

# **Universidad de las Américas**

**Facultad de Ingeniería**

**“Administración remota de Sistemas,  
utilizando herramientas de acceso para Internet”**

Trabajo de titulación presentado en conformidad a los requisitos para obtener el título  
de Ingeniero de Sistemas en Computación e Informática.

Profesor guía: Ing. Carlos Javier Luna Sevilla

Autor: Fernando Rafael Sandoval Galárraga

**2000**

Certifico que bajo mi dirección el presente trabajo fue  
realizado en su totalidad por el señor:

Sandoval Galárraga Fernando Rafael

---

Ing. Carlos Javier Luna Sevilla  
Tutor de trabajo de Titulación

## **AGRADECIMIENTO**

A todos los personeros de la Compañía Petróleos y Servicios, a la Unidad de Sistemas en la persona de la Tlga. Doris Lema Tapia, que me brindaron su colaboración, apoyo y toda la facilidad para la consecución de este trabajo.

De igual forma al Ing. Javier Luna Sevilla, tutor del presente trabajo, quien con carisma y paciencia, supo impartirme sus conocimientos durante este proyecto, y guiarme durante todos estos años de estudio.

## DEDICATORIA

A Dios, por permitirme la existencia, y por brindarme el entusiasmo, la fuerza, el coraje, y las bendiciones que he sentido cada día.

A mis padres que me dieron la vida y me siguen brindando la sabia luz que ilumina el camino que recorro, quienes con su ejemplo de dignidad, honradez y sabiduría me supieron guiar en cada momento, en las penas, en las glorias, y que han hecho posible el culminar con éxito mis estudios.

A Anita, que más que esposa, ha sido amiga, ha sido amor e inspiración. Gracias por estar siempre a mi lado.

A mis hermanos y amigos, que me ayudaron vigorosamente con su apoyo desinteresado, a superar pruebas y dificultades a lo largo de estos años.

Muchas gracias y que Dios les bendiga.

Fernando Rafael.

## **Resumen Ejecutivo**

La sociedad, y el mundo globalizado actual, hacen posible el acceso remoto a redes, permitiendo que un usuario pueda acceder a una LAN desde cualquier parte del mundo y permitiendo que no sólo las grandes empresas, sino las pequeñas y medianas empresas (PYMES), puedan utilizar la Internet, como una herramienta tecnológica que les permita reducir costos y aumentar sus ganancias.

Es en este contexto, en el cual se enfoca el trabajo tecnológico realizado en el presente documento, describiendo los procedimientos y protocolos de la Internet, así como, generando una aplicación llamada ARSP (Administración Remota de Sistemas para PYMES), la cual permite la administración remota de sistemas a través de una Intranet, con tecnología Internet, y de ésta manera, brindar una solución para el aumento de la productividad de las empresas ecuatorianas y a la vez, haciendo posible el continuar diseñando aplicaciones que funcionen sobre la Internet y que aporten al desarrollo de nuestra sociedad.

La implementación del sistema de administración remota desarrollado en éste trabajo, permitirá la validación de usuarios del sistema, el ingreso de información, su consulta y la actualización de la misma, la cual se encuentra en una Base de Datos Relacional.

Para mantener una política de unificación de Tecnología, se utilizan herramientas Microsoft. De esta manera, tenemos como sistema operativo, al sistema Windows NT Server. Como servidor Web: MS Internet Information Server. En lo que respecta a la base de datos, se utilizo MS SQL Server y como Browser para el acceso remoto de los clientes, se utilizo MS Internet Explorer. De igual manera la herramienta para el desarrollo de la aplicación ARSP, es MS Visual Interdev 6.0.

En definitiva, este trabajo posibilita la inserción de las PYMES ecuatorianas dentro del ambiente tecnológico actual, a un bajo costo y con alta productividad.

## Índice

<b>1. INTRODUCCIÓN</b> .....	<b>11</b>
<b>2. FUNDAMENTO TEÓRICO</b> .....	<b>12</b>
<b>2.1. Qué es Internet</b> .....	<b>12</b>
<b>2.2. Evolución de Internet</b> .....	<b>12</b>
2.2.1. Década de los '60 .....	12
2.2.2. Década de los '70 .....	12
2.2.3. Década de los '80 .....	12
2.2.4. Década de los '90 .....	12
<b>2.3. Características de Internet</b> .....	<b>13</b>
<b>2.4. Organismos relacionados a Internet</b> .....	<b>13</b>
2.4.1. World Wide Web Consortium (W3C).....	13
2.4.2. Internet Engineering Task Force (IETF) .....	13
2.4.3. Electronic Frontier Foundation (EFF).....	13
<b>2.5. Intranet</b> .....	<b>14</b>
<b>2.6. Extranet</b> .....	<b>14</b>
2.6.1. Que es Firewall (Corta fuegos).....	14
2.6.1.1. Filtrado de Paquetes .....	14
<b>2.7. Qué es VPN</b> .....	<b>15</b>
<b>2.8. Que es TCP / IP</b> .....	<b>16</b>
2.8.1. Descripción del Modelo de Capas de TCP/IP .....	17
2.8.1.1. Capa de Aplicación.....	17
2.8.1.2. Capa de Transporte.....	17
2.8.1.3. Capa Internet.....	18
2.8.1.4. Capa de Interface de Red.....	18
2.8.2. Suite de protocolos de TCP/IP .....	18
2.8.2.1. Internet Protocol (IP) .....	18
2.8.2.2. Address Resolution Protocol (ARP) .....	18
2.8.2.3. Internet Control Message Protocol (ICMP).....	19
2.8.2.4. Transmission Control Protocol (TCP) .....	19
<b>2.8.2.4.1. Puertos TCP</b> .....	<b>20</b>
2.8.2.5. User Datagram Protocol (UDP).....	20
<b>2.8.2.5.1. Puertos UDP</b> .....	<b>21</b>
<b>2.9. Protocolos de Internet</b> .....	<b>21</b>
2.9.1. HyperText Transfer Protocol (HTTP) .....	21
2.9.1.1. Funcionamiento General de HTTP .....	22
2.9.2. Simple Mail Transport Protocol (SMTP) .....	22
2.9.2.1. El Modelo SMTP .....	22
2.9.3. Internet Relay Chat (IRC) .....	23
2.9.4. Multipurpose Internet Mail Extensions (MIME) .....	23
2.9.5. Post Office Protocol (POP3) .....	24
2.9.6. Network News Transfer Protocol (NNTP).....	24
<b>2.10. Dominio</b> .....	<b>24</b>
2.10.1. Dirección en la Web (nombre de dominio) .....	25
2.10.2. Extensiones en una Dirección en la Web .....	25
2.10.3. Caracteres válidos para una Dirección en la Web y su longitud máxima.....	25
<b>2.11 Qué es un nodo Web</b> .....	<b>26</b>

2.12. URL(Localizador de Recursos Universal) .....	26
2.13. Servicios De Internet.....	26
2.13.1. Correo Electrónico (E-Mail) .....	27
2.13.2. Foros de Debate o Grupos de Noticias (News) .....	27
2.13.3. Conferencia Electrónica (IRC).....	27
2.13.4. Sesiones Remotas (Telnet) .....	27
2.13.5. Transferencia De Archivos (FTP) .....	28
2.13.6. Directorios de Información (Gopher).....	28
2.13.7. World Wide Web.....	28
2.14. El Crecimiento de Internet.....	29
<b>3. SEGURIDAD EN LA INTERNET.....</b>	<b>30</b>
<b>3.1. Criptografía .....</b>	<b>30</b>
<b>3.2. Privacidad en las transmisiones de Internet.....</b>	<b>31</b>
<b>3.3. Servicios de seguridad .....</b>	<b>32</b>
<b>3.4. Mecanismos de seguridad.....</b>	<b>33</b>
<b>3.5. Distribución de claves .....</b>	<b>34</b>
<b>3.6. El certificado digital.....</b>	<b>34</b>
<b>3.7. Protocolos de seguridad en Internet.....</b>	<b>35</b>
3.7.1. Secure Socket Layer (SSL) .....	35
3.7.1.1. Solicitud de SSL .....	35
3.7.1.2. SSL Handshake.....	36
3.7.1.3. Intercambio de datos .....	37
3.7.1.4. Terminación de una sesión SSL.....	37
3.7.2. Secure Electronic Transaction (SET) .....	37
<b>3.8. Algoritmos de firma digital.....</b>	<b>39</b>
3.8.1. Firmas de comprobación aleatoria (HASH).....	39
3.8.2. El algoritmo DSS.....	39
3.8.3. Algoritmo RSA.....	40
<b>3.9. Niveles de Seguridad en Redes .....</b>	<b>40</b>
3.9.1. Nivel D1 .....	40
3.9.2. Nivel C1 .....	41
3.9.3. Nivel C2 .....	41
3.9.4. Nivel B1 .....	41
3.9.5. Nivel B2 .....	41
3.9.6. Nivel B3 .....	41
3.9.7. Nivel A .....	41
<b>4. INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE PARA EL DESARROLLO EL PROYECTO .....</b>	<b>42</b>
<b>4.1. Configuración de Windows NT Server .....</b>	<b>42</b>
<b>4.2. Configuración de Internet Information Server.....</b>	<b>43</b>
4.2.1. Internet Information Server incluye los siguientes componentes: .....	43
4.2.2. Instalación de Internet Information Server.....	43
Proceso de instalación de Internet Information Server .....	45
4.2.1.2. Comprobar un servidor Web en una Intranet.....	46
4.2.1.3. Cómo se usa Internet Information Server .....	46
4.2.1.4. Escenarios de Intranet .....	46
<b>4.3. Configuración y administración de Internet Information Server (IIS)....</b>	<b>48</b>
4.3.1. Conexión a servidores Web.....	48
4.3.2. Inicio, detención y pausa en un servicio.....	51

4.3.3. Configuración y administración de servicios .....	51
<b>4.4. Publicación de información en una Intranet .....</b>	<b>51</b>
4.4.1. Sistemas de resolución de nombres .....	51
4.4.1.1. Uso de nombres de equipos con servidores de WINS .....	52
4.4.1.2. Uso de nombres de dominio con servidores DNS .....	52
4.4.1.3. Uso de DHCP en su Intranet .....	52
4.4.1.4. Uso de direcciones URL y creación de vínculos HTML para Intranet .....	52
4.4.1.5. Monitorización con SNMP .....	52
<b>4.5. Protección contra intrusos .....</b>	<b>53</b>
4.5.1. Funcionamiento de la seguridad de Internet Information Server .....	53
4.5.2. Control de accesos anónimos .....	54
4.5.3. Control del acceso por usuario o por grupo.....	55
4.5.4. Asignar un nombre de usuario y una contraseña.....	55
4.5.5. Como interactúan los inicios de sesión anónimos y la autenticación de clientes.....	56
4.5.5.1. Servicio WWW .....	57
4.5.5.2. Servicio FTP .....	57
4.5.6. Establecimiento de permisos de carpeta y archivo.....	58
4.5.6.1. Establecimiento de permisos NTFS.....	58
4.5.6.2. Establecimiento del acceso al directorio WWW .....	58
4.5.6.3. Control de acceso mediante la dirección IP.....	59
4.5.7. Seguridad en la transmisión de datos usando Secure Sockets Layer (SSL) .....	59
4.5.7.1. Generación de un par de claves .....	60
4.5.7.2. Adquisición de un certificado .....	61
4.5.7.3. Instalación de un certificado con un par de claves .....	61
<b>4.6. Diseño de los directorios de contenido y de los servidores virtuales .....</b>	<b>62</b>
4.6.1. Configuración de un único directorio de contenido .....	62
4.6.2. Definición del documento predeterminado y del examen de directorios .....	62
<b>4.7. Registro de la actividad del servidor .....</b>	<b>63</b>
4.8. Publicación de información y uso de una base de datos .....	63
4.8.1. Funcionamiento del Conector de bases de datos de Internet .....	63
<b>5. DESARROLLO DEL PROYECTO .....</b>	<b>65</b>
<b>5.1. Conceptos necesarios para la introducción del proyecto .....</b>	<b>65</b>
5.1.1. Proyectos Web con Microsoft Visual InterDev .....	65
5.1.1.1. Visual InterDev: plataforma de desarrollo de proyectos Web....	65
5.1.1.2. El asistente de creación de proyectos Web (Web Project Wizard) .....	65
5.1.1.3. Ficheros creados por defecto en el proyecto.....	66
<b>5.1.1.3.1. El fichero global.asa .....</b>	<b>66</b>
5.1.1.4. Ficheros y proyectos .....	66
5.1.2. Introducción a las Páginas Activas de Servidor .....	67
5.1.3. HTTP y las aplicaciones Web .....	67
5.1.4. Acceso a bases de datos en proyectos Web.....	68
5.1.4.1. Bases de datos y Web .....	69
5.1.4.2. Interfaz entre las aplicaciones y el gestor .....	69
5.1.4.3. Acceso a bases de datos en Visual InterDev y IIS.....	69



5.1.4.4. Creación de un proyecto que acceda a bases de datos .....	70
<b>5.1.4.4.1. Adición de una conexión de datos a una base de datos existente</b> .....	70
<b>5.1.4.4.2. Diseñador de consultas: Query Designer</b> .....	70
5.1.4.4.3. Formularios con acceso a datos .....	71
5.1.4.4.4. Controles en tiempo de diseño para bases de datos .....	71
5.1.4.4.5. Acceso avanzado a bases de datos .....	72
<b>5.1.4.4.5.1. ActiveX Data Objects (ADO)</b> .....	72
<b>5.1.4.4.5.2. Advanced Data Connector</b> .....	72
<b>5.2. Marco teórico del proyecto</b> .....	<b>74</b>
5.2.1. Diagrama de procesos de una Comercializadora de Combustibles.....	74
<b>5.3. Modelo de la Base de Datos de @rsp</b> .....	<b>77</b>
5.3.1. Información de tablas .....	77
<b>5.4. Modelo de control de accesos para @rsp</b> .....	<b>85</b>
5.4.1. Información de tablas .....	85
5.4.2. Triggers de control .....	86
<b>5.5. Listado de Hardware y Software necesario</b> .....	<b>89</b>
5.5.1. Software.....	89
5.5.2. Hardware .....	89
<b>5.6. Datos técnicos del sistema propuesto:</b> .....	<b>89</b>
<b>5.7. Presentación de las pantallas</b> .....	<b>90</b>
<b>6. CONCLUSIONES</b> .....	<b>102</b>
<b>BIBLIOGRAFÍA</b> .....	<b>104</b>
<b>WEBLIOGRAFÍA</b> .....	<b>104</b>
<b>ANEXOS</b> .....	<b>105</b>
<b>Glosario</b> .....	<b>105</b>

## 1. Introducción

Resaltamos el hecho de que en la actualidad una empresa u organización puede utilizar Internet, una red pública de transmisión de datos, para enlazar dos o más LANs. Sin Internet, la interconexión de redes situadas en ciudades o países distintos, estaba reservada únicamente a multinacionales. Pero gracias a Internet, también es posible para empresas mucho más pequeñas llamadas PYMES, debido a un factor clave: un coste mucho menor.

Otro punto importante para las aplicaciones sobre Internet, es que no hay diferencia entre empresas grandes y pequeñas en la red, incluso empresas medianas y pequeñas, con fuentes limitadas para administración y finanzas, son capaces de valerse de las oportunidades comerciales si saben aprovechar la administración y el comercio electrónicos.

En lo referente al acceso remoto a las redes, a la administración remota de los sistemas y por ende, de los negocios a través de la Internet, el gobierno estadounidense en 1998, las reconoció como las innovaciones claves de la segunda mitad del siglo veinte atribuyendo al uso de la Internet por las empresas, un papel significativo en el sorprendente crecimiento continuo durante más de diez años de la economía estadounidense. Este reconocimiento no hace más que ubicar al comercio y a la administración de los negocios a través de la Internet, como herramientas que afectan no solamente los medios para el intercambio de mercaderías y servicios, sino también los procedimientos internos de las organizaciones, rebajando costos en compras, controlando las relaciones con proveedores, con sistemas logísticos y de inventario más sofisticados, y mejorando la planificación de la producción.

Pero el acceso a una red o a la información está totalmente ligada a las personas, a sus instintos y a sus percepciones, por lo tanto en cualquier acceso a la información surge un problema importante: la seguridad.

No es admisible de ninguna manera, que la información que circule por Internet sea captada por terceros. En este caso es imprescindible utilizar sistemas de encriptación. Para resolver estos temas de seguridad están surgiendo nuevos protocolos, como por ejemplo, el PPTP (Point-to-Point Tunneling Protocol), el cual reduce el costo del acceso remoto a redes y proporciona un canal seguro en Internet entre LAN origen y destino. En el caso de servicios como el correo electrónico también es necesario la autenticación del origen de los mensajes, utilizando técnicas de firma electrónica, etc. Los mecanismos de seguridad se describen en extenso en el capítulo II de este trabajo tecnológico.

## **2. Fundamento teórico**

### **2.1. Qué es Internet**

La Internet es una red de redes. Actualmente conecta miles de redes para permitir compartir información y recursos en todo el mundo. Con la Internet los usuarios pueden compartir, prácticamente, cualquier cosa almacenada en una computadora.

La Internet tiene un vasto y valioso uso para los usuarios que navegan su espacio electrónico, e incluye: comunicación y colaboración a larga distancia; acceso a computadoras y redes remotas con el fin de compartir aplicaciones, documentos en formato de texto; acceso a bancos de datos y catálogos de librerías en línea; acceso a la "educación a distancia"; y finalmente la posibilidad de entrar a los archivos de supercomputadoras.

### **2.2. Evolución de Internet**

#### **2.2.1. Década de los '60**

En 1960, el Transmission Control Protocol y el Internet Protocol (TCP/IP) fueron desarrollados para proveer rápida comunicación entre dos dispositivos de red. Estos protocolos de red fueron desarrollados para proveer un enlace de comunicación, aún si algunos de los enlaces entre los dispositivos llegaron a fallar.

La corporación RAND, en conjunto con el Instituto de Massachusetts de Tecnología y la Universidad de California en los Angeles, desarrollaron ésta tecnología para el Departamento de Defensa de los Estados Unidos. Esta agencia de gobierno necesitaba una red a prueba de fallos, para asegurar la comunicación en caso de una guerra nuclear. En 1969, el Departamento de la Defensa de los Estados Unidos comenzó a usar ARPANET, la primera red basada en la tecnología de protocolos. ARPANET inicialmente conectaba cuatro supercomputadoras.

#### **2.2.2. Década de los '70**

Durante los 70s, instituciones educativas y de investigación comenzaron a conectarse a ARPANET para crear una comunidad de redes. A finales de los 70s, TCP/IP comenzó a ser el protocolo oficial usado en la Internet.

#### **2.2.3. Década de los '80**

En los 80s, la Fundación Nacional de Ciencia de los Estados Unidos, reemplazó ARPANET con una red de alta velocidad. Esta es la red que actualmente sirve como enlace principal (backbone) para la actual Internet. Cuando ARPANET fue usado en 1969, consistía solo de 213 host registrados, ya en 1986 existían mas de 2,300 host.

#### **2.2.4. Década de los '90**

A inicio de los 90s, la Fundación Nacional de ciencia de los Estados Unidos, transfirió el mantenimiento y supervisión de la Internet a fundaciones privadas y corporativas. Actualmente, la Internet tiene varios millones de computadoras conectadas en todo el

mundo. El desarrollo de otros protocolos y otras tecnologías, como el World Wide Web, ha contribuido a éste crecimiento.

### **2.3. Características de Internet**

- Internet no tiene dueño. Cada dueño de un host conectado a Internet, es dueño de una pequeña fracción de Internet.
- No hay un responsable de que Internet funcione. Por ser un sistema de multipropiedad, los administradores de cada nodo o subred son los únicos responsables de estar conectados a Internet.
- No existen leyes en Internet. Los servicios de Internet definen una forma de comunicarse y de gestionar información, más no determinan los contenidos comunicativos o informativos.
- No impone barreras de edad, raza, género, condición social o política. Más de 80 millones de usuarios de todo el mundo se comunican a través de Internet en forma privada o en foros públicos, apartando muchas veces los problemas étnicos, políticos y generacionales que los separan en la realidad.

### **2.4. Organismos relacionados a Internet**

#### **2.4.1. World Wide Web Consortium (W3C)**

W3C trabaja con la comunidad global para producir especificaciones de software. El consorcio está formado por miembros de la industria, pero sus productos son gratuitos. El Web de W3C se encuentra en el Laboratorio para la Ciencia de la Computación del Instituto de Massachusetts (MIT LCS) y en el Instituto Nacional de Francia para la Investigación de la Informática y la Automatización (INRIA), en colaboración con el Concilio Europeo para la Investigación Nuclear (CERN).

URL: <http://www.w3.org/History.html>

#### **2.4.2. Internet Engineering Task Force (IETF)**

Este organismo se encarga del desarrollo y la ingeniería de los protocolos de Internet. La IETF es una comunidad internacional de diseñadores de red, operadores, vendedores e investigadores preocupados con la evolución de la arquitectura de Internet y su buen funcionamiento. Está abierto para cualquier interesado.

URL: <http://www.isi.edu/irtf/>

#### **2.4.3. Electronic Frontier Foundation (EFF)**

La EFF, es una organización civil independiente que trabaja en el interés público de proteger la privacidad, la libre expresión y el acceso a los recursos en línea e información.

URL: <http://www.eff.org/>

## 2.5. Intranet

Intranet es la implantación o integración en una red local o corporativa de tecnologías avanzadas de publicación electrónica basadas en **WEB**, en combinación con servicios de mensajería, compartición de recursos, acceso remoto y toda una serie de facilidades cliente/servidor proporcionadas por el conjunto de *protocolos TCP/IP*, diseñado inicialmente para la red global *Internet*. Su propósito fundamental es optimizar el flujo de información con el objeto de lograr una importante *reducción de costos* en el manejo de documentos y comunicaciones internas.

Es una herramienta de gestión que permite una potente difusión de información y mecanismos de colaboración entre el personal.

## 2.6. Extranet

Un nuevo concepto está cobrando cada vez mayor fuerza en el ámbito de la comunicación en línea: las **extranet**. Una definición aproximada de extranet sería "tecnología para transferencia segura de datos entre Intranets protegidas por cortafuegos".

Una extranet es una red privada que usa los protocolos de Internet y el sistema público de telecomunicaciones para compartir, de modo seguro, parte de la información de un negocio o las operaciones con proveedores, vendedores, socios, clientes u otro tipo de negocios. Una extranet puede ser considerada como parte de la Intranet de una compañía que se amplía a usuarios que están fuera de la empresa. También se ha descrito como un "estado de ánimo" en el cual la Internet se percibe como una forma de hacer negocios con otras empresas así como para vender productos a sus clientes. Los mismos beneficios que el HTML, HTTP, SMTP y otras tecnologías de Internet han dado a la Red y a las Intranets corporativas, ahora parecen destinados a acelerar los negocios entre empresas.

Una extranet requiere seguridad e intimidad. Por tanto se hace necesaria la administración de un "firewall" o "corta fuegos" en el servidor, la emisión y uso de certificados digitales o medios similares para autenticar al usuario, la encriptación de mensajes y el uso de redes privadas virtuales (virtual private networks, VPNs) que corren de manera subterránea en la red pública.

### 2.6.1. Que es Firewall (Corta fuegos)

Es un punto de control y filtrado de la información entre Internet y una red privada. Un firewall restringe el flujo de información y protege las redes respecto de los accesos desde Internet de acuerdo a los parámetros que establece el usuario. Los firewalls se utilizan para impedir que incursiones externas no deseadas o no autorizadas, tengan acceso a la información de la red interna. Existen dos tipos de firewalls, los routers de filtrados por paquetes y los conocidos como proxy servers.

#### 2.6.1.1. Filtrado de Paquetes

Un filtro de paquetes consiste en una tupla <regla, acción> aplicada a los paquetes que circulan por una red.

Generalmente estas reglas se aplican en los niveles OSI de red, transporte y sesión definiendo mecanismos mediante los cuales se deniega o se otorga el acceso a determinados servicios. El mejor sitio para instalar un filtro de paquetes es el router que conecta a la red de la organización con el exterior.

Para definir un filtro de paquetes se toma el documento de las políticas de seguridad de la organización y se lo convierte en una tabla que tenga lo siguiente: Permitido, servicio, sentido y hosts. Esto va a ser de mucha ayuda a la hora de codificar un router de acceso.

