido por el nombre del encabezado. El servidor puede excluir cualquier encabezado que ya haya sido procesado, el ejemplo mas claro de esto son las autorizaciones.

Métodos de Respuesta.

Los métodos de respuestas son utilizados para indicar el propósito de la petición. Los tres métodos más comúnmente utilizados son: POST, GET y HEAD.

Respuesta

A continuación se da un ejemplo de respuesta en un servidor HTTP

```
HTTP/1.0 200 OK
Date: Wednesday, 02-Feb-95 23:04:12 GMT
Server: NCSA/1.3
MIME-version: 1.0
Last-modified: Monday, 15-Nov-93 23:33:16 GMT
Content-type: text/html
Content-length: 2345
* a blank line *
<HTML><HEAD><TITLE> ...
```

Línea 1:

El servidor está de acuerdo en utilizar la versión 1.0 de HTTP para comunicación y envía el estado 200 indicando que el proceso ha tenido éxito en la petición del cliente.

Líneas 2 y 3:

El servidor envía la fecha y se identifica así mismo como un servidor NCSA

Línea 4:

Se indica que se está utilizando la versión 1.0 de MIME para describir la información que es enviada y se incluye el tipo MIME de la información a ser enviada en el encabezado "Content-Type".

Finalmente, se envía el número de caracteres a ser enviados, seguido de una línea en blanco y de los propios datos.

ANÁLISIS DE FACTIBILIDAD

El presente capítulo es parte medular del desarrollo, ya que establece el análisis previo para la elección de las herramientas tecnológicas a utilizar, definiéndose los alcances de éstas como del proyecto en general.

3.1 Definición de los servicios institucionales

El mundo se mueve a través de la información, la herramienta más poderosa en la toma de decisiones es el conocimiento que se tenga de ésta. Banco de México tiene como una de sus actividades principales el dar a conocer, como fuente oficial, diferentes tipos de valores que influyen directamente en el Sistema Financiero, no solo Mexicano sino también Internacional.

Los servicios a ser incorporados dentro de una primera etapa para el servidor de web Banxico, están basados en la manipulación o generación de la información producida por el Banco, orientada tanto de usuarios externos (Sistema Financiero) como para usuarios internos (Intranet). El manejo y consecuentemente los servicios a ofrecer por medio del servidor de web pueden ser agrupados en tres aspectos: 1) Groupware, 2) Información Dirigida y 3) Servicios y Comunicaciones.

3.1.1 Groupware

"Groupware" es el Software para ambientes interactivos y compartidos. Es decir, permite que grupos de personas interactúen en una tarea común proporcionando la interfaz para un ambiente compartido.

Groupware es un subconjunto de un concepto más amplio denominado "Cómputo Corporativo". Cómputo corporativo es definido, según miembros de SUCCEED (Southeastern University and College Coalition for Engineering Education¹), como: "Tecnología de cómputo que permite a dos o más personas comunicarse entre ellas, para compartir información o coordinar sus actividades".

La principal diferencia, entonces, entre Groupware y Cómputo Corporativo es que Groupware es el Software que permite a las personas comunicarse, compartir información o coordinar, mientras que el Cómputo corporativo es la tecnología (hardware, software) que permite que estas actividades se lleven a cabo.

Para Banco de México el concepto de "Groupware" va más enfocado a sus actividades funcionales como organización, más que a su papel como institución reguladora de la economía Mexicana. Es decir, aspectos tales como la petición de algún servicio (mantenimiento, direcciones de correo, prestaciones, etc.) pueden ser manejados dentro de este concepto.

Por medio de workflow, que es una actividad inherente al concepto de Groupware, la solicitud por parte del usuario final es enviada a la persona indicada, para que ésta a su vez realice el trámite o, en su defecto, canalice la solicitud a la persona que forma parte de la cadena en el proceso de tramitación. Mientras, el usuario puede verificar el estado de su trámite así como quién o que lo podría estar deteniendo. Cabe mencionar que la petición se realizará por medio de una forma en Intranet, sin embargo dependiendo del proceso éste puede o no, ser realizado por el servidor de web o alguna otra herramienta propia de workflow.

3.1.2 Información Dirigida

En esencia el concepto de Información dirigida hace referencia a la información que es difundida por el Banco tanto a nivel de Institución como de organismo regulador del sistema financiero mexicano.

La información dirigida al sistema financiero y público en general son datos propios del comportamiento de la economía del país, los cuales sin lugar a duda gravitan en la toma de decisiones del mercado nacional e internacional. De este concepto lo que se busca es brindar la información necesaria con la debida oportunidad. Tratando de establecer un proceso automático, de tal manera que la fuente real de la información actualice las páginas de web con la mínima intervención humana, ganando tiempo, situación más que relevante en el sector financiero.

Así también, Banco de México ha tratado de mantenerse a la vanguardia en lo que a tecnología se refiere, caso claro son los diferentes sistemas utilizados por el Sistema Financiero realizados por Banco de México, para dichos sistemas es probable que, en un futuro, exista un desarrollo para su funcionamiento en Internet, previo análisis de factibilidad. Empezando por la simple difusión de manuales e información en general de los sistemas realizados por el Banco, hasta el total funcionamiento de estos sobre el servidor de web.

¹ <http://www.succeed.vt.edu>

La información dirigida, analizando al Banco como una organización donde laboran miles de empleados, básicamente se refiere a hacer del conocimiento de éstos, toda aquella información que sea de importancia para el desarrollo de sus actividades. Información tal como los servicios (actividades recreativas, prestaciones, etc.), capacitación, planes de contingencia o que hacer o a quién recurrir en una situación extraordinaria, es información que será colocada en Intranet, proporcionando a los empleados Banxico una herramienta que les permitirá un mejor aprovechamiento de su tiempo y consecuentemente una mejora en su desempeño.

3.1.3 Servicios y Comunicaciones

Servicios y comunicaciones es un aspecto que va de la mano con lo descrito como Groupware. Simplemente tratando de acentuar nuevamente los dos aspectos en los cuales el Banco se ve involucrado (como organización). Servicios como e-mail o envío de mensajes a un localizador, así como la continua retroalimentación o actualización tanto de información como de los propios sistemas que la manejan serán de vital importancia a ser considerados dentro de toda la estructura del servidor de web.

3.2 Definición de Alcances y Requerimientos.

El web Banxico deberá reflejar las visiones corporativas y los objetivos del Sistema Financiero Mexicano. Por ello, sus características principales estarán definidas como sigue:

- Deberá presentar la información de mayor interés para el sector financiero, público en general, así como para los usuarios potenciales.
- Dará a conocer la imagen de la institución, seria y formal.
- Brindará facilidades de búsqueda, al contener mucha información, este aspecto se vuelve primordial para facilitar al usuario la navegación, disminuyendo el tiempo de búsqueda, ganando nuevamente la oportunidad de información.
- Estará basado en la tecnología de WWW, tratando de explotar al máximo las facilidades que ésta ofrece, es decir, atractivo, dinámico, con facilidad en el uso de: tablas, formas, animaciones y, posiblemente, la interacción con programación externa (CGI, scripts y applets de Java), obteniéndose una manipulación, administración y presentación más simple de la información.
- La información estará contenida dentro de bases de datos y deberá ser accedida a través del browser por programas 4GL, manteniendo una arquitectura cliente/servidor y las ventajas que de ésta se desprenden.
- Estará conformado por páginas amigables y dinámicas, que permitan al público la obtención rápida de solo aquella información que éstos solicitan, evitando con esto abrumar al usuario con cientos de cifras de poco significado práctico.

- El servidor de web deberá tener un nivel de seguridad lo más cercano al 100% debido a la trascendencia de la información que dentro de él se contiene.
- Deberá mantener la facilidad de poder ser migrado, en un futuro, a mejores versiones así como para la implantación de nuevas tecnologías, manteniendo la integridad de los datos así como la funcionalidad de los programas que los manejan.

No existe lugar a duda que el medio actual para la disseminación de información de manera oportuna y eficaz es Internet, esto implica un esfuerzo en materia de tecnología y el correspondiente conocimiento de la misma.

Como primer acercamiento podría llegar a pensarse que Internet es sólo un browser, un servidor y una conexión. Sin embargo, para Banco de México, la selección de la infraestructura tecnológica para la implantación de un servidor de web va más allá. Es preciso un análisis profundo del servidor a usar, del browser estándar dentro de la Institución (Intranet), así como de las herramientas de desarrollo (HTML, Bases de Datos, etc.), con el objetivo de establecer la base de herramientas que permita un mejor acoplamiento a la infraestructura tecnológica ya existente en el Banco, tratando de reducir el costo al mínimo, tanto económico como de aprendizaje, sobre las nuevas tecnologías.

3.3 Estrategia.²

Internet es un instrumento que se encuentra en una etapa de adolescencia y tiene muchos aspectos que madurar aún. Los esfuerzos actuales están concentrados en el desarrollo de herramientas y la creación de una estructura de información y datos para la aplicación de esas herramientas.

El primer paso real en la creación del servidor de web para el Banco de México fue, desde luego, la identificación de la necesidad, una necesidad que veía su mejor solución en las herramientas de Internet y el constante crecimiento del área de comunicaciones por parte de Banco de México.

Se analizará el software sobre la base de las plataformas ya estudiadas y probadas que el Banco posee, tanto en el área de cómputo, como en comunicaciones, así como también, la implantación y estudio del lugar físico para el servidor y los costos asociados a este proyecto.

Una vez definida la estructura tecnológica a utilizar, se deberá realizar un análisis con respecto a las aplicaciones que el Banco posee con el objetivo de crear, sobre Internet o Intranet, un receptor de aplicaciones de tal manera que implique un esfuerzo mínimo el adaptar una aplicación, de la cual sobre la base de su diseño se determinó la factibilidad de su funcionamiento sobre Internet, a nuestro servidor de web.

El diseño del servidor debe tomar en consideración la posibilidad de crecimiento. El objetivo principal por parte de Banco de México es la difusión de información, sin embargo, como una segunda etapa, se plantea la posibilidad de transacciones y el

² Basado en lineamientos establecidos en Building a Corporate Internet Strategy, Maitra, ed. ITP

desarrollo de aplicaciones de groupware para Intranet, por lo cual la estrategia debe contemplar sin lugar a duda la posibilidad de expansión.

Una vez determinado todo el ámbito técnico se analizará la información Banxico para crear una página hogar que 1) Identifique plenamente una institución seria y formal y 2) dé la facilidad de acceso a la información. ¿Pero que existe detrás de esa página hogar? Administración, revisión, modificación y cambio sin perder los dos puntos prioritarios.

Resumiendo: Existen tres puntos principales que no deben ser perdidos de vista: Como manejar y que información colocar sobre Internet, como minimizar los costos de administración y aspectos legales (si se implanta el uso de transacciones) y por último y no por ello menos importante, establecer los lineamientos con respecto a seguridad.

Se desarrollará una política de Internet como transmisión y medio de información, ya sea esta generada con propósitos internos o externos. Dicha política incluirá, entre otros puntos:

Acceso:

Banco de México se reservará el derecho de monitorear, revisar y regular el acceso de Internet y cualquiera de sus servicios para asegurar que las políticas de la organización sean seguidas y los servicios usados exclusivamente con fines institucionales.

Diseminación de información sobre Internet:

El Banco de México proveerá información sobre Internet bajo la supervisión y control de los responsables de la información, permitiendo al Sistema Financiero y público en general, permanecer mejor informado para la toma de decisiones.

Efectividad y Eficiencia de uso:

Difundir las políticas de uso para Internet (acceso de software, diseño de seguridad, etc.) con el objetivo de guiar y satisfacer las necesidades del usuario sin perder los objetivos como institución.

Regular el uso de grupos de discusión y cualquier otra actividad que implique un contacto a nombre de Banco de México o bajo los medios propiedad de éste.

Diseño:

El diseño de cualquier página que se encuentre bajo el servidor de web de Banco de México deberá representar el profesionalismo y seriedad de la institución.

Autorizaciones:

Acorde a las políticas de uso, cualquier conexión o difusión de información deberá recibir la autorización del personal calificado.

Existirá supervisión y administración del personal con responsabilidad sobre los recursos de Internet para asegurar la uniformidad de los objetivos.

3.4 Infraestructura Tecnológica.

La mayor parte de los equipos utilizados en Banco de México son fabricados por la empresa Olivetti. Dichos equipos podemos clasificarlos en tres diferentes configuraciones, las cuales se explican a detalle en el punto 3.4.1

3.4.1.- Características: Plataformas Banxico

Los esquemas de cómputo, fuera de los equipos UNIX utilizados por el Banco, están basados en tres diferentes configuraciones:

- Configuración A, Procesador Intel Pentium II, 233 MHz, memoria Ram 64 MB, monitor color, disco duro de 3.1 GB, disco flexible 1.44 MB.
- Configuración B, Procesador Intel Pentium II, 300 MHz, memoria Ram 128 MB, monitor color, disco duro de 9.1 GB, disco flexible 1.44 MB.
- Configuración C, Procesador Intel Pentium II, 300 MHz, memoria Ram 256 MB, monitor color, dos discos duros de 18.1 GB, disco flexible 1.44 MB.

Equipos con procesador PENTIUM II a 233 Mhz. (configuración A):

- Procesador: Intel PENTIUM II.
- Velocidad de reloj: 233 MHz.
- Cache secundario mínimo: 512 kb.
- Capacidad de crecimiento de la memoria RAM: 192 MB en la tarjeta madre.
- Capacidad de expansión a través de ranuras libres: 1 ISA de 16 bits, 2 PCI y una compartida ISA-PCI (ranuras libres después de instalar la tarjeta de red).
- Memoria: 64 MB de RAM.
- Expansión de memoria utilizando DIMM's.
- Tiempo de acceso a memoria RAM: 60 ns.
- Capacidad de la fuente de poder: la necesaria para poder instalar la configuración necesaria (tarjeta de red, unidad de disco flexible, unidad de disco fijo y unidad de cinta, o bien, otro disco duro o un disco óptico).
- Capacidad para albergar dos dispositivos de 5.25" y media altura, una vez instalados el disco duro y la unidad de floppy.
- ROM BIOS tipo "Advanced Power Management" y "Plug and Play".
- Tipo de memoria del BIOS: memoria flash.
- De bajo consumo de energía eléctrica, de acuerdo con las normas del programa "EPA Energy Star" del gobierno de E. U. A.
- Compatible con el estándar de administración y monitoreo DMI 2.0.

Equipos con procesador PENTIUM II a 300 Mhz. (Configuración B):

- Procesador: Intel PENTIUM II
- Velocidad de reloj: 300 MHz.
- Cache secundario mínimo: 512 kb.
- Capacidad de crecimiento de la memoria RAM: 192 MB en la tarjeta madre.

- Capacidad de expansión a través de ranuras libres: 1 ISA de 16 bits, 1 PCI y una compartida ISA-PCI (ranuras libres después de instalar la tarjeta de red y la controladora de disco).
- Memoria: 128 MB de RAM.
- Expansión de memoria utilizando DIMM's.
- Tiempo de acceso a memoria RAM: 60 ns.
- Capacidad de la fuente de poder: la necesaria para poder instalar la configuración necesaria (tarjeta de red, unidad de disco flexible, unidad de disco fijo y unidad de cinta, o bien, otro disco duro o un disco óptico).
- Capacidad para albergar dos dispositivos de 5.25" y media altura, una vez instalados el disco duro y la unidad de floppy.
- ROM BIOS tipo "Advanced Power Management" y "Plug and Play".
- Tipo de memoria del BIOS: memoria flash.
- De bajo consumo de energía eléctrica, de acuerdo con las normas del programa "EPA Energy Star" del gobierno de E. U.
- Tarjeta controladora: con doble conector: un conector Fast SCSI-2 y uno Wide UltraSCSI y que acepte hasta 14 dispositivos.
- Compatible con el estándar de administración y monitoreo DMI 2.0.

Equipos con procesador PENTIUM II a 300 Mhz. (Configuración C):

- Procesador: Intel Pentium II.
- Velocidad de reloj: 300 MHz.
- Con posibilidad de añadir otro CPU de las mismas características, es decir, puede aceptar hasta 2 CPUs.
- Cache secundario mínimo por CPU: 512 kb.
- Capacidad de crecimiento de la memoria RAM: 512 MB.
- Memoria: 256 MB de RAM, con circuitería de corrección y detección de errores (ECC).
- Capacidad de expansión a través de ranuras libres: 1 ISA y 3 PCI (con la controladora de disco y la tarjeta de red ya instaladas).
- Tiempo de acceso a memoria RAM: 60 ns.
- Capacidad de la fuente de poder: la necesaria para poder instalar la configuración necesaria (tarjeta de red, unidad de disco flexible, unidad de disco fijo y unidad de cinta, o bien, otro disco duro o un disco óptico).
- Capacidad libre para albergar al menos 3 dispositivos de 5 1/4" y media altura y 4 dispositivos de 3 1/2" y media altura. Estas capacidades son después de instalados 2 discos duros de 18.1 GB y una unidad de floppy de 3 1/2".
- 2 discos duros instalados de 18.1 GB para hacer "mirroring" bajo NetWare 4.1 y superiores.
- Con una segunda fuente de poder redundante.
- Con ventiladores redundantes.
- La ventilación de los discos duros del servidor está diseñada para soportar discos a 10,000 rpm.
- Bus EISA-PCI.
- ROM BIOS tipo "Plug and Play".
- Trabajo soportado como servidores de archivos bajo el sistema operativo NetWare versión 4.1 y posteriores de Novell y Microsoft Windows NT V. 4.0 y posteriores.
- Sensores de temperatura.
- Tarjeta controladora de los dispositivos
- Fuente de poder para los voltajes 5, 12 y 3.3 V.
- Protección de encendido/apagado.

3.4.2.- Elección de Hardware para el Servidor

El equipo destinado por Banco de México para funcionar como servidor de web se encuentra clasificado para el uso de organizaciones de medio o gran tamaño. Una plataforma de sistema estable para tener suficiente tiempo de desarrollo en aplicaciones altamente específicas así como un alto desempeño. El equipo que mejor se acopla a estos requerimientos es un equipo Net Strada 7000, fabricado por la empresa Olivetti. Dado el hecho de que una de las plataformas utilizadas por Banco de México es Windows NT, dicho equipo satisface de sobremanera los requerimientos propios de este sistema operativo.

Características³

- **Procesador Quad 200/512 Pentium Pro.**
Net Strada 7000 combina las características de la tecnología Intel (procesadores Pentium Pro 200 Mhz con 512 KB de cache)
- **Escalable a 2 GB - Memoria ECC.**
Aplicaciones con uso de manejadores de bases de datos como Oracle o Sybase pueden llegar a requerir un gran consumo de memoria. El equipo Net Strada 7000 puede crecer de 64 MB a 1 GB de memoria en la tarjeta madre y hasta 2 GB utilizando una tarjeta de memoria de expansión, ambas actualizaciones utilizando la tecnología ECC (Error-Correcting Code). Dicha tecnología de protección puede ser extendida al sistema, dispositivos de I/O, cache en CPU y cache en disco, previendo una alta integración de datos en cada componente del sistema.
- **Discos SCSI**
La velocidad de transferencia es crítica al tener más de un disco. SCSI son discos que corren a 7200 rpm, logrando llegar a transferir datos a 40 MB/s.
- **Alta redundancia**
Los componentes electromecánicos son algo a lo que no siempre se le da la importancia que debería, el equipo Net Strada 7000 cuenta con dos fuentes de poder independientes (450 W cada una) y un conjunto duplicado de tres ventiladores.
- **Escalabilidad en disco**
Con una expansión de periféricos se podría llegar a implementar una capacidad de almacenamiento de 648 GB.
- **14 ranuras de expansión**
 - 2 conectores de CPU (hasta dos procesadores para cada tarjeta)
 - 1 conector de expansión (para expansión de memoria)
 - 7 PCI
 - 3 EISA

³ Fuente: <http://www.olivetti.com>

- 1 PCI/EISA
- Controlador de Video
SVGA dentro de la tarjeta madre con 1 MB DRAM
- Puertos
 - 1 interfaz de ratón
 - 1 interfaz de teclado
 - 1 interfaz paralela
 - Dos interfaces seriales
 - Un puerto de vídeo
 - Un puerto SCSI-2
- Unidades
 - 3 unidades lectoras de CD (SCSI-8x)
 - 1 unidad de disco de 3.5"
 - 1 unidad de cinta de 4 mm

3.4.3.- Servidor⁴

La mayor parte del tiempo el servidor no es tomado en cuenta por el usuario, sin embargo, los servidores de web son los verdaderos héroes de Internet. El tráfico en el web domina a Internet hoy en día, y todas y cada una de las páginas de web o gráficas provienen del servidor. La constante evolución en los browsers ocupa toda la atención, pero sin el servidor de web, bien podría no haber web.

Para cada servidor de web utilizado por empresas para desarrollar un sitio en Internet, decenas o cientos, están siendo desarrolladas dentro de las mismas empresas para sitios internos, también conocidos como Intranets. Los servidores de web prometen convertirse en una de las mayores incorporaciones a una red de cómputo. Intranet usualmente inicia como un vehículo para proveer información de carácter corporativo a los empleados, sin embargo se convierte en vehículo para colaboración. Mensajería, flujo de trabajo y cualquier otra función de red a nivel corporativo.

El web nació en un principio solo como páginas HTML, actualmente las necesidades van mas allá de eso, surgiendo aspectos tales como acceso a bases de datos, páginas dinámicas, etc. Por ello es necesaria la implementación de un servidor que involucre tales aspectos.

Que es un servidor de web

Los servidores de web realmente son de muy simple operación. Los web browsers se comunican con los servidores de web utilizando el protocolo de transferencia de hipertexto (HTTP -HyperText Transfer Protocol), una petición/respuesta para información es transferida utilizando TCP/IP. El servidor de web recibe la petición, localiza el archivo (o fuente de información) y la envía al browser, cancelando la conexión. Las gráficas son proporcionadas de la misma manera, desplegándose en el browser el documento HTML solicitado.

⁴ Fuente: PC Magazine, Oct 22 97

La figura 3.1 describe el proceso que sigue una petición en Internet, desde que esta es realizada hasta que la información solicitada es entregada al usuario.

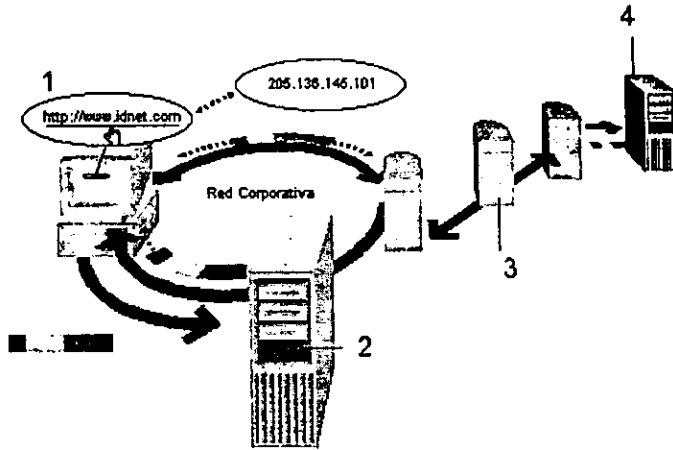


Figura 3.1 Proceso de petición/respuesta de una página de web

1. Uniform Resource Locators (URLs) únicamente identifica cada archivo en el Web cuando se especifica su nombre, en qué servidor se encuentra y dónde se localiza dentro de la estructura del directorio de dicho servidor. Llamando un URL directamente al navegador o seleccionando una liga con un URL asociado, se inicia una sesión que (cuando es exitosa) trae ese único archivo a tu PC. Las direcciones de Internet Protocol (IP) proveen un número de identificación de 32 bits único para cada computadora en Internet. Una vez que el navegador tiene la dirección IP del servidor que contiene el documento deseado, es posible iniciar la sesión de comunicación con dicho servidor.
2. Domain Name Server (DNS) es un tipo de servidor especializado de Internet que le indica al navegador la dirección IP del servidor de Internet referido en el URL seleccionado. El sistema local envía un URL al servidor DNS, el cual responde con la dirección IP del servidor al que se desea conectar. Esto lo realiza verificando una tabla donde se cruzan las referencias del DNS y las direcciones IP. El DNS puede estar incorporado a un "firewall" o ser mantenido por el proveedor Internet.
3. Los "ruteadores" son buscadores dentro de Internet. El flujo de paquetes puede pasar por un gran número de ruteadores, tanto en el interior como en el exterior de los límites incorporados, antes de llegar a su destino. Los ruteadores pueden pertenecer a corporaciones o proveedores de Internet o ser parte de la propia columna vertebral de la red local.
4. El servidor web remoto recibe y entrega la solicitud sobre un archivo específico. La dirección IP, quedando fija en los paquetes de salida, hace posible rutearlos de regreso al navegador.

Los servidores de web típicamente almacenan páginas y gráficas, sin embargo es posible incluir archivos de texto, documentos procesados, vídeo, o audio. Un Servidor, de igual manera, puede ejecutar aplicaciones, siendo las más comunes Máquinas de Búsqueda o procesos de conexión a bases de datos. Estándares como CGI (Common Gateway Interface), lenguajes Script o lenguajes de programación como Java y Visual Basic están siendo utilizados con este propósito.

Criterios de Revisión.⁵

Se estudiaron 8 servidores de web de los cuales, dependiendo de su plataforma de operación coincidente con la plataforma Banxico y de los resultados del estudio, se probaron 3 de ellos. En esencia se buscaron proveedores que al menos tuvieran el 1% del total de mercado.

Los aspectos básicos a considerar en este análisis fueron: Instalación, Configuración, Administración, Seguridad, Control de Acceso, Desarrollo de aplicaciones y Desempeño.

La plataforma base para Banco de México es Sun Solaris, Windows NT y Novell. Es decir, se busca un producto aplicable a una de las plataformas antes mencionadas. Las aplicaciones sobre correo electrónico, ya iniciadas en el banco, funcionarán sobre NT, dichas aplicaciones sin lugar a duda tendrán relación con el servidor de web, punto, no definitivo, pero si a tomar en cuenta sobre WinNT.

La instalación y sobre todo la configuración deben de ser prácticas, es decir que la inversión de tiempo en ellas no exceda de lo razonable y la posibilidad de algún error involuntario sea mínima.

La administración debe poder ser tan poderosa de manera local como remota, sin olvidar las características de flexibilidad y sencillez.

Los rubros de seguridad y control de acceso son tópicos relacionados. Ciertamente Banco de México (como primera etapa) no desarrollará aplicaciones de nivel crítico sobre Internet, a pesar de esto, se debe buscar un sistema de seguridad robusto, ya que la posibilidad de ejecutar transacciones de nivel crítico no se descarta en un futuro cercano. Sobre el contexto de Intranet si serán ejecutados procesos tales como préstamos, solicitudes de servicio, etc., procesos que deben ser monitoreados en línea, requiriendo de niveles confiables y eficientes de seguridad.

Para el desarrollo de aplicaciones se debe buscar la compatibilidad con aquellas ya existentes en el Banco en base al análisis de una posible migración.

Las características anteriores en conjunto con la respuesta interna del equipo (velocidad de procesamiento, expansión de procesadores, etc.) conforman el aspecto de desempeño.

⁵ Basados en los criterios establecidos para análisis de servidores de web publicados en la revista PC Magazine, Oct 22 1997

Opciones Analizadas

Basado en los puntos antes mencionados las opciones analizadas fueron:

Commerce Builder Pro (CBP) The Internet Factory Estudio	Purveyor Encrypt Web Server (PEW) Process Software Corp. Estudio
Internet Connection Secure Server For OS/2 Warp (ICSS) IBM Estudio	Stronghold Apache-SSL-US 1.2.5 Community ConneXion Inc Estudio.
Internet Information Server 4.0 (IIS) MICROSOFT Estudio - Prueba	Web Site Profesional 2.1(WSP) O'relly & Associates Inc Estudio.
NetScape Enterprise 3.5.1 (NES) Fast Track Server (NFTS) NetScape Corp. Estudio - Prueba	Java Web Server 1.1 Sun Microsystems Estudio
NetWare Web Server (NWS) Novell Inc Estudio - Prueba.	

Como podemos apreciar, las opciones a ser tomadas en cuenta para una prueba son aquellas coincidentes con las plataformas de Banco de México, ya que no tendría caso alguno, por gran desempeño que mostrara el servidor, escoger uno que no puede ser instalado en Banco de México o, en caso de hacer esto posible, convertirlo en un ente ajeno con una compatibilidad nula con respecto al resto de las aplicaciones Banxico.

Métodología de Prueba

Para los tres servidores probados se utilizaron el sistema operativo nativo de cada uno de éstos.

Debido a que la prueba funciona de forma independiente de la plataforma del servidor, los resultados serán medidos en todos los clientes, los cuales forman parte de la red Banxico y funcionan sobre equipos Pentium módulo 166 DT manufacturados por Olivetti.

Las peticiones de cada cliente son ejecutadas de forma incremental para adicionar carga de trabajo al servidor y acumular los resultados para cada prueba ejecutada. El número de clientes utilizados fue de 1 a 22, ejecutándose de uno a uno o en bloques de 5.

Se utilizó una carga de trabajo de 5 MB, aproximadamente 500 documentos HTML de diversos tamaños, con un tamaño promedio de 10 K.

Todos los servidores fueron probados utilizando TCP/IP, provisto por el propio sistema operativo.

Los detalles específicos de cada uno de los servidores son descritos en el apéndice A.

Análisis de Desempeño

El desempeño es importante, sin embargo va a estar directamente relacionado con la magnitud de servidor que se desea implementar. Si nos referimos a una Intranet, estamos haciendo relación a un servidor que no va a tener miles (o tal vez ni siquiera cientos) de peticiones en un solo día.

Para el caso de Banco de México al pensar en el servidor de Internet estamos hablando quizá de miles de peticiones, ya que la información financiera pudiera llegar a ser de interés para todo el mercado mundial. Sin embargo, las peticiones al servidor de web no serán las mismas que tenga una página como podría ser la de Microsoft por dar un ejemplo. Es decir, estamos hablando de un servidor de tamaño medio, el cual podría atender las peticiones tanto de una Internet como una Intranet.

Los resultados de desempeño de los servidores mencionados fueron bastante satisfactorios, sin embargo lo que sobresalen son: IIS y NES.

Análisis de Seguridad

Conforme aumentan las transacciones sobre Internet la seguridad cobra mayor relevancia. El método más común de proveer seguridad es llamado: *Autenticación básica*, donde la restricción es en base de direcciones IP o nombre de dominio. Este tipo de autenticación es soportado por la mayoría de los servidores de web.

IIS y CBP son capaces de agregar una capa mas de seguridad sobre el propio sistema operativo mientras que NWS esta completamente integrado con los servicios propios de Netware (como sistema operativo de red).

La autenticación básica no es suficiente en la actualidad, una de las mejoras recientes sobre seguridad es la implementación de SSL, soportada por todos los servidores analizados.

Construcción de Aplicaciones

Una de las partes más importantes de un servidor de web, es la parte más difícil de ver. El ambiente de desarrollo de una aplicación y la consecuente conexión a una base de datos son aspectos críticos en la actualidad. Es difícil establecer un análisis sobre este punto debido a que involucra aspectos ajenos al servidor en si, como son las API's (Application Program Interface), el lenguaje de programación el DBMS, etc. Sin embargo podemos decir que el servidor que presenta la mayor compatibilidad con los productos de desarrollo del mercado actual es IIS.

Herramientas de Administración de Información

Es importante tener un panorama de la organización del sitio y herramientas que permitan identificar la validez de ligas internas y externas. LiveWare de NES, es una de las mejores opciones para realizar lo anterior, ya que presenta una interfaz simple y completa. Un producto con similares características es FrontPage, el cual no sólo representa una excelente herramienta de administración, ya que incluye un editor de HTML sumamente versátil y poderoso. FrontPage, es completamente compatible con IIS.

La tabla 3.1 muestra la comparación de los aspectos más importantes entre los servidores analizados.

Conclusión:

El servidor de web que cumple con las necesidades del Banco de México y ofrece la mayor compatibilidad con el equipo ya manejado en la institución así como los mejores niveles de rendimiento en comparación es IIS. Definitivamente NES es un producto tan bueno como IIS en toda su extensión. Sin embargo se ha especulado sobre la posible venta de NetScape Corp., siendo un punto importante para el Banco la solidez de la compañía que realiza cualquiera de los productos en él empleados.

Así también, IIS no tiene costo ya que viene disponible dentro de Windows NT, plataforma utilizada en Banco de México. IIS provee una fácil instalación y configuración, por sí mismo o vinculado con el resto de las herramientas de Microsoft, provee varias herramientas para la generación de datos dinámicos cuya fuente es una base de datos.

3.4.4.- Cliente

Después de aproximadamente seis meses de versiones beta, Microsoft Internet Explorer (IE) 4.0 fue dado a conocer. Similarmente, la última versión de Netscape Communicator Pro 4.03 era lanzada al mercado. De esta manera los dos, y tal vez únicos, browsers de gran desempeño son puestos a prueba en el campo informático y de comunicaciones. A continuación se realiza un análisis de las características más importantes en los aspectos que conforman al cliente⁶:

⁶ Basados en los criterios establecidos para análisis de navegadores web publicados en la revista PC Magazine, May 27 1997

Concepto / Servidor	CBP	ICSI/S	II/S	NE/S	NFTS	NWS	PEW	Apache	WSP	JWS
Generales										
Servidores Virtuales	S	N	S	S	S	N	S	S	S	S
Redirección Automática de URL	S	S	N	S	S	S	S	S	S	N
Múltiples Puertos	S	S	N	S	S	S	S	S	S	N
Servidor Proxy	S	S	N	N	N	N	S	N	N	N
Máquina de Búsqueda	S	N	S	S	N	N	S	N	S	N
Agente S/NMP incluido	N	N	S	S	N	N	N	N	N	N
Herramientas de desarrollo en HTML	S	S	S	S	S	S	S	N	S	N
Herramientas de Administración para el web	S	N	S	S	B	S	S	N	S	S
Configuración y Administración										
El servidor puede ser manejado desde Consola/Cliente de Red/Browser	S/N/S	S/S/S	S/S/N	S/N/S	S/N/S	S/S/N	S/S/S	S/S/N	S/S/N	S/N/S
Archivos de configuración almacenados en Registro/directorio	S/N	N/S	N/S	S/S	S/S	N/S	S/N	N/S	S/N	S/N
Conexiones										
Formato común de log CERN/NCSA	S	S	N	S	S	S	S	S	S	S
Archivos de Log personalizables	S	S	N	S	S	S	S	S	S	S
Conexión a ODBC/Bases de datos SQL	S/S	N/N	S/S	S/S	S/S	N/N	N/N	N/N	N/N	S/N

Table 3.1 Análisis de servidores

Concepto / Servidor	CBP	ICS/S	lIS/S	NES	N/FTS	NWS	PEW	Apache	WSP	JWS
Sistemas Operativos Soportados										
Windows NT	S	N	S	S	S	N	S	N	S	S
Windows 3 x/95	N/S	N/N	N/N	N/N	N/N	N/N	ND	N/N	N/S	N/N
Solaris	N	N	N	S	S	N	N	S	N	S
SunOS	N	N	N	N	N	N	N	S	N	N
NetWare	N	N	N	N	N	S	N	N	N	N
OS/2	N	S	N	N	N	N	N	N	N	N
Seguridad										
Autenticación Basical/ Challenge-respon/Se	S/N	S/N	S/S	S/S	S/S	S/N	S/N	S/N	S/N	N/N
Soporte para SSL 3.0	N	N	S	S	S	S	N	N	S	S
Control de Acceso por Dominio/IP	S/S	S/S	N/S	S/S	S/S	S/S	S/S	N/N	S/N	S/S
Desarrollo de aplicaciones										
CGI/M/CGI	S/S	S/N	S/S	S/S	S/S	S/N	S/N	S/S	S/N	S/N
ISAPI/NSAPI	S/N	N/S	S/N	N/S	N/S	N/N	S/N	N/N	S/N	S/N

Tabla 3.1 Análisis de servidores

El Browser

El aspecto más importante de un browser es su habilidad para leer páginas de web, ambos browsers muestran un rendimiento muy bueno en este aspecto, ciertamente un poco más rápida la lectura de IE sobre Communicator. Existe todavía una considerable inconsistencia para el soporte de Java Script, algunas páginas son desplegadas correctamente solo en IE otras únicamente en Communicator, no existiendo una clara ventaja de uno sobre el otro en este aspecto.

Ambos browsers despliegan el mismo tamaño de letra, el cual puede ser modificado a través de la barra de herramientas.

El aspecto del servidor

Analizar un browser no es demasiado complejo. Sin embargo, Communicator e IE 4.0 no son solo browsers. Son en realidad un conjunto de herramientas que ofrecen mayor capacidad que solo desplegar el contenido de un servidor de web. IE y Communicator están distribuidos en cerca de 40 Mbytes que incluyen herramientas de productividad personal tales como clientes de correo, editores de HTML, clientes "push" y aplicaciones de conferencia en tiempo real, lo cual hace la decisión un poco más compleja.

Es necesario considerar el servidor tan bien como el cliente. Particularmente en el caso de correo electrónico, cada aplicación por parte del cliente requiere un servidor.

Seguridad y Administración

Mission Control e IEAK (Internet Explorer Administration Kit) generalmente completan las mismas tareas administrativas, siendo IEAK 4.0 para Win95 y WinNT un producto mayormente definido y flexible. Esto es elemento parcial de la arquitectura de Microsoft, agregando la posibilidad de una instalación personalizada en el cliente. Esto permite a los administradores escoger que aplicación o aplicaciones desean instalar sobre los equipo del usuario.

En contraste, Communicator 4.0 permite solo algunas opciones de instalación personalizadas. De hecho, el conjunto principal de instalación incluye el browser, el cliente de correo, herramientas de desarrollo para HTML y un programa para conferencia, debiendo todos estos componentes ser instalados. Actualmente Netscape ofrece solo de manera independiente la instalación del Browser.

No existe probablemente ningún administrador de servidores de web que piense que IE 4.0 o Communicator van a resolver sus problemas de seguridad o proteger de manera total a sus clientes, pero la mayoría aceptamos un buen principio de seguridad en ambos productos.

Zonas de Seguridad, módulo de configuración de IE 4.0, proporciona a los administradores y usuarios mayor flexibilidad que NetScape, dando un control más fino en la personalización de las características de seguridad del browser. Mas aún, dicho módulo provee el contexto para los certificados de autenticación digital de la tecnología Microsoft.

Como estándar existen tres Zonas predefinidas: Internet, Intranet y Sites Confiables. Intranet usualmente consiste en sitios detrás del firewall cooperativo. Sites confiables son aquellos que ya se han identificado y no presentan ningún riesgo, Internet son todos aquellos que no pertenecen a ninguna de las dos opciones anteriores. Es posible definir la seguridad para cada zona como baja, media o alta pero también es posible generalizar las características de seguridad para cada zona y configurar directamente cada objeto como son Scripts, controles Active X, Cookies y Applets, y la forma en que éstos serán manipulados.

Zonas de Seguridad no es un dogma, sin embargo, ofrece a los administradores la posibilidad de configurar el entorno del usuario, haciéndolo mas seguro y simple de confrontar en una contingencia.

PUSH

La idea detrás de los canales push es que un proveedor pueda enviar información directamente al cliente. Netscape tiene la ventaja en este aspecto, con mas de 700 canales. Para mediados de 98 se espera que el número de canales provistos por IE y Communicator sea aproximadamente el mismo.

Una aplicación push puede llegar a saturar el disco. Ambos browsers ofrecen herramientas para controlar las actualizaciones y nuevos accesos, permitiendo establecer cuanta memoria cache aceptar para cualquier canal y que tan seguido se realizarán las actualizaciones del mismo.

IE 4.0 va un poco mas allá de las características básicas de configuración para los canales, configurando, si se desea, el manejo de imágenes, sonido, video, applets, y/o controles Active X en las actualizaciones. Así también en IE 4.0 es posible definir si la actualización es automática o solo será notificada al usuario.

Integración

Una característica importante sobre integración es Active Desktop de IE 4.0, lo que permite poder navegar en el propio disco como un ambiente de web a través del propio browser. El resultado es una rápida y más intuitiva forma de interactuar con la computadora.

Mensajería y otras aplicaciones

Communicator e IE 4.0 poseen ambos su propio cliente de correo, soportando también accesos estándares a POP3 e IMAP4. A través de Microsoft's Outlook Express se da un soporte adicional al acceso de MS-Mail.

Banco de México tiene programado el desarrollo de aplicaciones con Exchange Server y Outlook, la compatibilidad de este proyecto con la interfaz de IE 4.0 le otorga cierta ventaja para la decisión en el esquema de estandarización de cliente dentro de la Institución

Como mencionábamos anteriormente, no es posible separar los componentes de Communicator, por tal motivo es molesto para el usuario acostumbrado a utilizar MS Exchange (caso Banco de México) el accionar las ligas de correo dentro de una página de web y no activar su herramienta de correo acostumbrada.

Para la creación de páginas tanto Microsoft's Frontpage Express como Netscape's Composer son adecuados para el desarrollo simple de HTML pero no más allá de este.

Una de las mayores características de Communicator, no incluida en IE 4.0, es Netscape Calendar, la cual requiere Netscape's Calendar Server, su contraparte sería Outlook para IE 4.0, producto ya utilizado en el desarrollo de aplicaciones de comunicación en Banco de México

Interfaz

IE 4.0 ha mostrado grandes características de navegación así como una máquina virtual de Java muy rápida. La barra de herramientas permite una búsqueda completa sobre Favoritos, Historia, resultados de búsquedas y canales push con un importante grado de facilidad. IE 4.0 es todavía el ambiente Java más rápido sobre Windows y una excelente plataforma para desarrollos serios en este lenguaje.

Communicator mejora significativamente sobre Navigator 3.x obteniendo una mejor estabilidad y cliente de correo mas adecuado.

La tabla 3.2 muestra la comparación entre diferentes áreas como características de ambos browsers. La calificación esta basada en desempeño y facilidad de uso, obteniendo un resultado en base a la diferencia en estos tópicos con respecto a su competidor y a los estándares informáticos establecidos por el propio Banco de México.

Conclusión

A pesar de una gran funcionalidad en común, existen importantes diferencias entre estas dos herramientas. Para decidir sobre el aspecto del cliente, es necesario tomar en cuenta aspectos tales como: Infraestructura Tecnológica de los clientes y servidores, como esta configurado el sistema de correo y que tan importante es la tecnología Microsoft en el desarrollo de las páginas de web.

Communicator es una opción viable sobre todo en un ambiente de desarrollo heterogéneo (UNIX, MAC's, Windows). Es disponible para la mayoría de las plataformas. A diferencia, Internet Explorer no tiene el mismo nivel de integración con otras plataformas que aquel que presenta con Windows 95 o Windows NT. Microsoft se encuentra a poco tiempo de ofrecer IE 4.0 para Mac's, Windows 3.1 y UNIX (seguramente para cuando esto sea leído existirán ya, al menos, las versiones beta en el mercado).

Microsoft ofrece una solución de administración con "Internet Explorer Administration Kit" y la tecnología de Active Setup. Mission Control de NetScape es demasiado costoso y no tiene la flexibilidad de IEAK, es seguro la mejora de Mission Control por parte de NetScape en un futuro cercano.

Desde luego si no se tiene un plataforma Windows a 32 –bit, Communicator es la única opción y todavía la mejor. Sin embargo, en Banco de México todos los clientes son Windows 95, el desarrollo sobre Active Server y el robusto soporte para el desarrollo de controles Active X hacen a IE la opción más viable para la Institución.

Concepto	IE 4.0	Communicator
Funcionalidad		
Rendimiento de página	Excelente	Excelente
Herramientas de búsqueda	Excelente	Buena
Actualización y transferencia de archivos	Regular	Excelente
Personalización de la barra de herramientas	Excelente	Buena
Interfaz exclusiva del teclado	Excelente	Buena
Soporte del botón derecho del ratón	Excelente	Bueno
Marcas	Excelente	Bueno
Soporte de tipos de letra	Excelente	Bueno
Soporte Multimedia	Excelente	Bueno
Soporte para Java Script	Bueno	Bueno
Aplicaciones		
Cliente Push	Bueno	Bueno
Disponibilidad de Canales	Bueno	Excelente
Integración	Buena	Regular
Correo		
Importación de correo	Excelente	Buena
Libreta de direcciones	Buena	Buena
Personalización de la interface de correo	Excelente	Buena
Herramientas de Soporte de HTML		
Formato de imágenes	Bueno	Bueno
Formato de texto	Excelente	Excelente
Formato de ligas	Excelente	Excelente
Edición WYSIWYG	Excelente	Excelente

Tabla 3.2 Comparación de las principales características de IE y Communicator

3.5 Costo Estimado de la Implementación

3.5.1 Software - Hardware

Actualmente Banco de México cuenta con un equipo Net Strada 7000, al cual no será necesario realizar ninguna adecuación de espacio en disco o memoria, dicho servidor conjuntamente a la licencia de uso de Windows NT 4.0 asciende a un costo de 19,000 usd. Con la licencia de Windows NT se incluye IIS así como algunas utilerías del mismo. Por parte del cliente, el 95 % del equipo en Banco de México cuenta con Windows 95, los cuales ya incluyen Internet Explorer.