Permitir	Servicio	Sentido	Hosts
SI	*	entrada/salida	*
NO	FTP	entrada	192.168.2.1
NO	SMTP	entrada/salida	192.168.2.1
SI	SMTP	entrada/salida	192.168.2.1

Se puede permitir conexiones desde afuera hacia adentro siempre y cuando la petición de la conexión haya sido realizada desde adentro. En la mayoría de routers y cortafuegos estas reglas se verifican en el orden en el que aparecen en la tabla hasta que puede aplicarse una de ellas.

Un firewall es un sistema o grupo de sistemas que deciden que servicios pueden ser accesados desde el exterior (internet en este caso) de una red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden ser ejecutados por los usuarios hacia el exterior.

Para realizar esta tarea todo el tráfico entre las dos redes tiene que pasar a través de él. En otras palabras un firewall deja pasar el tráfico autorizado desde y hacia el exterior.

No se debe confundir un firewall con un ruteador, un firewall no direcciona información (función que sí la realiza el enrutador), un firewall solamente filtra información.

Desde el punto de vista de seguridad un firewall delimita el perímetro de defensa y seguridad de la información.

El diseño tiene que ser el producto de una organización consciente de los productos que se necesitan, además hay que tener presentes los puntos vulnerables de toda la red, los servicios que se pone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones de acceso remoto.

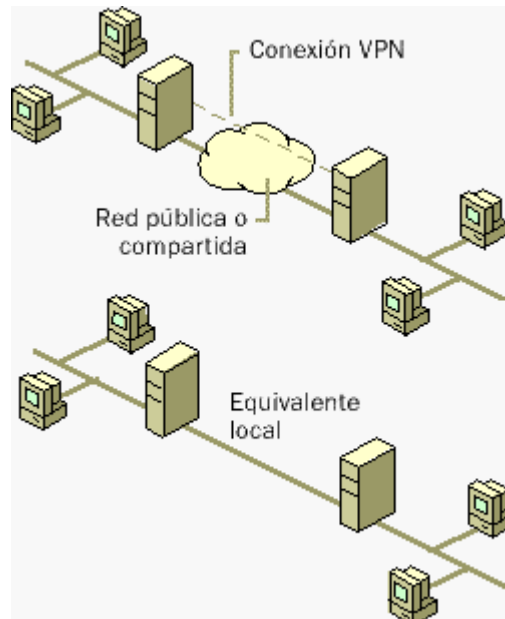
## 2.7. Qué es VPN

Una red privada virtual (*virtual private network*, VPN) es una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas como Internet. Con una VPN usted puede enviar datos entre dos computadoras a través de redes públicas o compartidas en una manera que emula las propiedades de un enlace punto a punto privado.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento (*routing*) que le permite atravesar la red pública o compartida para llegar a su destino. Para emular un enlace privado, los datos enviados son encriptados. Los paquetes (*packets*) que son interceptados en la red pública o compartida son indescifrables sin las claves de

encriptación. El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN).

La figura 1. ilustra el concepto lógico de una VPN.



Con las conexiones VPN los usuarios que trabajan en casa o de manera móvil pueden tener una conexión de acceso remoto a un servidor de la organización utilizando la infraestructura proporcionada por una red pública como Internet. Desde el punto de vista del usuario, la VPN es una conexión punto a punto entre la computadora, el cliente VPN, y el servidor de la organización, y el servidor VPN. La infraestructura exacta de la red pública o compartida es irrelevante porque desde el punto de vista lógico parece como si los datos fueran enviados por un enlace privado dedicado.

Con las conexiones VPN las organizaciones también pueden tener conexiones enrutadas (*routed connections*) con oficinas separadas geográficamente o con otras organizaciones por una red pública como Internet, manteniendo a la vez una comunicación segura. Una conexión VPN enrutada a través de Internet, opera desde el punto de vista lógico como un enlace WAN dedicado.

Con las conexiones VPN, tanto en las conexiones de acceso remoto como las conexiones enrutadas, una organización puede cambiar de líneas rentadas (*leased lines*) o accesos telefónicos (*dial-up*) de larga distancia a accesos telefónicos locales o líneas rentadas con un proveedor de servicio de Internet (*Internet Service Provider, ISP*).

[URL: http://netice.com/Advice/Countermeasures/VPN/default.htm](http://netice.com/Advice/Countermeasures/VPN/default.htm)

## 2.8. Que es TCP / IP

Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados a la red Internet. Este nombre viene dado a los protocolos estrella de esta familia:

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

El modelo básico en internet es el modelo Cliente/Servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona ese servicio.

La arquitectura de Internet esta basada en capas. Esto hace mas facil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (*International Standard Organization*) para la interconexión de sistemas abiertos (OSI). (Ver figura 1).

<b>Aplicación</b>						
<b>Presentación</b>	TELNET	FTP	SNMP	SMTp	DNS	HTTP
<b>Sesión</b>						
<b>Transporte</b>	TCP					
<b>Red</b>	IP					
<b>Liga de Datos</b>	802.2				X.25	LLC/SHAP
	802.3	802.5		LAPB		ATM
<b>Física</b>	Ethernet	Token Ring	FDDI	Línea Síncrona WAN		SONET

Figura 2. Relación del modelo TCP/IP con el modelo OSI

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implantación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en TCP/IP proponen cuatro capas en las que las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Enlace de Datos y Física son vistas como la capa de Interface a la Red. Por tal motivo para TCP/IP sólo existen las capas Interface de Red, la de Intercomunicación en Red, la de Transporte y la de Aplicación.

URL: <http://www.mcgreww.net/Training/NPS/nps-osi.htm>

## 2.8.1. Descripción del Modelo de Capas de TCP/IP

### 2.8.1.1. Capa de Aplicación.

Invoca programas que acceden servicios en la red. Interactúan con uno o más protocolos de transporte para enviar o recibir datos, en forma de mensajes o bien en forma de flujos de bytes.

### 2.8.1.2. Capa de Transporte.



Provee comunicación extremo a extremo desde un programa de aplicación a otro. Regula el flujo de información. Provee un transporte confiable asegurándose que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentran interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota, esto lo hace añadiendo identificadores de cada una de las aplicaciones. Realiza además una verificación por suma, para asegurar que la información no sufrió alteraciones durante su transmisión.

### **2.8.1.3. Capa Internet.**

Controla la comunicación entre un equipo y otro, decide qué rutas deben seguir los paquetes de información para alcanzar su destino. Conformar los paquetes IP que serán enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.

### **2.8.1.4. Capa de Interface de Red.**

Emite al medio físico los flujos de bit y recibe los que de él provienen. Consiste en los manejadores de los dispositivos que se conectan al medio de transmisión.

Cuando una aplicación transmite datos a otro nodo, cada capa añade su propia información como un encabezado. Al ser recibido el paquete la capa remueve su encabezado correspondiente y trata el resto del paquete como datos.

## **2.8.2. Suite de protocolos de TCP/IP**

- Internet Protocol (IP)
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

### **2.8.2.1. Internet Protocol (IP)**

IP es un protocolo no orientado a la conexión (connectionless), responsable principalmente del direccionamiento y ruteo de paquetes entre nodos.

Un protocolo no orientado a la conexión significa que no se establece una sesión antes del intercambio de datos. IP no garantiza la entrega, un paquete puede perderse, entregarse fuera de secuencia, duplicarse o retrasarse.

Una confirmación (acknowledgment) no es necesaria cuando un dato es recibido. El emisor o el receptor no son informados cuando un paquete se pierde o se manda fuera de secuencia. La confirmación de los paquetes es responsabilidad del protocolo de transporte de la capa superior.

URL: <http://www.gocrawl.com/web/Computers/Internet/Protocols/index.html>

### **2.8.2.2. Address Resolution Protocol (ARP)**

Cuando IP rutea los paquetes, necesita obtener la dirección física del destino. IP se ayuda de ARP para obtener la dirección física de los nodos TCP/IP sobre redes con uso de broadcasts, como Ethernet y token ring.

Cuando IP necesita una dirección física, ARP primero consulta su caché local buscando la dirección física que corresponda con la dirección IP destino. Si no esta en caché, ARP genera un paquete de solicitud ARP de la dirección física del host destino.

Para hacer las futuras comunicaciones más eficientes, las direcciones IP y físicas del nodo emisor también son incluidas en el paquete de solicitud. El paquete es entonces enviado por medio de un broadcast a la red local. Todos los nodos reciben la solicitud y el paquete es pasado a ARP. Si la dirección del host receptor corresponde a la dirección IP solicitada, una respuesta ARP es formulada con la dirección física, y es enviada directamente al nodo emisor. Todos los otros nodos añaden la dirección a su caché local y después desechan el paquete.

Cuando la dirección física es recibida, tanto la dirección IP y la física son almacenadas en la cache ARP local. Así el paquete IP puede ser enviado usando la dirección física del destino.

### 2.8.2.3. Internet Control Message Protocol (ICMP)

ICMP provee reporte de mensajes y errores. Por ejemplo, si IP no es capaz de entregar un paquete en el host destino, ICMP envía un mensaje de "destino no encontrado" (destination unreachable) al nodo emisor.

Los mensajes más comunes de ICMP son:

Mensaje	Tipo	Función
Echo request	8	Usado por PING para encontrar un host.
Echo reply	0	Usado por PING para confirmar que un nodo ha sido encontrado.
Redirect	5	Informa al nodo de una ruta preferida.
Source quench	4	Informa al nodo disminuir la cantidad de datagramas debido a congestionamiento en la red.
Destination unreachable	3	Informa al nodo que el datagrama no pudo ser entregado.

Los mensajes de ICMP están contenidos en datagramas IP. Esto asegura que el mensaje ICMP será ruteado al nodo apropiado.

### 2.8.2.4. Transmission Control Protocol (TCP)

TCP es un protocolo confiable y orientado a la conexión. Los datos son transmitidos en segmentos.

Orientado a la conexión significa que una sesión se estableció antes del intercambio de datos entre los nodos.

La confiabilidad se logra asignando un número de secuencia a cada segmento transmitido. Por medio de este mecanismo, el nodo destino sabe si han llegado todos los segmentos.

Una confirmación es utilizada para verificar que los datos fueron recibidos por el otro nodo. Por cada segmento enviado, el host destino debe regresar una confirmación (ACK) en un cierto periodo de tiempo. Si un ACK no es recibido o llegó dañado, los datos son retransmitidos.

TCP utiliza "byte-stream communications", esto es, los datos son tratados como una secuencia de bytes sin límite.

Todos los segmentos TCP tienen dos partes: datos y encabezado. Los siguientes campos son añadidos al encabezado TCP.

- **Puerto Emisor**
- **Puerto Destino**
- **Número Secuencial:** la secuencia de bytes transmitidos en un segmento. El número secuencial es usado para verificar que todos los bytes han sido recibidos.
- **Número de Confirmación:** el número secuencial del siguiente byte enviado al nodo receptor.
- **Checksum:** verifica que el encabezado no está corrupto.

#### 2.8.2.4.1. Puertos TCP

Un puerto TCP provee una localidad definida para la entrega de mensajes. Los números de puerto inferiores a 256 son puertos comúnmente utilizados, algunos se listan a continuación.

Número de Puerto	Descripción
21	FTP
23	Telnet
53	Domain Name Server (DNS)
80	HTTP
139	Servicio de sesiones Netbios

URL: <http://cheops.anu.edu.au/~avalon/ip-filter.html>

#### 2.8.2.5. User Datagram Protocol (UDP)

UDP provee un servicio de datagramas no orientado a la conexión (connectionless), es decir, la recepción de los datagramas no está garantizada; y tampoco lo está, si llegaron en la secuencia correcta los paquetes.

UDP es utilizado por aplicaciones que no requieren de confirmaciones de la recepción de datos y que típicamente transmiten pequeñas cantidades de datos al mismo tiempo.

El servicio de datagramas y nombres NetBios, y el Simple Network Management Protocol (SNMP) son ejemplos de servicios y aplicaciones que usan UDP.

### 2.8.2.5.1. Puertos UDP

Para usar UDP, la aplicación debe proveer la dirección IP y el número de puerto de la aplicación destino. Un puerto provee una dirección para enviar mensajes. Un puerto funciona como una cola de mensajes multiplexada, o sea, puede recibir varios mensajes al mismo tiempo. Cada puerto está identificado por un número único. Es importante mencionar que los puertos UDP son distintos e independientes a los de TCP aunque utilicen el mismo número de puerto.

Puerto	Llave (keyword)	Descripción
15	NETSTAT	Status de la red
53	DOMAIN	Domain Name Server
69	TFTP	Trivial Transfer Protocol
137	NETBIOS-NS	Servicio de nombres NetBIOS
138	NETBIOS-DGM	Servicio de datagramas NetBIOS
161	SNMP	Monitor de red SNMP

## 2.9. Protocolos de Internet

Un protocolo es un conjunto de reglas para realizar una acción. Los protocolos de Internet son estándares aprobados por la comunidad mundial, representada en el IETF (Internet Engineering Task Force). Estos estándares permiten realizar las mismas funciones en ambientes diferentes. A continuación se presentan los protocolos más importantes:

- **HTTP**
- **SMTP**
- **IRC**
- **MIME**
- **POP3**
- **NNTP**

### 2.9.1. HyperText Transfer Protocol (HTTP)

HTTP es un protocolo de aplicación con la sencillez y velocidad necesaria para sistemas de información distribuidos, colaborativos y de diferentes medios. Es un protocolo general, independiente y orientado a objetos usado para diferentes tareas, como sistemas de nombres de servidores y de administración de objetos distribuidos, a través de la extensión de sus métodos (comandos). Una característica de HTTP es la forma de representar los datos, permitiendo a los sistemas funcionar independientemente de los datos siendo transferidos. HTTP ha sido usado por el WWW desde 1990.

Los actuales sistemas de información necesitan una mayor funcionalidad en simples transferencias, búsquedas, actualización del front-end y notaciones. HTTP brinda un conjunto de métodos abiertos usados para indicar el propósito de la solicitud y el recurso accesado, apoyándose de las reglas definidas por el URI (Uniform Resource

Identifier), como localidad (URL) o como nombre (URN). Los mensajes son pasados en un formato similar al usado en el Internet Mail y MIME.

HTTP también es usado como un protocolo genérico para la comunicación entre agentes usuario(clientes) y proxies (intermediarios) y gateways (traductores) para otros protocolos de Internet como SMTP, NNTP, FTP, Gopher y WAIS, permitiendo acceso básico a diferentes medios a los recursos disponibles de diversas aplicaciones y simplificando la implementación de los agentes usuario.

### **2.9.1.1. Funcionamiento General de HTTP**

El protocolo HTTP esta basado en un esquema solicitud/contestación. Un cliente establece una conexión con el servidor y envía una solicitud al servidor en la forma de un "método de solicitud", URL, y la versión del protocolo, seguido por un mensaje del tipo MIME con los parámetros de la solicitud, la información del cliente, y posiblemente el cuerpo del mensaje.

El servidor responde con un "status line", incluyendo la versión del protocolo del mensaje y un código de éxito o fracaso, seguido por un mensaje del tipo MIME<sup>1</sup> con información del servidor, y posiblemente el cuerpo del mensaje.

La mayoría de la comunicación HTTP es iniciada por un agente usuario(cliente) y consiste de una solicitud de un recurso en algún servidor. En Internet, las comunicaciones HTTP generalmente se realizan sobre conexiones TCP/IP. El puerto predeterminado es el TCP 80, sin embargo otros puertos pueden ser usados. Esto no implica que HTTP no sea implementado sobre cualquier otro protocolo de Internet, u otras redes. HTTP solamente proporciona un transporte verificable, cualquier protocolo que provea estas garantías puede ser usado.

URL: <http://ds.internic.net/rfc/rfc1945.txt>

### **2.9.2. Simple Mail Transport Protocol (SMTP)**

Este protocolo está diseñado para transferir correo seguro y eficientemente. SMTP es independiente al servicio de transporte usado mientras utilice un canal de transmisión para enviar y recibir: comandos, texto y confirmaciones.

SMTP puede utilizar como servicio de transporte a TCP. En el caso de TCP utiliza el puerto 25 de TCP para intercambiar datos. Mientras las conexiones TCP transmiten bytes, los datos de SMTP envían caracteres ASCII de 7-bits.

#### **2.9.2.1. El Modelo SMTP**

El diseño del SMTP esta basado en el siguiente modelo de comunicación:

- Como resultado de la solicitud de correo del usuario, el emisor-SMTP establece un canal de transmisión bilateral con el receptor-SMTP. El receptor-SMTP puede ser intermediario o el destino final.

---

<sup>1</sup> Ver capítulo 2.9.4

- Los comandos SMTP son generados por el emisor-SMTP y enviados al receptor-SMTP.
- Las respuestas a los comandos SMTP son enviadas desde el receptor-SMTP al emisor-SMTP.

Cuando el mismo mensaje es enviado a múltiples recipientes el SMTP fuerza a la transmisión de una sola copia de los datos para todos los receptores en el mismo host destino.

Los comandos y las respuestas no diferencian entre mayúsculas y minúsculas, sin embargo, los nombres de los buzones de usuarios si. Como algunos hosts si diferencian el nombre del usuario, las implementaciones del SMTP respetan la sintaxis de los argumentos del buzón.

### **2.9.3. Internet Relay Chat (IRC)**

El protocolo IRC fue desarrollado como una forma para los usuarios de BBS para poder comunicarse entre ellos. El protocolo IRC es un protocolo basado en modo texto, un cliente y un servidor.

IRC por si mismo es un sistema de teleconferencia, el cual (a través del uso del modelo cliente-servidor) esta diseñado para ejecutarse en varias computadoras en un ambiente distribuido. Una instalación común involucra un solo servidor, convirtiéndose en un punto central para los clientes (o otros servidores) permitiendo que los mensajes sean entregados/multiplexados y otras funciones.

URL: [http:// www.irchelp.org/](http://www.irchelp.org/)

### **2.9.4. Multipurpose Internet Mail Extensions (MIME)**

“Mecanismos para especificar y describir el formato del cuerpo de los mensajes de Internet”

Desde su publicación en 1982, el RFC 822 ha definido un formato estándar de mensajes de correo en modo texto para Internet. Su éxito se ha debido a su implementación, parcial o total, en Internet y los sistemas basados en SMTP, sin embargo al ser mas usado, han crecido sus limitaciones.

MIME define varios mecanismos para resolver la mayoría de estos problemas sin ser incompatible con los sistemas de correo compatibles con el RFC 822.

MIME ha sido cuidadosamente diseñado como un mecanismo extensible, los tipos de contenido, subtipos y los nombres de tipos de caracteres pueden ser adaptados y aumentados. Para esto MIME define un proceso de registro el cual utiliza al Internet Assigned Number Authority (IANA) como un registro central para dichos valores.

Los valores de los tipos de contenido, subtipos y nombres de los parámetros usados en MIME no distinguen entre mayúsculas y minúsculas. Sin embargo, los valores de los parámetros si lo son a menos que se especifiquen.

URL: <http://www.oac.uci.edu/indiv/ehood/MIME/MIME.html>

### 2.9.5. Post Office Protocol (POP3)

En cierto tipo de nodos pequeños en Internet es impráctico mantener un sistema de transporte de mensajes. Por ejemplo, una estación de trabajo normalmente no tiene los suficientes recursos (procesador, espacio en disco, memoria) para permitir a un servidor SMTP comunicarse con un sistema de transporte de mensajes local residente y en ejecución continua. Así también, mantener una PC siempre conectada a una red TCP/IP sería demasiado caro.

#### Operación Básica

El servidor de POP3 inicia el servicio monitoreando el puerto TCP 110. Cuando un cliente desea hacer uso del servicio, el establece una conexión con el servidor. Cuando la conexión es establecida, el servidor POP3 envía una confirmación. El cliente y el servidor POP3 entonces intercambian comandos y respuestas (respectivamente) hasta que la conexión es cerrada o abortada.

Una sesión de POP3 involucra una serie de pasos.

- Una vez que la conexión TCP ha sido abierta y el servidor de POP3 ha enviado la "bienvenida" (greeting).
- La sesión entra en un estado de AUTORIZACIÓN, el cliente debe identificarse ante el servidor.
- El servidor reserva los recursos asociados con el recipiente del cliente. El cliente solicita acciones en el servidor POP3.
- Cuando el cliente ha generado el comando QUIT, la sesión entra en un estado de ACTUALIZACIÓN. El servidor desocupa los recursos involucrados y concluye la sesión.
- Cierra la conexión TCP.

### 2.9.6. Network News Transfer Protocol (NNTP)

NNTP especifica un protocolo para la distribución, solicitud, recuperación y envío de noticias, usando una transmisión en paquetes (stream transmission) en Internet. NNTP está diseñado para que las nuevas noticias sean almacenadas en una base de datos central permitiendo a un "suscriptor" seleccionar solamente aquello que desee leer. También cuenta con indexamiento, referencias y expiración de mensajes.

El servidor de noticias utiliza una conexión con transmisión de paquetes (como TCP) y comandos SMTP. Está diseñado para aceptar conexiones de otros hosts, y proveer una interface para la base de datos de noticias. Cuando es usado vía Internet TCP, el puerto asignado para la comunicación es el 119.

### 2.10. Dominio

Un dominio es el nombre de dirección que aparece entre (www) y (.com, .net, .org). Es la palabra o frase clave que marca su identidad en la Internet. Uno de los aspectos más



importantes de los dominios es que son únicos. Dos personas u organizaciones no pueden tener el mismo dominio de manera simultánea. Así que si usted registra el dominio en la Web, puede estar seguro que cualquiera en el mundo que escriba **www.Nombre-Dominio.com** en un buscador de la Web, será llevado directamente a su página.

### 2.10.1. Dirección en la Web (nombre de dominio)

Hablando en términos prácticos, su Dirección en la Web (registro de nombre de dominio) es el núcleo de su identidad en la Internet. Sus clientes recordarán este nombre y lo usarán para saber más sobre sus productos y servicios. Y puesto que dos partes nunca pueden tener la misma Dirección en la Web de manera simultánea, su identidad en la Internet es totalmente única.

Técnicamente, una Dirección en la Web es una construcción domiciliada que se usa para identificar y localizar computadoras en la Internet. En tanto que las computadoras utilizan números Internet Protocol (IP) para localizarse unas a otra en la Internet, las personas tienen dificultades para recordar dichos números. Por eso, las Direcciones en la Web fueron desarrolladas para permitir, mediante el uso de palabras y frases que fácilmente son recordadas, la identificación de direcciones en Internet.

### 2.10.2. Extensiones en una Dirección en la Web

COM, NET y ORG son dominios de máximo nivel en la jerarquía del Sistema de Nombres de Dominio. Estos dominios de máximo nivel se encuentran justo debajo de la "raíz", que es el comienzo de la jerarquía.

Cualquiera puede registrar Direcciones en la Web con COM, NET y ORG. De hecho, la mejor manera de proteger la exclusividad de su identidad y sus marcas en línea, es registrar o reservar Direcciones en la Web en todos los dominios de máximo nivel.

### 2.10.3. Caracteres válidos para una Dirección en la Web y su longitud máxima.

Las letras y los números siempre son caracteres válidos en una Dirección en la Web.

Los guiones también pueden ser utilizados, pero no pueden ser el inicio ni el final de su Dirección en la Web. Los espacios y los caracteres especiales, tales como los signos de admiración (!) y los guiones bajos (\_), no se permiten en una Dirección en la Web.

Una Dirección en la Web puede de ser de hasta 26 caracteres, incluyendo los cuatro caracteres usados para identificar el dominio de máximo nivel: .COM, .NET, .ORG o .EDU.

Dominios de la Internet para países.

.ar	Argentina	.ve	Venezuela	.mx	México
.at	Austria	.ca	Canadá	.es	España
.de	Alemania	.us	EE.UU.	.ch	Suiza
.bo	Bolivia	.uk	Reino Unido	.cl	Chile
.ec	Ecuador	.jp	Japón	.fr	Francia



## 2.11 Qué es un nodo Web

Un nodo Web es una colección de páginas Web conectadas entre sí mediante enlaces de hipertexto, de forma que cada página se encuentra asociada con las demás. Si se piensa en todos los posibles enlaces que pueden tener los documentos entre sí, y en todas las formas posibles en que se pueden hacer referencias cruzadas con el material contenido en su nodo Web es muy sencillo comprender él porque el nombre de Web.

## 2.12. URL(Localizador de Recursos Universal)

Todos los recursos en Internet tienen una dirección "familiar" conocida como Uniform Resource Locator (URL). La primera parte de un URL corresponde al protocolo del servicio usado. La segunda parte del URL corresponde a una dirección IP. Los ruteadores traducen una URL en una dirección numérica IP cuando localizan a los servidores en diferentes dominios.

"www." y "http://www" no se consideran parte de la dirección en la Web: Son parte de otro tipo de dirección de Internet usada en la World Wide Web (Web Mundial) llamada un Universal Resource Locator (URL). Un URL se usa para describir la ubicación exacta de un recurso específico en Internet, así como una página en Web, una computadora o una base de datos específica.

El siguiente es un ejemplo:

<http://www.ejemplo.edu/tesis/arq.html>

- http: Hypertext Hypertext Transfer Protocol
- www: nombre del subdominio (alias equivalente a una dirección IP como 131.107.2.200)
- ejemplo.edu: nombre del dominio lógico (alias equivalente a una dirección IP como 131.107.2.200)
- tesis: directorio lógico
- arq.html: nombre del recurso

Es importante mencionar, que los URLs hacen diferencias entre mayúsculas y minúsculas. La primera parte, <http://www.ejemplo.com>, no distingue entre mayúsculas y minúsculas. Todo lo que se escriba a continuación de esta dirección, sí hace una distinción. Por lo tanto:

<http://www.ejemplo.com/tesis>, es diferente a <http://www.ejemplo.com/TESIS>

## 2.13. Servicios De Internet

En Internet se puede enviar y recibir mensajes de correo electrónico (E-Mail), participar en debates en los grupos de noticias USENET (News), conseguir software gratuito y otros ficheros por FTP, charlar con otros internautas en IRC y consultar las vistosas páginas del WWW – World Wide Web.

- **Servicios de comunicación.**

- \* Correo electrónico (E-Mail)
- \* Foros de debate o grupos de noticias (News)
- \* Conferencia electrónica (IRC- Chat).

- **Servicios de Información**

- \* Sesiones remotas (Telnet)
- \* Transferencia de Archivos (FTP).
- \* Dirección de Información (Gopher)

- **El World Wide Web (WWW).**

### **2.13.1. Correo Electrónico (E-Mail)**

Utilizando el correo electrónico se podrá enviar mensajes, y en general cualquier tipo de información digitalizada, a un usuario de la red situado en cualquier parte del mundo.

Los mensajes de correo electrónico se identifican con las direcciones electrónicas de los usuarios remitente y destinatario, e incluyen campos adicionales con la fecha de envío del mensaje, el tema o subject, un título del contenido, y pueden incluirse anexos (o attachments); documentos elaborados con aplicaciones de optimización de oficina, imágenes, archivos de sonido o vídeo, y hasta programas.

### **2.13.2. Foros de Debate o Grupos de Noticias (News)**

Además de la gran cantidad de información que se puede obtener a través de los servicios de Internet, también es posible, utilizar los denominados foros de debate o newsgroups, que no es otra cosa que ponerse en contacto con personas de todo el mundo interesadas en una misma temática.

A través de los newsgroups se pueden leer mensajes sobre los temas más insospechados, así como participar activamente en ellos, enviando y contestando mensajes.

### **2.13.3. Conferencia Electrónica (IRC).**

Es otro servicio extendido de la red, IRC Chats o Internet Relay Chat (Charla), permite que el usuario se conecte a un programa para mantener una conversación por medio de intercambio instantáneo de mensajes en grupo, entre las modalidades existen habitaciones para charla, o canales de conferencia electrónica, en los que se conversa sobre un tema en particular como ciencia - ficción, tecnología, cine o chistes, cuando un mensaje es escrito en una sección aparecen casi simultáneamente en las pantallas de los usuarios interlocutores.

### **2.13.4. Sesiones Remotas (Telnet)**

El servicio Telnet le permitirá conectarse con otro computador y acceder a los servicios que éste último ofrezca. Permite que el usuario se conecte a un sistema informático como si fuera un terminal del mismo. Mientras se está conectado, todo lo que se escribe, se envía al terminal remoto y todo lo que el terminal remoto envía se visualizará en la pantalla del sistema local.

URL: <http://olymp.wu-wien.ac.at/manuals/rfc-telnet.html>

### **2.13.5. Transferencia De Archivos (FTP)**

Hay multitud de ordenadores en Internet que mantienen una biblioteca de programas u otro tipo de ficheros. Algunos sólo permiten a usuarios de su propia empresa o institución acceder a la misma. Pero hay muchos que dejan entrar a cualquiera (FTP anónimo). Para acceder a alguna biblioteca de estas, sólo hace falta tener un programa cliente de FTP y saber el nombre del ordenador servidor. Una vez conectado, verás los ficheros que hay (si los nombres no te dicen nada suele haber un fichero índice con una muy breve descripción de ellos) y podrás copiar (bajar) los que quieras a tu ordenador.

El protocolo de transferencia de archivos permite trasladar archivos desde un servidor FTP hasta la computadora de un usuario. Es el medio fundamental de descargar nuevas aplicaciones de Internet, como browsers, antivirus, o cualquier otro programa gratuito o disponible para prueba. El usuario debe conocer el nombre del nodo que funciona como servidor FTP y la localización de los archivos que desea “bajar” dentro de la estructura de almacenamiento de archivos de ese servidor.

URL: <http://www.nizkor.org/how-to-ftp.html>

### **2.13.6. Directorios de Información (Gopher)**

Es un servicio de acceso a otros servidores de información por medio de clasificación de archivos en forma de directorios que sirven de puerta de acceso, actualmente los servidores gopher han migrado al www.

### **2.13.7. World Wide Web**

Se ha descrito al World Wide Web como un documento de decenas de millones de páginas conexas y distribuidas por todo el planeta. Los millones de autores son empresas, universidades, organizaciones, gobiernos y personas, que han querido aportar su granito de arena por una variedad de razones. Algunos quieren dejarse conocer, promocionarse, vender algún producto o servicio, compartir sus conocimientos sobre algún tema, o simplemente abrir una vía de comunicación hacia los otros millones de usuarios de Internet.

Los documentos residen en unos ordenadores que los ofrecen a través de software servidor de Web. Para poder solicitar alguna página necesitas un programa cliente o *navegador*. Lo único que le hace falta decir a tu navegador es el URL (Uniform Resource Locator o *Localizador Uniforme de Recursos*<sup>2</sup>, una especie de dirección en Internet) de la página.

---

<sup>2</sup> Ver capítulo 2.12

El URL especifica el ordenador en que se hospeda, el directorio y el nombre del fichero. Si no se conoce el URL, puedes echar mano al URL de alguno de los índices de búsqueda para el WWW, como [Altavista](#), [Yahoo](#) y seguir los enlaces que allí se encuentre.

Este servicio no estaba incluido en Internet inicialmente, pero es el que más ha contribuido a la difusión de la Red, hasta el punto de que hablar de Internet sea, para muchos, prácticamente equivalente a hablar de WWW, como también se le conoce.

World Wide Web es un conjunto de miles y miles de documentos multimedia situados en computadoras de todo el mundo, a los cuales es posible acceder utilizando un programa denominado Navegador o Browser. Estos documentos se caracterizan por estar escritos en un lenguaje especialmente desarrollado para ello, HyperText Markup Language (HTML), y por contener enlaces hipertexto que permiten conectar con otros documentos, formando así, todos ellos, una gran tela de araña mundial.

## **2.14. El Crecimiento de Internet**

Según estimaciones, en el año 2000 el número de personas conectadas a la Red podría superar los trescientos millones.

Estas cifras indican, por ejemplo, que en el siglo XXI los usuarios de Internet podrían alcanzar la cifra numérica de los que ven televisión actualmente. En resumen, Internet se está convirtiendo en una realidad de nuestro tiempo y puede provocar una pequeña revolución en nuestra forma de vida, del mismo modo que lo han hecho los teléfonos móviles o los discos compactos.

Este fenómeno ha atraído los intereses de multitud de empresas de todos los sectores, que ven en Internet un vehículo ideal para actividades comerciales, técnicas o de marketing, además de un medio de distribución directa de software y en general de información de todo tipo.

### **3. Seguridad en la Internet**

La evaluación de este punto es uno de los más importantes en la interconexión del Web con bases de datos. A nivel de una red local, se puede permitir o impedir, a diferentes usuarios el acceso a cierta información, pero en la red mundial de Internet se necesita de controles más efectivos en este sentido, ante posible espionaje, copia de datos, manipulación, etc.

La identificación del usuario es una de las formas de guardar la seguridad. Las identidades y permisos de usuarios están definidas en los Archivos de Control de Acceso.

Pero la seguridad e integridad total de los datos puede conservarse, permitiendo el acceso a distintos campos de una base de datos, solamente a usuarios autorizados para ello. En este sentido, los datos pueden ser presentados a través del Web de una forma segura, y con mayor impacto en todos los usuarios de la red mundial.

Para la integración de bases de datos con el Web es necesario contar con una interfaz que realice las conexiones, extraiga la información de la base de datos, le dé un formato adecuado de tal manera que puede ser visualizada desde un browser del Web, y permita lograr sesiones interactivas entre ambos, dejando que el usuario haga elecciones de la información que requiere.

El reciente aumento del uso de la Red ha dirigido la atención del mundo entero a un problema crucial: la privacidad, hasta el momento, no ha existido una protección real que garantice que los mensajes que usted envía o recibe no sea interceptados, leídos o incluso alterados por algún desconocido, ya que nadie en realidad dirige o controla Internet.

Para que el comercio electrónico cobre verdadero auge en la Red Internet, cada una de las entidades que participan necesitan contar con una manera de verificar la identidad de la otra, y establecer un nivel de confianza

#### **3.1. Criptografía**

Una característica básica de un documento autentico es su integridad. En un documento tradicional como un contrato o cheque, si se aprecian modificaciones o tachones, el documento es prácticamente invalidado. En un documento electrónico, en donde por errores de transmisión o fallas en el medio de almacenaje o, intencionadamente se modifica el contenido original del documento entonces el documento pierde su integridad y por tanto su autenticidad.

Si un documento es autentico entonces es integro pero no viceversa. Estos problemas, confidencialidad, integridad, autenticidad y no-repudiación se resuelven mediante la tecnología llamada "Criptografía". La criptografía es una rama de las matemáticas, que al aplicarse a mensajes digitales, proporcionan las herramientas idóneas para solucionar los problemas antes mencionados. Al problema de la confidencialidad se le relaciona comúnmente con técnicas denominadas de "encriptación" y el problema de la autenticidad mediante técnicas denominadas de "firma digital", aunque ambos en realidad se reducen a procedimientos criptográficos de encriptación y desencriptación.

El fundamento y los procedimientos de operación para efectivamente dar solución a un problema específico constituyen un criptosistema.

El criptoanálisis es la actividad que se encarga de estudiar las debilidades de un criptosistema y su objetivo es el de encontrar soluciones fáciles al reto implantado en el criptosistema. Ambas actividades, la criptografía y el criptoanálisis son parte de la disciplina denominada criptología.

En un sistema en donde la forma tradicional de realizar operaciones comerciales esta siendo reemplazado por métodos electrónicos resulta de suma importancia contar no sólo con la tecnología, sino con un marco legal que norme la validez de los documentos electrónicos. Es importante que en nuestro país contemos con una base legal que conceda, a los documentos firmados digitalmente, un tratamiento similar a la de los documentos tradicionales firmados autógrafamente. El problema de la confidencialidad no es tampoco un problema estrictamente técnico también es conveniente estudiar las implicaciones legales del uso de esta tecnología que permite al individuo mantener información confidencial.

### **3.2. Privacidad en las transmisiones de Internet**

La transmisión de datos confidenciales a través de Internet ofrece poca seguridad. El problema no es tanto el hecho de que el mensaje pueda "perdersé" sin alcanzar su destino, sino algo más grave: que un tercero obtenga una copia de los datos sin que nosotros lo sepamos.

Si realizamos una compra o realizamos un contrato a través de Internet, es muy probable que tengamos que rellenar un formulario o enviar un mensaje con datos personales, incluyendo el nombre, número de la tarjeta de crédito, etc. No es demasiado difícil que alguna persona pueda "interceptar" esa información, con el riesgo consiguiente.

El problema es el mismo tanto si enviamos datos rellenando un formulario de una página Web o si enviamos un mensaje de correo electrónico, en pocas palabras una transacción en la Internet. Para protegernos cabe la posibilidad de emplear un sistema de encriptación de forma que sólo los que tengan la clave adecuada puedan descifrarlo. Un mensaje de estos no tiene ninguna utilidad para quien lo intercepta, puesto que no lo puede interpretar. El sistema de codificación más extendido es conocido con el nombre Pretty Good Privacy, abreviado como PGP. Se basa en una clave doble: para cada usuario existe una clave pública que se puede divulgar sin problemas, y también existe una clave privada que es realmente secreta y que nunca es enviada a otros. Cuando yo deseo que alguien me envíe un mensaje confidencial, primero le transmito la clave pública que será utilizada para codificar (cerrar) los datos privados. Así el mensaje se transmite encriptado y solo es posible leerlo si previamente se descodifica con mi clave privada.

El sistema PGP está pensado para las transmisiones de correo electrónico. También es aplicable (en algunos casos) a los formularios del Web, aunque de forma más incómoda y limitada. PGP es un sistema tan seguro que está prohibido en Francia y en otros países;

esos gobiernos alegan que sería un método de proteger las transmisiones de los delincuentes evitando la vigilancia policial.

Para enviar un mensaje encriptado y firmado, ambas partes deben tener el software PGP e intercambiar sus llaves públicas.

El manejo de llaves en PGP se hace mediante llaveros. Un usuario puede tener varios pares de llaves para él, para permitir cambiarlas en caso de que sospeche que una llave ya no es segura, pero permitiendo que los mensajes enviados recientemente puedan ser reconocidos. Estas llaves están en el llavero de llaves privadas, que está protegido mediante una frase clave, en caso de que sea robado.

Un usuario tiene un llavero de llaves públicas, donde almacena las llaves públicas de sus amigos y de aquellos con quien intercambia correspondencia.

URL: [http://www.wlsoft.com/security/pretty\\_good\\_privacy.htm](http://www.wlsoft.com/security/pretty_good_privacy.htm)

### **3.3. Servicios de seguridad**

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente.

#### Confidencialidad:

Requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda.

#### Autenticación:

Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

#### Integridad:

Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera.

#### No repudio:



Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

#### Control de acceso:

Requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.

#### Disponibilidad:

Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

### **3.4. Mecanismos de seguridad**

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

Intercambio de autenticación: Corroborar que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

Cifrado: Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos.

Integridad de datos: Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

Firma digital: Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.



**Control de acceso:** Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

**Control de encaminamiento:** Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

**Unicidad:** Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

### **3.5. Distribución de claves**

Sin duda alguna, el problema central de todo sistema de gestión de claves lo constituyen los procedimientos de distribución de éstas. Esta distribución debe efectuarse previamente a la comunicación. Los requisitos específicos en cuanto a seguridad de esta distribución dependerán de para qué y cómo van a ser utilizadas las claves. Así pues, será necesario garantizar la identidad de su origen, su integridad y, en el caso de claves secretas, su confidencialidad.

Las consideraciones más importantes para un sistema de gestión de claves son el tipo de ataques que lo amenazan y la arquitectura del sistema. Normalmente, es necesario que la distribución de claves se lleve a cabo sobre la misma red de comunicación donde se está transmitiendo la información a proteger. Esta distribución es automática y la transferencia suele iniciarse con la petición de clave por parte de una entidad a un Centro de Distribución de Claves (intercambio centralizado) o a la otra entidad involucrada en la comunicación (intercambio directo). La alternativa es una distribución manual (mediante el empleo de correos seguros, por ejemplo), independiente del canal de comunicación. Esta última alternativa implica un alto coste económico y un tiempo relativamente largo para llevarse a cabo, lo que la hace descartable en la mayoría de las situaciones. La distribución segura de claves sobre canal inseguro requiere protección criptográfica y, por tanto, la presencia de otras claves, conformando una jerarquía de claves

La distribución de claves se lleva siempre a cabo mediante protocolos, es decir, secuencias de pasos de comunicación (transferencia de mensajes) y pasos de computación. Muchas de las propiedades de estos protocolos dependen de la estructura de los mensajes intercambiados y no de los algoritmos criptográficos subyacentes. Por ello, las debilidades de estos protocolos provienen normalmente de errores cometidos en los niveles más altos del diseño.

### **3.6. El certificado digital**

El Certificado Digital es en si un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificadora, dicho documento establece una liga entre un sujeto y su llave pública. Es decir, el Certificado Digital es un documento firmado por la **Autoridad Certificadora (AC)**, el documento contiene el nombre de un sujeto y su llave pública.

URL: <http://iec.csic.es/criptonomicon/obtenercert.html>

Si el Certificado es auténtico y confiamos en la AC, entonces, podemos confiar en que el sujeto identificado en el Certificado Digital posee la llave pública que se señala en dicho certificado. Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la llave pública de la AC podrá autenticar el documento.

Por varias razones es conveniente que los Certificados Digitales tengan un periodo de validez, este parece ser un principio básico en la emisión de cualquier tipo de identificación. Existe otra razón de carácter técnico y se refiere a que de vez en vez es conveniente que el usuario renueve sus llaves, cada vez aumentando ligeramente el tamaño.

El estándar, internacionalmente aceptado, para Certificados Digitales, es el denominado X.509 de la UIT.

URL: <http://www.itu.int>

El número de serie es un número asignado por la Autoridad Certificadora y tiene el objeto de identificar unívocamente a cada certificado emitido por dicha AC. Por otra parte, debido a que las operaciones electrónicas se pueden realizar entre puntos geográficos muy diferentes, con diversidad de horarios, las fechas a las que hacemos referencia en este documento, estarán expresadas en la notación conocida como Tiempo Universal Coordinado (UTC) o Tiempo del Meridiano de Greenwich. Una fecha en formato UTC, contiene el año, mes, día, hora, minutos y segundos siempre con relación a la hora del meridiano de Greenwich.

### **3.7. Protocolos de seguridad en Internet**

#### **3.7.1. Secure Socket Layer (SSL)**

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como *SSL Handshake*. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Luego que la transacción ha sido completada, se termina SSL.

##### **3.7.1.1. Solicitud de SSL**

Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio.

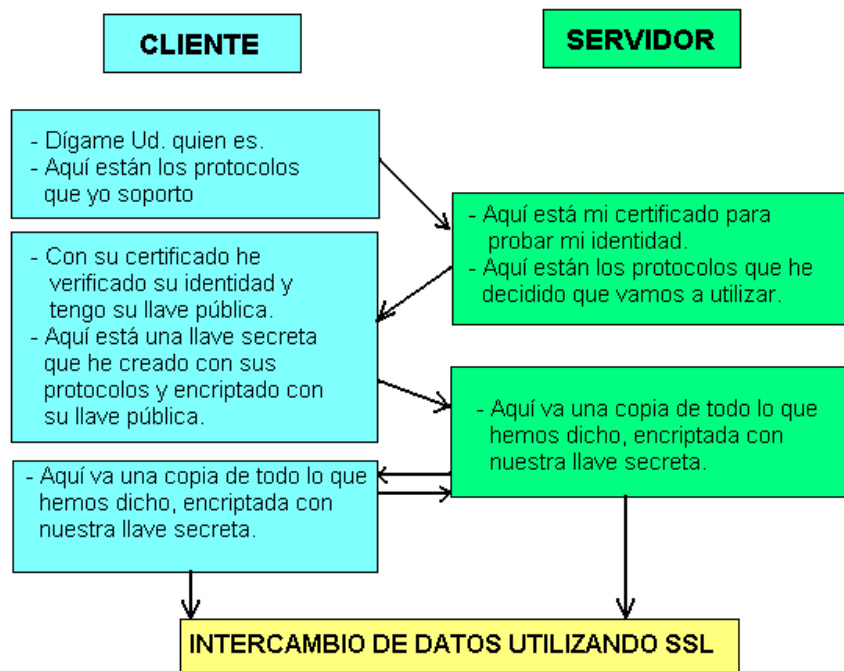
Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el *SSL Handshake* (*manos libres*).

### 3.7.1.2. SSL Handshake

Durante el *handshake* se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El handshake se realiza solo una vez y se utiliza una llave secreta por sesión.

En la figura 3. se ilustra el proceso de handshake:



### 3.7.1.3. Intercambio de datos

Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash de una vía acordado durante el handshake), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

### 3.7.1.4. Terminación de una sesión SSL

Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiéndole que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

URL: <http://www.openhere.com/tech1/security-and-encryption/internet/ssl-tls/>

## 3.7.2. Secure Electronic Transaction (SET)

El estándar SET para transacciones electrónicas seguras en redes abiertas como Internet fue desarrollado por Visa, Master Card y American Express con la asesoría de empresas como IBM, Netscape y RSA entre otras. Está basado en la criptografía más segura, la criptografía de llaves públicas y privadas RSA.

SET agrupa a las siguientes entidades en un solo sistema de pago:

- Tarjetahabiente: Aquella persona poseedora de una tarjeta de crédito.
- Emisor : Entidad financiera que emite la tarjeta.
- Comerciante : Conocido en la literatura SET como el mercader, es la empresa que vende bienes o intercambia servicios por dinero.
- Adquiriente : Institución financiera que establece una cuenta con el Comerciante y procesa autorizaciones y pagos.
- Intermediario para pago : Dispositivo operado por un adquirente o designado a un tercero para que procese los mensajes de pago, incluyendo instrucciones de pago de un tarjetahabiente.
- Marcas : Las instituciones financieras emiten tarjetas con marcas en ellas, para hacer publicidad a la marca y establecen ciertas reglas de uso y aceptación de sus tarjetas y proveen redes que las interconectan a las instituciones financieras.
- Terceros: Los emisores y los adquirentes pueden asignar a terceros para el procesamiento de las transacciones.

Para poder hacer una transacción SET, cada uno de los participantes debe estar registrado por una entidad certificadora, que como su nombre lo indica emite un certificado electrónico en el que se hace constar la identidad de una entidad.

SET fue diseñado para lograr:

- Confidencialidad de la información.
- Integridad de los datos
- Autenticación de la cuenta del tarjetahabiente
- Autenticación del comerciante
- Interoperabilidad

A diferencia de una transacción o compra persona a persona, por teléfono o correo, donde la transacción la inicia el comerciante, en SET la transacción la inicia el tarjetahabiente.

Una vez todos los participantes estén registrados ante una autoridad certificadora, pueden empezar a realizar transacciones seguras. A continuación se muestra como sería el proceso de una solicitud de compra:

- El tarjetahabiente inicia la solicitud luego de haber seleccionado los ítems a comprar. Antes de iniciar el proceso SET, el tarjetahabiente ha sido presentado con un formulario que ha aprobado y en donde se especifican las mercancías a comprar y los términos del pago y por supuesto que tarjeta de crédito a utilizar (no el número). Para poder enviar mensajes SET, es necesario obtener una copia de la llave pública del intermediario de pago. El proceso se inicia cuando se hace una solicitud del certificado del intermediario. El mensaje del tarjetahabiente indica que tarjeta va a ser utilizada para la transacción.
- El comerciante asigna un identificador único a la transacción y le envía al tarjetahabiente su certificado y el certificado del intermediario de pago para la tarjeta seleccionada, además del identificador de la transacción.
- El tarjetahabiente recibe la respuesta, verifica la autenticidad de los certificados. El software SET del tarjetahabiente genera la orden de compra y la información de pago y una firma doble para ambas obteniendo y concatenando los *message digest* (hash) de las dos, computando el digest de la concatenación y encriptándolo utilizando su llave privada. El software SET del tarjetahabiente genera una llave aleatoria simétrica de encriptación y la utiliza para encriptar la firma doble. Luego se encripta el número de cuenta del tarjetahabiente así como también la llave simétrica utilizando la llave pública del intermediario de pago. Finalmente se transmite el mensaje que contiene la orden de compra y la información de pago.
- Cuando el comerciante recibe la orden, verifica la firma del tarjetahabiente utilizando su certificado y además chequea que el mensaje no haya sido alterado, haciendo uso del message digest. El comerciante envía la información de pago al intermediario. Luego de procesar la información de la orden, el comerciante genera y firma un mensaje de respuesta en el que indica que la orden fué recibida. Si luego se logra autorización del pago, el comerciante envía las mercancías o presta el servicio por el que se le pagó.
- Cuando el software del tarjetahabiente recibe la respuesta del comerciante, verifica la autenticidad de éste, si todo sale bien, entonces muestra al usuario un mensaje de que la orden se realizó exitosamente. El tarjetahabiente puede luego averiguar el estado de su orden enviando una solicitud en un mensaje diferente, para saber si fué aprobado el pago, cuando le fué enviada la mercancía, etc.