El espacio físico dentro del cual será implementado el servidor se encuentra en pleno funcionamiento con el resto de los servidores propiedad de Banco de México, por esta razón no existirá ningún costo adicional por espacio físico.

3.5.2 Comunicaciones

Por parte del área de comunicaciones es difícil calcular un costo exclusivo, ya que los diferentes dispositivos no son únicos de uso al servidor de web. Las variables involucradas en este servicio se encuentran definidas por: a) Renta de canal a TelMex, b) Renta al ISP (2,000 usd mensuales), c) Hardware invertido, d) Uso de Red local y e) Mantenimiento (10% del costo del equipo).

3.5.3 Recursos Humanos

Es necesario agregar al esquema anterior el costo de recursos humanos involucrados en este proyecto, desde el área de comunicaciones hasta aquellas personas que alimentarán la información dentro del servidor de web, dichos parámetros serán detallados en el capítulo 4.

DISEÑO Y DESARROLLO

El objetivo que tiene el presente capítulo es definir el plan de trabajo y división de actividades, ya establecido el software y hardware a utilizar, así como delimitar los parámetros que influyen de forma directa en el servidor de web, siendo parte de su entorno de operación.

4.1 Estructura de los Servicios Institucionales

Las aplicaciones con tecnología Internet para Banco de México son clasificadas en tres grandes grupos: 1) Aquellas aplicaciones o información que es de uso interno y exclusiva para la comunidad banxico, 2) Aquellas aplicaciones o información que son utilizadas por Banco de México y el Sistema Financiero e 3) Información para el público en general. Si analizamos estos tres aspectos podemos apreciar tres contextos diferentes, pero ya existentes dentro de la tecnología de web: 1) Intranet, 2) Extranet e 3) Internet.

El análisis tecnológico desarrollado en el capítulo anterior es completamente aplicable para cualquiera de los tres aspectos mencionados. La instalación y configuración de los servidores será la misma. Desde luego el punto físico de conexión es completamente diferente para cada uno de los servidores.

- **Intranet**

El servidor Intranet será físicamente conectado a un punto de la red Banxico, dicha conexión no podrá ser vista por equipos fuera de la red interna. El tipo de información a manejar estará directamente vinculada con las funciones internas del banco como organización: Servicios médicos, prestaciones, actividades administrativas, etc., siendo su ámbito de ejecución de carácter exclusivamente interno, pudiendo realizar operaciones que van desde difusión de información hasta tramitación en general.

- **Extranet**

El servidor Extranet estará conectado a la red propiedad del Banco y puede ser accedido desde cualquier terminal Banxico, sin embargo también podrá ser visto desde terminales conectadas al Sistema Financiero, es decir, estará conectado físicamente a una subred visible para el Sistema Financiero, siendo la información manejada en él, de uso para las dos entidades (Banco de México - Sistema Financiero). Dicha información podrá ir desde difusión de información hasta la posible ejecución de sistemas de información.

- **Internet**

El servidor de Internet podrá ser consultado desde cualquier terminal en el mundo conectada a Internet, desde luego este conjunto incluye tanto al Sistema Financiero como al personal Banxico. La información será de carácter internacional y totalmente pública.

No se descarta la posibilidad, en cualquiera de las tres clases de servidores, la existencia de un subconjunto de terminales con privilegios exclusivos, es decir, podrá existir información que solo será vista por un grupo selecto de personas. Esto último afectará las capas de seguridad internas que se tengan planteadas para cada servidor de web, que en esencia, funcionarán bajo un mismo esquema, esta es la ventaja de tener una plataforma homogénea y estándar para un servicio como lo es Internet.

4.2 Plan de Implementación

El plan de implementación describe las etapas en las cuales está dividido el proyecto, así como la duración de cada una de ellas. Dicho plan contempla a los tres servidores mencionados anteriormente (Intranet, Extranet e Internet), con la única diferencia en el aspecto concerniente a la conexión física, donde cada servidor ocupa un punto diferente en la red de Banco de México. Es decir, para los servidores, su proceso de instalación y configuración será en esencia idéntico, para la conexión física se seguirán procesos diferentes, una vez realizada esta, el proceso continuará siendo el mismo para los tres servidores. La interfaz con su entorno se verá alterada en función de su localización física.

El plan de implementación se clasifica en las siguientes etapas:

a) **Instalación del software y hardware requerido¹**

La instalación del software se efectuará en dos equipos, los cuales serán utilizados para las pruebas piloto descritas posteriormente. El primero de éstos, funcionará a manera de cliente y el otro como servidor, éste último es un equipo NetStrada 7000 con las características descritas en el punto 3.4.2. En dicho servidor se instalarán los siguientes componentes:

- Sistema Operativo WinNT 4.0

¹ Basado en recomendaciones de Microsoft, fuente <http://www.microsoft.com>

- Option Pack 4.0
 - IIS 4.0 (previa instalación de IIS 3.0)
 - Transaction Server
 - Index Server
 - Certificate Server
 - Data Access Component
 - Site Server Express
 - Message Queue Server
 - ICS for RAS
 - Administration and development components
- Software de red
 - Protocolos de comunicación

Se utilizará una computadora con las siguientes características para ser utilizada como cliente de pruebas:

- Computadora Olivetti modelo PC 100
- 32 Mb en memoria
- 1.2 GB en disco duro

Es necesario hacer notar que estas son las características de un equipo medio dentro de Banco de México. Dicho equipo existe (no involucra ningún gasto) y se encuentra en operación dentro de la red del Banco. Se contempla su instalación a partir de cero para evitar cualquier causa de error ajena al objetivo de la prueba.

Así también es necesario mencionar que, para poder realizar la instalación de IIS 4.0 es necesario instalar IIS 3.0, ya que IIS 4.0 es una actualización y no un producto. La descripción de la instalación de IIS 3.0 puede ser obtenida de servidor de web de Microsoft en la dirección <http://www.microsoft.com>

El cliente tendrá al menos los siguientes componentes instalados:

- Sistema operativo Windows 95
- Software de red
- Internet Explorer 4.01 SP1

b) Conexión física a la red Banxico

Esta etapa estará compuesta por las siguientes actividades:

- Altas de direcciones IP en ambos equipos (cliente - servidor)
- Alta del servidor en el DNS (servidor)
- Conexión física a la red
 - Red Banxico (Intranet)
 - Red Banxico -Segmento compartido con el sistema financiero (extranet)
 - Zona desmilitarizada (Internet)²
- Pruebas de comunicaciones

² Zona de la red con características suficientes para que se permita acceso al resto del mundo a través de un browser.

c) Mecanismos de Administración y Control

- **Estructura de directorios**
Los servidores de web establecen un directorio virtual a manera de raíz, debajo del cual deberán ser creadas las carpetas con información, estas carpetas tendrán un orden y una nomenclatura específica.
- **Monitoreo de servicios y desempeño**
Serán monitoreados el desempeño del servidor (conexiones, porcentaje de uso, etc.), así como el correcto funcionamiento de los servicios básicos: www y ftp.
- **Administración del servidor,**
El aspecto crucial en cualquier administración es la seguridad (analizada en el punto 4.3) y los estándares a implementar.
- **Administración de la información**
Existirá un control para el alta de la información, con el objetivo de proporcionar la independencia necesaria al desarrollador con respecto del administrador (webmaster) sin perder el orden y la homogeneidad de las páginas.

e) Esquemas de Seguridad

- **Definición de niveles y estructura de seguridad**
Los niveles de seguridad serán variados en función del tipo de información que se este manejando, sin embargo es necesario establecer una estructura de seguridad básica para cualquier tipo de página.
- **Integridad de la información**
Se vigilará que la información siempre sea funcional, y en caso de la existencia de procesos funcionando detrás de una página, que esta se presente de forma adecuada y precisa.
- **Procesos de respaldo y replicación**
Se tienen contemplado que los respaldos se realicen de forma automática a cinta dos veces por día, conservando un histórico de hasta dos semanas. Por otro lado, y de forma también diaria, el servidor de web replicará a un servidor alterno, de tal forma que, en caso de existir una contingencia, será posible restablecer el servicio en no más de 15 minutos.

f) Formas de Acceso

Con el objetivo de proporcionar mayor facilidad en la navegación, será posible llegar a la misma información por medio de tres formas diferentes:

- **Estructura**
Cualquier tipo de información podrá ser accedido en base a la fuente que la genera, es decir el usuario podrá tener acceso a la información por una parte específica de la organización a través de una sola página.
- **Servicio**
El acceso por servicio será independiente de la fuente de información, es decir, existirán rubros definidos que traten de contemplar en la medida de lo posible toda la información que contiene el servidor de web, de esta manera el usuario final tendrá acceso a la información, sin importar quién sea la fuente de la misma.
- **Diccionario de datos**
El diccionario de datos definirá las diversas formas para acceder un mismo tema, esta diversidad estará definida por el dueño de la información (persona que conoce esta) y será mejorada en base a la interacción con el usuario final.

La tabla 4.1 muestra el detalle de tareas y los recursos asignados, una gráfica de la cual se puede extraer la duración de cada tarea y la secuencia que debe ser seguida para cada una de ellas, tratando de evitar que éstas se traslapen una con otra.

La tabla 4.2 describe los costos asociados a cada tarea y, por tanto, el costo de material humano para el proyecto. Es necesario mencionar que se contemplan solo costos directos, ya que obtener un costo exacto es necesario considerar factores como: luz, inmuebles, depreciación de equipo, etc.

Similar a 4.2, la tabla 4.3 describe la definición de cada recurso y su costo asociado por hora, por último, la tabla 4.4 se proporciona a manera de resumen del proyecto, destacando tiempo, recursos y costo directo, este último dividido como material humano y equipo.

Plan de Implementación

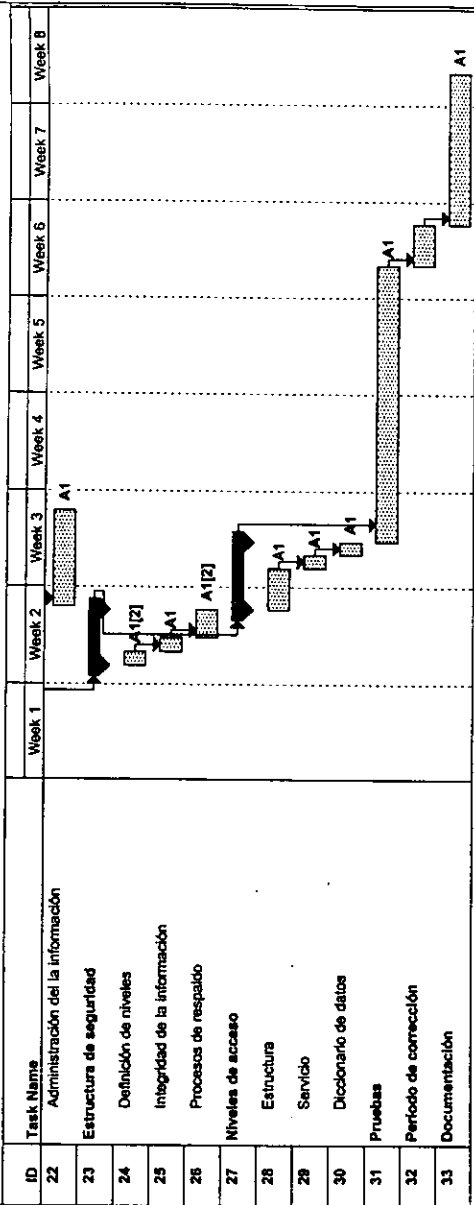
ID	Task Name	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
1	Instalación del Software y Hardware	[Task bar spanning Weeks 1-2]							
2	Instalación del servidor	[Task bar spanning Weeks 1-2]							
3	Sistema operativo WinNT	[Task bar spanning Weeks 1-2]							
4	Instalación IIS 3.0	[Task bar spanning Weeks 1-2]							
5	Option Pack 4.0	[Task bar spanning Weeks 1-2]							
6	Software de red	[Task bar spanning Weeks 1-2]							
7	Instalación de un cliente	[Task bar spanning Weeks 1-2]							
8	Sistema operativo Win95	[Task bar spanning Weeks 1-2]							
9	software de red	[Task bar spanning Weeks 1-2]							
10	Internet Explorer 4.0	[Task bar spanning Weeks 1-2]							
11	Conexión Física (servidor)	[Task bar spanning Weeks 1-2]							
12	Altas de direcciones IP	[Task bar spanning Weeks 1-2]							
13	Alta de el servidor en el DNS	[Task bar spanning Weeks 1-2]							
14	Conexión Física (Red Banxico)	[Task bar spanning Weeks 1-2]							
15	Conexión Física (Segmento Sistema Financiero)	[Task bar spanning Weeks 1-2]							
16	Conexión Física (Zona Desmilitarizada)	[Task bar spanning Weeks 1-2]							
17	Pruebas de comunicaciones	[Task bar spanning Weeks 1-2]							
18	Mecanismo de Administración y Control	[Task bar spanning Weeks 1-2]							
19	Estructura de directores	[Task bar spanning Weeks 1-2]							
20	Monitoreo de servicios	[Task bar spanning Weeks 1-2]							
21	Administración del servidor	[Task bar spanning Weeks 1-2]							

Project: www/MPP
Date: Ft 12/02/99



Tabla 4.1 Detalle de Tareas

Plan de Implementación



Project: www.MPP
Date: Fri 12/02/99

Tabla 4.1 Detalle de Tareas

Plan de Implementación

ID	Task Name	Resource Names	Cost
1	Instalación del Software y Hardware		\$1,134.00
2	Instalación del servidor		\$924.00
3	Sistema operativo WinNI	A1	\$336.00
4	Instalación IIS 3.0	A1	\$210.00
5	Option Pack 4.0	A1	\$336.00
6	Software de red	A1	\$42.00
7	Instalación de un cliente		\$210.00
8	Sistema operativo Win95	A1	\$126.00
9	software de red	A1	\$42.00
10	Internet Explorer 4.0	A1	\$42.00
11	Conexión Física (servidor)		\$2,142.00
12	Alias de direcciones IP	C2	\$21.00
13	Alias de el servidor en el DNS	C2	\$21.00
14	Conexión Física (Red Banxico)	A1,C1,C2	\$252.00
15	Conexión Física (Segmento Sistema Financiero)	A1,C1,C2	\$252.00
16	Conexión Física (Zona Desmilitarizada)	A1,C1,C2	\$252.00
17	Pruebas de comunicaciones	A1,C2	\$1,344.00
18	Mecanismo de Administración y Control		\$4,536.00
19	Estructura de directores	A1	\$168.00
20	Monitoreo de servicios	A1 Z1	\$672.00
21	Administración del servidor	A1 Z1	\$2,016.00
22	Administración del la información	A1	\$1,680.00
23	Estructura de seguridad		\$2,352.00
24	Definición de niveles	A1 Z1	\$672.00

Tabla 4.2 Costo Total y por recurso

Plan de Implementación

ID	Task Name	Resource Names	Cost
25	Integridad de la información	A1	\$336.00
26	Procesos de respaldo	A1[2]	\$1,344.00
27	Niveles de acceso		\$1,008.00
28	Estructura	A1	\$336.00
29	Servicio	A1	\$336.00
30	Diccionario de datos	A1	\$336.00
31	Pruebas	A1	\$4,704.00
32	Periodo de conexión		\$0.00
33	Documentación	A1	\$2,352.00

Tabla 4.2 Costo Total y por recurso

Definición de Recursos	Nombre del Recurso	Inicial	Costo/h
Analista de Sistemas	A1	A	N\$42.00/h
Especialista en Comunicaciones	C2	C	N\$42.00/h
Especialista en Comunicaciones	C1	C	N\$42.00/h

Tabla 4.3 Definición de Recursos y costo por hora

Fechas			
Inicio	19/05/98	Término	23/06/98
Duración			
Calendarizado	35d		
Trabajo			
Calendarizado	280h		
Costo			
Calendarizado	29526 - 171000		
Tareas			
Tareas por empezar	31		

Tabla 4.4 Resumen del proyecto

4.3 Seguridad

Para Banco de México la seguridad de los servidores de web esta compuesta de 5 capas: 1) Un sistema de filtros a través de un ruteador, 2) Firewall, 3) Sistema Operativo del servidor de web (Windows NT), 4) Seguridad proporcionada por el servidor de web e 5) Internet Security Scanners. La capa 1 y 2 no son funcionales para el servidor de Intranet y Extranet, no así las capas 3, 4 y 5.

Existen tres puntos que podrían llegar a ser vulnerables sobre la base de la figura 4.1. El primero de ellos es la posibilidad de un ataque externo a través de Internet, el segundo, un ataque interno, cuyo origen es la propia red Banxico, y por último, existe la posibilidad de un ataque directo desde la consola de cualquiera de los tres servidores de web. Cada una de éstas capas tiene su propio nivel de acoplamiento en las capas del modelo OSI ya descritas en el capítulo anterior.

A continuación se analizará cada una de las cinco capas de seguridad y su repercusión directa para uno o más de los puntos de vulnerabilidad.

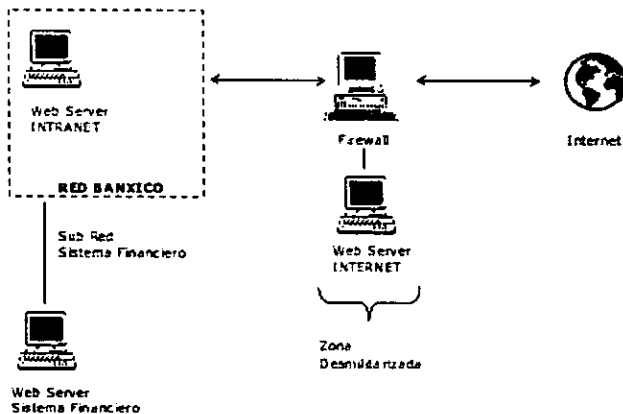


Figura 4.1 Esquema general de seguridad Servidores de web Banxico

4.3.1 Sistema de filtros a través de un ruteador

Los ruteadores convencionales ofrecen un mecanismo que aumenta la funcionalidad normal de un ruteador, permitiendo el procesamiento de paquetes de información. A este proceso se le denomina "Filtrado de Paquetes", el mecanismo requiere que un administrador indique la manera en que el ruteador dispondrá de cada paquete. Por ejemplo, se puede elegir filtrar todos los paquetes que provienen de una dirección en particular o aquellos utilizados por una aplicación en particular, mientras se permite el acceso de otros paquetes a su destino.

El "Filtrado de paquetes" no guarda un registro o histórico de paquetes previos. En su lugar, considera cada paquete de forma independiente. Cuando un paquete llega, el ruteador analiza el paquete por medio de sus filtros antes de realizar cualquier otro proceso. Si el filtro rechaza el paquete, éste es eliminado inmediatamente por el ruteador.

Debido a que TCP/IP no dicta un estándar para el filtrado de paquetes, cada ruteador es libre de ser configurado con sus propias características a este respecto. Algunos ruteadores permiten la configuración independiente de cada una de sus interfaces, mientras otros solo permiten una configuración global para todas sus estas. Usualmente, el administrador define cualquier combinación de direcciones IP origen, direcciones IP destino, protocolo, número de protocolo origen y número de protocolo destino.

Este sistema, para Banco de México tiene una función principal sobre la posibilidad de un ataque proveniente de Internet. El ruteador, al recibir el paquete, lo abre, revisa y arma, identificando con esto si es un servicio válido (vinculado directamente con una capa del modelo OSI - ftp por ejemplo), el número de puerto que se trata de acceder y si proviene de una dirección IP válida.

Para ser efectivo es necesario especificar lo que es permisible y dejar el resto fuera, debido a que si partimos del esquema contrario, cualquier omisión podría verse reflejada en un potencial hoyo de seguridad. El filtrado de paquetes que permite al administrador especificar que paquetes admitir, en lugar de cuales rechazar, puede hacer las restricciones fáciles de especificar.

En caso de que el ruteador determine que es una petición no válida, telnet por ejemplo, el paquete es eliminado, regresando el ruteador a su estado de "escucha". En caso contrario, lo canaliza a su destino inmediato: el firewall.

4.3.2 Firewall³

El filtrado de paquetes siempre ha sido una simple forma de no permitir acceso a paquetes no deseados de información, leyéndolos, y rechazando aquellos que no cumplan con el criterio programado en el ruteador.

Desafortunadamente, el filtrado de paquetes no es suficiente para garantizar la seguridad de una servidor de web. Un servidor puede ser amenazado por muchas nuevas innovaciones de los protocolos que tienen la habilidad de traspasar aquellos filtros con muy poco esfuerzo. Los firewalls convierten el aspecto de seguridad en una plataforma mucho más allá del filtrado de paquetes.

El firewall, en el sentido más sencillo, es un ruteador o computadora colocado entre la red interna y el mundo de Internet. Su propósito, como una compuerta de seguridad, es proveer seguridad a aquellos componentes dentro de la misma, así también controlar quién (o que) esta permitido a entrar o salir dentro de este ambiente protegido.

Un firewall debe funcionar como un punto único de acceso. Por esto muchas ocasiones, se encuentran firewalls integrados con un ruteador.

La selección del firewall fue realizada en base al Hardware ya instalado, el conocimiento del personal de comunicaciones en Banco de México, el costo y las posibilidades del mercado.

Con el firewall es posible lograr la protección de conexiones arbitrarias y establecer herramientas de rastreo, las cuales pueden ayudar a evaluar los esquemas de "logs", como origen de las conexiones, la cantidad de tráfico en el servidor e incluso establecer si existieron intentos de violación a la seguridad.

³ Fuente: Protecting your web site with firewalls, Goncalvez, Ed. Prentice Hall

De ninguna manera el firewall es infalible, éste permite aumentar la seguridad, no garantizarla.

En la institución se analizaron firewalls comerciales, comúnmente denominados *OS shell*, los cuales son instalados sobre el sistema operativo. A pesar de combinar filtrado de paquetes con aplicaciones *proxy* capaces de monitorear datos y comandos, un *OS shell* no cumple con las expectativas de seguridad de la Institución. No sólo sus configuraciones no son visibles a los administradores, configurándolos a un nivel de kernel, también se fuerza la inclusión de herramientas extras para ayudar a su completa administración.

Un firewall estático es aquel que permite cualquier servicio a menos que este sea expresamente negado o niega cualquier servicio a menos que éste sea expresamente permitido, a diferencia, un firewall dinámico permite/niega cualquier servicio cuando y cuanto tiempo sea determinado, este es el modelo utilizado por Banco de México.