No es necesario hacer la autorización antes de enviar un mensaje al tarjetahabiente, este proceso se puede llevar a cabo después entre el comerciante y el intermediario de pago.

URL: <http://www.lafacu.com/apuntes/informatica/set/default.htm>

URL: <http://www.informatik.uni-rostock.de/~ljubich/SET-Wallet-SoftWare-Provider/index.html>

### **3.8. Algoritmos de firma digital**

En la literatura académica se han descrito numerosos algoritmos de firma digital. En la práctica, destacan tres de ellos: la firma de comprobación aleatoria (hash), el Digital Signature Standard (DSS) del gobierno de EE.UU. y RSA, que utiliza el algoritmo clásico desarrollado por Roven Rivest, Adi Shamir y Len Adlemln. Los tres algoritmos tienen usos y requisitos distintos.

#### **3.8.1. Firmas de comprobación aleatoria (HASH).**

Las funciones de comprobación aleatoria son similares a las de cifrado (de hecho, algunas de ellas son funciones de cifrado con ligeras modificaciones). La mayoría de estas funciones toma un bloque de datos y lo somete reiteradamente a una sencilla función de desordenación (scramling) para alterar sus elementos. Si esta operación se repite un cierto número de veces, no existe forma práctica conocida de predecir el resultado. Es imposible modificar un documento de un modo determinado y estar seguro de que la función de comprobación aleatoria producirá el mismo resultado.

Este tipo de firma utiliza una función de comprobación aleatoria criptográficamente segura, como *Message digest 5* (MD-5) o *Secure Hash Algorithm* (SHA), para producir un valor de comprobación aleatoria a partir de un archivo. El procedimiento de comprobación aleatoria encadena su clave secreta. El destinatario también tiene una copia de la clave secreta y la utiliza para evaluar la firma.

La principal limitación de la firma de comprobación aleatoria es que el destinatario también debe poseer una copia de la clave secreta para verificar la firma. Esto podría permitir que el receptor falsificara una firma. Mantener estas claves secretas comporta ciertas molestias, por lo que muchos usuarios emplean una infraestructura secreta compartida.

#### **3.8.2. El algoritmo DSS.**

En este algoritmo existen dos claves para cada persona. Una de ellas crea la firma y se mantiene secreta. La otra - la clave pública - verifica la firma.

El DSS fue desarrollado por el U.S. National Institute of Standards and Technology (NIST) con la colaboración de la National Security Agency (NSA). Sólo están obligadas a utilizarlo las compañías que mantienen negocios con el gobierno americano, y muchas prefieren no hacerlo porque es un sistema exclusivamente de firma. El NIST eligió esta solución limitada, porque el gobierno de EE.UU. pretende desalentar el uso de cualquier software de cifrado que cercene su capacidad para fisgonear en asuntos ajenos. El software que sólo proporciona autenticación, como el DSS, puede exportarse libremente en los productos, mientras que el software que emplea RSA para cifrado general está sometido a severas restricciones.

### 3.8.3. Algoritmo RSA.

Las firmas RSA son, las más populares, gracias en parte al marketing agresivo, la política de patentes y el desarrollo a largo plazo que ha adoptado RSA Data Security. Esta empresa controla muchas de las patentes más importantes en este campo, y aunque ha tenido que hacer frente a numerosos litigios, RSA ha sabido utilizar su posición para consolidarse definitivamente como líder. Su software y sus bibliotecas se encuentran en el núcleo de muchos productos, y la compañía sigue contando entre sus filas con algunos de los criptógrafos más reconocidos.

RSA Data Security fue la firma encargada de integrar el software de firma digital con el sistema operativo Macintosh mucho antes de que floreciera el Web, por ejemplo. También añadió a PowerTalk (el software cooperativo de Apple) applets de firma de Arrastrar y soltar que permitían que cualquier usuario incrustara una firma digital en un formulario electrónico con sólo arrastrarlo hasta el icono. RSA Data Security ha otorgado licencia sobre sus patentes a los principales vendedores de sistemas operativos, incluidos Microsoft, IBM, Sun y Digital, y cada uno de ellos ha incorporado prestaciones similares a sus líneas de productos, aunque sin alcanzar el mismo nivel de integración. A diferencia de DSS, RSA también puede utilizarse para cifrar datos y proporcionar seguridad, además de autenticidad.

Tanto en los algoritmos de clave pública como en los de comprobación aleatoria, el nivel de seguridad puede mejorarse verificando que los secretos y las claves contengan el número suficiente de bits como para resistir cualquier ataque conocido. Las firmas de comprobación aleatoria son más susceptibles de violación, dado que el secreto que se usa para crear la firma es conocido por ambas partes. Una fisura en el ordenador central o el allanamiento del domicilio del usuario podrían comprometer una firma de comprobación aleatoria.

### 3.9. Niveles de Seguridad en Redes

De acuerdo con los estándares de seguridad en computadoras desarrollado por el departamento de los Estados Unidos (Libro Naranja) se utilizan varios niveles de seguridad para proteger de un ataque al hardware, al software y a la información guardada.

Los niveles describen diferentes tipos de seguridad física, autenticación de usuario, confiabilidad del software tanto del sistema operativo como de las aplicaciones.

#### 3.9.1. Nivel D1

- Es la forma más elemental de seguridad disponible
- Parte de la base de que todo sistema no es confiable
- No hay protección disponible para el hardware
- El sistema operativo se compromete con facilidad
- No hay autenticación con respecto a los usuarios para tener acceso a la información que se encuentre en la computadora.
- Este nivel de seguridad se refiere a los sistemas operativos MS-DOS, MS-Windows y System7 de Macintosh



### **3.9.2.Nivel C1**

- El nivel c tiene 2 niveles de seguridad: C1 y C2.
- El nivel C1 describe la seguridad disponible en un sistema típico UNIX.
- Existe algún nivel de protección para el hardware puesto que no puede comprometerse tan fácil aunque es posible.
- Los usuarios deberán identificarse con el sistema por medio de un nombre y una contraseña.
- Esta combinación se utiliza para determinar que derechos de acceso a los programas e información tiene cada usuario.
- No es raro encontrar en una organización 2 o 3 personas que saben la contraseña raíz, es un problema porque no se puede distinguir quien realizó diferentes acciones.

### **3.9.3.Nivel C2**

- Crea un medio de acceso controlado
- Refuerza las restricciones a los usuarios en la ejecución de algunos comandos o de algunos archivos, basado no solo en permisos sino en niveles de autorización.
- Requiere auditorías de sistema, esto incluye la creación de un registro de auditoría para cada evento que ocurre en el sistema, la desventaja es que puede degradar el sistema y utilizar más recursos.
- Con uso de autorizaciones adicionales es posible que los usuarios de un sistema C2 tengan la autoridad para realizar tareas de manejo de sistema sin necesidad de la contraseña raíz, esto mejora la tarea del rastreo de las tareas de administración.

### **3.9.4.Nivel B1**

- El nivel B de seguridad tiene 3 niveles
- El nivel B1 o protección de seguridad etiquetada, es el primero que soporta seguridad multinivel como secreta y ultrasecreta.

### **3.9.5.Nivel B2**

- Conocido como protección estructurada, requiere que se etiquete cada objeto.
- Los dispositivos como discos, cintas o terminales pueden tener un nivel sencillo o múltiple de seguridad

### **3.9.6.Nivel B3**

- Nivel de dominios, refuerza los dominios con la instalación de hardware.
- Este nivel requiere que el terminal de usuario se conecte al sistema por medio de un sistema de acceso seguro

### **3.9.7.Nivel A**

- Es el nivel más elevado
- Requiere todos los componentes de los niveles inferiores
- El diseño requiere ser verificado en forma matemática
- Es necesario realizar un análisis de los canales encubiertos y de hardware y software incluidos en su expedición para evitar violaciones a los sistemas de seguridad.



En el proyecto @rsp se tiene implementado em modelo de seguridad en el nivel C2 y queda para en un futuro muy cercano, alguna persona retome el proyecto e implemete los sistemas de seguridad para llegar al nivel A.

#### **4. Instalación y configuración de software para el desarrollo el proyecto**

En este capitulo describiremos el software necesario y su configuración para el desarrollo del presente proyecto.

##### **4.1. Configuración de Windows NT Server**

Microsoft Windows NT Server es un sistema operativo diseñado para su uso en servidores de red de área local (LAN). Ofrece la potencia, la manejabilidad y la capacidad de ampliación de Windows NT en una plataforma de servidor e incluye características, como la administración centralizada de la seguridad y tolerancia a fallos más avanzada, que hacen de él un sistema operativo idóneo para servidores de red.

Windows NT Server es a la vez un sistema operativo para computadoras personales y un sistema operativo para red. Puesto que incorpora funciones de red, las redes de Windows NT Server se integran de forma óptima con el sistema operativo básico, facilitando el uso y la administración de las funciones.

A continuacion se describe los pasos para instalar un servidor Windows NT

- Instalar el Sistema Operativo Windows NT Server 4.0
  - Configurarlo con las siguientes opciones
  - Como servidor principal
  - Configurar el adaptador de red
  - Configurar protocolo TCP/IP
  - Inicializar los servicios de TCP/IP
- Una vez instalado el Sistema Operativo Windows NT Server Ver. 4.0 procedemos a instalar el Service Pack Versión 3.0
- Finalizada la instalación del Service Pack 3, procedemos a instalar el Internet Explorer Versión 4.01.
- Instalar el Windows NT Service Pack 4,
  - Dentro de la carpeta I386 seleccionar la carpeta UPDATE.
  - Dentro de i386 seleccionar la carpeta UPDATE, seleccionar el ejecutable UPDATE que dará inicio a la instalación del Service PACK.
- Instalar el Internet Explorer 4.01 Service Pack 1, Incluido con el Service Pack 4, carpeta msie401.
- Instalar, Microsoft Data Access Components 2.0, Incluido en el Service Pack 4 carpeta MDAC.
- Instalar el Microsoft Site Server Express 3.0 incluido en el Service Pack 4, carpeta SSX
- Instalar el Gestor de Bases de Datos MS SQL Server 7.0
- Instalar el Microsoft Visual Interdev 6.0
- Instalar el Microsoft Front Page 98.
- Instalar el Windows NT Option Pack

## 4.2. Configuración de Internet Information Server

Con Microsoft Internet Information Server (IIS), un equipo que ejecuta Windows NT Server se convierte en un sólido servidor Web de alto volumen que puede publicar información para usuarios locales o por todo el mundo. Internet Information Server resulta ideal para redes empresariales con equipos basados en Windows NT ya que puede instalar servidores Web de gran potencia en el hardware ya existente. Internet Information Server está integrado en el sistema operativo Windows NT Server y aprovecha sus características de seguridad y capacidades de rendimiento.

Mediante Internet Information Server puede desarrollar un sitio Web que puede utilizarse para:

- Publicar en Internet una “página principal” de su organización que presente boletines de noticias, información comercial u ofertas de empleo.
- Publicar un catálogo y aceptar pedidos de sus clientes.
- Publicar programas interactivos.
- Ofrecer a su equipo de ventas remoto un acceso sencillo a la base de datos de ventas.
- Usar una base de datos de seguimiento de pedidos.
- Publicar un manual de empleados.

Internet Information Server también proporciona otros servicios de información y es compatible con un gran número de interfaces que pueden utilizarse para desarrollar otras características para su sitio Web.

- Crear aplicaciones cliente-servidor de alto rendimiento usando la Interfaz de programación de aplicaciones servidoras de Internet de Microsoft (ISAPI).
- Personalizar el servicio WWW mediante la creación de programas ISAPI de tipo filtro que sigan las peticiones de entrada o de salida y realicen automáticamente ciertas acciones, como registros mejorados.
- Ejecutar aplicaciones o archivos de comandos de la Interfaz de puerta de enlace o gateway común (CGI).
- Transmitir o recibir archivos usando el servicio FTP.
- Publicar archivos de información, repartida en varios equipos, usando el servicio Gopher.

### 4.2.1. Internet Information Server incluye los siguientes componentes:

- Servicios de Internet: WWW, FTP y gopher.
- Administrador de servicios de Internet, la herramienta para administrar los servicios de Internet.
- Conector de bases de datos de Internet, el componente para enviar consultas a bases de datos.
- Administrador de claves, la herramienta para la instalación de las claves de Secure Sockets Layer (SSL).

### 4.2.2. Instalación de Internet Information Server

Puede instalar Internet Information Server mientras instala Windows NT Server o después de haberlo instalado.

Para instalar Internet Information Server durante la instalación de Windows NT Server

1. Cuando se le pida, asegúrese de que la casilla de verificación **Instalar Microsoft Internet Information Server** esté activada y haga clic en el botón **Siguiente**.

El programa de instalación de Internet Information Server comenzará.

2. Siga las instrucciones que aparecerán en la pantalla. Si tiene alguna pregunta, haga clic en el botón **Ayuda** en cualquier cuadro de diálogo.

Si no instala Internet Information Server durante la instalación de Windows NT Server, puede instalarlo por separado posteriormente. Para instalar Internet Information Server por separado, debe haber iniciado una sesión con privilegios de administrador.

### **Para instalar Internet Information Server después de haber instalado Windows NT Server**

1. Inserte el disco compacto de Windows NT Server en la unidad de CD-ROM.
2. Haga doble clic en el icono Instalar Internet Information Server del escritorio de Windows NT Server.
3. Siga las instrucciones que aparecerán en la pantalla. Si tiene alguna duda, haga clic en el botón **Ayuda** en cualquier cuadro de diálogo.

También puede instalar Internet Information Server mediante el Panel de control de Windows NT.

1. Inserte el disco compacto de Windows NT Server en la unidad de CD-ROM.
2. En la barra de tareas de Windows NT, haga clic en **Inicio**, señale a **Configuración** y, a continuación, haga clic en **Panel de control**.
3. En el Panel de control, haga doble clic en el icono **Red**.
4. En la hoja de propiedades **Red**, haga clic en la ficha **Servicios**.
5. Haga clic en el botón **Agregar**.
6. Desde la lista **Servicios de red**, seleccione **Microsoft Internet Information Server** y, a continuación, haga clic en **Aceptar**.
7. En el cuadro **Instalado desde**, escriba la letra de la unidad de disco donde está ubicado su disco compacto y haga clic en el botón **Aceptar**.
8. Siga las instrucciones que aparecerán en la pantalla. Para obtener información acerca de cualquier cuadro de diálogo de instalación, haga clic en el botón **Ayuda**.

De manera alternativa, puede instalar Internet Information Server directamente desde el disco compacto de Windows NT Server.

1. Inserte el disco compacto de Windows NT Server en la unidad de CD-ROM.
2. En el Explorador de Windows NT o en el símbolo del sistema, cambie a la unidad de disco que contenga el disco compacto.
3. Inicie Instalar:
  - Para iniciar Instalar desde el Explorador de Windows NT, haga doble clic en el archivo llamado Inetstp.exe, en la carpeta Inetsrv del disco compacto.
  - Para iniciar Instalar desde el símbolo del sistema, cambie a la carpeta Inetsrv del disco compacto y escriba **inetstp**.
4. Siga las instrucciones que aparecerán en la pantalla. Si tiene alguna pregunta, haga clic en el botón **Ayuda** en cualquier cuadro de diálogo.

## Proceso de instalación de Internet Information Server

Esta sección explica el proceso de instalación y ofrece pautas para la instalación de Internet Information Server.

1. Cuando inicie el programa de instalación aparece el cuadro de diálogo de bienvenida a Microsoft Internet Information Server. Haga clic en el botón **Aceptar**.

2. Todas las opciones del segundo cuadro de diálogo están seleccionadas de manera predeterminada. Haga clic en el botón **Aceptar** para instalarlas todas. Si no desea instalar un elemento en particular, desactive la casilla situada a su lado y, a continuación, haga clic en el botón **Aceptar** para instalar el resto.

**Administrador de servicios de Internet** instala el programa de administración para controlar los servicios:

- **Servicio World Wide Web** crea un servidor de publicación WWW.
- **Servicio Gopher** crea un servidor de publicación Gopher.
- **Servicio FTP** crea un servidor de publicación FTP.
- **Administración y controladores ODBC** instala los controladores Open Data Base Connectivity (ODBC). Estos controladores son necesarios para registrar la actividad en archivos ODBC y para permitir el acceso a ODBC mediante el Conector de bases de datos de Internet (IDC) desde el servicio WWW.

Si tiene una aplicación en ejecución que usa ODBC, puede que aparezca un mensaje de error indicando que hay varios componentes actualmente en uso. Antes de continuar, cierre todas las aplicaciones y los servicios que usen ODBC.

Para agregar o quitar componentes puede usar posteriormente el programa Instalar. También se puede usar Instalar para quitar todos los componentes de Internet Information Server.

3. Acepte la carpeta de instalación predeterminada (C:\Winnt\System32\Inetsrv) o haga clic en el botón **Cambiar directorio** y escriba una nueva carpeta.

**Nota** Si tiene instalado Internet Information Server, pero lo quiere instalar de nuevo en otra carpeta, debe quitar la siguiente clave del Registro de configuraciones: \HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\INetStp. Si no elimina esta clave, el botón **Cambiar directorio** aparecerá atenuado y no podrá cambiar la carpeta predeterminada.

4. Haga clic en el botón **Aceptar**. Cuando se le pida, haga clic en **Sí** para crear la carpeta de instalación.

Aparecerá el cuadro de diálogo **Directorios de publicación**.

Acepte las carpetas predeterminadas de los servicios de publicación instalados o cambie las carpetas.

5. Haga clic en el botón **Aceptar**.

6. Cuando se le pregunte si desea crear las carpetas de servicio (de forma predeterminada, Wwroot, Gophroot y Ftproot), haga clic en **Sí**.

7. El programa Instalar copiará los archivos restantes de Internet Information Server.
8. Si se ha seleccionado la opción **Administración y controladores ODBC**, aparecerá el cuadro de diálogo **Instalar controladores**.

Para instalar un controlador, selecciónelo en el cuadro de lista **Controladores ODBC disponibles** y haga clic en el botón **Aceptar**.  
Instalar terminará de copiar los archivos.

9. Cuando aparezca el cuadro de diálogo **Instalación completa**, haga clic en el botón **Aceptar** para terminar la instalación.

Este último paso completa la instalación de Servicios Web punto a punto. Ahora debe cerrar la hoja de propiedades **Servicios** y reiniciar su equipo para que surtan efecto los cambios.

Los pasos anteriores es todo lo que se necesita para una instalación. Ya puede publicar información en Internet o en su Intranet

#### **4.2.1.2. Comprobar un servidor Web en una Intranet**

1. Asegúrese de que su equipo tiene una conexión activa con la red y que el servicio servidor de WINS (u otro método de resolución de nombres) está activado.
2. Inicie Internet Explorer.
3. Escriba la dirección URL del directorio particular de su nuevo servidor.  
La dirección URL será "http://" seguido del nombre de red Windows del servidor, seguido de la ruta del archivo que quiere ver .

#### **4.2.1.3. Cómo se usa Internet Information Server**

Internet Information Server es lo bastante flexible como para realizar muchas funciones importantes dentro de su organización. Es escalable ya que admite desde un sitio con un único servidor hasta grandes instalaciones con varios servidores. Por ejemplo, www.microsoft.com y www.msn.com están actualmente entre los sitios Web de Internet con más tráfico y ambos usan varios servidores que ejecutan Microsoft Internet Information Server.

Uno de los principales factores que determinan la configuración y el uso de Internet Information Server es el hecho de que lo vayan a usar internamente los empleados dentro de su Intranet o de que vaya a estar conectado a Internet.

Los siguientes escenarios se incluyen para ayudarle a comprender el gran número de posibilidades de uso de Internet Information Server.

#### **4.2.1.4. Escenarios de Intranet**

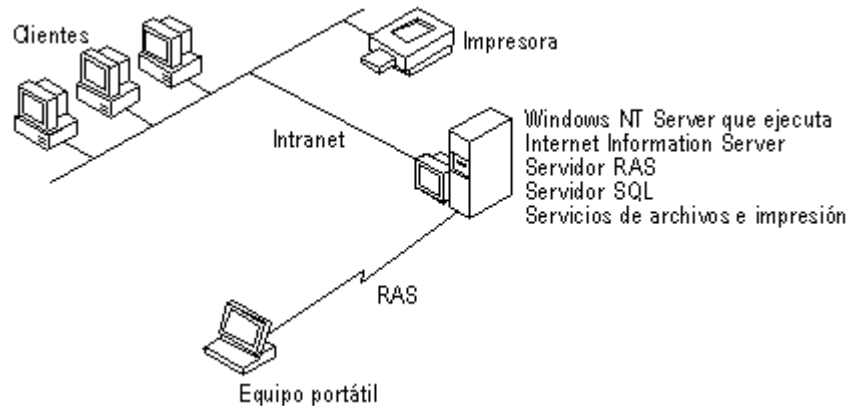
Internet Information Server se integra bien en la mayoría de los entornos existentes.

Como Internet Information Server integra las capacidades de redes y seguridad de Windows NT, casi siempre podrá agregar el software a equipos existentes y usar las

cuentas de usuario ya creadas. No es necesario usar un equipo dedicado para ejecutar Internet Information Server.

Por ejemplo, en un pequeño grupo de trabajo puede agregar Internet Information Server a un servidor de archivos y de impresión existente. El servidor Web del grupo de trabajo puede albergar páginas personales de estilo Web, aplicaciones de grupo de trabajo personalizadas, servir como interfaz para la base de datos del Lenguaje de consulta estructurado (SQL) del grupo de trabajo o utilizar Servicio de acceso remoto (RAS) para otorgar acceso telefónico a los recursos del grupo de trabajo desde sitios lejanos.

Figura 4.



En grandes organizaciones con varios departamentos o grupos de trabajo, cada departamento podría ejecutar Internet Information Server en un servidor de archivos existentes de cada grupo de trabajo. Se podría usar un servidor central de información para almacenar la información general de la organización, como el manual del empleado o el directorio de la organización.

### 4.3. Configuración y administración de Internet Information Server (IIS)

Internet Information Server incluye una herramienta de administración gráfica llamada Administrador de servicios de Internet que puede utilizarse para monitorizar, configurar y controlar los servicios de Internet.

El Administrador de servicios de Internet es la ubicación central desde la que se pueden controlar todos los equipos que ejecuten Internet Information Server en su organización.

El Administrador de servicios de Internet puede ejecutarse desde cualquier equipo con Windows NT Workstation, Windows 95, Windows 98 o Windows NT Server y que se encuentre conectado a través de la red con su servidor Web. Con la administración remota puede administrar sus servidores Web desde el propio equipo servidor, desde una estación de trabajo de administración en la red de área local (LAN) de la organización o, incluso, desde Internet.

El Administrador de servicios de Internet utiliza el modelo de seguridad de Windows NT, por lo que sólo los administradores validados podrán administrar servicios y las contraseñas de los administradores se transmiten de forma codificada a través de la red.

#### 4.3.1. Conexión a servidores Web

Es posible administrar cualquier Internet Information Server de la red conectándose a él en el Administrador de servicios de Internet. Puede especificar un servidor Web escribiendo el nombre de host con el Sistema de nombres de dominios (DNS), su dirección IP (Protocolo Internet) o su nombre NetBIOS (o nombre de equipo).

También puede encontrar todos los equipos de su red que ejecuten Internet Information Server.

Para conectarse a un servidor Web

1. En el menú **Propiedades** del Administrador de servicios de Internet, seleccione **Conectar a servidor**.
2. En el cuadro **Nombre de servidor**, escriba el nombre de host del servidor Web, su dirección IP o el nombre NetBIOS.

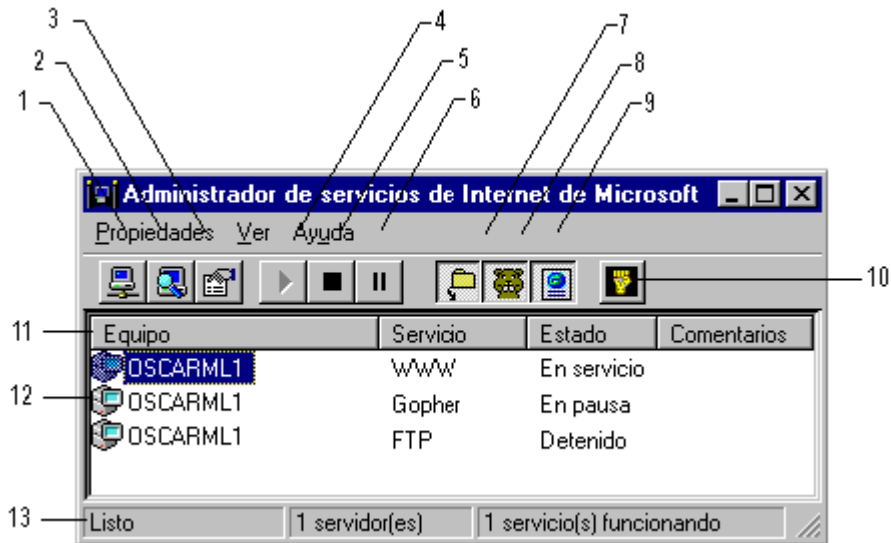
Para conectarse seleccionando un servidor Web de una lista

1. En el menú **Propiedades** del Administrador de servicios de Internet, seleccione **Buscar todos los servidores**.
2. En la lista de servidores que aparece, haga clic en el servidor al que desee conectarse.