4.3.3 Sistema Operativo: Windows NT

Los administradores de sistemas en UNIX han aprendido en décadas como configurar UNIX para sobrevivir en un ambiente hostil y abierto como lo es ahora Internet. Conforme Internet aumente en su campo de operación, en ese mismo ambiente hostil, los administradores de NT tendrán que desarrollar técnicas similares a las aprendidas por sus contrapartes en UNIX.

El esquema de seguridad sobre NT tiene aplicación también para el servidor de web interno, Intranet, y cubre la posible amenaza de un ataque interno, que, si analizamos, podría llegar a ser incluso más peligroso que uno de tipo externo, ya que el usuario interno conoce el esquema general de la red, el tipo de direcciones IP e incluso el lugar físico del equipo.

A continuación se presenta un análisis de seguridad, el cual, es implementado en los tres servidores de web del Banco.⁴

Uso de NTFS, no FAT

Los volúmenes de NTFS (NT File System) son aplicables al control y acceso de listas (Access Control List - ACL) para archivos y directorios; estos controles trabajan en conjunción con permisos sobre directorios compartidos. El volumen FAT (File Allocation Table) soporta solo el último nivel de seguridad. Tiene mayor ventajas el establecer no uno, sino varios niveles de seguridad cuando estos se encuentran disponibles, por tal motivo se utilizó NTFS.

⁴ Basada en la publicación Resource Kit of WinNT, Microsoft

Si NTFS ACL's proporciona un acceso completo sobre la red a una cierta partición, pero el permiso de "compartir" (share) da solo acceso de lectura, entonces el acceso real y definitivo es solo de lectura. Windows NT toma la intersección de NTFS ACL's y permisos de "compartir".

Renombrar la cuenta de administración

La mayoría de los ataques a un servidor inician bajo el método de "fuerza bruta", es decir tratar en base a cientos de intentos de adivinar alguna contraseña. Es posible configurar el equipo para que después de tres intentos rechace totalmente la cuenta, sin embargo esto último no funciona sobre la cuenta más peligrosa en una red: "Administrator". De esta forma alguien que trate de adivinar la contraseña deberá adivinar primero el nombre de la cuenta.

Así también es recomendable inhabilitar la cuenta de GUEST sobre cualquier sistema de conexión a Internet y utilizar solo la cuenta IUSR_ *nombredelcomputador* para acceso anónimo y asegurar que el grupo "everyone" no tiene acceso en directorios de relevancia.

Activación de la auditoría

Una forma de realizar esto es recolectar suficiente información pero nunca demasiada. Es posible auditar tanto éxitos como fallas de diversas operaciones, siendo estas últimas menores en cantidad que los primeros, sin embargo, más interesantes desde una perspectiva de seguridad. La figura 4.2 muestra una posible combinación en las operaciones de auditoría.

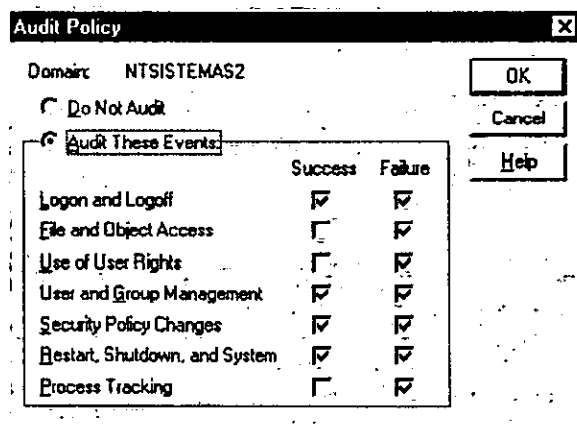


Figura 4.2 Parámetros de auditoría recomendados

Inhabilitar NetBIOS sobre TCP/IP

NetBIOS es el protocolo de redes de Windows, si éste, sobre TCP/IP se encuentra habilitado se corre el riesgo de permitir el acceso a la red interna, ya que NetBIOS no esta capacitado por si solo a hacerlo, pero TCP/IP si lo esta. La ventaja en este sentido es que Windows NT provee un control muy preciso acerca del uso de NetBios sobre TCP/IP.

Inhabilitar puertos no necesarios

En el sentido estricto, para lograr una funcionalidad sobre Internet sólo es necesario mantener habilitados dos puertos: 21 de ftp y 80 de http. Desde luego podrían llegar a existir aplicaciones que necesiten mantener habilitado un puerto, sin embargo es preciso establecer un equilibrio entre seguridad y desempeño y tratar de mantener habilitados solo aquellos puertos que sean estrictamente necesarios.

Eliminar el permiso de "acceso desde red"

NT permite que cualquier persona dentro de la red pueda ver e intentar establecer comunicación con el servidor en base a el usuario "everyone". Por tal motivo es recomendable eliminar el derecho de "Access from Network" a este usuario y aun mantener el servicio de web funcionando perfectamente.

El servidor de FTP, el cual esta incorporado con NT, podría llegar a presentar problemas en este esquema debido a su requerimiento de realizar "log-on" sobre la red. Sin embargo, el servicio de FTP, el cual realiza este mismo proceso, no se ve afectado por el cambio de privilegios en el usuario "everyone".

4.3.4 Servidor de Web: Internet Information Server

La seguridad aislada de IIS realmente es mínima, sin embargo, la combinación de características entre IIS y Windows NT aumentan considerablemente la seguridad proporcionada por el servicio de www, ftp y gopher.

A continuación se describen los aspectos a considerar en el esquema de seguridad planteado⁵:

Control de Acceso Anónimo

El acceso de WWW, FTP y gopher es anónimo para IIS, es decir, la petición por parte del cliente no contiene un nombre de usuario como tampoco una contraseña. Lo anterior ocurre en los siguiente casos:

- Un acceso a través de FTP con el usuario "anonymous"
- Todas las peticiones al servicio de gopher
- Una petición a través de un browser, la cual no contiene un nombre de usuario y contraseña en el encabezado de HTTP (servicio estándar)

⁵ Basado en la publicación IIS Resource Kit, Microsoft

A pesar de que el usuario no está conectado como un usuario identificado, es posible controlar y monitorear el acceso anónimo. Cada servicio en Internet tiene asignado un usuario y contraseña de Windows NT, la cual es utilizada para procesar las peticiones anónimas. Cuando una de estas peticiones es recibida, el servicio define la configuración del usuario como su acceso anónimo. La petición tiene éxito si el usuario de acceso anónimo tiene permisos suficientes para acceder el recurso solicitado, esto es determinado por el ACL. Si el usuario anónimo no tiene permiso suficiente, la petición es rechazada. Es posible configurar el servicio de WWW para responder a una petición anónima fallida requiriendo usuario y contraseña, este proceso es denominado "Autenticación".

La cuenta *IUSR_nombre_del_equipo* es automáticamente creada durante la instalación de IIS. Por definición, todas las peticiones de web utilizan esta cuenta, la cual permite solo la autenticación local en el servidor, permiso necesario para ejecutar el servicio de FTP.

No es conveniente proporcionar el permiso de autenticación local al usuario *IUSR_nombre_del_equipo*.

Controlando Acceso por Usuario o Grupo

Es posible controlar el acceso al servidor de web utilizando el Administrador de Usuarios de Windows NT para especificar a que usuarios o grupos de usuarios le es permitido la conexión al servidor.

El servicio de WWW provee dos formas de autenticación: básica y Windows NT Challenge Response (NTLM). La autenticación básica no encripta las transmisiones entre el cliente y el servidor.

El servicio de FTP soporta solo autenticación básica, por lo tanto, el servidor es más seguro si solo se permiten conexiones anónimas.

Establecer Permisos en Carpetas y Archivos

El acceso a carpetas y archivos es controlado de dos formas:

- Estableciendo permisos en NTFS
- Estableciendo permisos en el Administrador de los Servicios de Internet.

Es conveniente que los documentos sean colocados en particiones de NTFS. Es posible limitar el acceso a porciones al sistema de archivos (file system) por usuarios y servicios específicos utilizando NTFS. Resulta una buena idea aplicar los permisos de ACL para los archivos de cualquier servicio de publicación en Internet.

La lista de permisos sobre ACL es configurada utilizando el explorador de Windows. El sistema de archivos de NTFS proporciona un control muy fino sobre los archivos, permitiendo accesos y definiendo el tipo de éstos.

Existen tres tipos de acceso posible sobre carpetas:

- **Read:** Es posible leer los documentos del directorio pero no así cambiarlos o adicionar nuevos.
- **Execute:** Con este permiso un usuario puede iniciar aplicaciones o scripts contenidos en el directorio correspondiente.
- **Requiere de un canal SSL:** Cuando la opción de SSL es instalada en el servidor (mas adelante se explicará SSL) esta opción es disponible para establecer transmisiones privadas de información.

Estableciendo Acceso al Directorio de WWW

Cuando se crea un directorio de publicación para servicios de WWW (carpeta) en el Administrador de Servicios de Internet, es posible establecer los permisos para el directorio hogar definido o el directorio virtual, y todas las carpetas contenidas en este.

Secure Sockets Layer (SSL)

IIS ofrece el soporte para proveer una capa de seguridad de datos entre el protocolo de servicio (HTTP) y TCP/IP. Esta capa de seguridad, conocido como SSL, provee la encriptación de los datos, la autenticación del servidor, y mensajes de integridad para una conexión TCP/IP. Este tipo de seguridad provee las siguientes características:

- La encriptación asegura que los datos no serán leídos por alguien más que el servidor y el cliente que han negociado el canal de seguridad.
- La integridad de los datos asegura que estos serán transferidos sin alteración
- Si se utiliza autenticación básica (donde normalmente la contraseña es enviada como texto plano), SSL mejora este nivel de seguridad al encriptar la información del cliente antes de ser transmitida.

Para habilitar la seguridad SSL sobre un servidor de web es necesario realizar los siguientes pasos:

- Generar las capas de SSL
- Solicitar un certificado a una autoridad certificadora como Verisign (www.verisign.com)
- Instalar el certificado en el servidor
- Activar la seguridad SSL sobre el servicio de WWW.

4.3.5 Internet Security Scanners⁶

Las herramientas de exploración son programas que fueron diseñados para auxiliar a los administradores de red en la detección de hoyos de seguridad y otros problemas en las redes. Un tipo de herramienta de exploración se conecta a un sistema determinado e inicia el proceso de exploración.

⁶ Fuente: *Protecting your web site with firewalls*, Goncalvez, Ed. Prentice Hall

Un servidor funcionando sobre el protocolo TCP/IP, caso específico de un servidor de web, posee varios puntos de acceso denominados puertos. Un puerto es por donde un servicio en particular como FTP o HTTP realiza conexiones con usuarios externos. Por ejemplo, cuando se realiza una conexión a un servidor de web sobre Internet, la conexión tiene lugar en el puerto 80 del servidor. Los servidores de FTP utilizan el puerto 21 para este servicio⁷. Algunas aplicaciones abren puertos pero no los cierran, creando un hoyo potencial de seguridad. Por ejemplo un "hacker"⁸ puede utilizar TELNET para intentar penetrar un firewall a través de un puerto activo que ha sido dejado abierto por algún proceso previo. Desde luego, algunos puertos deben permanecer abiertos como es el caso del puerto 80 para servidores de web. La estrategia es: bloquear todos los puertos y entonces abrir solo aquellos necesarios.

El administrador está facultado a utilizar las herramientas de exploración para identificar servicios ejecutándose de manera no autorizada.

Desafortunadamente los *hackers* pueden utilizar este mismo tipo de herramientas para tratar de identificar potenciales hoyos de seguridad identificando aquellos servidores que pueden ser objetivo de un ataque.

Actualmente las herramientas de exploración son capaces de detectar cuando un sistema es explorado por un usuario no autorizado. Sin embargo, según C. Klaus miembro de "Internet Security Systems", este tipo de detección puede ser una falsa alarma, ya que es necesario que la herramienta de exploración realice una conexión completa para poder ser identificada, siendo que algunos intrusos utilizan una técnica denominada "half-open" para detectar puertos abiertos, la cual no realiza una conexión completa.

Las dos herramientas más comunes para la exploración de servidores son: SATAN (Security Administrator Tool for Analyzing Networks) e Internet Scanner SafeSuite (ISSS).

⁷ El servicio de FTP puede ser implementado sobre un servidor de web y el puerto de uso será siempre el 21.

⁸ Hacker es el término utilizado para hacer referencia a las personas que intentan violar la seguridad de un sistema de cómputo.

IMPLANTACIÓN Y PRUEBAS

Para el presente capítulo se analizarán todos los aspectos necesarios para realizar la implantación de los servidores de web. Se tomarán en cuenta las características del lugar físico donde operarán los servidores, realizando un plan de prueba y capacitación, así como el proceso de respaldo y replicación de la información.

5.1 Preparación del lugar físico

En relación con la preparación del lugar físico se deben considerar las características generales de seguridad; aspectos físicos tales como las paredes y el techo, piso falso, iluminación, control de temperatura, etc. Banco de México cuenta ya con instalaciones de este tipo.

Dentro de los principales elementos a considerar tenemos:

Puertas de Acceso

- Acceso restringido al personal
- Autorización sobre la base de los derechos otorgados a la credencial del Banco
- Puertas de doble hoja y de 1.6 mts de ancho por hoja.
- Salida de emergencia

Paredes y Techo

- Paredes de pintura plástica lavable.
- Techo y placas de plafón.
- Se utilizan placas metálicas o de madera prensada para el piso falso con soporte y amarres de aluminio.
- Altura entre piso y plafón de aproximadamente 2.70 y 3.30 mts

Piso Falso

- Aisla los cables de comunicación entre la unidad central de proceso y los dispositivos periféricos de conexión y cables de alimentación eléctrica.
- El espacio entre los dos suelos actúa como una cámara plena de aire
- Altura de 60 cm.
- Elaborado de material sintético resistente al fuego
- Soportado por pedestales
- Cubierto con pintura antipolvo
- Se considera la resistencia eléctrica transversal de recubrimiento del piso falso para evitar cargas electrostáticas.

Iluminación

- El área de máquinas se mantiene a un promedio mínimo de 450 luxes a 70 cm. del suelo
- No existe penetración de luz solar directa.
- Son diferentes las fuentes de alimentación y equipo de cómputo.
- Del 100% de iluminación, se distribuye el 25% para iluminación de emergencia.

Vibraciones

- Se evita todo tipo de vibración.
- Si existen vibraciones superiores a las normales, estas se estudian antes de colocar cualquier equipo.

Acústica

- El suelo amortigua la transmisión de vibración de otras áreas.
- Las paredes evitan que el ruido pase de lugares adyacentes.
- Las puertas se mantienen siempre cerradas.

Aire Acondicionado

- Disipación térmica de las máquinas.
- Disipación térmica de personas.
- Las cargas caloríficas del equipo de computo y sus periféricos las proporciona el proveedor del equipo y se especifican comúnmente en BTU/hora o en Kcal/hora.
- La cantidad de aire requerida por los ventiladores del equipo es proporcionada de igual forma por el proveedor, por lo general en m³/h.
- La alimentación del equipo es directa de la planta de generación de energía eléctrica para emergencia; no se conecta la salida del equipo al No-Brake, ya que por el encendido y apagado automático de motores y compresores se podría ocasionar una disminución en el voltaje y ruido eléctrico al equipo de cómputo.

Condiciones de Temperatura y Humedad

- Son indicadas por el proveedor del equipo.
- Cifras aproximadas: Rango de temperatura entre 16 y 20 °C.
- Humedad relativa (HR) de 20% a 80%.
- Cuando el aire frío es inyectado a los equipos su temperatura no es inferior a 17 °C y su HR no es superior a 80%.

Filtros

- Se utilizan filtros de tipo absoluto con una eficiencia del 99% sobre partículas de 3 micrones.
- El aire de renovación o ventilación es tratado antes de ser introducido en la sala, tanto en temperatura y humedad como en filtrado.

Distribución del aire de la sala

- Los componentes de las máquinas se refrigeran mediante la circulación rápida del aire por ventiladores.
- La entrada del aire se efectúa por debajo de las máquinas a través de un sistema de rejillas.
- El aire de ventilación es en función del volumen de la sala. Se proyecta para obtener de 1.5 a 2 renovaciones por hora y para crear una sobrepresión que evita la entrada de polvo.

Distribución del aire a través del piso falso

- El espacio entre el suelo del edificio y el piso falso se utiliza como una cámara plena de aire.
- El aire de la sala es descargado a través de rejillas en el suelo.
- El aire es retornado a la unidad acondicionadora a través de rejillas en el techo.
- El sistema tiene controladores de temperatura de aire.
- Se cuenta con un sistema de recalentamiento para controlar la humedad relativa del aire antes de que éste entre a la sala.
- Las rejillas y retornos están colocados a manera de no crear tiros de aire frío o caliente.

Ductos

- No existe desprendimiento de partículas al paso del aire.
- No tienen revestimientos internos de fibras.
- Ningún objeto obstruye los ductos.

Protección contra incendios

- Las paredes, techo falso y piso son incombustibles.
- El techo de la sala y área de almacenamiento de discos y cintas es impermeable.

- Existen detectores de humo.
- El sistema de detección de humo no interrumpe el paso de corriente eléctrica al equipo de computo.
- Presencia de extintores portátiles de CO₂

Almacenamiento de Información

- Las cintas, discos magnéticos y CD's se almacenan en una sala independiente.

Instalación eléctrica.

- Se comprobaron los voltajes de trabajo especificados por el proveedor para los equipos.
- La tolerancia en tensión no es mayor de 10% ni menor de 8% de la tensión nominal que especifica el fabricante del equipo de computo.
- La tolerancia en frecuencia es de 0.5 Hz.
- La variación en voltaje entre fase no es mayor de 2.5% de la media aritmética de las tres fases.
- Respecto al contenido de armónicas el máximo es inferior al 5% con el equipo desconectado.
- La acometida de energía eléctrica que alimenta al equipo de computo es completamente independiente y no recibe ninguna otra carga a fin de evitar interferencias.
- La acometida llega desde el equipo de fuerza ininterrumpida y de ahí se alimenta a un tablero de distribución situado en un lugar visible y accesible desde cualquier punto de la sala.
- La toma de tierra física es independiente, con una resistencia total de 3 ohm que incluye conductor más electrodo.
- Las terminales, microcomputadoras e impresoras, localizadas en la sala de computo, están alimentadas por energía eléctrica regulada.

5.2 Plan de pruebas¹

El propósito de esta sección pretende determinar las etapas y metodología que se emplearán para que el sistema sea probado, de tal manera que el usuario cuente con una herramienta que contenga un margen de error mínimo.

5.2.1. Objetivos de la prueba

A continuación se establecen una serie de reglas, las cuales serán implementadas a manera de objetivos para las pruebas:

- La prueba es un proceso de ejecución de un programa con la intención de descubrir un error.

¹ Tomado de : Ingeniería del Software, R. Pressman, ed. McGrawHill

- Un buen caso de prueba es aquel que tiene una alta probabilidad de mostrar un error no descubierto hasta entonces.
- Una prueba tiene éxito si se descubre un error no detectado hasta entonces.

Los objetivos anteriores suponen un cambio dramático de punto de vista. Nos quitan la idea de que normalmente se tiene de que una prueba tiene éxito si no se descubren errores. El objetivo es diseñar pruebas que sistemáticamente muestren diferentes tipos de errores, haciéndolo con la menor cantidad de tiempo y esfuerzo.

5.2.2. Diseño de casos de prueba

Un producto de ingeniería puede ser probado de una de dos formas: 1) conociendo la función específica para la que fue diseñado, llevando a cabo pruebas que demuestren que cada función es completamente operativa; 2) conociendo el funcionamiento del producto, se pueden desarrollar pruebas que aseguren que todas las piezas embonan, es decir, que la operación interna se ajusta a las especificaciones y que todos los componentes internos se han comprobado de forma adecuada. La primera aproximación de prueba se denomina *prueba de la caja negra* y la segunda *prueba de la caja blanca*.

La prueba de la caja blanca es un método de diseño de casos de prueba que usa la estructura de control de diseño procedimental para derivar los casos de prueba. Por tal motivo, esta prueba no es aplicable al análisis, implantación, diseño y administración de un servidor de web. A diferencia, los métodos de prueba de la caja negra se centran en los requerimientos funcionales del software. La prueba de la caja negra permite derivar conjuntos de condiciones de entrada que ejerciten completamente todos los requerimientos funcionales de un sistema.

Mediante las técnicas de prueba de la caja negra se deriva un conjunto de casos de prueba que satisfacen los siguientes criterios: 1) casos de prueba que reducen, en un coeficiente que es mayor que uno, el número de casos de prueba adicionales que se deben diseñar para alcanzar una prueba razonable, y 2) casos de prueba que nos dicen algo sobre la presencia o ausencia de clases de errores en lugar de un error asociado solamente con la prueba particular que se encuentre disponible.

5.2.3. Técnica de grafos de causa - efecto.

El uso de diagramas de causa y efecto es una técnica de diseño de casos de prueba que proporciona una concisa representación de las condiciones y sus correspondientes acciones. La técnica sigue cuatro pasos:

1. Se listan para un módulo las causas (condiciones de entrada) y los efectos (acciones), asignando un identificador a cada uno de ellos.
2. Se desarrolla un grafo de causa y efecto.
3. Se convierte el grafo en una tabla de decisión.
4. Se convierten las reglas de la tabla de decisión a casos de prueba.

El análisis de la prueba en nuestro proyecto se establece de la siguiente manera y con los siguientes flujos:

Lista de causas y acciones

Causas:

- 1.- Información del sistema de red
- 2.- Información solicitada (conexión - URL)

Efectos:

- 101.- Mensaje de error en proceso.
- 102.- Conexión establecida.
- 103.- Envío con éxito

2.- Diagrama de causa y efecto.

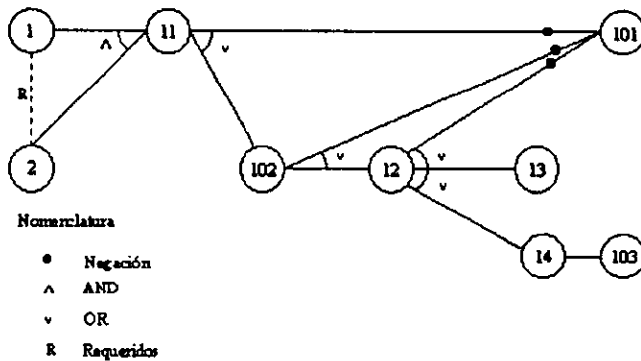


Figura 5.1 Diagrama Causa - Efecto

3.- Tabla de decisión.