El modo de ver Informe es el predeterminado. Este modo muestra alfabéticamente los equipos seleccionados, con sus servicios instalados en líneas separadas. Haga clic en los encabezados de columna para ordenar alfabéticamente toda la lista. El modo de ver Informe es probablemente el más útil en sitios con uno o dos equipos que ejecuten Internet Information Server



Figura 5.



### Conectar con servidores y ver hojas de propiedades

- 1 Conecta con un servidor Web específico.
- 2 Busca todos los servidores Web de la red.
- 3 Presenta hojas de propiedades para configurar el servicio seleccionado.

### Iniciar, detener y hacer una pausa en un servicio

- 4 Inicia el servicio seleccionado.
- 5 Detiene el servicio seleccionado.
- 6 Hace una pausa en el servicio seleccionado.

### Seleccionar los servicios que se deben presentar

- 7 Presenta el servicio FTP en la ventana principal del Administrador de servicios de Internet.
- 8 Presenta el servicio Gopher en la ventana principal del Administrador de servicios de Internet.
- 9 Presenta el servicio WWW en la ventana principal del Administrador de servicios de Internet.

### Iniciar el Administrador de claves para crear una clave de Security Sockets Layer

- 10 Muestra la ventana del Administrador de claves.

### Hacer los ajustes necesarios en los servicios

- 11 Ordena las listas cuando hace clic en los encabezados de columna.
- 12 Presenta las hojas de propiedades de un servicio cuando hace doble clic en él.
- 13 Presenta el estado del servidor y del servicio.



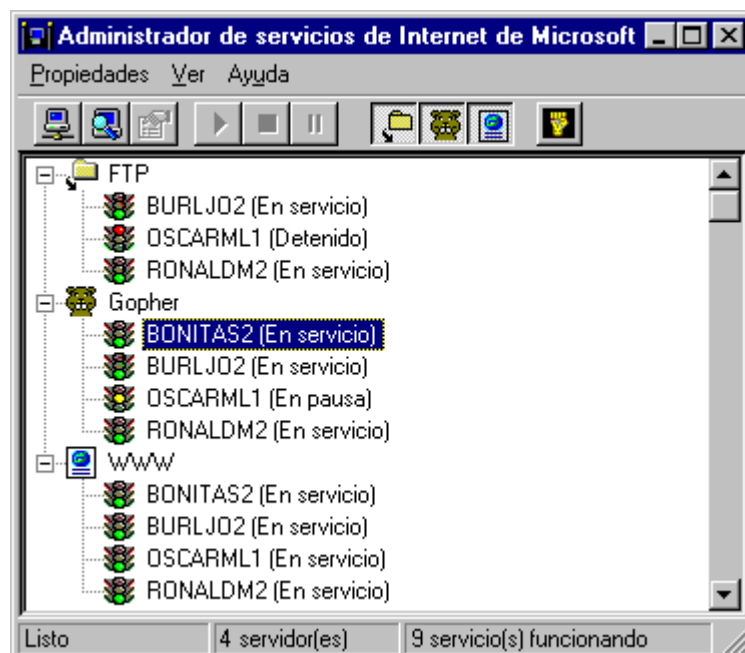
El modo de ver Servidores presenta los servicios que se ejecutan en los servidores de la red agrupados por nombre de equipo. Haga clic en el símbolo más que aparece junto al nombre de un equipo para ver los servicios que se ejecutan en él. Haga doble clic en el nombre de un servicio para ver sus hojas de propiedades. El modo de ver Servidores es el más útil en sitios con varios servidores Web cuando necesite conocer el estado de los servicios instalados en un equipo específico.

Ver figura 6.



El modo de ver Servicios enumera los servicios de cada equipo seleccionado, agrupados por nombre de servicio. Haga clic en el símbolo más que aparece junto al nombre de un servicio para ver los equipos en los que se ejecuta.

Ver figura 7.



**Haga doble clic en el nombre de un equipo bajo un servicio para ver las hojas de propiedades del servicio que se ejecuta en dicho equipo. El modo de ver Servicios es el más útil en sitios con servidores Web ampliamente distribuidos cuando necesite saber qué equipos ejecutan un servicio determinado.**

#### **4.3.2. Inicio, detención y pausa en un servicio**

Desde el Administrador de servicios de Internet se puede iniciar, detener o poner en pausa rápidamente un servicio.

Para iniciar, detener y hacer una pausa en un servicio

1. En el Administrador de servicios de Internet, seleccione el servicio que desee iniciar, detener o poner en pausa.
2. En el menú **Propiedades**, elija **Iniciar servicio**, **Detener servicio** o **Hacer una pausa en el servicio**.

#### **4.3.3. Configuración y administración de servicios**

Es posible configurar y administrar los servicios WWW, FTP y Gopher utilizando el Administrador de servicios de Internet. La siguiente información se centra en el servicio WWW, ya que es el utilizado más frecuentemente.

En el Administrador de servicios de Internet, haga doble clic en el nombre de un equipo o de un servicio para presentar sus hojas de propiedades. Haga clic en la ficha que aparece en la parte superior de cada hoja de propiedades para ver las propiedades de cada categoría. Después de establecer las propiedades del servicio, haga clic en **Aceptar** para volver a la ventana principal del Administrador de servicios de Internet. En los siguientes capítulos sobre seguridad, directorios y registro puede encontrar información detallada acerca de cada hoja de propiedades.

#### **4.4. Publicación de información en una Intranet**

Microsoft Internet Information Server, también se puede usar en cualquier red TCP/IP privada para proporcionar archivos y aplicaciones a los usuarios de la red. En esta sección se explica cómo diseñar la publicación en una Intranet o red privada. Entre los aspectos que se deben considerar cabe citar los siguientes:

- Sistemas de resolución de nombres
- Uso de DHCP
- Uso de nombres de equipo en direcciones URL
- Monitorización de SNMP (si la utiliza en su sitio)

##### **4.4.1. Sistemas de resolución de nombres**

Si quiere que los usuarios de su Intranet puedan usar nombres sencillos dentro de Internet Explorer al explorar los servidores de Web, tiene que ofrecer un sistema de resolución de nombres a los clientes.

Windows NT Server le ofrece la ventaja de la administración automática de direcciones IP con los métodos de servidores DHCP y WINS para la resolución de nombres que ofrecen los servidores de WINS.

#### **4.4.1.1. Uso de nombres de equipos con servidores de WINS**

Un servidor de WINS es un equipo que tiene instalado Windows NT Server y que ejecuta el software Microsoft TCP/IP y servidor de WINS. Un servidor de WINS mantiene una base de datos que asocia direcciones TCP/IP a nombres de equipos NetBIOS de redes Windows.

Microsoft Internet Information Server usa el software del servidor de WINS para asignar direcciones TCP/IP a nombres de equipos de la red. WINS usa nombres de equipos de redes Microsoft, lo que hace que la resolución de nombres sea más flexible que con DNS. WINS también proporciona una reducción drástica del tráfico de difusiones IP en conjuntos de redes, al tiempo que permite que los equipos cliente encuentren fácilmente sistemas remotos a través de redes de área local o de área extensa. Si usa servidores de WINS en Internet, sus equipos deberán usar direcciones IP de Internet válidas.

#### **4.4.1.2. Uso de nombres de dominio con servidores DNS**

Puede mantener un servidor DNS y los nombres de dominio TCP/IP asignados por Internet. Si piensa conectar su red con Internet, sus direcciones IP y la configuración de encaminamiento de su servidor DNS tienen que ser válidas dentro de Internet.

#### **4.4.1.3. Uso de DHCP en su Intranet**

Puede aprovechar las ventajas de la administración automática de direcciones IP que ofrece el servidor de DHCP.

Un servidor de DHCP es un equipo que tiene instalado Windows NT Server y que ejecuta el software Microsoft TCP/IP y servidor de DHCP.

Si usa servidores de DHCP, tiene que usar servidores de WINS para que los clientes dispongan de la resolución automática de nombres a direcciones IP en un entorno de red de área extensa (WAN).

#### **4.4.1.4. Uso de direcciones URL y creación de vínculos HTML para Intranet**

Cuando se conecta con un servidor o crea archivos y vínculos HTML en su Intranet, debe asignar nombres a sus equipos de acuerdo con el sistema de resolución de nombres implementado en su red. Por ejemplo, si en su red usa servidores de WINS, los vínculos usarán nombres de equipos de Windows, como <http://ventas1/principal.htm>, donde ventas1 es el nombre del equipo que ejecuta Internet Information Server.

#### **4.4.1.5. Monitorización con SNMP**

Si monitoriza su red usando el protocolo SNMP, puede usar las Bases de datos de información de administración (MIB) de SNMP proporcionadas por Microsoft Internet Information Server para monitorizar su servidor Web.

Los monitores SNMP de otros fabricantes pueden usar los archivos MIB incluidos en la carpeta \sdk del disco compacto de Microsoft Internet Information Server para permitir

la monitorización SNMP de los servicios WWW, Gopher y FTP de Microsoft Internet Information Server.

#### **4.5. Protección contra intrusos**

Si un servidor Web maneja miles de accesos directamente en Internet o mantiene documentos departamentales en su Intranet, hay que vigilar seriamente la seguridad. Cuando conecta equipos a una Intranet o a Internet, puede comunicarse con personas y con equipos de todo el mundo. Esta gran flexibilidad impone un cierto grado de riesgo: no sólo puede comunicarse con personas de otras redes, sino que también es posible que usuarios de otras redes intenten comunicarse con su red. Aunque la conexión con servidores Web se realiza normalmente con buenas intenciones, hay usuarios que intentan infiltrarse en las redes internas.

El sistema operativo Windows NT se diseñó para ayudarle a proteger su sistema contra intrusos. Internet Information Server agrega el modelo de seguridad de Windows NT y proporciona características adicionales de control y seguridad:

- Funcionamiento de la seguridad de Internet Information Server.
- Cómo controlar el acceso anónimo a su sitio Web.
- Cómo controlar el acceso mediante el nombre de usuario o de grupo.
- Cómo requerir un nombre y una contraseña de usuario para acceso autenticado.
- Cómo controlar el acceso mediante el establecimiento de permisos de carpetas y archivos.
- Cómo proteger las transmisiones de datos con SSL.

##### **4.5.1. Funcionamiento de la seguridad de Internet Information Server**

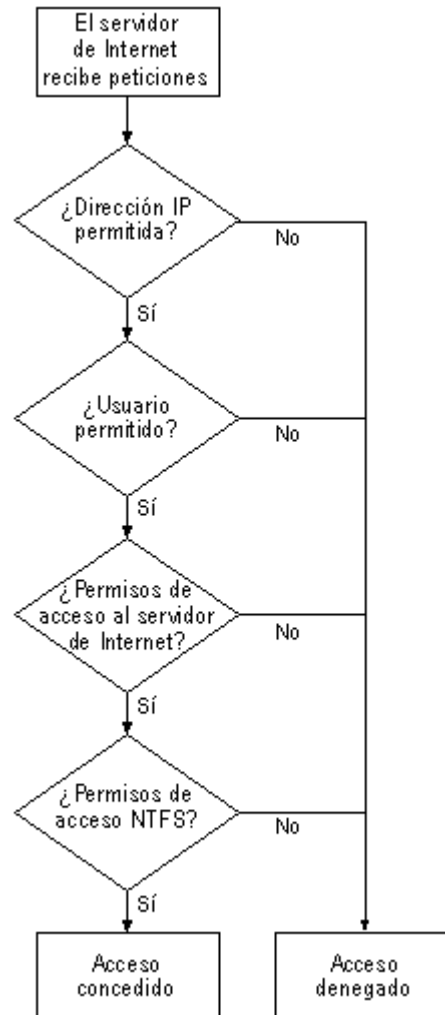
Internet Information Server se ha construido basándose en el modelo de seguridad de Windows NT. La seguridad de Windows NT le ayuda a proteger su equipo y sus recursos mediante el requisito de cuentas de usuario y contraseñas asignadas.

Puede controlar el acceso a los recursos del equipo limitando los derechos de usuario de estas cuentas. Puede utilizar el Sistema de archivos de Windows NT (NTFS) para asignar permisos a las carpetas y los archivos de su equipo. Puede controlar el acceso a carpetas y archivos impidiendo que los usuarios copien archivos hacia o desde una carpeta, o impidiendo que los usuarios ejecuten archivos en ciertas carpetas.

Además de las características de seguridad de Windows NT, puede establecer directorios virtuales de sólo lectura o de sólo ejecución utilizando el Administrador de servicios de Internet. Internet Information Server también proporciona una manera de denegar el acceso de los usuarios a equipos con determinadas direcciones IP. Es compatible con el protocolo Secure Sockets Layer (SSL), que codifica con seguridad las transmisiones de datos entre clientes y servidores.

Cuando un servidor Web de IIS recibe una petición de información de un explorador, determina si la petición es válida. En la siguiente figura se muestra una perspectiva simple general del proceso de seguridad que se utiliza en cada petición

Figura 8.



#### 4.5.2. Control de accesos anónimos

En muchos servidores Web, la mayoría del acceso a WWW, FTP y Gopher es anónimo; es decir, la petición del cliente no contiene un nombre y una contraseña de usuario. Esto ocurre en los siguientes casos:

- Un cliente FTP inicia una sesión con el nombre de usuario “anonymous”.
- Todas las peticiones de Gopher.
- La petición de un explorador de Web no contiene un nombre y una contraseña de usuario en el encabezado HTTP (esta es la forma predeterminada en las conexiones Web nuevas con la mayoría de los exploradores).

Aunque el usuario no inicie la sesión con un nombre y una contraseña de usuario individual, todavía puede controlar y monitorizar el acceso anónimo. Cada servicio de Internet mantiene un nombre de usuario y una contraseña de Windows NT que se utiliza para procesar las peticiones anónimas. Cuando se recibe una petición anónima, el

servicio “suplanta” al usuario configurado como usuario con “inicio de sesión anónimo”. La petición tiene éxito si el usuario con inicio de sesión anónimo tiene permiso de acceso al recurso solicitado, según lo determina la ACL (Lista de control de acceso) del recurso. Si el usuario con inicio de sesión anónimo no tiene permiso, la petición falla. Puede configurar el servicio WWW para que responda a un petición anónima fallida solicitando al usuario que proporcione un nombre y una contraseña válidos de Windows NT, proceso que se denomina autenticación.

#### 4.5.3. Control del acceso por usuario o por grupo

Puede controlar el acceso a su sitio Web utilizando el Administrador de usuarios de Windows NT con el fin de especificar lo que se permite hacer a ciertos usuarios o grupos en su servidor. Puede controlar aún más el acceso solicitando a las peticiones de clientes Web que proporcionen un nombre de usuario y una contraseña que confirma Internet Information Server antes de completar la petición.

La seguridad de Windows NT le ayuda a proteger el equipo y sus recursos al requerir cuentas de usuario asignadas. Todas las operaciones en un equipo que ejecuta Windows NT identifican quién está haciendo la operación. Por ejemplo, el nombre de usuario y la contraseña que utiliza para iniciar la sesión en Windows NT identifica quién es y define lo que se le autoriza a hacer en ese equipo.

Las acciones que un usuario puede realizar en un equipo se configuran con el Administrador de usuarios definiendo **Derechos del usuario** en el menú **Directivas**. Los derechos del usuario autorizan a un usuario para la realización de ciertas acciones en el sistema, incluyendo el derecho de **Iniciar sesión en modo local**, que es necesario para que los usuarios puedan emplear los servicios de Internet si se está utilizando la autenticación Básica.

#### 4.5.4. Asignar un nombre de usuario y una contraseña

Puede restringir el acceso a un sitio Web solamente a los clientes *autenticados*, es decir, a clientes de Web que proporcionan un nombre de usuario y una contraseña válidos de Windows NT. Cuando utiliza la autenticación, no se permite el acceso a menos que se proporcione un nombre de usuario y una contraseña válidos. La autenticación de la contraseña es útil si desea autorizar el acceso solamente a personas individuales a su sitio Web o a partes específicas controladas por NTFS. Puede tener activados al mismo tiempo tanto el acceso de inicio de sesión anónimo como el acceso autenticado.

El servicio WWW proporciona dos formas de autenticación: Básica y Desafío/Respuesta de Windows NT (al que a veces se denomina “NTLM”).

La autenticación Básica no codifica las transmisiones entre el cliente y el servidor. Puesto que la autenticación Básica envía la contraseña y el nombre de usuario de Windows NT del cliente en forma esencialmente decodificada a través de las redes, los intrusos podrían aprender fácilmente los nombres y las contraseñas de los usuarios.

La autenticación Desafío/Respuesta de Windows NT, compatible actualmente tan sólo con la versión 2.0 o posterior de Microsoft Internet Explorer, protege la contraseña, proporcionando un inicio de sesión seguro a través de la red. En la autenticación Desafío/Respuesta de Windows NT, la cuenta de usuario que se obtiene de un cliente es

con la que el usuario inicia la sesión en el equipo cliente. Puesto que esta cuenta, incluyendo su dominio de Windows NT, debe ser una cuenta válida en el servidor basado en Windows NT que ejecuta Internet Information Server, la autenticación Desafío/Respuesta de Windows NT es muy útil en un entorno de Intranet, donde el equipo del cliente y el del servidor están en los mismos dominios o en los de confianza. Debido al aumento en la seguridad, se recomienda utilizar el método de autenticación de contraseñas Desafío/Respuesta de Windows NT siempre que sea posible.

De forma predeterminada están activadas tanto la autenticación Básica como la autenticación Desafío/Respuesta de Windows NT. Si el explorador es compatible con Desafío/Respuesta de Windows NT, utiliza ese método de autenticación. De lo contrario, utiliza la autenticación Básica. La autenticación Desafío/Respuesta de Windows NT sólo es compatible actualmente con la versión 2.0 o posterior de Internet Explorer.

Puede requerir la autenticación del cliente para todas las peticiones del servicio FTP o sólo para las peticiones anónimas que fallan. El servicio FTP sólo es compatible con la autenticación Básica; por tanto, su sitio está más seguro si permite conexiones anónimas. La mayor seguridad para su sitio se consigue permitiendo solamente las conexiones FTP anónimas.

Para habilitar la autenticación para el servicio WWW

1. En el Administrador de servicios de Internet, haga doble clic en el servicio WWW para mostrar sus hojas de propiedades y, a continuación, haga clic en la ficha **Servicio**.
2. Seleccione **Básica (Texto simple)**, **Autenticación Windows NT** o ambas.
3. Haga clic en **Aceptar**.

Para habilitar la autenticación para el servicio FTP

1. En el Administrador de servicios de Internet, haga doble clic en el servicio FTP para mostrar sus hojas de propiedades y, a continuación, haga clic en la ficha **Servicio**.
2. Para habilitar la autenticación para conexiones anónimas fallidas, desactive la casilla de verificación **Permitir sólo conexiones anónimas**.
3. Para solicitar la autenticación de todas las peticiones de los clientes, desactive la casilla de verificación **Permitir conexiones anónimas**.

**Advertencia:** La autenticación Básica de FTP y WWW envía contraseñas a través de la red en forma de texto simple (es decir, sin codificar), al igual que la autenticación Básica de HTTP

#### **4.5.5. Como interactúan los inicios de sesión anónimos y la autenticación de clientes**

Puede habilitar tanto conexiones anónimas como autenticación de clientes para el servicio WWW y para el servicio FTP. Esta sección explica cómo un servidor Web de IIS responde a estos métodos de acceso cuando ambos están activados.

Si no está permitida la autenticación de cliente y sí las conexiones anónimas, una petición de cliente que contenga una contraseña y un nombre de usuario se procesará



como una conexión anónima, y el servidor pasará por alto la contraseña y el nombre de usuario.

#### **4.5.5.1. Servicio WWW**

Cuando un servicio WWW recibe la petición de un cliente que contiene credenciales (un nombre de usuario y una contraseña), la cuenta de usuario del “inicio de sesión anónimo” no se utiliza en el procesamiento de la petición. En su lugar, el servicio utiliza el nombre de usuario y la contraseña recibidos por el cliente. Si al servicio no se le concede permiso de acceso al recurso solicitado mientras utiliza el nombre de usuario y la contraseña especificados, la petición falla y se devuelve una notificación de error al cliente.

Cuando una petición anónima falla porque la cuenta de usuario de “inicio de sesión anónimo” no dispone de permiso de acceso al recurso deseado, la respuesta al cliente indica qué esquemas de autenticación son compatibles con el servicio WWW. Si la respuesta indica al cliente que el servicio está configurado para la autenticación Básica de HTTP, la mayoría de los exploradores de Web mostrarán un cuadro de diálogo de nombre de usuario y contraseña, y volverán a realizar la petición anónima como una petición con credenciales, incluyendo el nombre de usuario y la contraseña introducidos por el usuario.

Si un explorador de Web es compatible con el protocolo de autenticación Desafío/Respuesta de Windows NT y el servicio WWW está configurado para este protocolo, una petición WWW anónima que falle debido a los permisos inadecuados traerá como consecuencia una utilización automática del protocolo de autenticación Desafío/Respuesta de Windows NT. Entonces, el explorador enviará un nombre de usuario y una contraseña codificada desde el cliente al servicio. La petición del cliente se vuelve a procesar, utilizando la información de usuario del cliente.

Si el servicio WWW está configurado para ser compatible tanto con la autenticación Básica como con Desafío/Respuesta de Windows NT, el explorador de Web devuelve ambos métodos de autenticación al explorador de Web en un encabezado. Entonces, el explorador de Web elige qué método de autenticación va a utilizar. Como el protocolo Desafío/Respuesta de Windows NT aparece el primero en el encabezado, un explorador que sea compatible con el protocolo Desafío/Respuesta de Windows NT lo utilizará. Un explorador que no sea compatible con ese protocolo de Windows NT utilizará la autenticación Básica. Actualmente, sólo la versión 2.0 o posteriores de Internet Explorer son compatibles con la autenticación Desafío/Respuesta de Windows NT.

#### **4.5.5.2. Servicio FTP**

Cuando el servicio FTP recibe la petición de un cliente que contiene credenciales (nombre de usuario y contraseña), la cuenta de usuario de “inicio de sesión anónimo” no se utiliza en el procesamiento de la petición. En su lugar, el servicio utiliza el nombre de usuario y la contraseña recibidos por el cliente. Si no se concede al servicio permiso de acceso al recurso solicitado durante la utilización del nombre de usuario y la contraseña especificados, la petición falla y se devuelve al cliente una notificación de error.



Cuando falla una petición anónima porque la cuenta de usuario de “inicio de sesión anónimo” no tiene permiso de acceso al recurso solicitado, el servidor responde con un mensaje de error. La mayoría de los exploradores de Web mostrarán un cuadro de diálogo de nombre de usuario y contraseña, y volverán a realizar la petición anónima como una petición con credenciales, incluyendo el nombre de usuario y la contraseña introducidos por el usuario.

#### **4.5.6. Establecimiento de permisos de carpeta y archivo**

Cada acceso a un recurso, como por ejemplo un archivo, una página HTML o una aplicación de API de Internet Server (ISAPI) lo llevan a cabo los servicios en nombre de un usuario de Windows NT. El servicio utiliza el nombre de usuario y la contraseña de ese usuario en el intento de leer o ejecutar el recurso para el cliente. Puede controlar el acceso a archivos y carpetas de dos maneras:

- Estableciendo permisos de acceso en el Sistema de archivos de Windows NT (NTFS)
- Estableciendo permisos de acceso en el Administrador de servicios de Internet

Las particiones del sistema de archivos Tabla de asignación de archivos (FAT) no permiten el control de acceso. Sin embargo, una partición FAT puede convertirse en NTFS.

##### **4.5.6.1. Establecimiento de permisos NTFS**

Debe poner sus archivos de datos en una partición NTFS. NTFS proporciona seguridad y control de acceso a sus archivos de datos. Puede limitar el acceso a partes del sistema de archivos a determinados usuarios y servicios usando NTFS. En particular, se recomienda aplicar Listas de control de acceso (ACL) a sus archivos de datos para cualquier servicio de publicación de Internet.

Las ACL conceden o deniegan el acceso a la carpeta o al archivo asociado mediante cuentas de usuario o grupos de usuarios específicos de Windows NT. Cuando un servicio de Internet intenta leer o ejecutar un archivo en nombre de la petición de un cliente, la cuenta de usuario ofrecida por el servicio debe tener permiso, según lo determina la ACL asociada con este archivo, para leer o ejecutar el archivo, según sea apropiado. Si la cuenta de usuario no tiene permiso de acceso al archivo, la petición falla y se devuelve una respuesta, informando al cliente de que se ha denegado el acceso.

##### **4.5.6.2. Establecimiento del acceso al directorio WWW**

Cuando se crea un directorio (carpeta) de publicación Web en el Administrador de servicios de Internet, puede establecer permisos de acceso para el directorio particular o virtual definido y para todas las carpetas contenidas en él. Estos permisos son los proporcionados por el servicio WWW y se suman a los proporcionados por el sistema de archivos NTFS. Los permisos son:

**Lectura** El permiso de lectura permite a los clientes Web leer o copiar archivos almacenados en un directorio particular o virtual. Si un cliente envía una petición de un archivo que se encuentra en un directorio sin permiso de Lectura, el servidor Web

devuelve un error. Generalmente, debe conceder permiso de Lectura a los directorios que contengan información para publicar (archivos HTML, por ejemplo). Debe desactivar el permiso de Lectura para los directorios que contengan aplicaciones de Interfaz de gateway común (CGI) y archivos DLL de Interfaz de programación de aplicaciones servidoras de Internet (ISAPI) para impedir que los clientes copien archivos de la aplicación.

**Ejecución** El permiso de ejecución permite que un cliente Web ejecute programas y archivos de comandos almacenados en un directorio particular o virtual. Si un cliente envía una petición para ejecutar un programa o un archivo de comandos en una carpeta que no tenga permiso de ejecución, el servidor Web devuelve un error. Por razones de seguridad, no otorgue a las carpetas de contenido permiso de ejecución

#### **4.5.6.3. Control de acceso mediante la dirección IP**

Microsoft Internet Information Server puede estar configurado para conceder o denegar acceso a determinadas direcciones IP. Por ejemplo, puede excluir un individuo hostil denegando el acceso a su servidor desde una dirección IP en particular o evitar que redes enteras tengan acceso a su servidor. Por el contrario, puede elegir que solamente ciertos sitios tengan acceso a su sistema. La seguridad de dirección IP es probablemente la más útil en Internet para excluir a todo el mundo excepto a los usuarios conocidos.

La dirección IP origen de todos los paquetes que se reciben se confronta con las configuraciones de Internet Information Server en la hoja de propiedades **Avanzadas**. Si Internet Information Server está configurado para permitir el acceso a todos los equipos excepto a aquellos que aparecen en una lista como excepciones a esa regla, se deniega el acceso a cualquier equipo cuya dirección IP esté incluida en esa lista. Por el contrario, si Internet Information Server está configurado para denegar todas las direcciones IP, se deniega el acceso a todos los usuarios remotos excepto a aquellos a cuyas direcciones IP se les haya concedido acceso de manera específica.

#### **4.5.7. Seguridad en la transmisión de datos usando Secure Sockets Layer (SSL)**

En esta sección se describen los protocolos que usan la Criptografía para proteger las transmisiones de datos desde y hacia su servidor.

Microsoft Internet Information Server ofrece un protocolo para proporcionar seguridad de datos por niveles entre sus protocolos de servicio (HTTP) y TCP/IP. Este protocolo de seguridad, llamado Secure Sockets Layer (SSL)<sup>3</sup>, proporciona codificación de datos, autenticación de servidor e integridad de mensajes para una conexión TCP/IP.

SSL es un protocolo enviado al grupo de trabajo W3C acerca de la seguridad para su consideración como método de seguridad estándar para exploradores de Web y servidores de Internet. SSL proporciona un “protocolo de intercambio” de seguridad que se utiliza para iniciar la conexión TCP/IP. Este protocolo de intercambio tiene como resultado que el cliente y el servidor se pongan de acuerdo sobre el nivel de seguridad que utilizarán y lleva a cabo cualquier requisito de autenticación para la conexión. A partir de entonces, el único papel de SSL es codificar y decodificar la corriente de bytes del protocolo de aplicación que se esté utilizando (por ejemplo, HTTP). Esto significa

---

<sup>3</sup> Ver capítulo 3.7.1

que toda la información tanto en la petición HTTP como en la respuesta HTTP está totalmente codificada, incluyendo la dirección URL que está solicitando el cliente, el contenido de cualquier formulario (como por ejemplo números de tarjetas de crédito), cualquier información de autorización de acceso HTTP (nombres de usuario y contraseñas) y todos los datos devueltos por el servidor al cliente.

Un servidor con SSL habilitado puede enviar y recibir comunicaciones privadas por Internet a clientes con SSL habilitado (exploradores), como por ejemplo la versión 2.0 y posteriores de Microsoft Internet Explorer.

Las transmisiones codificadas SSL son más lentas que las que no lo están. Para evitar reducir el rendimiento de todo su sitio, considere la posibilidad de utilizar SSL sólo para carpetas virtuales que contienen información muy delicada, como por ejemplo el envío de un formulario que contenga información acerca de tarjetas de crédito.

La activación de la seguridad SSL en un servidor de Web requiere los siguientes pasos:

1. Generar un archivo de pares de claves y un archivo de petición.
2. Solicitar un certificado a una autoridad de certificación.
3. Instalar el certificado en el servidor.
4. Activar la seguridad SSL en una carpeta de servicio WWW.

**Importante** Al activar la seguridad SSL, tenga en cuenta lo siguiente:

- Puede activar la seguridad SSL en la raíz de su sitio Web (\InetPub\Wwwroot de forma predeterminada), o en una o varias carpetas virtuales.
- Una vez activado y correctamente configurado, sólo los clientes con SSL activado podrán comunicarse con las carpetas WWW con SSL activado.
- Las direcciones URL que señalen a documentos en carpetas WWW con SSL activado tienen que usar “https://” en lugar de “http://” en la dirección URL. Todos los vínculos que usen “http://” en la dirección URL no funcionarán sobre una carpeta protegida.

#### 4.5.7.1. Generación de un par de claves

Como parte del proceso de habilitar la seguridad Secure Sockets Layer (SSL) en su servidor de Web, necesita generar un par de claves y, a continuación, adquirir un certificado SSL. La nueva aplicación Administrador de claves (instalada con el producto y ubicada en el grupo de programas Internet Server) simplifica este procedimiento.

**Para generar un par de claves**

1. En el submenú **Microsoft Internet Server**, haga clic en **Administrador de claves** o haga clic en el icono Administrador de claves de la barra de herramientas del Administrador de servicios de Internet.
2. En el menú **Clave**, haga clic en **Crear nueva clave**.
3. En el cuadro de diálogo **Crear nueva clave y petición de certificado**, complete la información solicitada.
4. Tras completar el formulario, haga clic en **Aceptar**.
5. Cuando se le pida, vuelva a escribir la contraseña que escribió en el formulario y haga clic en **Aceptar**.

A medida que se crea la clave aparece un icono. Cuando ya se ha creado, aparece una pantalla con información acerca de claves nuevas y cómo obtener un certificado.

6. Tras leer la pantalla **Información de la nueva clave**, haga clic en **Aceptar**.
7. Para guardar la clave nueva, en el menú **Servidores** elija **Guardar cambios ahora**.
8. Cuando se le pregunte si desea guardar todos los cambios ahora, haga clic en **Aceptar**.

Su clave aparecerá en la ventana del Administrador de claves bajo el nombre del equipo para el cual se creó la clave. De forma predeterminada se genera una clave en su equipo local.

#### 4.5.7.2. Adquisición de un certificado

La clave generada por el Administrador de claves no es válida para su utilización en Internet hasta que obtenga para ella un certificado válido de una Autoridad de certificación como por ejemplo VeriSign. Envíe el archivo de petición del certificado a la Autoridad de certificación para obtener un certificado válido. Hasta que haga esto, la clave existirá en su equipo host, pero no se podrá utilizar. Para obtener instrucciones acerca de la adquisición de un certificado de VeriSign, consulte el sitio Web de VeriSign en <http://www.verisign.com/microsoft/>.

#### 4.5.7.3. Instalación de un certificado con un par de claves

Tras haber realizado la petición de su certificado, recibirá un certificado firmado de la Autoridad de certificación. El programa administrador de claves creará un archivo similar al del siguiente ejemplo:

```
-----BEGIN CERTIFICATE-----  
JIEBSDSCEXoChQEwLQMJSOzILvONVQECsQAwcSETMRkOAMUTBhMuVrM  
mIoAnBdNVBAoTF1JTSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYDVQ  
QLExNQZXXJzb25hIENlcnRpZmljYXRlMSQwIgwYDVQQDEXPcGVuIE1hc  
mtldCBUZXN0IFNlcnZlcjAeMTAwHhcNOTUwNzE5MjAyNzE1MjYwOTYw  
NTE0MjAyOTUwOTUwOTUwOTUwOTUwOTUwOTUwOTUwOTUwOTUwOTUwOTUw  
hdGEgU2VjdXJpdHksIEluYy4xHDAaBgNVBAsTElBlcnNvbmEgQ2VydG  
lmaWNhdGUxJDAiBgNVBAMTG09wZW4gTW9ya2V0IFRlc3QgU2VydMvYi  
DEXMDBCMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDU/7lrgR6vkVNX40BA  
q1poGdSmGkD1iN3sEPfSTGxNJXY58XH3JoZ4nrF7mIfvpghNiltayim  
vhhBPNqYe4yLPagMBAAEwDQYJKoZIhvcNAQECBQADQQBqyCpws9EaAj  
KKAefuNP+z+8NY8khckgyHN2LLpfhv+iP8m+bf66HNDULFz8ZrVOu3W  
QapgLpV90kIskNkXX3a  
-----END CERTIFICATE-----
```

#### Para instalar un certificado

1. En el grupo de programas Internet Server, haga clic en **Administrador de claves**.
2. En la ventana **Administrador de claves**, seleccione el par de claves correspondiente a su certificado firmado.
3. En el menú **Clave**, elija **Instalar certificado de clave**.
4. Seleccione en la lista el archivo de certificado (Certif.txt, por ejemplo), y haga clic en **Abrir**.
5. Cuando se le pida, escriba la contraseña que utilizó al crear el par de claves. La clave y el certificado se combinan y almacenan en el registro del servidor.

6. En el menú **Servidores**, elija **Guardar cambios ahora**.

7. Cuando se le pregunte si desea guardar todos los cambios ahora, haga clic en **Aceptar**.

**Nota** Si no especifica una dirección IP al instalar el certificado, el mismo certificado se aplicará a todos los servidores virtuales creados en el sistema. Si tiene varios sitios en un único servidor, puede especificar que el certificado sólo se va a utilizar para una determinada dirección IP de servidor agregando la dirección IP; por ejemplo:

192.168.2.1

#### 4.6. Diseño de los directorios de contenido y de los servidores virtuales

En sitios Web pequeños, los archivos de contenido Web suelen encontrarse en un árbol de directorios. Los sitios Web de mayor tamaño a menudo almacenan archivos de contenido HTML, aplicaciones Web y bases de datos en varios directorios del mismo equipo o en varios equipos de la red. Para que el contenido de los directorios que se encuentran en otros equipos aparezca en el sitio Web de su equipo, puede crear directorios virtuales.

Con Internet Information Server también puede crear servidores virtuales, que permiten que un único servidor aparezca como varios servidores. Puede asociar cada directorio de contenido con un servidor virtual específico.

##### 4.6.1. Configuración de un único directorio de contenido

Si sus archivos HTML de contenido se encuentran debajo de un árbol de directorios, basta con copiarlos al directorio particular de World Wide Web (WWW) predeterminado (\InetPub\Wwwroot) o cambiar el directorio particular para que haga referencia a la ubicación que contiene sus archivos. Sin embargo, si sus archivos residen en varios directorios o incluso en varios equipos de su red, tendrá que crear directorios virtuales para que dichos archivos estén disponibles desde su sitio Web.

##### 4.6.2. Definición del documento predeterminado y del examen de directorios

Si un usuario remoto envía una petición sin un nombre de archivo concreto (por ejemplo, <http://www.microsoft.com/>), el servicio WWW devolverá el documento predeterminado especificado, si existe en ese directorio. Puede colocar en cada directorio un archivo con el nombre de archivo del documento predeterminado.

Si no hay disponible ningún documento predeterminado, el servicio WWW devolverá un error, a menos que se habilite el examen de directorios. En ese caso, aparecerá una lista de aquellos directorios que contienen vínculos con los archivos y carpetas de dicho directorio.

Puede incluir un documento predeterminado en todos los directorios de WWW. En la hoja de propiedades **Directorios** del servicio WWW, cambie la entrada **Documento predeterminado** por el nombre de archivo predeterminado que vaya a usar en su sistema. Con frecuencia el documento predeterminado es un archivo de índice (Index.htm) del contenido de dicho directorio (o de todo el sitio Web). El nombre de archivo predeterminado es Default.htm.

Si el usuario no especifica ningún archivo dentro de un directorio en particular, se devolverá una lista en hipertexto de los archivos y los directorios.

#### 4.7. Registro de la actividad del servidor

Cada uno de los servicios contenidos en Microsoft Internet Information Server puede configurarse para registrar información acerca de quiénes han tenido acceso al servidor y la información a la que han tenido acceso. Estos datos le facilitan el ajuste del sitio, el diseño del número de usuarios que suelen tener acceso al sitio, la evaluación del contenido y las auditorías de seguridad.

#### 4.8. Publicación de información y uso de una base de datos

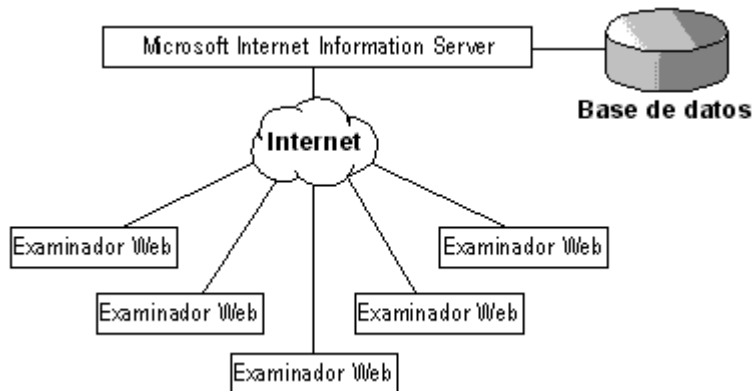
Con el servicio WWW y los controladores ODBC que proporciona Internet Information Server, puede:

- Crear páginas Web con información contenida en bases de datos.
- Insertar, actualizar y eliminar información de la base de datos según la entrada del usuario en una página Web.
- Ejecutar otros comandos del Lenguaje de consulta estructurado (SQL).

##### 4.8.1. Funcionamiento del Conector de bases de datos de Internet

En el siguiente diagrama se muestra conceptualmente el acceso a bases de datos desde Internet Information Server.

Figura 9.



Los exploradores de Web (como Internet Explorer o los exploradores de otros fabricantes como Netscape) remiten peticiones al servidor Internet usando HTTP. El servidor Internet responde con un documento en formato HTML. El acceso a las bases de datos se realiza mediante un componente de Internet Information Server llamado Conector de bases de datos de Internet (IDC). El Conector de bases de datos de Internet, Httpodbc.dll, es una DLL ISAPI que utiliza ODBC para tener acceso a las bases de datos.

La siguiente figura muestra los componentes de Internet Information Server para conectar con las bases de datos.

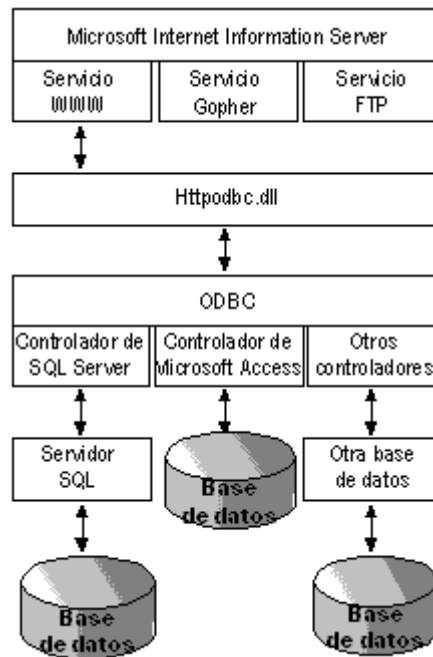


Figura 10.

El IDC utiliza dos tipos de archivos para controlar la forma de acceso a la base de datos y el modo en que se construye la página Web de salida. Dichos archivos son archivos del Conector de bases de datos de Internet (.idc) y archivos de extensión HTML (.htx).

Los archivos del Conector de bases de datos de Internet contienen la información necesaria para conectar con el origen de datos ODBC adecuado y ejecutar la instrucción SQL. Además, contienen el nombre y la ubicación del archivo de extensión HTML.

El archivo de extensión HTML constituye la plantilla para el documento HTML real que se devolverá al explorador de Web cuando el IDC haya combinado su información con la base de datos.



## 5. Desarrollo del proyecto

A continuación se describe los lineamientos necesarios para el desarrollo del proyecto denominado ARSP (Administración Remota de Sistemas para Pymes).

### 5.1. Conceptos necesarios para la introducción del proyecto

#### 5.1.1. Proyectos Web con Microsoft Visual InterDev

El World Wide Web está modificando el modo en el que los usuarios acceden a la información convirtiéndose de manera creciente en la vía preferida para la transmisión y acceso a la información, información que a veces será sensible desde el punto de vista comercial. Por ello se plantea la necesidad de dotar a WWW de los mecanismos para manejar datos de manera similar a como lo haríamos, por ejemplo, en un entorno de red local.

En este ámbito, las sedes Web se están convirtiendo en auténticas aplicaciones. La funcionalidad de este sistema requiere que las sedes Web se diseñen adecuadamente, utilizando un cierto modelo de aplicación y nuevas técnicas de desarrollo. Para nuestro caso, vamos a centrarnos en el escenario en el que la aplicación Web va a residir en un servidor Microsoft Internet Information Server sobre Windows NT Server 4.0, los mecanismos de programación van a girar alrededor de las páginas activas de servidor (Active Server Pages) y en el que la herramienta de desarrollo va a ser Microsoft Visual Interdev.

Uno de los aspectos que se refleja más directamente en la funcionalidad de la sede Web, es el aspecto de las páginas que la integran. De nada servirá diseñar una sede Web extraordinariamente potente si sus contenidos no se presentan de un modo lo suficientemente atractivo como para que el usuario que visite la sede no encuentre de manera sencilla y amable la información que solicita.

Los costos para desarrollar un proyecto con una base de datos distribuida, utilizando todas las Herramientas Microsoft, podría llegar a costar entre USD \$5000 y USD\$ 10000.

##### 5.1.1.1. Visual InterDev: plataforma de desarrollo de proyectos Web

Visual InterDev ha sido diseñado para, utilizando la interfaz de desarrollo Microsoft Developer Studio que comparten Visual C++ y Visual J++, lo cual permite el desarrollo de proyectos Web para Internet Information Server utilizando las tecnologías activas de servidor.

##### 5.1.1.2. El asistente de creación de proyectos Web (Web Project Wizard)

Visual InterDev proporciona un asistente para facilitar la creación de un proyecto Web. Web Project Wizard es accesible desde el menú **File /New**. Una vez pulsado este elemento de menú nos aparecerá el cuadro de diálogo, en el que podemos elegir el tipo de nuevo elemento que deseamos crear. Debemos elegir la opción Projects, en este cuadro de diálogo el elemento Web Project Wizard, y un nombre para el proyecto y la



ubicación en nuestra máquina local en la que se almacenará el fichero del proyecto y las copias de los ficheros que se traigan del servidor para su edición.

Esto quiere decir que la creación de un proyecto Web supone a su vez, como hemos comentado, la creación de un directorio virtual a partir del cual se ubicarán los ficheros del proyecto en el servidor al cual estemos accediendo.

### **5.1.1.3. Ficheros creados por defecto en el proyecto**

Visual InterDev genera por defecto los siguientes ficheros en el proyecto creado con Web Project Wizard

- Una carpeta \Images en la que se almacenarán las imágenes de la sede Web
- Un fichero global.asa
- Un fichero search.htm si hemos seleccionado que deseábamos dotar a la sede Web de funciones de búsqueda, algo que sucede por defecto

#### **5.1.1.3.1. El fichero global.asa**

Este fichero se añade al proyecto para permitir a los desarrolladores escribir scripts con funciones que se ejecuten como respuesta a ciertos eventos, sobretodo de inicialización o terminación de la aplicación o sesión Web. La aplicación Web se inicia cuando el primer usuario accede a la página inicial de la sede Web por vez primera y durará todo el tiempo en el que haya un usuario que esté visualizado una de las páginas Web de la sede. Una sesión Web se inicia cuando un usuario accede a la sede y finaliza cuando el usuario no ha visitado la sede durante un tiempo de desconexión que puede configurarse.

El entorno proporciona dos objetos Session y Application que proporcionan información acerca de la sesión y aplicación activas. En el fichero gloabl.asa es posible controlar los eventos de estos dos objetos, concretamente los que se disparan cuando se inicia o termina la aplicación del servidor o la sesión de navegación del usuario que accede a nuestra sede Web. Estos eventos, su manejo, para ser más estrictos, resultan muy útiles para llevar a cabo tareas de inicialización de la sesión, como podrían ser dar valores a variables de sesión, como un identificador del usuario o, por ejemplo, para incrementar un contador de visitas.

#### **5.1.1.4. Ficheros y proyectos**

Una vez el proyecto ha sido creado pueden añadirse al mismo tantos ficheros como deseemos, simplemente utilizando el menú Projects/Add To Project/ Files. Posteriormente, estos ficheros podrán ser editados utilizando los editores incorporados con Visual InterDev, u otras herramientas asociadas, como Microsoft Photo Editor, para la edición de ficheros de imagen, o Microsoft FrontPage Editor para la manipulación de documentos HTML:

La creación y manipulación de un fichero incluido en el proyecto supone varias tareas:

- Obtener el fichero del servidor o crearlo en el directorio del servidor asociado al proyecto.
- En segundo lugar se hace una copia de dicho fichero en el directorio de la máquina local asociado al mismo proyecto.
- Modificación del fichero, si procede.
- Almacenamiento del fichero modificado en el servidor

Una tarea costosa en un proyecto Web es la de mantener actualizados los vínculos entre los diversos ficheros que en él se integran. Cualquier modificación del nombre de un fichero al que se haga referencia en algún vínculo puede hacer que el proyecto entero se resienta perdiendo su funcionalidad.

### **5.1.2. Introducción a las Páginas Activas de Servidor**

Microsoft Active Server Pages (ASP) es un entorno de scripting que Internet Information Server proporciona para la creación de aplicaciones Web. ASP, en la práctica se constituye como un filtro ISAPI ubicado en el servidor Web para completar y extender la funcionalidad de Internet Information Server.

Las Active Server Pages son procesadas, como hemos dicho, en el servidor Web. Para que este proceso pueda llevarse a cabo es necesario que el servidor disponga de una extensión a tal efecto. En particular, tan sólo Microsoft Internet Information Server está dotado de extensiones para el proceso de ASP. ASP se basa en la ejecución de scripts en servidor que lleven a cabo las tareas de aplicación. Los scripts en servidor son pequeños programas, interpretables, escritos en lenguajes de script tales como VBScript o JavaScript, similares a los que se encuentran en los documentos HTML para su ejecución en el cliente.

Cuando un usuario solicita, en su navegador, el visionado de una ASP, el servidor llama a la extensión para procesar la página. Esta extensión ejecuta los scripts de servidor, se comunica con los componentes, construye un documento HTML puro sin que quede constancia alguna del script de servidor que lo ha generado, y lo envía por la red al cliente.

En definitiva una página activa de servidor es un fichero con extensión .asp que contiene una combinación de código HTML y scripts. Por lo tanto, la tarea de escribir páginas activas de servidor implica el conocimiento del lenguaje HTML, así como de uno de los lenguajes de scripting

Los scripts se insertan entre el código HTML, enmarcados entre las etiquetas `<% %>` o utilizando la etiqueta `<SCRIPT RUNAT = server >`.