La tabla de decisión queda establecida de la siguiente manera en base a lógica booleana.

	Tarea	Caso 1	Caso 2	Caso 3	Caso 4
Causas	1	0	0	1	1
	2	0	1	0	1
Efectos	101	0	0	0	1
	102	1	1	1	0
	103	0	0	0	1

Tabla 5.1 Tabla de decisión de la técnica de grafos de causa y efecto

En la tabla 5.1 se hace referencia a los siguientes términos: posibles entradas se expresa como 0= entrada incorrecta, y 1=entrada correcta. Los datos siguientes de los efectos finales indican 0 = salida de datos incorrecta y 1=salida de datos correcta.

4.- Reglas

Los efectos de prueba quedarían establecidos de la siguiente manera:

- a) Para datos incorrectos el efecto debe ser error.
- b) Para un dato incorrecto y uno correcto el efecto debe ser error.
- c) Para datos correctos el efecto debe ser elegido de la entrada.

5.3 Procesos de Respaldo.

Los respaldos son requisito en cualquier sistema de cómputo, implica también que se tenga un lugar seguro de almacenamiento, ya que la información que se guarda en cintas de respaldo es extremadamente vulnerable. Lo anterior puede observarse en la operación de cualquier centro de cómputo, mientras la información reside en la computadora, los mecanismos de seguridad del sistema operativo protegen de cualquier intento de acceso no autorizado; sin embargo, cuando la información es respaldada en cinta, cualquier persona puede adueñarse de ésta y manipular su contenido. Por esta razón deben protegerse los respaldos al igual que como normalmente se protege el equipo de cómputo.

A continuación se listan los procedimientos que normalmente se siguen en Banco de México para asegurar la información que se encuentra almacenada en cintas.

- No realizar respaldos en equipos que sean accesibles a las demás personas.
- No utilizar mensajeros para la transportación de cintas de respaldo.
- Eliminar los datos de las cintas o destruirlas físicamente antes de desecharlas.

Los respaldos deben ser verificados periódicamente para asegurarse que éstos contiene datos válidos. Es necesario revisar los respaldos de varios meses atrás ya que la información en medios magnéticos puede, algunas veces, llegar a ser borrada debido a las condiciones ambientales. La única forma de saber que lo anterior esta ocurriendo es restaurando el respaldo para verificar que la información en él contenida es válida. Al menos una vez al año, una muestra de las cintas de respaldo, debe ser revisada.

Para maximizar las posibilidades de recuperación en caso de una contingencia, debe considerarse la posibilidad de almacenar las cintas de respaldo en un lugar diferente al que se encuentra el equipo de cómputo.

En la figura 5.2 se muestra el esquema de respaldo empleado tanto para la información que se publica (páginas estáticas, dinámicas y bases de datos) como para la información que reside en el *file system*. El número que aparece en la esquina inferior derecha indica un identificador, el número situado en la esquina superior izquierda indica el día del mes. Del esquema puede deducirse que la misma cinta es ocupada para todos los lunes de un mes. Lo mismo es aplicable para los martes, miércoles y jueves; a diferencia, en el caso de los días viernes, es empleada una cinta diferente para conservar una copia del estado de la información al final de cada semana durante el último mes.

Las cintas son reutilizadas al siguiente mes, es decir, en el primer viernes del siguiente mes se reutilizará la cinta 5, el segundo viernes la cinta 6 y así sucesivamente.

Al final de cada mes la cinta es almacenada, a diferencia de las cintas semanales, las cuales no vuelven a ser utilizadas y pasan a formar parte de la cintoteca del centro de cómputo de Banco de México.

Las cintas, como todos los medios de acceso magnético, sufren un deterioro debido al tiempo y a los procesos normales de lectura y escritura, por tanto, es importante conocer el número de veces que una cinta ha sido utilizada, para Banco de México el periodo de uso de una cinta es de no más de 30 grabaciones. Después de este número la cinta es reemplazada.
























Lunes	Martes	Miércoles	Jueves	Viernes
1  1	2  2	3  3	4  4	5  5
8  1	9  2	10  3	11  4	12  5
15  1	16  2	17  3	18  4	19  7
22  1	23  2	24  3	25  4	26  8
29  1	30  2	1  1	2  4	3  5

Figura. 5.2 Esquema de respaldos

Los procesos de respaldo serán ejecutados de forma automática a través de la utilidad *ntbackup* de Windows NT, que no es más que un proceso de grabación ejecutado de forma automática en un horario determinado. La hora en que será ejecutado dicho proceso es fuera del horario de oficina, es decir por la noche, ya que para enviar cualquier error los servicios WWW y FTP deben ser detenidos, así también con esto se garantiza

que la información permanece sin cambios durante o después del respaldo para un día en específico, asegurando la integridad de la información.

Ntbackup es una utilidad propia de Windows NT con una interfaz interactiva para el usuario, el proceso que será ejecutado será producido en "background", es decir no desplegará ninguna ventana en pantalla. Con este proceso serán respaldados los volúmenes, el registro de Windows NT, una vez realizado lo anterior se verificará, también de forma automática, la validez del proceso antes ejecutado.

Ntbackup generará un archivo de log, del cual podrá extraerse la información necesaria referente al proceso en sí, como al contenido final de la cinta.

La cinta a ser utilizada será de 4mm, 120 m. Con capacidad de 8 Gb compactados o 4 GB sin compactar, con capacidad de multivolumen, es decir, si la información sobre pasa los 8 Gb de capacidad, pueden emplearse tantas cintas como sea necesario. El código responsable de la ejecución de Ntbackup se define a continuación:

```
ntbackup backup
c: d: e: f: /b /d "WEBINTERNO" /l
"e:\destec\respaldo.log" /t normal /v
```

Sobre el servidor de Internet se efectuará un proceso de replicación de forma asíncrona, es decir, cuando un cambio sea realizado será efectuado en el servidor principal y el de respaldo. En procesos más complejos sobre bases de datos se utilizará el método "two-phase-commit", lo que significa que una transacción no será dada como válida hasta ser efectuada en los lugares definidos.

Debido a que se planea tener dos equipos diferentes para el proceso de respaldo y en lugares físicos diferentes, es por lo que se utiliza replicación y no espejeo, ya que este está orientado a dos discos ubicados uno cerca del otro.

El proceso de replicación será realizado a través de *replication manager*, herramienta propia de Windows NT descrita posteriormente en este mismo capítulo.

5.4 Instalación.

IIS 4.0 provee varias características nuevas con respecto a versiones anteriores, a continuación se mencionan las más importantes²:

- Se aumenta la protección contra aplicaciones móviles (aplicaciones ejecutables desde el browser), lo que significa que una aplicación de este tipo, no podría detener el servicio de WWW.
- TASP (Trasaccional Active Server Pages) permite a las aplicaciones con scripts y componentes realizar múltiples acciones. Si una falla ocurre durante una transacción en particular, IIS automáticamente regresa el servidor al inicio de la transacción.

² Fuente: IIS 4, Mueller – Sheldon, Ed MacGrawHill

- ASP Script Debugger. Permite encontrar errores en un script ASP con relativa facilidad.
- Múltiples procesos www y una sola IP.
- Uso de ancho de banda regulado, lo cual reduce la posibilidad de que un conjunto de páginas ocupen todo el ancho de banda.
- IIS soporta HTTP 1.1, certificados digitales X.509, NNTP estándar y servidores de correo SMTP.
- Nuevas herramientas administrativas incluyendo una consola integrada en Windows, el uso de administración sobre un browser, y script desde líneas de comando.
- El uso de certificados digitales X.509 implica un aumento en la seguridad.
- Una máquina de búsqueda (Index Server 2.0) permitiendo realizar búsquedas avanzadas con ASP, Active X y consultas SQL.
- Multihoming, más de un dominio en una solo equipo.

IIS es también una plataforma de desarrollo. Un desarrollador podría utilizar Internet Server Application Programming Interface (ISAPI), lo cual provee un ambiente de construcción para aplicaciones específicas de Internet.

5.4.1 Requerimientos de Instalación³.

IIS funciona sobre un servidor Windows NT con el protocolo TCP/IP instalado y al menos 32 Mb de memoria.

El servidor de Internet estará conectado a una red TCP/IP y de ahí al ISP (ver capítulo 2). El dominio seleccionado por Banco de México y aprobado por InterNIC (<http://www.internic.net>) será dado de alta como : **banxico.org.mx**

Para los servidores internos (Intranet y Extranet) el proceso es más simple. Solo es necesario asignar una dirección IP y una máscara de subred para establecer la conexión entre los servidores y la red Banxico, logrando tomar ventaja de los dominios ahí ubicados.

5.4.2. Inicio y Configuración.

Es posible seleccionar tres tipos de instalación: mínima, la cual instala solo aquello absolutamente necesario para ejecutar IIS; típica, la cual instala aquello que Microsoft cree es posible necesitar; y personalizada, la cual instala aquello que es seleccionado por la persona que realiza la instalación. Este último será el proceso a realizar, ya que de esta forma se logra una mayor flexibilidad. Durante la instalación personalizada de IIS se pregunta por los siguientes componentes:

- Certificate Server: Permite crear o solicitar certificados digitales X.509 para autenticación.

³ Basado en: IIS Resource Kit, Microsoft

- **Front Page 98 Server Extensions.** Habilita el soporte para Front Page y Visual Interdev
- **Internet Information Server.** Instala el soporte de web básico (servidores WWW, FTP y gopher), Front Page Transaction, ASP, conexión a base de datos.
- **Internet Mail Server.** Provee el soporte básico de SMTP (el cual no incluye soporte para POP3).
- **Internet News Server.** Provee el soporte básico para NNTP, lo cual incluye todo lo necesario para la creación de grupos.
- **Microsoft Index Server.** Permite a los usuarios realizar búsquedas sobre el servidor de web.
- **Microsoft Script Debugger.** Permite la búsqueda de errores sobre scripts de ASP.
- **Microsoft Site Server Express-Posting Acceptor.** Permite al servidor aceptar peticiones usando HTTP POST.
- **Microsoft site Server Express-Site Analyst.** Permite administrar el servidor de web mediante un esquema visual, análisis de contenido, administración de vínculos y reportes.
- **Microsoft Site Server Express - Usage Analyst.** Detecta el uso de tareas en el servidor, lo cual permite una administración más especializada.
- **Microsoft Site Server Express - Web Publishing wizard 1.5.** Automatiza el proceso de publicación en el servidor de web.
- **Microsoft Transaction Server.** Instala los componentes básicos necesarios para el uso y verificación de transacciones.
- **Windows Scripting Host.** Permite al servidor ejecutar scripts en una variedad de lenguajes, incluyendo VBScript y Java Script. El servidor provee la capacidad para la interpretación independiente del lenguaje de script, lo cual significa que un tercero podría agregar el soporte para otros lenguajes como PERL o REXX.

No es necesario instalar todos los componentes bajo la premisa que en un momento podrían llegar a ser necesarios, ya que siempre es posible ejecutar el programa de instalación y agregar o incluso remover los componentes que se deseen. Por tal motivo, durante el proceso de instalación para Banco de México solo serán seleccionados los siguientes componentes en los tres servidores de web⁴:

- **Certificate Server.**
- **Front Page 98 Server Extensions.**
- **Internet Information Server.**
- **Microsoft Index Server.**
- **Microsoft Script Debugger.**
- **Windows Scripting Host.**

⁴ En base al manual de instalación de IIS Microsoft, y necesidades de la institución.

5.4.3 Configuración del servidor de Internet.

Para establecer la conexión entre el servidor NT, es necesario instalar y configurar TCP/IP. Los protocolos se configuran ejecutando la utilidad de red en el panel de control de Windows NT. Es necesario considerar lo siguiente:

- La dirección IP del servidor debe ser establecida. No es posible obtener una dirección de forma dinámica a partir de un servidor DHCP.
- Establecer la dirección IP, la máscara de subred y el gateway estándar, este último será responsable del ruteo de paquetes.
- El sistema debe conocer la ubicación del DNS (Domain Name System) más próximo para poder resolver nombres a direcciones IP.

5.4.4 Configuración de los Servidores Internos.

Para los dos servidores internos será necesario especificar el servidor responsable de resolver nombres a direcciones IP. Los nombres están diseñados para ser "amigables" y fáciles de recordar, siendo utilizados por la mayoría de las personas en lugar de la dirección IP cuando se hace referencia a otras computadoras dentro de la red. Sobre Internet, el DNS realiza esta tarea, pero sobre una red interna, Windows Internet Naming Service (WINS) es comúnmente utilizado.

Sin embargo y dada la magnitud de uso planeado para los servidores internos, el DNS utilizado para Internet tendrá dentro de sus tablas para la resolución de nombre a los dos servidores internos así como sus correspondientes direcciones IP. Para la sección de desarrollo correspondiente a los servidores internos, será necesario especificar un servidor WINS, el cual, por efectos prácticos, será habilitado en el propio servidor de Intranet.

5.4.5 Prueba de Instalación.

Una vez que el servidor ha sido instalado es necesario realizar una prueba de conexión al servidor y sus documentos. Esta prueba se realizará a través de tres computadoras, uno de ellos conectado a la red banxico, otro conectado a la subred del sistema financiero y un último completamente ajeno a la red de Banco de México.

Los resultados obtenidos de las pruebas son los siguientes:

Servidor	Internet	Intranet	Extranet
Equipo red Banxico	Conexión establecida	Conexión establecida	Conexión Denegada
Equipo en subred del Sistema Financiero	Conexión establecida	Conexión denegada	Conexión establecida
Equipo ajeno a la red Banxico	Conexión establecida	Conexión denegada	Conexión Denegada

Lo que significa que los tres servidores fueron instalados correctamente.

Respuesta en el Cliente⁵

Se ejecutaron pruebas para conocer que tiempo era necesario para mostrar una página HTML en el browser. La página (mostrada en la figura 5.3) contiene aproximadamente 1,254 bytes en código HTML con un gráfico incrustado. El gráfico, el cual es enviado como un elemento de forma independiente al cliente, agrega 13 K adicionales a toda la página. Se realizaron dos pruebas: una dentro de la red y otra a través de un módem. Los resultados de estas pruebas se muestran en la tabla 5.1.

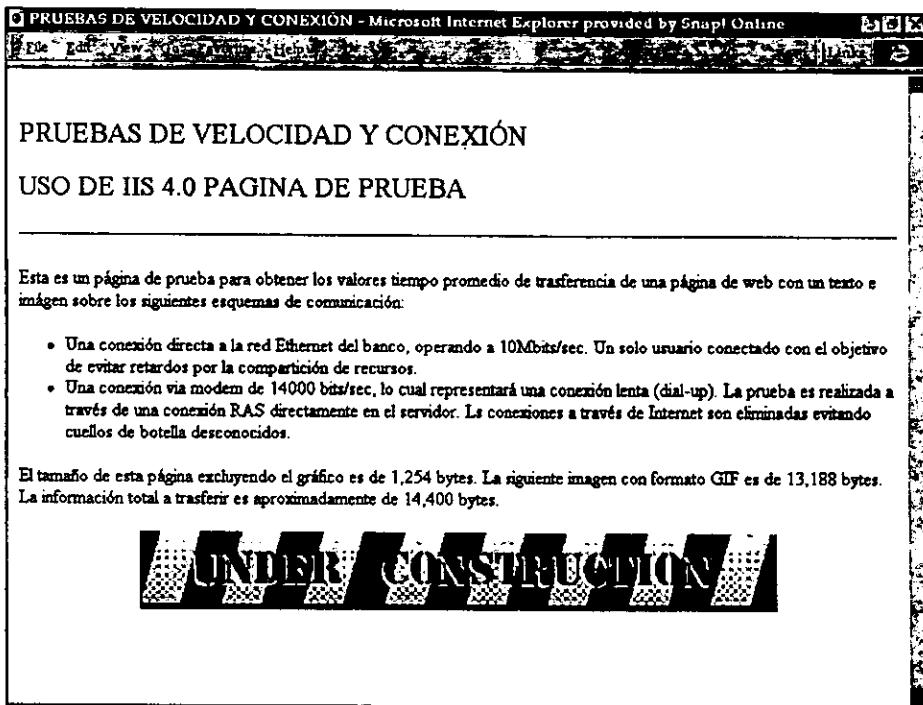


Figura 5.3 Página de prueba HTML

- **Prueba de Red.** Para la prueba en red, el cliente y el servidor fueron conectados a 10 Mbps. La carga de trabajo sobre una red Ethernet es aproximadamente 5 Mbps, pero esto es todavía mucho más rápido que un canal T1, lo que representa una buena prueba de alto rendimiento.

⁵ Tanto la prueba de instalación como la prueba del cliente fueron guiadas por la información proporcionada en : IIS 4, Mueller-Sheldon, ed MacGrawHill

- Prueba en módem. Para las pruebas por módem, le cliente marca al servidor con un módem de velocidad 14.4 Kbps utilizando la conexión a servidor remota (RAS), creando una liga PPP entre los dos sistemas. Internet fue evitado en la conexión con el objetivo de eliminar cualquier retraso inesperado sobre la conexión en Internet.

Es necesario considerar la memoria en el servidor, para nuestro caso, el servidor IIS sobre un equipo NetStrada posee suficiente memoria siendo todas las páginas almacenadas en el cache después de ser mostradas al cliente. A continuación se mencionan factores que importantes que se consideraron durante las pruebas:

- No existe contención sobre las líneas durante la prueba, es decir, no existen usuarios compartiendo la red o conexión de módem o tratando de acceder las páginas sobre el servidor.
- Las conexiones no fluyen a través de Internet para evitar cualquier tipo de retardo que pueda ser introducido.
- Todos los caches en el cliente fueron eliminados antes de las pruebas, con lo que se obliga al servidor a enviar completamente la página de datos al cliente.

Mientras más clientes accedan al servidor, el desempeño de este se vera reducido, siempre y cuando los clientes accedan el servidor exactamente al mismo tiempo. Un cliente con un módem LifeStyle de Motorola a 28.8 Kbps puede recibir la página mostrada en la figura 5.3 en aproximadamente tres segundos.

Tipo	Página e imagen fuera Del cache	Página e imagen en cache
Conexión LAN (10 Mbps)	4 segundos	2 segundos
Conexión módem (14.4 Kbps)	13 segundos	6 segundos

Tabla 5.1 Traslferencias de alta y baja velocidad.

5.4.6 Configuración del Servidor⁶.

Los patrones generales de configuración descritos a continuación son establecidos para los tres servidores de web propiedad de Banco de México. Dichos patrones son establecidos a través de la utileria *Internet Service Manager (ISM)*, a continuación se describen las acciones realizadas:

- Uso de conexiones a través de clientes remotos.
- Configuración de permisos para clientes remotos.
- Especificación de los directorios "home" y directorios virtuales.
- Configuración de opciones de encriptación.
- Vistas de sesiones activas (solo FTP).

⁶ En base al manual de instalación de IIS Microsoft, y necesidades de la institución.

IIS 4.0 posee una versión del ISM la cual opera sobre el browser y posee una funcionalidad similar a la versión estándar. Sin embargo, esta última no permite una administración remota de forma directa.

Los servicios son configurados sobre ISM a través de hojas de propiedades, las cuáles no son otra cosa que cajas de dialogo donde se establecen cada una de las opciones necesarias.

La figura 5.4 muestra la consola de administración de Microsoft (Microsoft Management Console - ventana de ISM). Esta vista muestra los elementos de un lado y el contenido de éstos en el otro. ISM despliega una lista de servidores y los servicios ejecutados en cada computadora. Sobre esto es posible realizar las siguientes tareas:

- Desplegar y configurar las hojas de propiedades, desplegado de los elementos de diferentes niveles y diferente ámbito.
- Iniciar, detener (momentáneamente), detener (definitivamente) los servicios ejecutados sobre el servidor de web seleccionado.
- Administración de llaves X.509
- Monitor de desempeño, vistas de eventos y administración de usuarios y servicios.

5.4.7 Configuración de propiedades⁷.

Las configuraciones específicas de IIS se realizan seleccionando el servidor o servicio en específico accionando el botón de propiedades. La siguiente lista muestra las propiedades importantes para los servidores web banxico.

- Web Site. Define las características del servicio de www, incluyendo su descripción y dirección IP. Esta propiedad incluye el manejo de dos puertos: Uno para TCP y otro para SSL. Es posible limitar el número de conexiones así como habilitar o deshabilitar el acceso.
- FTP Site. Define las características del servicio de FTP, incluyendo su número de puerto, descripción y dirección IP. Es posible limitar el número de conexiones así como habilitar o deshabilitar el acceso.
- SMTP Site. Define las características del servicio de SMTP, incluyendo su número de puerto, descripción y dirección IP. Es posible limitar el número de conexiones así como habilitar o deshabilitar el acceso.
- Cuentas de Seguridad. Define quién ha accedido el servidor WWW, FTP o NNTP. Contiene entradas para acceso anónimo o vía operador.

⁷ En base a: IIS 4, Mueller – Sheldon, ed MacGrawHill

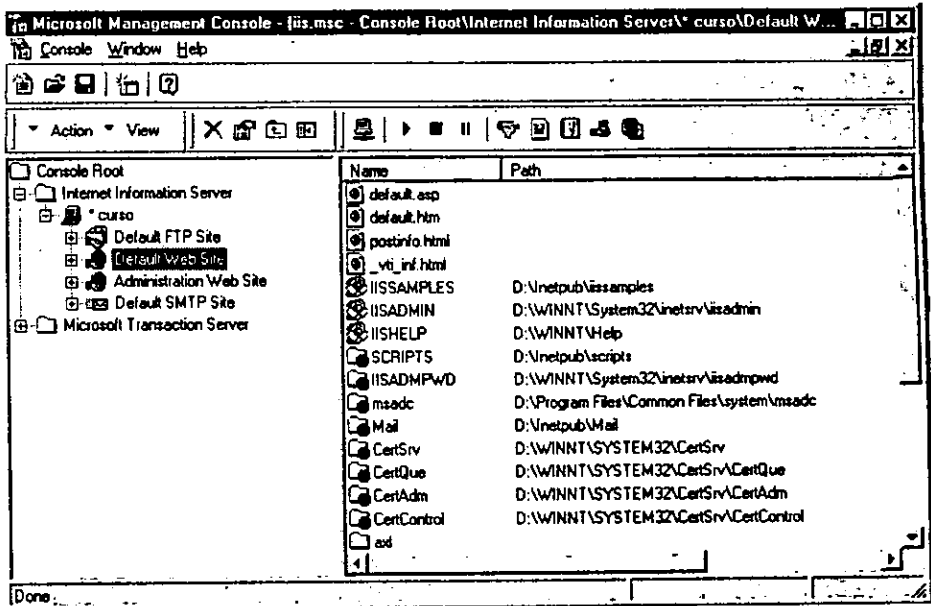


Figura 5.4 Microsoft Management Console

- **Desempeño.** Es posible especificar el ancho de banda a ser utilizado o las conexiones esperadas durante el día.
- **Directorio Hogar.** Define el directorio raíz para WWW, FTP o NNTP (Net News Transfer Protocol) . Para el servicio de WWW, es posible definir la ubicación del directorio raíz, los tipos de permisos, características de control de contenido y aplicación. Para FTP es posible definir la ubicación del directorio (local o remoto), el nivel de acceso (lectura y escritura), donde el acceso es permitido y el tipo de listados para los directorios. Para NNTP es posible habilitar o no las opciones de envío.
- **Documentos.** Define los documentos estándar para el servidor de web. Es posible utilizar diferentes documentos para diferentes browsers.
- **Directorio de seguridad.** Determina que tipo de seguridad es habilitada para los servicios WWW, FTP, NNTP.
- **Encabezados HTTP.** Permite realizar tareas especiales: habilitar la expiración del documento, configurar parámetros MIME, etc.
- **Personalización de errores.** Permite definir los mensajes de error. IIS provee un conjunto estándar de mensajes de error para el servidor de web. Sin embargo es posible definir mensajes personalizados según las necesidades se incrementen. Por ejemplo es posible utilizar un filtro ISAPI que establezca como salida un cierto mensaje bajo una condición específica.