### **5.1.3. HTTP y las aplicaciones Web**

Los proyectos Web son bastante diferentes a las que estamos acostumbrados a desarrollar en entornos locales. En nuestras aplicaciones convencionales estamos acostumbrados a almacenar información, por ejemplo en variables globales, cuando el usuario abandona un cuadro de diálogo y pasa a otro. En una aplicación en una sede Web resulta mucho más difícil conseguir esto, porque entre la petición de distintas páginas estamos conectándonos y desconectándonos en el marco de diversas conexiones HTTP. El protocolo HTTP (Hyper Text Transfer Protocol), es el utilizado para transferir los contenidos Web, es decir, los documentos HTML, a través de una conexión TCP/IP. La comunicación entre el servidor Web y los clientes se lleva a cabo mediante peticiones y respuestas HTTP en el marco de una sesión

Para lograr el objetivo de hacer que la información entre diversas páginas Web, es decir, lo que el usuario, por ejemplo, ha introducido en un cierto formulario, sea persistente y

almacenable, es necesario disponer de un mecanismo adicional. Este mecanismo son los objetos de servidor. Estos objetos son ejemplares persistentes de variables de clase que existen en el ámbito del servidor durante la totalidad de una sesión o aplicación del servidor. Estos objetos nos van a permitir almacenar variables de estado o simplemente nos van a dar acceso a las informaciones que el usuario nos ha enviado en una petición HTTP.

Internet Information Server incluye un conjunto de objetos de servidor, de entre los que podemos mencionar, como los más útiles:

- El objeto request. Contiene los valores que el usuario pasa al servidor en una petición HTTP, por ejemplo cuando el usuario pulsa el botón Submit de un formulario. En este caso se genera un mensaje de petición en el que se envían al servidor los valores de los controles en el formulario, para su proceso. Cada uno de estos valores será almacenados en una variable del objeto request.
- El objeto response. El servidor envía información al usuario cuando solicita una página Web. Una vez examinada la solicitud del cliente al servidor mediante un mensaje de petición HTTP, el servidor puede controlar la respuesta utilizando el objeto Response. Métodos importantes de este objeto son write, que permite escribir código HTML directamente sobre la respuesta enviada al navegador cliente, y redirect, que permite reenviar al cliente a una página web diferente.
- El objeto session permite almacenar información respecto a una sesión particular de usuario, es decir, mantiene valores durante todo el tiempo en el que el usuario se halla visitando páginas de la sede Web. Cada vez que un usuario ingresa en la sede Web, el servidor crea un nuevo objeto Session, que será destruido cuando el tiempo destinado a la sesión se consume, o bien, cuando el usuario abandona la sede.
- El objeto application permite almacenar información a la que tendrán acceso todos los usuarios que accedan a la aplicación Web.
- El objeto server proporciona acceso a todos los recursos residentes en el propio servidor.

#### **5.1.4. Acceso a bases de datos en proyectos Web**

A continuación se presenta las técnicas que Visual InterDev facilita para el acceso a bases de datos en un proyecto Web. El acceso a bases de datos es el punto en el que acaban convergiendo la mayoría de las aplicaciones y las que se desarrollan en el ámbito del Web no son una excepción. En un proyecto Web el acceso a bases de datos puede servir, por ejemplo, para almacenar información recabada a los usuarios o, simplemente, para almacenar información de las empresas.

Realizar accesos a datos, según la arquitectura Web de Internet Information Server y Visual InterDev es una tarea que conlleva escribir scripts en Active Server Pages. Visual InterDev facilita enormemente esta tarea mediante varias herramientas que se encargan de escribir gran parte del código de script de manera automática: Data Form Wizard, los controles de datos en tiempo de diseño de Visual InterDev, y Query Designer. En ocasiones, sin embargo, no podremos escribir nosotros mismos todo el código, como en el caso de utilizar técnicas más avanzadas para el acceso a bases de datos, como por ejemplo ADO (Active Data Objects).

#### 5.1.4.1. Bases de datos y Web

En un sistema de bases de datos existe, invariablemente un elemento que resulta imprescindible: el gestor de bases de datos. Este gestor o motor de bases de datos se encargará de gestionar las informaciones contenidas en la mismas, facilitándonos el acceso a ellas y manejándolas de manera que no se produzcan errores ni incoherencias en la adición y eliminación de datos. Ejemplo de gestores de bases de datos podrían ser Access, Microsoft SQL Server, Sybase, Oracle o Informix.

#### 5.1.4.2. Interfaz entre las aplicaciones y el gestor

La multiplicidad de gestores de bases de datos existentes en el mercado, con arquitectura y sintaxis diversas, conlleva en que las aplicaciones que acceden a los datos deban, en principio, someterse a las particularidades del gestor a la hora de interactuar con él. Esto motivaría que las aplicaciones sirviesen exclusivamente para un gestor en particular y que fuese necesario, para el desarrollador, conocer multitud de diferentes sintaxis de acceso. Para evitar estos problemas se han creado diversas interfaces que permiten un acceso a las diversas plataformas de datos utilizando medios comunes.

Esta interfaz suele estar conformado por un driver que estandariza las llamadas a los gestores de bases de datos. De este modo se definen funciones que pueden ser utilizadas para acceder a los datos de cualquier gestor que disponga del citado driver. Este traduce las llamadas al lenguaje y sintaxis propia del gestor.

Las dos interfaces de bases de datos a los que podemos hacer referencia en Visual InterDev son:

- Open Database Connectivity (ODBC): Esta interfaz es la más utilizada para gestores de bases de datos relacionales. Cada uno de esos gestores proporciona un driver ODBC que permite a los desarrolladores acceder a los datos desde diversas plataformas y lenguajes de programación.
- OLE DB: Es un conjunto de interfaces que Microsoft propone como el nuevo estándar. Permite acceder a datos, se constituyan o no en tablas, siempre que tengan naturaleza de conjuntos de registros.

#### 5.1.4.3. Acceso a bases de datos en Visual InterDev y IIS

Una vez descritos las diferentes interfaces disponibles vamos a ver las diferentes tecnologías de acceso a bases de datos de las que podemos hacer uso para ello desde páginas Web, concretando estas tecnologías, expresadas en herramientas, en Visual InterDev y Internet Information Server

- Internet Database Connector (IDC): Esta herramienta permite enviar consultas a cualquier base de datos ODBC desde Internet Information Server. De otro modo: Internet Database Connector permite a cualquier página Web servida por IIS acceder a bases de datos ODBC.
- Advanced Data Connector (ADC): Es un conjunto de controles ActiveX que permiten acceder a la base de datos. Los controles ActiveX se descargan hacia la máquina cliente en el marco de la página Web y desde allí se comunican con el servidor, tanto si la base de datos es ODBC como si es OLE DB.
- ActiveX Data Objects (ADO): Esta nueva tecnología no sólo es utilizable en IIS y Visual InterDev, sino también desde Visual Basic, Visual C++, o cualquier

otro controlador de automatización OLE. De hecho, ADO no son más que objetos que, mediante automatización OLE, acceden a una base de datos OLE DB o ODBC y modifican la información de la misma.

#### **5.1.4.4. Creación de un proyecto que acceda a bases de datos**

Existen básicamente dos modos de conseguir el acceso a bases de datos ODBC en un proyecto Web en Visual InterDev. El primero de ellos es crear una fuente de datos en el gestor de fuentes de datos ODBC y añadir una conexión de datos a un proyecto existente. La segunda es crear la propia base de datos y fuente de datos utilizando un asistente de proyecto de bases de datos y posteriormente utilizar esa fuente de datos en nuestro proyecto Web.

##### **5.1.4.4.1. Adición de una conexión de datos a una base de datos existente**

Para nuestro caso disponemos de SQL Server 7.0 en el que se halla una base de datos a la que nos proponemos acceder desde nuestras páginas Web. Nuestro objetivo en este punto es incorporar esta base de datos a nuestro proyecto Web creando una fuente de datos ODBC que represente a esta base de datos. Una fuente de datos representa un servidor y una base de datos en el mismo servidor, es conocida por un nombre descriptivo que permite hacer referencia a ella con comodidad.

Para crear esta fuente de datos deberemos acudir al panel de control de Windows 95, localizar el icono ODBC 32 y pulsarlo. Aparecerá un cuadro de diálogo, en el que deberemos pulsar el botón Agregar. Una vez pulsado el citado botón, se nos permite elegir el driver a utilizar. Elegiremos SQL Server.

El sistema nos permitirá entonces configurar la fuente de datos. Elegiremos un nombre descriptivo.

Una vez completado el proceso de creación de la fuente de datos, deberemos añadir la conexión a la citada fuente de datos en nuestro proyecto Web. Para ello pulsaremos con el botón derecho en el proyecto y elegiremos el menú Add Data Connection en el menú desplegable que aparecerá. El entorno nos solicitará entonces la fuente de datos a la que deseamos añadir una conexión. El entorno nos añadirá una fuente de datos, presentada como un elemento más del proyecto que dependerá del fichero global.asa

##### **5.1.4.4.2. Diseñador de consultas: Query Designer**

La funcionalidad del diseñador de consultas puede resumirse de su propia estructura de presentación de resultados. Query Designer presenta los datos en cuatro vistas: en la primera, denominada DiagramPane, se nos presenta una descripción visual de las tablas y campos implicados en la consulta, similarmente a lo que podemos encontrar en el editor visual de consultas de Access; el segundo, denominado SQL pane nos permite escribir y comprobar las sentencias SQL de la consulta que vamos a llevar a cabo, facilitándonos la comprobación de la coherencia sintáctica de la citada sentencia; el tercero, Grid Pane, nos muestra una visión alternativa, tipo hoja de cálculo, de la información presentada en el Diagram Pane; mientras que el último, Results Pane, nos permite ver los resultados de la consulta y modificarla añadiendo, editando o eliminando registros, si la consulta es actualizable.

Los tres primeros paneles tienen como objeto diseñar la consulta, mientras que el último de ellos nos permite la inspección y manipulación de los datos. Una vez la consulta ha sido diseñada, el diseñador de consultas nos permite ejecutarla, comprobando su corrección.

#### **5.1.4.4.3. Formularios con acceso a datos**

Visual InterDev que permite crear formularios que accedan a los datos almacenados en las citadas bases de datos desde el navegador de cualquier usuario que visite la sede Web.

Data Form Wizard realiza esta tarea creando páginas activas de servidor que incluyen el código necesario para acceder a estos datos, generar un documento HTML en el que estos datos se muestren, y presentarlo en el navegador. Este acceso no será tan sólo para la lectura o consulta de los mismos, sino, bien al contrario, para la actualización o adición de nuevos registros.

El acceso a estos datos se llevará a cabo utilizando ADO (Active Data Objects). El código necesario para la creación de estos objetos es escrito automáticamente por el asistente, de manera que no es preciso crear código alguno. Sin embargo, resulta interesante conocer las técnicas de utilización de estos objetos, para poder crear formularios de funcionalidad más avanzada de manera asistida con los controles en tiempo de diseño, o manualmente, de manera personalizada. Acometeremos esta tarea más adelante.

Para utilizar este asistente, deberemos acudir al menú File / New / File Wizards. En este cuadro de diálogo debemos especificar el nombre del proyecto al que deseamos añadir el formulario. A partir de ese momento se irán sucediendo los diversos pasos del asistente en los que se nos solicitará la información necesaria.

Dependiendo de las opciones elegidas a lo largo del asistente, se crearán de uno a tres ficheros asp, es decir de una a tres Active Server Pages:

ficheroForm.asp: Este fichero existirá si se ha elegido que el asistente permita la visualización de los registros en modo ficha. Presentará los registros de uno en uno, con cada uno de los campos en una caja de edición de texto. El formulario podrá incluir botones para navegar por los registros y modificar los existentes.

ficheroList.asp: Presenta todos los registros de una consulta en una tabla y existirá si se ha solicitado en el asistente la presentación en modo lista. También se incluirán botones de navegación.

ficheroAction.asp: Esta página confirma las acciones que lleva a cabo el usuario, tales como la adición o la eliminación de registros.

#### **5.1.4.4.4. Controles en tiempo de diseño para bases de datos**

Visual InterDev proporciona una serie de controles en tiempo de diseño que permiten la escritura asistida de los scripts de servidor. Dos de estos controles facilitaban el acceso a bases de datos: el Data Range Header y el Data Range Footer. Estos dos controles se utilizan conjunta e inseparablemente con el objeto de definir el conjunto de registros que se desean recoger de una base de datos. Los controles generarán un script que el



servidor procesará cuando se soliciten datos, entregando un documento HTML con los registros solicitados.

El control Header crea una estructura para almacenar el conjunto de registros e inicia un bucle para procesar los registros individualmente. Por su parte, el Footer cierra el bucle y presenta una barra de navegación para recorrer los registros. Entre ambos deberá escribirse el código necesario para los registros en pantalla.

Estos controles permiten mayor flexibilidad que el asistente pero, paralelamente, resultan más difíciles de utilizar. En principio, los controles tan sólo nos permiten la consulta de datos, y no la actualización, aunque el código ADO que se genera puede ser modificado para permitir la edición de registros. En este artículo no vamos a entrar en detalle en la utilización de estos controles.

#### **5.1.4.4.5. Acceso avanzado a bases de datos**

Hasta este punto hemos aprendido a utilizar bases de datos en nuestras sedes Web, pero utilizando asistentes, de uno u otro modo. Si bien la funcionalidad de las páginas así obtenidas es muy interesante, existen técnicas más generales y al tiempo potentes para obtener y actualizar información de bases de datos, utilizando el Advanced Data Connector (ADC) y los objetos de acceso a datos ActiveX Data Objects (ADO)

##### **5.1.4.4.5.1. ActiveX Data Objects (ADO)**

Los ActiveX Data Objects (ADO) es la propuesta de Microsoft para sustituir y ampliar el modelo de interconectividad que hasta ahora se había venido utilizando en las plataformas de desarrollo de la casa. Para aquellos que se hallen un poco familiarizados con el desarrollo de aplicaciones de bases de datos, no les resultará una sorpresa cuando comente que los dos modelos más ampliamente utilizados son DAO Data Access Objects y Remote Data Objects (RDO). El primero de ellos está estrechamente ligado con el motor de bases de datos de Access, fue introducido con Visual Basic 3.0 y utiliza el citado motor de Access y ODBC para acceder a bases de datos. El segundo se sitúa por encima del API ODBC y no utiliza el motor de bases de datos de Access, siendo introducido en Visual Basic 4.0.

Microsoft está implicado en el proyecto de unificar estas dos plataformas de acceso a bases de datos utilizando un nuevo estándar denominado OLE DB, que se impondrá, a buen seguro, en los próximos tiempos, y que tiene como característica primordial el que permite acceder a bases de datos con información que ni siquiera sea manipulada mediante el lenguaje SQL.

ADO ha sido creado para ser utilizado no sólo en las páginas Web sino para quedarse, facilitando el proceso con los modelos de bases de datos actuales, aportando simplicidad y buenos rendimientos, coherencia en la notación e integración en las soluciones. Por otra parte, ADO ha sido diseñado conjuntamente con OLE DB y facilitará, por tanto, la migración al nuevo modelo.

##### **5.1.4.4.5.2. Advanced Data Connector**

Microsoft Advanced Data Connector es una nueva tecnología para el acceso sencillo desde aplicaciones Web a bases de datos heterogéneas. Esta nueva tecnología nos

permite construir aplicaciones Web que accedan a cualquier base de datos ODBC. Aun siendo nueva, en la implementación que se ofrece con Visual InterDev, no es esta la última versión de la misma, ya que con la llegada de Internet Explorer 5 y HTML dinámico, está siendo sometida a revisión.

ADC está constituido como un conjunto de controles ActiveX que, ubicados en una página Web, permiten acceder a la base de datos ubicada en el servidor. La principal característica de ADC, esta en que el proceso de acceso a las bases de datos se gobierna desde el cliente, no desde el servidor. Los controles ActiveX ubicados en el cliente realizan una conexión con el servidor y cachean los datos en la máquina local, reduciendo al mínimo el número de accesos al servidor. Esto resulta extremadamente interesante cuando se trata de obtener datos a través de Internet. Una vez los datos han sido obtenidos los presentaremos en controles vinculados a datos.

Los componentes ADC pueden dividirse en dos categorías: los componentes cliente y los de servidor. Los componentes de cliente ADC son controles ActiveX que se ejecutan en la página Web, en el navegador. Uno de ellos, AdvancedDataControl, es el encargado de ejecutar las consultas, enviarlas al servidor y recibir los resultados que aquel le remita, en forma de recordsets. AdvancedDataSpace es un segundo control que crea ejemplares de objetos de negocio que han sido construidos como ActiveX server components y que residen en el servidor.



## 5.2. Marco teórico del proyecto

El presente estudio tiene por objeto brindar a la compañía Petróleos y Servicios C.A., Comercializadora de Combustibles, una solución a la problemática que en la actualidad se presenta en el manejo de la información concerniente a la facturación y despachos de combustibles.

Este estudio se basa en las experiencias recopiladas, conjuntamente con el contacto directo con el sistema actual.

De acuerdo con lo acotado anteriormente, este proyecto es el resultado de una recolección de los lineamientos establecidos en la compañía, del estudio y análisis de los procesos con los cuales opera PyS, así como del plan estratégico de Tecnología y Sistemas, de relaciones e información corporativa., que espero ayude a mantener a PyS a la vanguardia de las Comercializadoras de Combustible en el Ecuador.

### 5.2.1. Diagrama de procesos de una Comercializadora de Combustibles

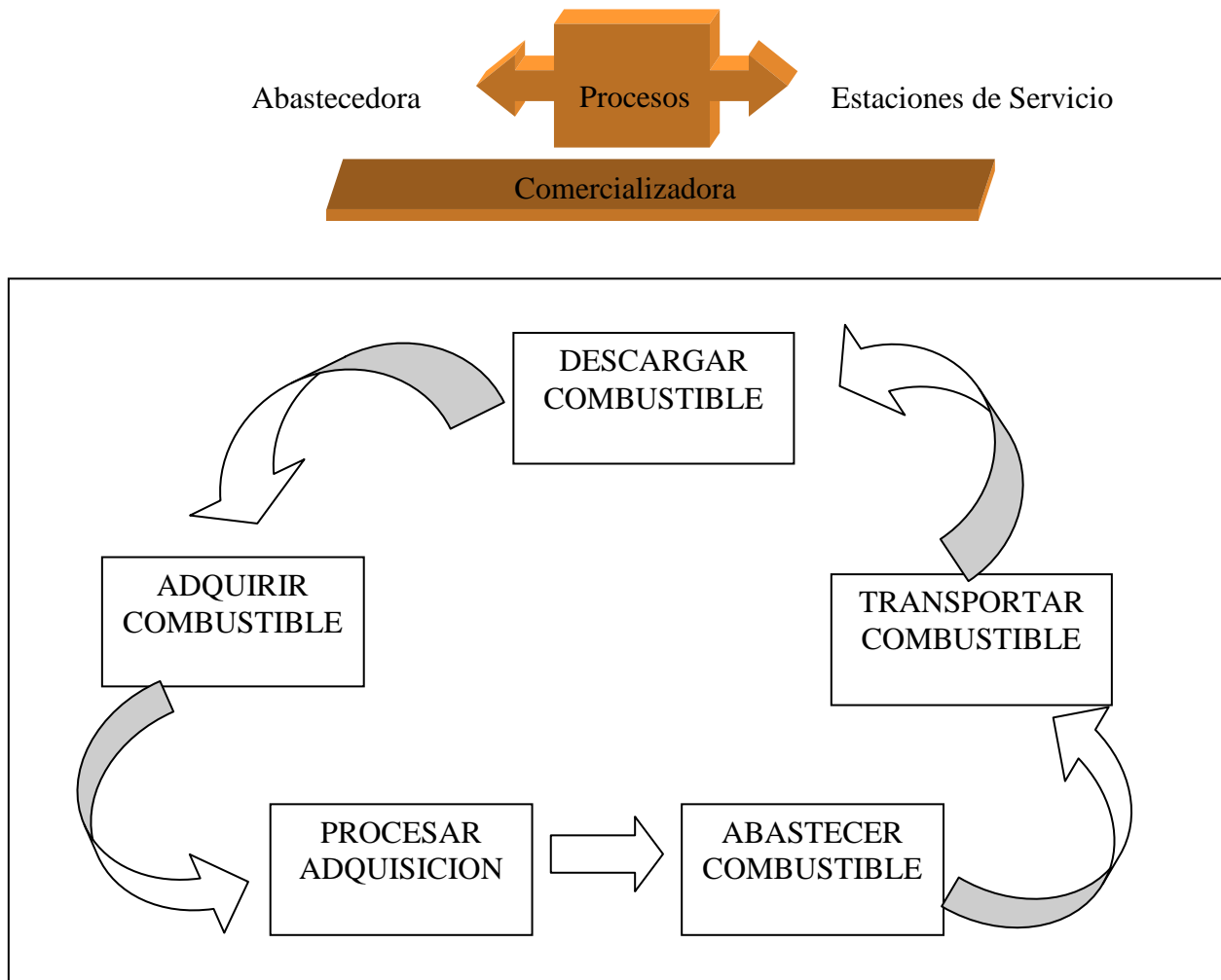


Figura 11.

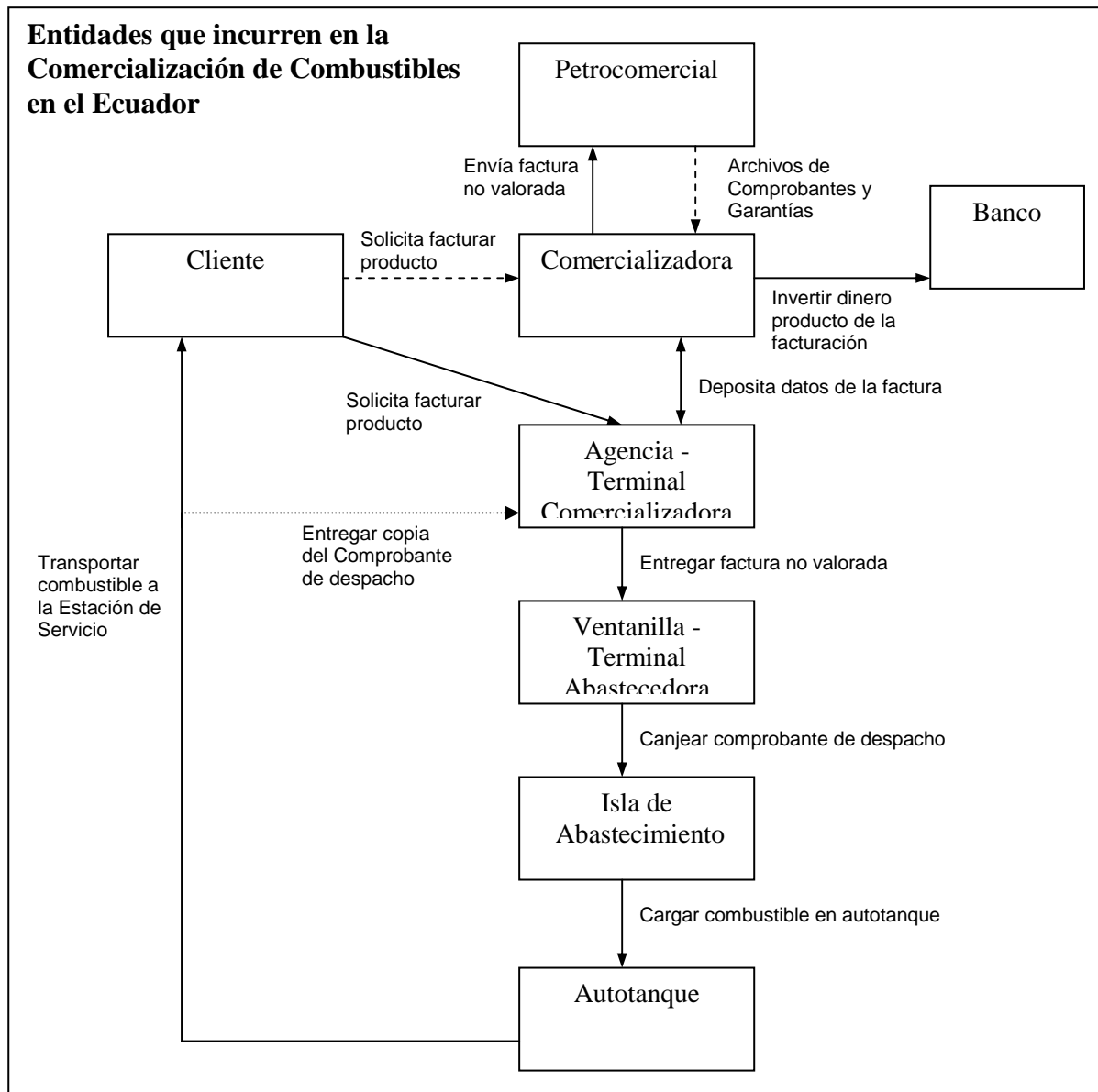
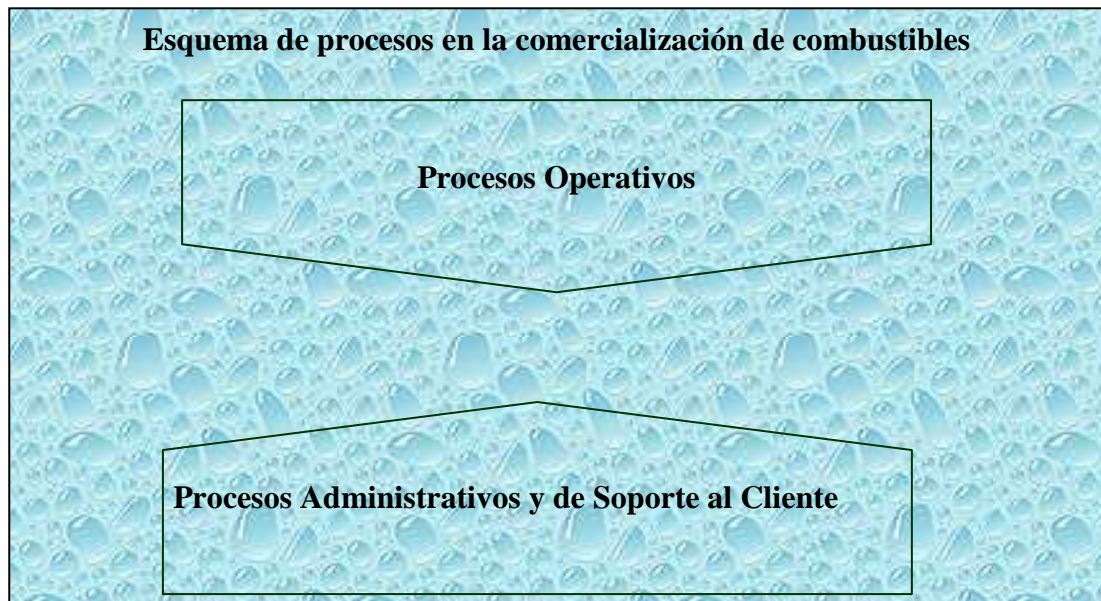


Figura 12.