- Mensajes (FTP). Existen tres mensajes posibles de desplegar para un servidor FTP: Bienvenida, Salida y conexiones máximas. El primero aparece cuando el usuario se conecta al servidor, el segundo al momento de desconectarse y el tercero solo es desplegado cuando el número máximo de conexiones en el servidor ha sido excedido.
- Mensajes (SMTP) . Permite delimitar el tamaño de los mensajes ha ser recibidos por el servidor SMTP, así también IIS es configurado para manejar aquellos mensajes que no concuerden de alguna manera.
- Características NNTP. Permite limitar el tamaño de los mensajes para el servidor NNTP. Así también es posible moderar grupos y otras entidades así como definir el contenido sobre los servidores de news.
- Grupos. Permite establecer y administrar grupos sobre el servidor NNTP. Cada grupo tiene su propio directorio sobre el servidor.
- Seguridad. Permite definir las operaciones para el servicio SMTP. Es posible restringir el acceso a través de filtros utilizando direcciones IP.
- Envío. Permite definir como los mensajes son enviados sobre el servidor SMTP, cuantos intentos, en que intervalos, etc.

5.4.8 Configuración de seguridad⁸.

Cualquier servidor debe ser protegido de accesos no autorizados, incluso aquellos dentro de la red interna ya que estos usuarios conocen la estructura de sistemas, convirtiéndolos en usuarios peligrosos. Los esquemas de seguridad utilizados para los servidores de web fueron ya mencionados en el capítulo 4, sin embargo a continuación se describen los puntos configurados directamente sobre IIS durante la etapa de instalación:

- Cuenta de Visita. Los usuarios que se conectan a los servidores web bancario a través de un browser utilizan la cuenta *IUSR_maquina*, donde máquina es el nombre del servidor de web. Es decir, no es necesario proveer un nombre de cuenta o contraseña. Los permisos asignados a esta cuenta solo permitirán conexiones anónimas y garantizarán el acceso de solo lectura para los documentos debajo del directorio raíz en el servidor de web.

Es necesario verificar que la cuenta *IUSR_maquina*, el grupo *GUESTS* y *Everyone* no posean otros privilegios mas allá de solo lectura.

- Formas de Autenticación. Cuando se desea dar permisos a ciertos usuarios o dominios a través de Internet, Windows NT incorpora tres diferentes niveles de autenticación para dichos usuarios:

⁸ En base a: IIS 4, Mueller – Sheldon, ed MacGrawHill

1. Autenticación Básica. Los nombres de usuarios y contraseñas no son encriptados antes de la transmisión. Por lo tanto, es posible que por medio de monitoreo estos elementos puedan ser interceptados. Este tipo de autenticación será incorporado si solo se desea saber quien es el usuario y que información necesita.
2. Windows NT challenge/response. Provee un mayor nivel de seguridad al encriptar el nombre de usuario y contraseña antes de la transmisión. Este método será utilizado solo en el servidor de Intranet, ya que requiere que los usuarios tengan IE, el cual realiza la encriptación antes de transmitir la información.
3. Secure Socket Layer. Utiliza los certificados digitales X.509 para asegurarse que tanto cliente como servidor sean quien dicen ser. Para utilizar este proceso es necesario la intervención de una autoridad certificadora (p. Ej. VeriSign <http://www.verisign.com>). Este proceso será utilizado sobre el servidor de Internet en caso de ser necesario.

SSL será también utilizado sobre los servidores Internos utilizando como autoridad certificadora al propio Banco de México, a través del uso de "certificate Server", descrito al inicio del proceso de instalación.

- NTFS. El sistema de archivos a través de NTFS provee control de acceso y seguridad para proteger los archivos de datos sobre el servidor de Internet.

5.5 Operación y Administración.

Internet Service Manager (ISM) es la herramienta principal para la administración de Internet Information Server. Sin embargo Windows NT presenta su propio conjunto de herramientas de administración, las cuales son:

- Performance Monitor. Registros, monitoreo de eventos y estadísticas.
- Replication Manager. Copia información de forma automática de un servidor a otro.
- Disk Manager. Administración de discos, instalación de discos espejo y arreglos de discos.
- Backup. Almacena y recobra archivos almacenados en cinta.
- Auditing System. Registra la actividad realizada por el usuario.
- Network Monitor. Registra la transmisión de información sobre redes internas.
- TCP/IP Network Utilities. Maneja la información acerca de las conexiones TCP/IP.
- MS Site Server Express. Colabora en la administración del servidor proporcionando una visualización de éste, análisis del contenido, administración de ligas y reporte de capacidades. Este producto es muy similar a Front Page 98, el cual será descrito posteriormente.

Las herramientas mencionadas no sustituyen a ISM, por el contrario, son un complemento para alcanzar una administración lo más completa y funcional.

ISM permite la configuración de varios servicios a través de la consola de administración (MMC). De inicio, la ventana principal muestra cuatro atributos principales: el nombre de la computadora, si la conexión es local o remota, el tipo de conexión y el estado de ésta. De igual forma, los servicios tales como WWW y FTP pueden ser iniciados, detenidos o pausados desde esta misma ventana (ver figura 5.4).

5.5.1 Administración de los servicios

Servicio WWW

Las características propias de este servicio, se definen a través de la carpeta de WWW (figura 5.5), incluyendo su descripción y dirección IP, así como dos números de puertos: uno de TCP y otro para SSL. Sobre esta misma carpeta, es posible limitar el número de conexiones permitidas.

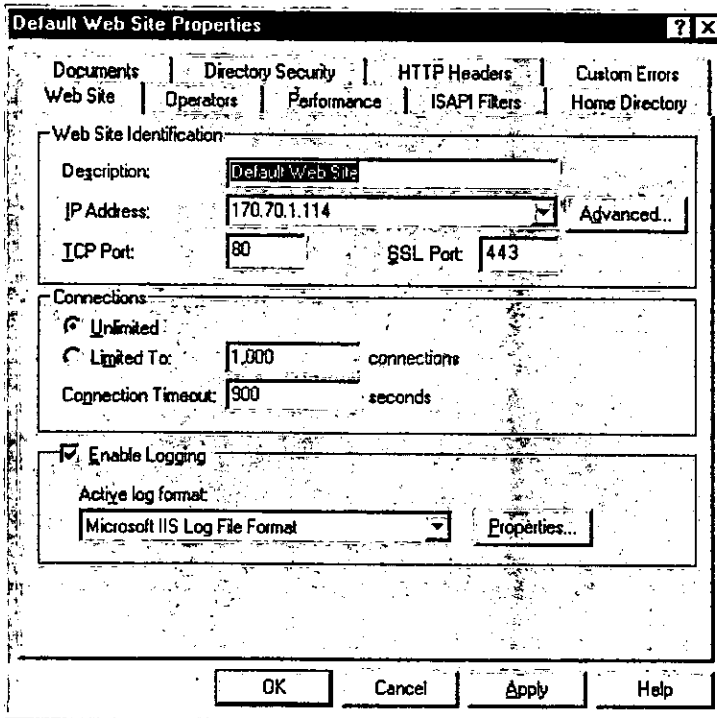


Figura 5.5 Propiedades del servicio www

A continuación se mencionan los atributos a definir para los servidores de web Banxico sobre el servicio de WWW:

- Dirección IP. Este campo define la dirección IP que será utilizada por este servicio. Es posible elegir una dirección específica o la opción *All Unassigned*, es decir, cualquier dirección IP se verificará de la lista de direcciones disponibles utilizándose todas estas, solo aquellas que estén asignadas a un servicio en específico no serán tomadas en cuenta. Para el caso de los tres servidores de web Banxico será definida una dirección en específico.
- Avanzado. Esta carpeta permite la configuración de *entidades*, es decir combinación de dominios, direcciones IP y números de puerto de TCP y SSL.
- Puerto TCP. Esta propiedad especifica el puerto de TCP para el servicio de WWW, se conservará el puerto estándar el los tres servidores de web, es decir 80.
- Puerto SSL. Esta propiedad especifica el puerto estándar para SSL para comunicaciones seguras, trabajo en conjunto con Certificate Server. El puerto definido como estándar a ser aplicado en los servidores de web es el 443.
- Conexiones. IIS permite definir si el soporte en el servicio de WWW será ilimitado (con las restricciones propias del sistema) o se establecerá un límite en el número de conexiones. Se mantendrán los parámetros de conexión acorde a la capacidad del equipo.
- Tiempo de Respuesta. Esta propiedad especifica cuanto tiempo el servidor mantendrá una conexión "viva" sin recibir respuesta. Este valor será especificado en 300 seg⁹.
- Uso de Log. Con el uso de log será habilitado con el objetivo de mantener un registro de estadísticas tales como el número de accesos, o cierto tipo de eventos (descarga de archivos por ejemplo). Para este elemento se definirán los atributos de formato y formas de remplazo para los archivos históricos.

Cuentas de Seguridad

Define los niveles de acceso al servidor de WWW, FTP o NNTP. Conteniendo entradas para accesos anónimos o a través de cuentas definidas.

- Usuario. Esta propiedad especifica el nombre con el cual un usuario anónimo accederá el equipo. Se mantendrá el nombre estándar proporcionado para NT *IUSR_equipo*.
- Contraseña. Define la contraseña sobre el usuario anónimo. IIS provee una contraseña de forma aleatoria como estándar. Es necesario mantener esta contraseña establecida en caso de generar nuevas cuentas anónimas.

⁹ Recomendación Microsoft. IIS Resource Kit

Desempeño

Esta propiedad definirá los parámetros de comunicaciones para el servidor, tales como: ancho de banda y conexiones esperadas.

- **Desempeño.** Esta carpeta permite definir el número de conexiones esperadas por día, proporcionando tres opciones: menos de 1000, menos de 10,000 y más de 10,000. Para los servidores de Banco de México se establecerá el parámetro intermedio, ya que el balance de memoria y velocidad para este parámetro es el de más alto rendimiento.
- **Ancho de Banda.** Permite especificar el uso de ancho de Banda para el servidor. Sin embargo, esta propiedad no será establecida, ya que el consumo del ancho de banda para las conexiones a Internet es regulado a través del FireWall.
- **Conexiones activas.** Permite mantener la conexión abierta durante un proceso. Esta opción se mantendrá activada, ya que en caso contrario, el cliente deberá reconectarse durante grandes periodos de procesamiento, reduciendo la eficiencia del servidor.

Filtros ISAPI

Determina que filtros serán utilizados al cargar páginas de un servidor en particular. Dichos atributos no son aplicables a ninguno de los servidores de web banxico a manera de inicio.

Directorios Raíz

Se definen los directorios raíz para los servidores WWW, FTP y NNTP. Para el servidor de WWW son definidos: la ubicación del directorio raíz, los tipos de permiso y atributos de contenido y aplicación; para el servidor de FTP se definen: la ubicación del directorio raíz (local o remota), los niveles de acceso (lectura - escritura), si el acceso es anónimo o no y el estilo para el desplegado de directorios.

Documentos

Se definen los documentos estándar como *default.htm* y *default.asp*, sin incluir elementos predefinidos.

Seguridad en Directorios

Se define que tipo de seguridad será habilitado para los servidores de WWW, FTP o NNTP. Garantizando acceso a cualquiera o limitando éste a través de direcciones IP y/o dominios. Así también para el servicio de WWW, se establecen los métodos de autenticación de contraseñas y la administración de certificados digitales (ambos conceptos descritos en el punto 5.4.8).

Encabezados HTTP

Se configuran tres opciones:

- Expiración de contenido. Esta opción es implementada para actualizar páginas de forma automática, dicha actualización puede ser realizada en base a tres diferentes niveles: Actualización inmediata, actualización por periodo de tiempo, actualización por fecha.
- Encabezados HTTP personalizados. Los encabezados de las páginas establecen tareas para el browser una vez que la página es transmitida. Sobre los servidores Banxico, se establecen solo los encabezados estándar de IIS.
- Tipos MIME. *Multipurpose Internet Mail Extensions*. Asocia extensiones de archivo a una tarea en particular. Debido a que Banco de México proporciona archivos con formato CSV, es conveniente verificar esta opción que, al ser parte de Office, IE presenta como estándar.

Personalización de errores.

IIS presenta una lista de aproximadamente 80 errores diferentes y los archivos html asociados a estos, por tal motivo se modificaron todas las páginas correspondientes a cada uno de estos errores, de tal forma que las personas que naveguen por cualquiera de los servidores de web del Banco de México, en caso de efectuarse un error, la página que se presente sea más amigable y les proporcione una mayor información al respecto.

Servicio de FTP

Para el servidor de FTP se definen parámetros tales como número de puerto y dirección IP, así también como el límite de conexiones.

- Número de Puerto. Especifica el número de puerto que el servicio utiliza, se mantendrá el estándar para los tres servidores, 21.
- Conexiones. Para los tres servidores de web se mantiene un límite de conexiones no mayor a 100.
- Tiempo de respuesta. Define el tiempo que el servidor mantendrá activa una conexión, definiéndose en 300 seg.
- Uso de Log. El uso de log será habilitado con el objetivo de mantener un registro de estadísticas tales como el número de accesos, o cierto tipo de eventos (descarga de archivos por ejemplo). Para este elemento se definirán los atributos de formato y formas de remplazo para los archivos históricos.

Mensajes FTP

Sobre los tres servidores de web se presentarán los mensajes asociados a conexión, desconexión y conexiones máximas como sigue:

Evento	Intranet	Extranet	Internet
Conexión.	Bienvenido al webinterno Banxico	Bienvenido al servidor web. Sistema Financiero	Bienvenido al servidor web. Banco de México
Desconexión	Desconectando... Webinterno Banxico	Desconectando... Sistema Financiero	Desconectando... Banco de México
Conexiones Máximas	Demasiadas conexiones establecidas. Favor de intentar mas tarde.	Demasiadas conexiones establecidas. Favor de intentar mas tarde.	Demasiadas conexiones establecidas. Favor de intentar mas tarde.

Servicio NNTP

Se define número de puerto, dirección IP y número límite de conexiones. Así como los puertos para TCP y SSL y manejo de identidades. Los valores en los tres servidores de web serán definidos como: TCP - 119, SSL - 563. Estableciendo un límite de 300 conexiones con un período máximo de 300 seg. Al igual que los servicios de FTP y WWW, se habilita el uso de bitacoras con los formatos y propiedades correspondientes. Este servicio solo estará disponible para el servidor Intranet estableciendo limite en el tamaño de los mensajes.

Servicio de SMTP

Se define el número de puerto, 25 para los dos servidores de web donde es habilitado el servicio (Intranet y Extranet) así como dirección IP. Limitándose el número de conexiones permisibles. El objetivo de habilitar este servicio es la compatibilidad con Exchange Server, el cual se tiene contemplado como herramienta de correo dentro de Banco de México. Se restringe el acceso por dominio para uso de este servicio.

5.5.2 Operación

Front Page 98 (FP98) es un producto Microsoft diseñado para simplificar la administración y operación de un servidor de web. A diferencia de lo descrito anteriormente, FP98 se concentra en la administración del contenido, es decir en la información.

El producto consta de 4 módulos:

- Explorador de Front Page. Se utiliza para crear la estructura o diseño del servidor de web, organizar los archivos y carpetas, importar y exportar archivos, probar y reparar hipervinculos, administrar los privilegios de acceso, realizar el seguimiento de las tareas. Así también, el explorador de FP98 es utilizado para publicar las páginas ya terminadas en el servidor de web correspondiente.
- Editor de FP98. Es utilizado para crear diseños y modificar páginas. Las modificaciones es posible hacerlas en el ambiente propio del editor o bien, desde formato HTML.
- Extensiones del Servidor de FP98. Aceptan la creación y administración de sitios web, junto con la funcionalidad de FP98 en tiempo de exploración. Es decir, cuando un autor esta modificando un sitio web, las Extensiones del servidor permiten copiarlo o publicarlo en otros servidores web, crear una tabla de contenido para el web, agregar temas y una estructura de exploración al mismo y actualizar los hipervinculos a las páginas que se hayan movido o cuyos nombres hayan cambiado. Mediante las extensiones de servidor, un administrador puede asignar a un usuario o un grupo de usuarios un determinado grupo de permisos para modificar, explorar o administrar un servidor de web.

El módulo que será utilizado para la administración de los servidores de web Banxico es el Explorador de FrontPage exclusivamente.

Los servidores de web de Banco de México estarán conformados por páginas HTML, imágenes, documentos y carpetas, en su mayoría. Los autores podrán crear, eliminar, abrir, modificar, y cerrar el conjunto de documentos que conforman su universo de trabajo.

El conjunto de información que compete a cada usuario puede ser manipulado como un sub-web, hijo del web principal o web raíz, el cual solo podrá ser modificado a través de la cuenta de administración

Básicamente las tareas a realizar para la operación de los servidores de web a través de FP98 son:

- **Mostrar la estructura del web.**
Mostrar y mantener los archivos, carpetas, hipervinculos y diseño a través de una de las siete vistas proporcionadas por FP98 (descritas al final del capítulo).
- **Importar y exportar Archivos.**
Se mantiene el concepto de Windows por medio de arrastrar y pegar, esto se hará en la vista de carpetas. Donde se podrá ver una lista jerárquica de las carpetas del servidor de web así como el contenido de cada una de ellas.

- Probar y reparar hipervinculos.

Será utilizado para verificar los hipervinculos existentes, ya que a través de un ambiente gráfico es fácil detectar el estado de cada uno de los hipervinculos que componen las páginas del sitio web. Así también, en caso de modificar el nombre de un archivo es recomendable hacerlo desde el propio explorador, ya que así FP98 corregirá automáticamente los hipervinculos de las páginas que ocupen dicho archivo.

- Seguimiento de tareas.

Mediante la vista de tareas del explorador de FP98 es posible realizar el seguimiento de las tareas, las cuales fueron creadas por el propio autor durante el proceso de desarrollo.

- Publicación.

El comando publicar del explorador de FP98 transferirá las páginas y los archivos al servidor de web a la vez que comprobará automáticamente las direcciones de las páginas y las rutas de acceso de los archivos. El desarrollador trabajará siempre sobre su disco local, al momento de estar terminado el sitio web, éste será publicado por medio de FP98 o en su defecto a través de FTP.

Las vistas (formas de presentar información a través de FrontPage) que serán utilizadas para la operación de los tres servidores de web Banxico son:

- Carpetas. Permite ver la estructura de archivos y carpetas del sitio web. Mostrando las carpetas y su contenido al igual que el explorador de Windows.
- Todos los archivos. Muestra una lista completa de todos los archivos del sitio web, incluyendo información acerca de cada archivo de forma individual. No se muestran carpetas.
- Exploración. Proporciona un esquema de la estructura del sitio web. La vista se divide de forma gráfica (panel de exploración) y una lista de archivos y carpetas (Vista de Carpetas).
- Hipervinculos. Muestra los hipervinculos que conectan las páginas y archivos y una lista jerárquica de los mismos, empezando por la página principal. Así también, se indican las imágenes de una página y los archivos incluidos en ella.
- Estado de hipervinculos. Se obtiene un informe del estado de los hipervinculos del sitio web. Los hipervinculos solo se muestran si son erróneos o su estado es desconocido. Una vez que los hipervinculos erróneos son identificados, su corrección se efectúa a través de la vista de Hipervinculos.
- Temas. Esta vista no será utilizada en ninguno de los servidores de web del Banco, ya que su propósito es un vista previa y aplicar elementos de diseño proporcionados por FP98.

- **Tareas.** Muestra una lista de tareas asociadas con un sitio web. Es decir, el administrador del sitio deberá organizar su construcción en base al uso de tareas, más aún si es un desarrollo con un equipo de trabajo, validando el trabajo de cada desarrollador en lo que corresponde a su avance.

Permisos

A través de FP98 es posible asignar permisos, sin embargo el proceso de administración de usuarios se seguirá manteniendo desde la administración de Windows NT. Los permisos por medio de FP98 solo serán asignados en el caso de existir un grupo de trabajo de un sub-web. Estos permisos serán administrados por el líder de proyecto, es decir, administrador de un sitio web en específico.

Los permisos a otorgar son:

- Exploración.
- Creación
- Administración.

TENDENCIAS A FUTURO

6.1 Tendencias tecnológicas

Es difícil especular acerca del futuro de Internet debido a los tremendos saltos tecnológicos que pueden llegar a ocurrir en un corto período. Internet esta en un punto crucial, los clientes solicitan un mayor uso mientras que los proveedores buscan ruteadores más poderosos y nuevas tecnologías.

6.1.1 HTML?

Una página de web, siempre conservará su estructura básica escrita en HTML, no importa si interactúa con un applet o contiene comandos asp.

Debido a la necesidad de incorporar mayores elementos que le proporcionen al usuario una mayor interacción, HTML esta cambiando. Conjuntamente con la incorporación de Scripts en las páginas de web, lo que da origen a DHTML (Dynamic HTML), aparecen dos perspectivas diferentes: MHTML y XML.

MHTML esta relacionando con las dos grandes aplicaciones que podemos encontrar sobre Internet, WWW y e-mail. Es un intento para enviar gráficas o sonidos incluidos dentro de una página HTML. MHTML ciertamente abre posibilidades interesantes, incluyendo una nueva forma de proveer tecnología push¹, sin embargo, podría convertirse en carga innecesaria de la red al enviar correos de gran tamaño.

¹ Descrita en el capítulo 3.

Por otro lado, Extensible Markup Language (XML) esta ya próximo a ser estándar. XML es un subconjunto de SGML (Standard Generalized Markup Language), el cual permite a los usuarios asignar marcas (tags) que definan y validen formatos de documentos sobre el web.

XML no ha sido integrado a los navegadores y existen todavía muchos detractores de esta tecnología. XML no es reemplazo para HTML es, como su propio nombre lo indica, una extensión de éste, ya que HTML por si solo ha dejado de ser suficiente.

6.1.2 HTTP

En el área de protocolos seguramente existirán tres cambios sobresalientes, nos referimos al uso común de S-HTTP (Secure HTTP), HTTP 1.1 y HTTP-NG²

Secure Hypertext Transfer Protocol, provee una forma de encriptar información que es intercambiada entre el cliente y el servidor. S-HTTP utiliza una llave pública desarrollada por RSA Data Security Inc. En un sistema de llave pública una organización genera dos llaves vinculadas que son usadas en transacciones. Una de las llaves es hecha publica mientras que la otra es mantenida de forma privada por la organización. Cualquiera que desee generar una transacción segura encripta con la llave pública. La organización entonces descrypta la transacción con la llave privada.

Una de las grandes ventajas en el uso de HTTP 1.1 es el uso de encabezados para poder identificar un servidor. Anteriormente sólo era posible hacer esto por medio de su dirección IP, actualmente con el uso de *multihoming* (múltiples servidores de web utilizando una dirección IP) esto deja de ser funcional convirtiendo el uso de encabezados en una necesidad. El resultado será que en Internet el uso de direcciones IP será utilizado más eficientemente.

Así también con HTTP 1.1 entrará un nuevo concepto: URI (Uniform Resource Identifiers). Los cuales son cadenas formateadas que identifican un recurso en Internet utilizando un nombre, ubicación o cualquier otra característica. La evolución del concepto de Internet esta constantemente involucrando nuevos tipos de recursos, URI's, por tanto, es probablemente una garantía.

HTTP-NG (Next Generation), es la siguiente implemetación de HTTP que proveerá un mejor desarrollo adicionando nuevas características para soportar aplicaciones de uso comercial tales como seguridad y autenticación. Algunas de estas mejoras y cambios son:

- HTTP establece una nueva conexión para cada petición, HTTP-NG permite que diferentes peticiones sean enviadas a través de la misma conexión, mejorando de esta forma el desempeño. El cliente no necesita esperar una respuesta del servidor antes de enviar otra petición.
- Los servidores pueden responder a peticiones en cualquier orden e interrelacionar los datos de múltiples objetos, permitiendo que la información sea trasmitida en paralelo.

² Fuentes: <http://www.ics.uci.edu/pub/ietf/http/rfc1945.html>
<http://www.stars.com/Internet/Protocols/HTTP/>

- HTTP-NG utiliza el concepto de canales, en los cuales los mensajes y datos son enviados sobre diferentes conexiones.
- HTTP-NG con formato multicanal, esta mejor preparada para tomar ventaja de futuras redes de alta velocidad y el eminente arribo de ambientes multimedia.

6.1.3 Las aplicaciones³

Java es el primer paso real en la evolución del WWW, pero todavía no es suficiente. Java ofrece una gran flexibilidad en el medio ambiente de aplicaciones distribuidas, pero actualmente el paradigma de aplicaciones cliente/servidor no es soportado aún. Para lograr esto, Java necesita ser enriquecido con una infraestructura de objetos distribuidos, es aquí donde CORBA de OMG entra en la escena. CORBA provee el vinculo faltante entre el ambiente de aplicaciones portables en Java y el mundo de los servicios finales de Internet. La intersección entre Java y las tecnologías de objetos de CORBA es el siguiente paso natural en la evolución del WWW, el cual, con Java y CORBA proveerá una plataforma ubicua para la computación red-centralizada.

Como resultado de esto, la creación de un nuevo modelo de desarrollo sobre Internet esta por emerger. La figura 6.1 muestra el modelo de aplicaciones tres capas cliente/servidor. La primera capa pertenece al cliente. En este caso, al navegador, aplicaciones Java y applets. La segunda, es provista por cualquier servidor que soporte clientes HTTP y CORBA. La tercer capa permanece sobre los servidores tradicionales.

Los objetos CORBA como servidores intermedios de aplicación encapsulan la lógica del negocio e interactúan con los componentes cliente a través de Java ORBlet. Por supuesto los objetos CORBA sobre el servidor pueden interactuar unos con otros utilizando CORBA ORB y establecer comunicación con aplicaciones de la tercera capa utilizando SQL o cualquier otra forma de software intermedio. La tercera capa es todo aquello con lo cual un objeto CORBA pueda entablar comunicación, TP Monitors, MOMs, DBMSs, ODBMSs y e-mail.

HTTP es utilizado para enviar y recibir páginas de web, applets e imágenes; CORBA será utilizado para comunicaciones cliente/servidor con Java.

³ Fuente: Java and Corba, Orfali, ed. Wiley

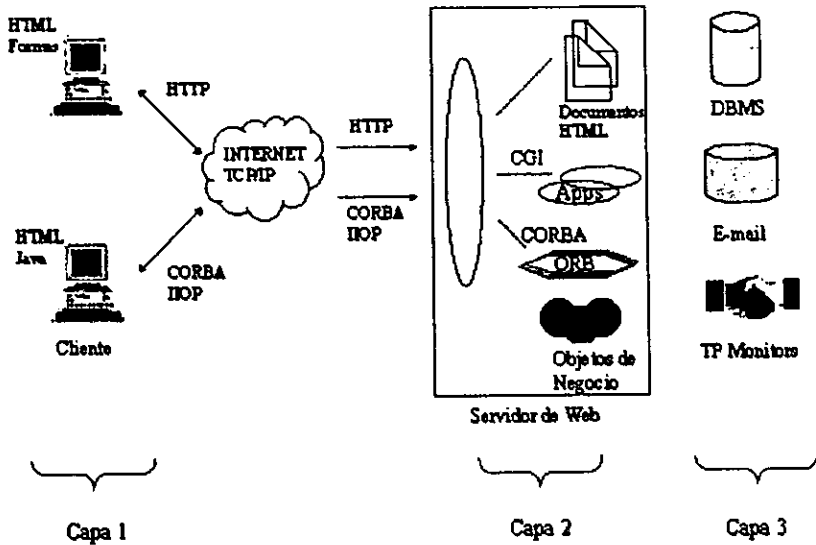


Figura 6.1 Modelo de Web basado en clientes Java y CORBA ORBs.

6.1.4 Servidor

Los primeros servidores de web disponibles estaban basados en plataformas UNIX y eran libremente distribuidos. Por años los ambientes UNIX han tenido ventajas en desempeño, estabilidad y administración remota sobre Windows NT. Conjuntamente, el ambiente UNIX ha podido resolver problemas específicos permitiendo combinar servicios tradicionales - como los servidores de web- con otras herramientas para proporcionar aplicaciones más sofisticadas.

Por mucho tiempo la plataforma de Windows NT fue tratada como un juguete por la comunidad de Internet. A pesar de contar con una interfaz amigable, los desarrollos sobre NT eran inestables y lentos en lo que respecta a los servicios de Internet. Sin embargo, dos hechos cambiaron esta perspectiva: el surgimiento de una computación completa basada en procesadores Intel y la gradual mejora del software soportado por éstos.

Los servidores Windows NT todavía no ofrecen un desempeño y escalabilidad comparable con las plataformas UNIX. Sin embargo, NT compite ofreciendo ventajas substanciales en instalación configuración y administración. Así también, las herramientas de desarrollos sobre NT no tienen paralelo en el ambiente UNIX. Estas herramientas son comerciales y cuentan con un soporte establecido, en contraste "freeware"⁴ domina el ambiente UNIX.

⁴ Software obtenido de forma gratuita.

En los últimos 12 meses Windows NT se ha convertido en la plataforma de más amplio desarrollo para los servidores de web. Esto no es porque sea superior a UNIX, es por la integración que presenta con las herramientas de escritorio y el software de desarrollo.

UNIX permanece como la mejor solución en transacciones y uso de bases de datos, pero las herramientas que explotan y manipulan estas bases de datos (para su uso en Internet) esta dejando de ser en UNIX.

6.1.5 I2

Al hablar de tendencias a futuro no podemos dejar de mencionar Internet2 -I2-, aunque todavía existe una gran confusión acerca de este proyecto y sus objetivos.

La distinción más significativa sobre I2 es que ésta no remplazará de ninguna forma a Internet. El objetivo es que los desarrollos y descubrimientos que surjan del trabajo continuo sobre I2 eventualmente encontrarán su funcionalidad sobre los diferentes tipos de redes, incluyendo Internet.

I2 no es una red separada, por el contrario esta tratando de establecer conexiones a GigaPOPs⁵ adecuando los servicios de redes de los actuales proveedores.

El objetivo de I2 es facilitar y coordinar el desarrollo, operación y avance tecnológico, así como acelerar la disponibilidad de nuevos servicios y aplicaciones sobre Internet.

Resumiendo podríamos establecer que:

- Las computadoras personales continuarán dominando como el dispositivo de acceso al web; pero el teléfono, asistentes digitales (PDA's), y otros dispositivos cobrarán importancia.
- Terminales compartidas tomarán lugar en sitios públicos donde cualquier persona podrá usarlas por un pequeña cantidad de dinero.
- Internet se volverá más segura, y el número de negocios y transacciones se verá radicalmente incrementado.
- El contenido del web se volverá más rico y atractivo con el arribo de multimedia.
- Los navegadores trabajarán más para el usuario. Organizarán la información que presentan, lugares de visita y detalles en las transacciones.

Los administradores se verán beneficiados de nuevas tecnologías y productos. Será más fácil la creación de páginas, la interacción con bases de datos, la administración del servidor de web (hiperligas, accesos, monitoreo, etc.) será más simple.

⁵ Giga POP's son rutedores con conexiones de alta velocidad

Los desarrolladores tomarán ventaja de la tecnología orientada a objetos, haciendo real la frase "la red es la computadora".

6.2 Tendencias Institucionales.

El Sistema Financiero Mexicano constantemente esta evolucionando en su aspecto económico-financiero, convirtiéndose en un ente mucho más complejo; como una consecuencia de esto, su contraparte tecnológica requiere avanzar en paralelo a esta evolución. Los sistemas computacionales que representan un vínculo entre el sistema Financiero y Banco de México se encuentran inmersos en este avance.

Banco de México avanza hacia un modelo estructural en el área de cómputo y comunicaciones. Por una parte, aquellos sistemas de uso interno se pretende sean funcionales a través del servidor de web, con lo cual se obtendrá un mejor aprovechamiento del tiempo y eficiencia en el trabajo. Pero atrás de este funcionamiento se encuentran inmersos diferentes tópicos (Sybase, Power Builder, Java), los cuales circunscriben la periferia de la tecnología Banxico.

El diseño de estas herramientas en la institución, se busca sea orientado a objetos, desarrollado a través del uso de una metodología estándar, con la utilización de objetos compartidos dentro de un ambiente transaccional.

Definitivamente el uso de bases de datos es aspecto prioritario, tratar de vincular la información, convirtiéndola en una sola, es decir el uso probable de *datawarehouse*⁶. Por supuesto, la seguridad no esta ajena a este avance tecnológico, se planea implementar una arquitectura para la seguridad de la información y su infraestructura, incluyendo aplicaciones, sistemas operativos así como el segmento de comunicaciones.

El trabajo por realizar es mucho todavía, pero los primeros avances y la plataforma para su desarrollo ya ha sido establecida.

⁶ Para mayor información es posible consultar: <http://datawarehouse.dci.com/>

CAPÍTULO 7

RESULTADOS Y CONCLUSIONES

Con la realización del presente trabajo se ha conseguido establecer la plataforma necesaria para el desarrollo de aplicaciones en Internet y la consecuente explotación que se puede obtener a través de éstas.

El éxito en el uso de un servidor de web, radica en que se implanta un sistema completamente abierto a la innovación. Permitiendo establecer la estructura necesaria para la construcción, difusión, administración y operación de sistemas, sin necesidad de instalación de clientes, reduciendo tiempo y eliminando la posibilidad de error por factor humano (usuario final).

El desarrollo de aplicaciones web esta basado sólo en cuatro índices:

- Escribir páginas web
- Instalar servidores de web
- Desarrollar sistemas de información para uso en un servidor de web
- Escribir código para páginas web.

De forma práctica los resultados obtenidos son:

- Mayor capacidad y calidad de servicios, ya que se reduce el tiempo en distribución de información por parte del organismo que la genera, sea interno o externo.
- Menor especulación por la carencia de información, obteniéndose ésta casi en línea y con un trato directo hacia el sistema financiero y público en general.

- Las soluciones de "groupware" aumentarán las capacidades corporativas.
- Reducción de costos administrativos, ya que con el servicio de web muchos de los trámites anteriormente realizados en papel serán efectuados de forma electrónica, aumentando el uso eficaz de tiempo de personal.
- La facilidad de consulta, ya que no es necesario tener acceso a directorios o instructivos, el empleado Banxico desde su hogar podrá realizar consultas y desde el Banco transacciones, sin tener que desplazarse.
- La seguridad es un elemento más que importante, se tiene un esquema confiable basado en varias capas de seguridad, dependiendo de la información a manejar.
- La administración de los sistemas en Internet podrá ser efectuada de manera remota y se podrá tener un control casi absoluto de los clientes que interactúan con dichos sistemas.

Definitivamente el servicio podrá ser mejorado, con la estructura tecnológica establecida por Banco de México donde la incorporación de los servidores de web esta ya contemplada, conformando un esquema global para todos los servicios proporcionados por esta institución. Complementando el desarrollo con lenguajes 4GL, servidores de transacciones, y DBMS's.

La incorporación del desarrollo en CORBA y programación en objetos, vendrá a reforzar el desarrollo de aplicaciones web en el futuro próximo de Banco de México.

Aspectos trascendentales como la interacción con los servicios de correo será crucial para el éxito de los servidores de web, ya que en la medida que facilite la vida al usuario final serán aceptados, la mejora en la calidad del servicio, el mejor aprovechamiento del tiempo, y la oportunidad de información serán consecuencias lógicas a este hecho.

BIBLIOGRAFIA

LIBROS

<ul style="list-style-type: none"> • Roger S. Pressman Ingeniería del Software Ed. McGrawHill 	<ul style="list-style-type: none"> • Cricket Litu, Jerry Peck Managing Internet Information Services Ed O'Reilly
<ul style="list-style-type: none"> • Marcus Goncalves Protecting Your Web Site with Firewalls Ed. Prentice Hall 	<ul style="list-style-type: none"> • Amit K. Maitra Building a Corporate Internet Strategy Ed. ITP
<ul style="list-style-type: none"> • John Muller, Tom Sheldon IIS 4 The Complete Reference Ed McGrawHill 	<ul style="list-style-type: none"> • IIS Resource Kit Microsoft Press
<ul style="list-style-type: none"> • Cornelio Robledo Redes de computadoras Ed. FOC 	<ul style="list-style-type: none"> • Java and Corba Orfali Ed. Wiley
<ul style="list-style-type: none"> • William Stallings Local Networks Ed Macmilan 	<ul style="list-style-type: none"> • MS Windows NT Resource Kit Microsoft Press
<ul style="list-style-type: none"> • Kris Jamsa Programación en Internet Ed McGrawHill 	<ul style="list-style-type: none"> • Tom Sheldon Windows NT Security Handbook Ed. Osborn
<ul style="list-style-type: none"> • Martin James Security Accuracy and Privancy in CS Ed MCGrawHill 	<ul style="list-style-type: none"> • Parker Timothy Aprenda TCP/IP en 14 días Ed. Prentice Hall

Referencias

<p>Redes de Area local http://web.svr.edu/~jmwobus/lans/</p>	<p>Protocolo HTTP http://www.stars.com/Internet/Protocols/HTTP/ http://www.ics.uci.edu/pub/ietf/http/rfc1945.html</p>
<p>Internet Service Provider http://www.cnam.fr/Network/Internet-access/how_to_select.html</p>	<p>Microsoft http://www.microsoft.com</p>
<p>NetLingo: The Internet Language Dictionary http://www.netlingo.com</p>	

Publicaciones Periódicas

<ul style="list-style-type: none">• PC Magazine Octubre 22 /97 Vol 15 Num 18	<ul style="list-style-type: none">• PC Magazine Mayo 27/97 Vol 16 Num 10
<ul style="list-style-type: none">• Banca Electrónica Enero 1998 Número 41	<ul style="list-style-type: none">• Mundo Ejecutivo Agosto 97 Numero 208
<ul style="list-style-type: none">• LAN Special Report Noviembre 97	

Apndice A

**ANÁLISIS A DETALLE DE CADA SERVIDOR DE WEB ESTUDIADO/PROBADO
POR BANCO DE MÉXICO**

**Commerce Bulder Pro (CBP)
The Internet Factory
Estudio**

A pesar que Commerce Builder Pro posee características interesantes, como son servidores virtuales y un servidor proxy, el sistema de configuración no es tan robusto como en otros productos.

Commerce Builder Pro puede ser ejecutado como una aplicación en Windows 95 o Windows NT y como un servicio sobre este último. CBP posee un panel de control a través de un applet, el cual permite establecer parámetros a nivel global (para el sistema entero de CBP), a nivel de clase (todos los servidores del mismo tipo, como servidores proxy) y a nivel local (un servidor en específico).

La configuración es confusa, se provee un archivo de ayuda, sin embargo este no puede ser accedido de manera directa, ya que no presenta ningún acceso para poder ejecutar dicha ayuda desde la utilidad de administración, es decir, se debe conocer el lugar exacto donde reside este archivo para poder utilizarlo. La nueva versión de CBP denominada Merchat Builder (disponible para cuando esto se lea) promete la corrección de este problema.

Con CBP es posible dar de alta cuentas de grupo y usuario, las cuales permiten personalizar el acceso a ciertas partes del sistema. Así como también, crear filtros de control de acceso que restringen las funciones que usuarios específicos pueden realizar sobre el servidor. Otra característica de CBP, es la posibilidad de restringir acceso desde el servidor por dominio, rango de direcciones IP o páginas específicas.

Si no se desea dar de alta un usuario dos veces, CBP puede tener acceso a las bases de datos propias de WinNT, opción bastante útil hablando de una Intranet. Solo IIS provee una característica similar sobre WinNT.

CBP provee soporte para SSL 2.0 (Secure Sockets Layer), autenticando la identidad del servidor y encriptando datos entre cliente y servidor. Communications Builder Pro es un producto idéntico a CBP a excepción por el soporte de SSL.

Con CBP es posible implementar 16 servidores virtuales sobre un solo sistema físico, dando a cada uno de ellos diferente nombre de dominio y direcciones IP o bien, asignar a cada servidor virtual diferentes números de puerto con la misma dirección IP. Los servidores virtuales son básicamente usados para el desarrollo de Intranet.

El lenguaje de macros propietario de CBP, Server Macro Expansion (SMX), permite establecer conexiones a cualquier fuente de datos de ODBC. Se espera que Merchat Builder incluya una aplicación escrita en SMX que permita el procesamiento de formas, una máquina de búsqueda, así como soporte para CGI.

Internet Connection Secure Server for OS/2 Warp (ICSS) **IBM** **Estudio**

ICSS es complejo para configurar y carece de servidores virtuales. Es uno de los pocos servidores de web basados en OS/2, sin embargo, la versión 4 existe también para Windows NT. Incluye un servidor proxy, no incluye herramientas de administración o una máquina de búsqueda. ICSS no permite múltiples nombre de host para un solo servidor, es decir, servidores virtuales.

Es posible configurar ICSS de dos formas diferentes, a través de la interfaz proporcionada por el browser o manualmente configurando el archivo HTTPD.CNF.

ICSS soporta todos los métodos estándares de HTTP: get, head y post. Posee un poderoso pero complicado esquema de seguridad y control de acceso. El servidor incluye tanto SSL 2.0 como S-HTTP (secure-http) para comunicaciones encriptadas, generando sus propios certificados SSL sin necesidad de trabajar con un tercer certificado de autoridad.

El control de acceso puede trabajar a través de un nombre de usuario y contraseña o filtrando la dirección IP o nombre del dominio. Sin embargo, definir este tipo de protecciones resulta complejo. Cuando se desea definir un parámetro específico, no es sencillo identificar el lugar dentro del archivo de configuración. Mientras que el control de acceso resulta ser poderoso, sin embargo, parece fácil cometer un error.

ICSS posee un grupo completo de opciones para formateo de documentos, como podría ser la elección de un archivo estándar (en caso que el usuario no especifique ninguno), listas de directorios que pueden describir documentos y decir cuando estos fueron modificados.

Un registro de acceso, como también de operaciones hechas por el servidor, es incluido, el cual es accedido en tiempo real sobre el servidor. Por último, el ambiente de programación de ICSS permite el soporte para CGI.

**Internet Information Server 4.0 (IIS)
MICROSOFT
Estudio - Prueba**

IIS provee un proceso fácil de instalación así como una integración total sobre WinNT. A diferencia del servidor de web de Netscape, el cual ofrece una variedad de plataformas de uso, IIS solo es disponible para WinNT. Sin embargo, IIS tiene un desempeño mejor sobre sus competidores.

IIS viene en conjunto con el paquete denominado por Microsoft como Option Pack, el cual incluye Front Page 98, MS Certificate Server, Index Server, Message Queue Server y Transaction Server (MTS), herramientas útiles en la creación de servidores de web dinámicos y seguros.

MMC (Microsoft Management Console), toma ventaja de su integración con WinNT permitiendo administrar otros servicios de NT tales como MTS. Así también es posible acceder los servicios de web, FTP, SMTP y NNTP desde MMC.

IIS provee administración remota a través del browser, presentando una interfaz y funcionalidad muy similar a la proporcionada por MMC.

En esta nueva versión se ofrecen los servicios de directorios virtuales y "multihosting", la cual es una de las características más fuertes de IIS. WinNT permite establecer varias direcciones IP para una sola tarjeta de red, de tal forma que cada servidor virtual pueda tener su propia dirección IP.

La integración con WinNT permite un proceso de instalación muy simple en solo unos minutos. IIS crea una cuenta de usuario genérica sobre NT, la cual posee derechos de solo lectura sobre los directorios a ser utilizados para la publicación de páginas de web, lo cual permite que dichas páginas puedan ser importadas de algún otro servidor en tan solo unos minutos.

IIS incluye los servicios de un servidor de FTP y de web. Como estándar, durante el proceso de instalación, ambos servicios (www, ftp), son activados y funcionan como servicios propios de NT. Internet Service Manager, incluido como parte de MMC, es un panel de control que permite iniciar, detener y configurar cada uno de estos tres servicios.

Internet Service Manager maneja el control de acceso, especifica directorios de servidores y establece las opciones de conexión. IIS produce un "log" el cual es posible almacenar como un archivo de texto o escribirlo directamente a una base de datos ODBC.

Un aspecto mas que importante es la seguridad, la cual puede estar bien integrada con WinNT, ya que es posible configurar el servidor para requerir una cuenta y contraseña para acceso al servidor de web o cualquier página o dirección sobre el mismo. Es posible también, permitir o negar acceso basado en una dirección IP o un rango específico de estas. IIS utiliza la base de datos de usuarios de WinNT, es decir es posible administrar la lista de usuarios de web con las mismas herramientas utilizadas para los usuarios comunes de NT. Eliminando la necesidad de una base de datos separada para usuarios de web.

Con Internet Service Manager es posible asignar una dirección IP diferente para especificar directorios sobre el servidor NT. Esta característica permite la implementación de varios servidores virtuales dentro de la misma máquina física. Los webs virtuales aparentan a los usuarios estar funcionando sobre diferentes servidores, los cuales pueden tener un host y/o nombre de dominio único.

IIS provee el soporte para CGI y PERL así como una aplicación ISAPI que permite la conexión a bases de datos ODBC. No posee ninguna herramienta propia de desarrollo de páginas, sin embargo su integración con Front Page 98 es sin duda bastante buena.

**NetScape Enterprise 3.5.1 (NES)/ Fast Track Server (NFTS)
 NetScape Corp.
 Estudio - Prueba**

Podríamos decir que NES construye sobre NFTS un bloque más sólido, incluyendo características como el compartir páginas en el desarrollo y administración por un equipo de trabajo, certificado de autenticación por parte del cliente, una máquina de búsqueda, soporte a Simple Network Management Protocol (SNMP), administración del contenido del web a través de livewere¹ y un controlador de versiones.

Ambos productos están disponibles para Windows NT y Solaris. Todos los servidores web de NetScape incluyen Navigator Gold (Browser que analizaremos en el siguiente tema) y soporte para HTTP 1.1, así como el correspondiente soporte para Java y Java Script.

El proceso de instalación para ambos paquetes resulta sencillo, sobre todo en la plataforma de Windows NT donde basta con dar click en un icono. Sobre solaris, es necesario descomprimir un archivo que contiene, entre otras cosas, el archivo de instalación. Una vez instalados, el proceso de configuración para ambos es el mismo: a través del browser utilizando Netscape Server Manager (NSM). Como un resultado de esto, no es necesario diferenciar la configuración dependiendo de la plataforma o sistema operativo en particular, ya que es posible administrar el web server de manera remota.

Dentro de la misma herramienta de administración es muy simple dar de alta usuarios, sin embargo, la situación se complica un poco cuando se desea restringir acceso a los directorios, debiéndose mantener una lista separada de usuarios y contraseñas con el servidor.

NSM permite especificar servidores virtuales, lo cual da como resultado el mapeo de páginas a dominios separados sobre una misma máquina, como también el restringir accesos en base a dominio o direcciones IP.

¹ Lenguaje de programación de scripts.

El manejo de los archivos de "log" en NFTS es adecuado, ya que maneja de forma separada el archivo de acceso y de errores, dichos archivos pueden ser vistos a través del browser, sin embargo no se almacenan ciertos eventos como son: la ejecución de CGI o el encabezado de los campos de HTTP. En el caso de Enterprise Server esto no ocurre, ya que es posible monitorear los eventos de CGI y otras actividades utilizando las opciones personalizadas para los archivos de log.

NSM y NFTS permiten a los desarrolladores escribir programas en C directamente sobre las API del servidor. Ambos servidores están provistos de un editor de páginas HTML en base a WYSIWYG HTML. NFTS aumenta una característica más: LiveWare, lo cual permite crear aplicaciones compiladas utilizando JavaScript.

NES posee una herramienta propiedad de MKS (Mortice Kern Systems) para el control de versiones así como una máquina de búsqueda y la extensión de "AutoCatalog", que permite al usuario establecer vistas de documentos por autor, fecha de modificación o rango de consulta. "AutoCatalog" puede ser ejecutado de manera automática, proporcionando última información sin la intervención del administrador (webmaster).

**NetWare Web Server (NWS)
Novell Inc
Estudio - Prueba.**

Aparenta ser una excelente opción sobre, sobre todo por la compatibilidad sobre las redes Novell (caso Banco de México), sin embargo tiene características de acceso limitadas y carece de soporte sobre SSL, servidores virtuales y herramientas de administración. La empresa Novell ha comentado que agregará la mayoría de estas características para sus próximas versiones.

El Servidor de web de Novell es un conjunto de NLMs (Netware Loadable Module) que se ejecutan sobre NetWare 4.x. Para hacer funcionar el servidor es necesario instalar TCP/IP NLM, el cual está incluido dentro del sistema operativo Novell.

Las características de administración son muy simples. El servidor se administra a través de una utilidad llamada Web Manager. Aplicaciones de NLM proveen algunas características básicas de monitoreo y reportes, pero ninguna a un nivel detallado.

La seguridad es manejada a través de NDS (Netware Directory Services). Garantizando el acceso a grupos o usuarios basado en la identificación de direcciones IP o nombres de dominio no así por nombre de host. Sin embargo, si se desea dar acceso a todos los elementos de la red excepto a uno, es necesario agregar a todos los usuarios dentro de la lista de control de acceso.

Netware Web Server provee una no muy robusta máquina de búsqueda, así como solo el soporte estándar para CGI y PERL, incluyendo también un intérprete básico para JavaScript y un lenguaje local propietario de Novell para el Common Gateway Interface (CGI). A diferencia de las comunicaciones estándares de CGI, las cuales se comunican a través de sockets de TCP/IP, LCGI utiliza un programa denominado STREAMS.NLM. Utilizando LCGI es posible escribir aplicaciones que interactúen con otros NLM's sobre el

servidor, tales como bases de datos. Sin embargo, NWS no provee una conexión directa con bases de datos no-Netware, lo cual se espera que realice en versiones posteriores.

La guía de desarrollo, incluida con el servidor de web, es un camino apropiado para iniciar en LCGI así como para otras herramientas de soporte del propio web. Novell incluye varias aplicaciones ejemplo y scripts escritos en CGI, PERL, BASIC y LCGI dentro de esta guía.

**Purveyor Encrypt Web Server (PE)
Process Software Corp.
Estudio**

PE contiene un amplio conjunto de utilerías de administración así como una administración remota bastante robusta, sin embargo, el desempeño sobre Windows NT es por debajo de IIS o NES. PE es instalado como un servicio sobre Windows NT, el cual puede iniciar de manera automática en conjunto con el servidor.

A través de la ventana de administración (se presupone un ambiente gráfico) es posible configurar el uso de servidores virtuales así como de servidores proxy. Estas actividades pueden ser ejecutadas de igual manera de forma remota utilizando el web browser. La configuración de archivos, en el aspecto de seguridad, corre a cargo del administrador de archivos propio de NT. Sin embargo PE agrega extensiones para convertirla en un aspecto por demás simple. Estableciendo restricciones sobre directorios, direcciones IP o grupos de estas.

Las rutas virtuales sobre el servidor no son desplegadas por el administrador de archivos de NT, por tal motivo es preciso recordar la ruta exacta para su localización. Al igual que IIS, PE tiene acceso a las bases de datos propias del servidor con las ventajas que ya hemos mencionado.

Entre las herramientas de administración de documentos, PE cuenta con un traductor para HTML, el cual no es tan simple de manejar y no cuenta con la característica de WYSIWYG, por tal motivo es necesario estar abriendo la página en el browser para evaluar los resultados.

El acceso a base de datos es realizado por medio de los controladores de ODBC, incluidos muchos de estos dentro de PE. Las opciones de log son configuradas a través de "templates" o bien personalizadas al crear una plantilla propia a través de comandos de script.

Otra características de PE es el soporte para SSL 2.0, lo que permite la creación de llaves certificadas, las cuales deben ser enviadas a una autoridad certificadora; una vez echo esto, es posible colocarlas en una base de datos para su administración y entonces ser asignadas a servidores virtuales.

**Stronghold Apache-SSL-US 1.2.5
Community ConneXion Inc
Estudio.**

Apache es un servidor de web basado en UNIX, requiriendo un conocimiento experto del mismo. Referente al soporte técnico, a diferencia del resto de los productos, este solo es disponible a través de correo electrónico.

Las versiones gratuitas de apache soportan la mayoría de las plataformas UNIX así como OS/2. El código fuente al ser modificable, brinda la flexibilidad para la personalización del servidor en base a los requerimientos propios, así como el soporte para SSL.

Apache no posee ningún tipo de interfaz gráfica, tanto la instalación como configuración son procesos que se realizan en base a archivos o comandos de tipo *shell* de UNIX. Existen cinco archivos de log que reportan la actividad del servidor de web, la actividad de SSL y errores asociados.

No existen herramientas o utilerías de administración, como tampoco algún tipo de máquina de búsqueda, sin embargo a través del archivo HTTPD.CONF es posible implementar varios niveles de control administrativo.

Modificando el archivo HTTPD.CONF es posible implementar un control de acceso al web así como a páginas del mismo, configurar la seguridad de SSL y manejar múltiples sitios web sobre el mismo servidor. Alternativamente, es posible utilizar autenticación, conectividad a bases de datos o herramientas de administración, utilizando CGI y las API's propias de Apache.

Como característica extra, apache soporta cualquier lenguaje de script compatible con UNIX, como PERL, Python o Java.

**Web Site Profesional 2.1 (WSP)
O'relly & Associates Inc
Estudio.**

WSP incluye una muy buena documentación así como un grupo de herramientas de administración, un editor de HTML y herramientas para indexación de documentos. Sin embargo, los niveles de desarrollo sobre una red con tráfico considerable se ven disminuidos sustancialmente.

WSP sobre Windows NT puede ser ejecutado como una aplicación o un servicio. La administración es transparente en un ambiente gráfico, mostrando diez carpetas diferentes perfectamente documentadas, sin embargo lo anterior no se aplica cuando la administración es de manera remota. La administración remota requiere de una instalación complicada debido a que es necesario manejar el registro de información del propio Windows.

Es posible configurar el servidor de web con múltiples nombres de dominio, así como con rutas virtuales (permitiendo almacenar archivos en diferentes lugares físicos dentro del servidor). Mientras, por otro lado, una interfaz realiza la comparación entre de las rutas lógicas URL con los directorio físicos.

A diferencia de servidores como IIS, no es posible combinar la base de datos de WSP con Windows NT, es decir, el administrador deberá mantener dos bases de usuarios de manera independiente.

WSP soporta SSL, manejando los niveles de autenticación en base a una autoridad de certificación para la generación de llaves. Así también, incluye un conjunto de herramientas para el desarrollo de aplicaciones y API's, una muy buena documentación, ejemplos y el soporte para la conexión a bases de datos a través de ODBC.

WebSite Professional permite la publicación de páginas en base a la implementación de NetScape, es decir, es posible publicar páginas editadas directamente en el browser, pero es imposible crear directorios desde el mismo punto. WSP mantiene tres archivos configurables de log: Accesos remotos, error, (por parte de peticiones de clientes) y un rastreador de las aplicaciones de CGI, este ultimo incluye estadísticas de red.

WebIndex, es una máquina de búsqueda que reside en el servidor, permite a los usuarios de WSP realizar búsquedas por medio de un programa escrito en CGI llamado WebFind.

**Java Web Server 1.1 (JWS)
Sun Microsystems Inc.
Estudio.**

JWS es un servidor de web escrito totalmente en Java, cuyas herramientas de administración no se encuentran al nivel de otras aplicaciones en lo que a su interfaz gráfica se refiere.

JWS solo esta disponible para Windows NT y Solaris y esta basado sobre el nuevo modelo de Servlet. Un Servlet puede proveer funciones de web tales como: mostrar páginas, mantener sesiones y analizar logs.

La ventaja de JWS es que cualquier cosa que pueda ser desarrollada en Java puede ser incrustada al servidor, por tanto, es posible tomar ventaja de todas las características de este lenguaje de programación², tales como: conexiones JDBC y Java beans, para el desarrollo de aplicaciones dinámicas sobre Internet.

² Para mayor información acerca de Java es posible consultar : <http://java.sun.com>

Como plataforma para aplicaciones JWS es la mejor opción para desarrollo en Java. La característica denominada "compilación de página" permite incrustar código Java directamente en las páginas HTML, dejando el resto como tarea para el servidor. Esta función es similar a lo que presenta IIS con ASP, sin embargo la "compilación de página" no es a través de scripts, es código Java compilado con los servlets en tiempo de ejecución.

El diseño de páginas es relativamente fácil con el uso de plantillas basadas en servlets, las cuales permiten modificar la vista del servidor al modificar dichas plantillas. No existe un buen soporte para CGI, sin embargo si se considera trabajar sobre Java, CGI resulta poco práctico.

La parte de administración es a través del browser, es decir, funciona por medio de un applet con la facilidad de cualquier ventana de un ambiente Windows. Sin embargo características como "multihoming" y la creación de certificados, requieren de una utilidad denominada "Addservice", cuya función es por medio de comandos en línea lo que implica un mayor dificultad. La mayor parte de los cambios son ejecutados en línea, sin embargo acciones como establecer SSL para una transmisión requieren del re-inicio total del servidor.

La creación de directorios virtuales requiere de conocer la ruta física exacta del directorio, ya que no es posible navegar por el disco duro para poder tener acceso a ésta. JWS soporta alias basados en servlet, es decir, el URL puede ser mapeado directamente a un servlet.

4GL

Lenguaje de cuarta generación

ActiveX

Conjunto de tecnologías creadas por Microsoft, que habilita un contenido interactivo sobre el WWW. Con ActiveX es posible utilizar efectos multimedia, objetos interactivos y aplicaciones sofisticadas sobre las páginas de web.

API

Application Programming Interface

Serie de funciones que los programas pueden utilizar para realizar trabajo sobre el sistema operativo.

Applet

Equipo que puede ser cargado de forma rápida y utilizado por cualquier computadora equipada con un browser que soporte Java o ActiveX.

ASCII

American Standard Code for Information Interchange

Estándar mundial para los números código utilizados por las computadoras para representar letras, números, puntuación, etc. Utilizado también para describir archivos almacenados en texto plano.

ASP

Active Server Pages

Tecnología desarrollada por Microsoft, diseñada para crear páginas HTML de forma interactiva. Parte del concepto denominado *plataforma activa* desarrollado para WinNT y IIS.

Browser

Programa que permite a los usuarios acceder documentos sobre WWW. Los browsers son capaces de manipular texto o gráficas, con la capacidad de leer código HTML que reside sobre el servidor e interpretarlo.

Cache

El cache existe en diferentes tipos, pero actúa siempre de la misma forma: almacena información para su rápido acceso. El cache de un browser almacena el código de las páginas HTML así como sus gráficas y elementos multimedia, de esta forma, cuando se regresa a una página, no es necesario cargar otra vez todo de nuevo ya que el acceso al disco duro es más rápido que el acceso a Internet.

CGI**Common Gateway Interface**

Estándar utilizado para la ejecución de programas desde un servidor de web. Los programas o scripts son programas ejecutables capaces de invocarse a si mismos. Creados como programas externos con el objetivo de poder funcionar bajo diferentes plataformas. Pueden ser escritos en cualquier lenguaje capaz de producir un ejecutable incluyendo: C o C++, Perl, Python, TCL, shells, etc.

DBMS**DataBase Managment System.**

Sistema de administración de Base de datos. Entre los más comunes destacan: Sybase y Oracle.

DHCP**Dynamic Host Configuration Protocol.**

Protocolo que permite a computadoras individuales sobre una red obtener su configuración de un servidor (DHCP server), en particular, los servidores no tienen información exacta acerca de los computadores individuales hasta que estos realizan una petición.

DNS**Domain Name System**

Sistema que permite traducir una dirección IP a un nombre de dominio. Un DNS es un servicio de nombres jerárquicos, utiliza TCP/IP y es utilizado por los servidores sobre Internet. Permite a los usuarios especificar computadoras remotas basado en el host o dirección IP.

Extranet

La conexión de dos o más intranets. Una Intranet es un servidor de web Interno el cual permite a los usuarios dentro de la institución comunicarse e intercambiar información, conectando dos espacios virtuales, de esta forma se logra una extranet.

File System

Sistema de archivos y directorios de los sistemas operativos.

Groupware

Software para ambientes interactivos y compartidos. Es decir, permite que grupos de personas interactúen en una tarea común proporcionando una interfaz para un ambiente compartido.

Host

Cualquier computadora que pueda funcionar como principio y fin en una transferencia de datos. Un host en Internet tiene una dirección IP y nombre de dominio únicos.

HTML**HyperText Markup Language**

Método de codificación utilizado para dar formato a documentos sobre WWW. Las páginas de web es posible verlas en parte por el código HTML el cual es interpretado por el browser.

HTTP**HyperText Transfer Protocol**

Protocolo de transferencia de recursos del WWW, el cual permite que un servidor maneje más conexiones y distribuya datos de una forma más rápida que la mayoría de los protocolos existentes.

Internic**INTERNet Network Information Center**

Repositorio de información acerca de Internet. Es dividido en dos partes: 1) Directorio de Servicios y 2) Registro de servicios. Fundado parcialmente por La Fundación Nacional De Ciencia (NSF). Entre sus funciones destacan la asignación homologada de direcciones IP.

Intranet

Término utilizado para la implementación de las tecnologías Internet dentro de una organización corporativa.

IP**Internet Protocol**

Protocolo de bajo nivel que enruta paquetes de datos a través de redes separadas vinculadas por ruteadores.

ISAPI**Internet Server Application Program Interface**

Implementación de Microsoft para ejecutar tareas similares a las realizadas por CGI utilizando librerías dinámicas (DLL's).

ISP**Internet Service Provider**

Compañía que provee el acceso a Internet. Antes de establecer la conexión a Internet es necesario generar una cuenta con el ISP. El proveedor de servicios en Internet es elemento sustancial dentro del esquema de conexión a Internet ya que es la conexión física al NAP, punto final para la información en Internet.

JAVA

Lenguaje de programación orientado a objetos de propósito general desarrollado por Sun Microsystems.

LAN**Local Area Network**

Una red de área local es una red de computadoras confinada a un espacio, edificio o grupo de edificios adyacentes. Una red similar pero a mayor escala es referida como WAN (Wide Area Network) o en algunos casos mas específicamente MAN (Metropolitan Area Network).

MIME**Multipurpose Internet Mail Extensions**

Protocolo para correo sobre internet, el cual permite la transmisión de datos no textuales como gráficas, audio video y otros tipos de datos binarios.

Modem**MOdulator, DEModulator**

Dispositivo conectado a la computadora y a la línea telefónica el cual permite que ésta pueda comunicarse con otras computadoras a través del sistema telefónico.

NAP**Network Access Point**

Los puntos de acceso a Internet (NAP's) son puntos de intercambio de tráfico en Internet. Los ISP's conectan sus redes al NAP para propósitos de intercambio con otros ISP's. Esto permite a los ISP's regionales conectarse al backbone de los grandes proveedores, ruteo, resolución de direcciones y asistencia. Los proveedores del backbone nacional conectados al NAP obtienen los beneficios de la base de clientes del ISP regional.

NFS**Network File System**

Conjunto de Protocolos desarrollados por Sun Microsystems que permite a diferentes computadoras ejecutar diferentes sistemas operativos para compartir recursos y almacenamiento en disco.

ORB**Object Request Broker**

Estándar para objetos distribuidos desarrollado por el Object Management Group (OMG), el cual es un grupo de distribuidores de software y usuarios finales. El nombre formal del estándar es CORBA (Common Object Request Broker Architecture), permite proporcionar mecanismos en los cuales los objetos de forma transparente hacen solicitudes y reciben peticiones. Esta arquitectura soporta interoperatividad entre objetos construidos en diferentes lenguajes, funcionando en diferentes plataformas en un ambiente heterogéneo.

Protocolo

Especificación que describe como las computadoras pueden comunicarse unas con otras sobre una red.

Proxy**o proxy server**

Técnica utilizada para el manejo de la información almacenada sobre un servidor de web a forma de cache, actúa como un intermediario entre el cliente y el servidor. Básicamente trabaja sobre la más común y reciente información utilizada sobre el WWW para proveer acceso rápido e incrementar la seguridad.

POP**Post Office Protocol**

Protocolo utilizado por clientes de correo para obtener mensajes de un servidor de correo. Existen POP1, POP2 y POP3, donde el número denota la versión del protocolo.

Ruteador

Hardware o software que permite conectar redes locales a Internet. Los ruteadores gastan su tiempo buscando las direcciones destino de los paquetes que pasan a través de él y decidiendo a que ruta enviarlos.

Script

En el contexto de WWW, un script es un programa que se ejecuta sobre el servidor y procesa peticiones basadas en la información proporcionada por el browser.

Shell

La capa más externa de una aplicación que proporciona la interfaz con el usuario o con otras aplicaciones.

SQL**Structured Query Language**

Lenguaje de consulta estructurado. Utilizado para la petición de datos en un DBMS

SSL**Secured Sockets Layer**

Protocolo que habilita la autenticación en un servidor, encriptación de datos, e integridad de los mensajes. SSL opera entre las conexiones de TCP/IP y el servicio de HTTP. Esto permite a SSL operar de forma independiente de los protocolos de aplicación de Internet. Con SSL implementado en ambos extremos (cliente – servidor), las comunicaciones en Internet son transmitidas de forma encriptada.

Trama

Unidad de transmisión en la capa de enlace de datos del protocolo TCP/IP

Two phase Commit

Método de alta consistencia para distribuir datos en diferentes servidores.

URL**Uniform Resource Locator**

Describe la localización y método de acceso hacia un recurso en Internet, por ejemplo, el URL <http://www.banxico.org.mx> describe el tipo de método de acceso siendo utilizado (http), y la localización del servidor (www.banxico.org.mx). La nomenclatura completa de un URL sería *protocolo://servidor:puerto/ruta*.

WINS**Windows Internet Name Service**

Servicio que mantiene una base de datos en una computadora acerca de mapeos entre nombres y direcciones IP.

WorkFlow

Flujo de trabajo, conjunto de herramientas que permite el trabajo en grupo estableciendo las rutas y el control de un proceso determinado.

WWW**o web o W3**

Técnicamente sistema global de hipertexto que utiliza Internet como su medio de transporte. En un sistema de hipertexto se navega accionando hiperligas, las cuales despliegan otros documentos, los cuales contienen a su vez otras hiperligas.