Desde el año 1997 se está manteniendo el mismo esquema de facturación, el cual consiste en el siguiente proceso: El Distribuidor se acerca al Banco y solicita la factura, el banco emite la factura valorada y no valorada por cada producto solicitado y receipta el cheque por el valor total de la factura. Con la factura no valorada el distribuidor la canjea por el comprobante de despacho en Petrocomercial y procede al cargueo. Al salir pasa por la oficina de Petróleos y Servicios en los terminales para registrar el despacho y proceder al sellaje del autotanque, para finalmente desplazarse hasta la Estación de Servicio.



Actualmente el uso de la tecnología es aislada.

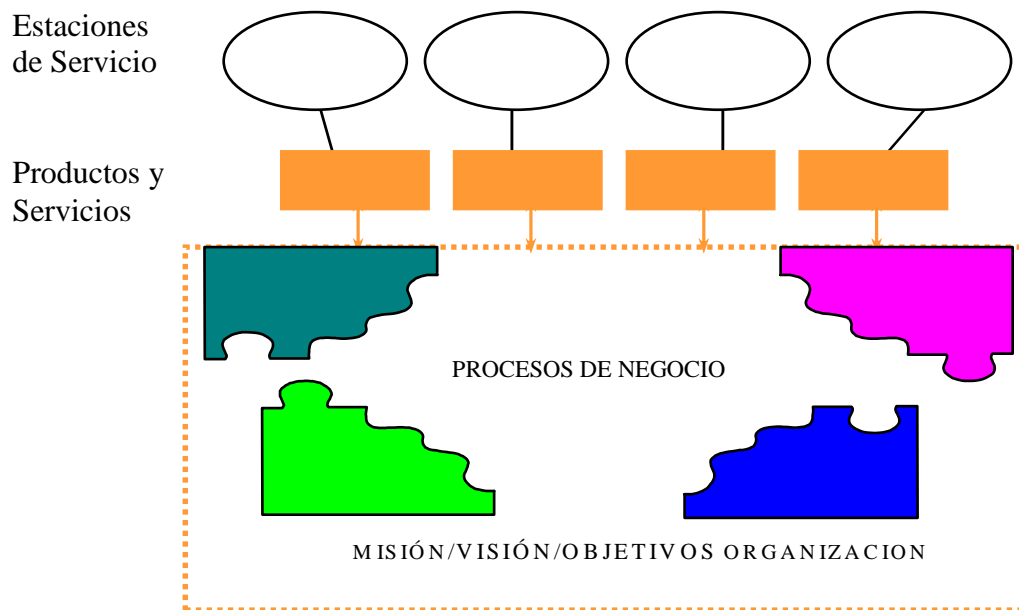


Figura 13.

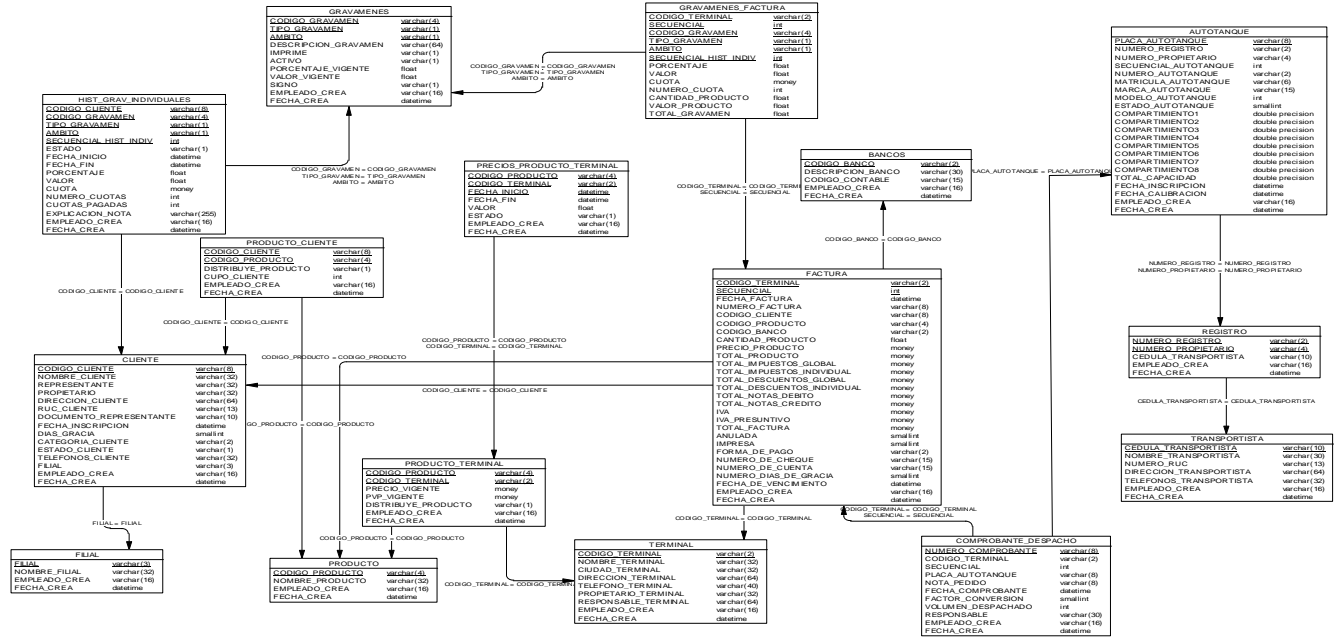
La política de cambio tecnológico que PyS, deberá promover, será consecuencia de un mayor interés hacia esta área, para mejorar las condiciones de servicio. El acceso de la mayoría de personas a la Internet, hará que sea posible utilizar este medio para la implementación de nueva tecnología.

Cuando la información se encuentre disponible en todas las áreas, se propondrá crear una infraestructura de workflow. En PyS debe existir, más que un correo electrónico, una aplicación multimedial, que permita el trabajo en grupos, una conectividad más transparente al interior y exterior; con lo cual potenciamos el compartir información en

cualquier momento donde dicha información sea requerida y por supuesto en cualquier instante.

En resumen, un sistema de información, que utilice tecnología de la Internet, que permita automatizar un conjunto de procesos de negocios críticos para la comercialización de Combustibles.

### 5.3. Modelo de la Base de Datos de @rsp



#### 5.3.1. Información de tablas

#### Lista de Tablas

Nombre	Código	Number
Autotanque	AUTOTANQUE	3
Bancos	BANCOS	
Cliente	CLIENTE	
Comprobante de despacho	COMPROBANTE_DESPACHO	
Cupos	CUPOS	
Factura	FACTURA	
Filial	FILIAL	1
Gravamenes	GRAVAMENES	
Gravamenes Factura	GRAVAMENES_FACTURA	
Historia gravamenes individuales	HIST_GRAV_INDIVIDUALES	
LOG_ACCESOS_ARSP	LOG_ACCESOS_ARSP	
PAGINA_ARSP	PAGINA_ARSP	
PERMISOS_USUARIO_ARSP	PERMISOS_USUARIO_ARSP	
Precio Venta Publico	PVP	
Precios Producto Terminal	PRECIOS_PRODUCTO_TERMINAL	
Producto	PRODUCTO	
Producto Cliente	PRODUCTO_CLIENTE	
Producto Terminal	PRODUCTO_TERMINAL	

Nombre	Código	Number
Registro	REGISTRO	
Secuenciales	SECUENCIAL	
Terminales	TERMINAL	
Transportista	TRANSPORTISTA	
USUARIO_ARSP	USUARIO_ARSP	

### Tabla autotanque

<b>Nombre:</b>	autotanque
<b>Código:</b>	AUTOTANQUE

Nombre	Código	Tipo
Placa autotanque	PLACA_AUTOTANQUE	varchar(8)
Numero registro	NUMERO_REGISTRO	Varchar(2)
Numero propietario	NUMERO_PROPIETARIO	Varchar(4)
Secuencial autotanque	SECUENCIAL_AUTOTANQUE	Int
Numero autotanque	NUMERO_AUTOTANQUE	Varchar(2)
Matricula autotanque	MATRICULA_AUTOTANQUE	Varchar(6)
Marca autotanque	MARCA_AUTOTANQUE	Varchar(15)
Modelo autotanque	MODELO_AUTOTANQUE	Int
Estado autotanque	ESTADO_AUTOTANQUE	Smallint
Compartimiento1	COMPARTIMIENTO1	Double precision
Compartimiento2	COMPARTIMIENTO2	Double precision
Compartimiento3	COMPARTIMIENTO3	Double precision
Compartimiento4	COMPARTIMIENTO4	Double precision
Compartimiento5	COMPARTIMIENTO5	Double precision
Compartimiento6	COMPARTIMIENTO6	Double precision
Compartimiento7	COMPARTIMIENTO7	Double precision
Compartimiento8	COMPARTIMIENTO8	Double precision
Total capacidad	TOTAL_CAPACIDAD	Double precision
Fecha inscripcion	FECHA_INSCRIPCION	Datetime
Fecha calibracion	FECHA_CALIBRACION	Datetime
Empleado crea	EMPLEADO_CREA	Varchar(16)
Fecha crea	FECHA_CREA	Datetime

### Tabla Bancos

<b>Nombre:</b>	Bancos
<b>Código:</b>	BANCOS

Nombre	Código	Tipo	P	M
Código banco	CODIGO_BANCO	Varchar(2)	Yes	Yes
Descripción banco	DESCRIPCION_BANCO	Varchar(30)	No	Yes
Código contable	CODIGO_CONTABLE	varchar(15)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Cliente

<b>Nombre:</b>	Cliente
<b>Código:</b>	CLIENTE

Nombre	Código	Tipo	P	M
Código cliente	CODIGO_CLIENTE	varchar(8)	Yes	Yes
Nombre cliente	NOMBRE_CLIENTE	varchar(32)	No	Yes
Representante	REPRESENTANTE	varchar(32)	No	Yes
Propietario	PROPIETARIO	varchar(32)	No	Yes
Dirección cliente	DIRECCION_CLIENTE	varchar(64)	No	Yes
Documento cliente	RUC_CLIENTE	varchar(13)	No	Yes
Documento representante	DOCUMENTO_REPRESENTANTE	varchar(10)	No	No
Inscripción cliente	FECHA_INSCRIPCION	datetime	No	Yes
Días gracia	DIAS_GRACIA	smallint	No	Yes
Categoría cliente	CATEGORIA_CLIENTE	varchar(2)	No	Yes
Estado cliente	ESTADO_CLIENTE	varchar(1)	No	Yes
Teléfonos cliente	TELEFONOS_CLIENTE	varchar(32)	No	No
Filial	FILIAL	varchar(3)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
Fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Comprobante de despacho

<b>Nombre:</b>	Comprobante de despacho
<b>Código:</b>	COMPROBANTE_DESPACHO

Nombre	Código	Tipo	P	M
Número comprobante	NUMERO_COMPROBANTE	varchar(8)	Yes	Yes
Código terminal	CODIGO_TERMINAL	varchar(2)	No	Yes
Secuencial	SECUENCIAL	int	No	Yes
Placa autotank	PLACA_AUTOTANQUE	varchar(8)	No	No
Número nota pedido	NOTA_PEDIDO	varchar(8)	No	Yes
Fecha comprobante	FECHA_COMPROBANTE	datetime	No	Yes
Factor conversión	FACTOR_CONVERSION	smallint	No	No
Volumen despachado	VOLUMEN_DESPACHADO	int	No	No
Responsable	RESPONSABLE	varchar(30)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
Fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Factura

<b>Nombre:</b>	Factura
<b>Código:</b>	FACTURA

Nombre	Código	Tipo	P	M
Código terminal	CODIGO_TERMINAL	varchar(2)	Yes	Yes
Secuencial	SECUENCIAL	int	Yes	Yes
Fecha factura	FECHA_FACTURA	datetime	No	Yes
Número factura	NUMERO_FACTURA	varchar(8)	No	No
Código cliente	CODIGO_CLIENTE	varchar(8)	No	Yes
Código producto	CODIGO_PRODUCTO	varchar(4)	No	Yes
Código banco	CODIGO_BANCO	varchar(2)	No	No
Cantidad producto	CANTIDAD_PRODUCTO	float	No	Yes
Precio producto	PRECIO_PRODUCTO	money	No	Yes
Total producto	TOTAL_PRODUCTO	money	No	Yes
Total impuestos global	TOTAL_IMPUESTOS_GLOBAL	money	No	Yes
Total impuestos individual	TOTAL_IMPUESTOS_INDIVIDUAL	money	No	Yes
Total descuentos global	TOTAL_DESCUENTOS_GLOBAL	money	No	Yes
Total descuentos individual	TOTAL_DESCUENTOS_INDIVIDUAL	money	No	Yes
Total notas debito	TOTAL_NOTAS_DEBITO	money	No	Yes
Total notas credito	TOTAL_NOTAS_CREDITO	money	No	Yes
Iva	IVA	money	No	Yes
Iva presuntivo	IVA_PRESUNTIVO	money	No	Yes
Total factura	TOTAL_FACTURA	money	No	Yes
Anulada	ANULADA	smallint	No	Yes
Impresa	IMPRESA	smallint	No	Yes
Forma de pago	FORMA_DE_PAGO	varchar(2)	No	Yes
Número de cheque	NUMERO_DE_CHEQUE	varchar(15)	No	No
Número de cuenta	NUMERO_DE_CUENTA	varchar(15)	No	No
Número días de gracia	NUMERO_DIAS_DE_GRACIA	smallint	No	Yes
Fecha de vencimiento	FECHA_DE_VENCIMIENTO	datetime	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
Fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Filial

<b>Nombre:</b>	Filial
<b>Código:</b>	FILIAL

Nombre	Código	Tipo	P	M
Filial	FILIAL	varchar(3)	Yes	Yes
Nombre filial	NOMBRE_FILIAL	varchar(32)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	No
fecha crea	FECHA_CREA	datetime	No	No

## Tabla Gravámenes

<b>Nombre:</b>	Gravámenes
<b>Código:</b>	GRAVAMENES

Nombre	Código	Tipo	P	M
Código gravamen	CODIGO_GRAVAMEN	varchar(4)	Yes	Yes
Tipo gravamen	TIPO_GRAVAMEN	varchar(1)	Yes	Yes
Ambito	AMBITO	varchar(1)	Yes	Yes
Descripción gravamen	DESCRIPCION_GRAVAMEN	varchar(64)	No	Yes
Imprime	IMPRIME	varchar(1)	No	Yes
Activo	ACTIVO	varchar(1)	No	Yes
Porcentaje actual	PORCENTAJE_VIGENTE	float	No	No
Valor actual	VALOR_VIGENTE	float	No	No
Signo	SIGNO	varchar(1)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
Fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Gravámenes Factura

<b>Nombre:</b>	Gravámenes Factura
<b>Código:</b>	GRAVAMENES_FACTURA

Nombre	Código	Tipo	P	M
Código terminal	CODIGO_TERMINAL	varchar(2)	Yes	Yes
Secuencial	SECUENCIAL	int	Yes	Yes
Código gravamen	CODIGO_GRAVAMEN	varchar(4)	Yes	Yes
Tipo gravamen	TIPO_GRAVAMEN	varchar(1)	Yes	Yes
Ambito	AMBITO	varchar(1)	Yes	Yes
Secuencial_hist_indivi	SECUENCIAL_HIST_INDIV	int	Yes	Yes
Porcentaje	PORCENTAJE	float	No	Yes
Valor	VALOR	float	No	Yes
Cuota	CUOTA	money	No	Yes
Numero cuota	NUMERO_CUOTA	int	No	Yes
Cantidad producto	CANTIDAD_PRODUCTO	float	No	Yes
Valor producto	VALOR_PRODUCTO	float	No	Yes
Total gravamen	TOTAL_GRAVAMEN	float	No	Yes



## Tabla historia gravámenes individuales

<b>Nombre:</b>	historia gravámenes individuales
<b>Código:</b>	HIST_GRAV_INDIVIDUALES

Nombre	Código	Tipo	P	M
Código cliente	CODIGO_CLIENTE	varchar(8)	Yes	Yes
Código gravamen	CODIGO_GRAVAMEN	varchar(4)	Yes	Yes
Tipo gravamen	TIPO_GRAVAMEN	varchar(1)	Yes	Yes
Ambito	AMBITO	varchar(1)	Yes	Yes
Secuencial_hist_indivi	SECUENCIAL_HIST_INDIV	int	Yes	Yes
Estado	ESTADO	varchar(1)	No	Yes
Fecha inicio vigencia	FECHA_INICIO	datetime	No	Yes
Fecha fin vigencia	FECHA_FIN	datetime	No	No
Porcentaje	PORCENTAJE	float	No	No
Valor	VALOR	float	No	No
Cuota	CUOTA	money	No	Yes
Numero cuotas	NUMERO_CUOTAS	int	No	No
Cuotas pagadas	CUOTAS_PAGADAS	int	No	Yes
Explicacion nota	EXPLICACION_NOTA	varchar(255)	No	No
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
Fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Precios Producto Terminal

<b>Nombre:</b>	Precios Producto Terminal
<b>Código:</b>	PRECIOS_PRODUCTO_TERMINAL

Nombre	Código	Tipo	P	M
Código producto	CODIGO_PRODUCTO	varchar(4)	Yes	Yes
Código terminal	CODIGO_TERMINAL	varchar(2)	Yes	Yes
fecha inicio vigencia	FECHA_INICIO	datetime	Yes	Yes
fecha fin vigencia	FECHA_FIN	datetime	No	No
Valor	VALOR	float	No	Yes
Estado	ESTADO	varchar(1)	No	Yes
empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Producto

<b>Nombre:</b>	Producto
<b>Código:</b>	PRODUCTO

Nombre	Código	Tipo	P	M
Código producto	CODIGO_PRODUCTO	varchar(4)	Yes	Yes
Nombre producto	NOMBRE_PRODUCTO	varchar(32)	No	Yes

Nombre	Código	Tipo	P	M
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

### Tabla Producto Cliente

<b>Nombre:</b>	Producto Cliente
<b>Código:</b>	PRODUCTO_CLIENTE

Nombre	Código	Tipo	P	M
Código cliente	CODIGO_CLIENTE	varchar(8)	Yes	Yes
Código producto	CODIGO_PRODUCTO	varchar(4)	Yes	Yes
Distribuye producto	DISTRIBUYE_PRODUCTO	varchar(1)	No	Yes
Cupo cliente	CUPO_CLIENTE	int	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

### Tabla Producto Terminal

<b>Nombre:</b>	Producto Terminal
<b>Código:</b>	PRODUCTO_TERMINAL

Nombre	Código	Tipo	P	M
Código producto	CODIGO_PRODUCTO	varchar(4)	Yes	Yes
Código terminal	CODIGO_TERMINAL	varchar(2)	Yes	Yes
Precio vigente	PRECIO_VIGENTE	money	No	No
pvp vigente	PVP_VIGENTE	money	No	No
Distribuye producto	DISTRIBUYE_PRODUCTO	varchar(1)	No	No
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

### Tabla Registro

<b>Nombre:</b>	Registro
<b>Código:</b>	REGISTRO

Nombre	Código	Tipo	P	M
Numero registro	NUMERO_REGISTRO	varchar(2)	Yes	Yes
Numero propietario	NUMERO_PROPIETARIO	varchar(4)	Yes	Yes
Cedula transportista	CEDULA_TRANSPORTISTA	varchar(10)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Terminales

<b>Nombre:</b>	Terminales
<b>Código:</b>	TERMINAL

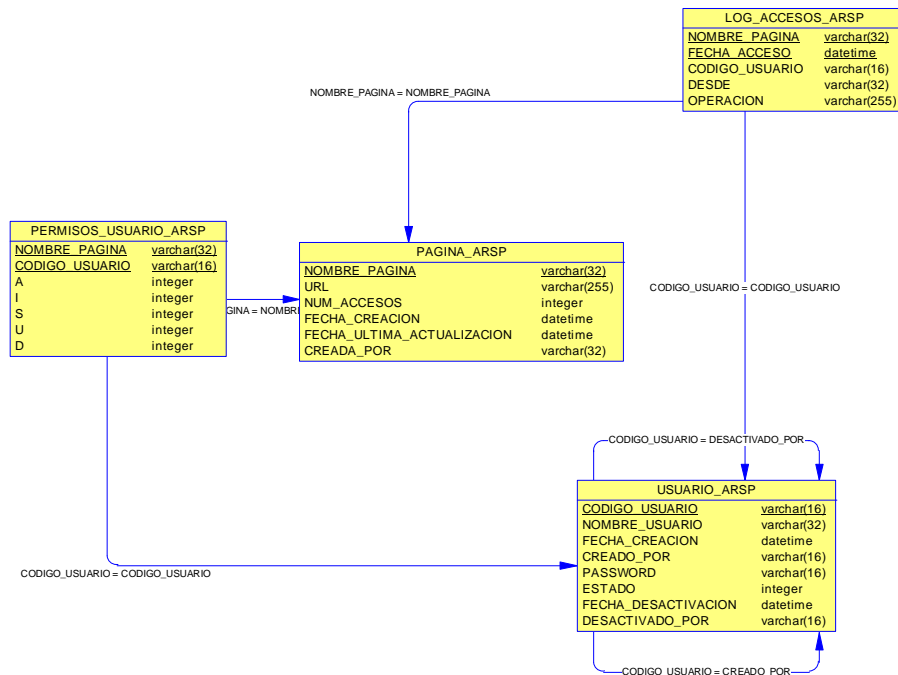
Nombre	Código	Tipo	P	M
Codigo terminal	CODIGO_TERMINAL	varchar(2)	Yes	Yes
Nombre terminal	NOMBRE_TERMINAL	varchar(32)	No	Yes
Ciudad terminal	CIUDAD_TERMINAL	varchar(32)	No	Yes
Direccion terminal	DIRECCION_TERMINAL	varchar(64)	No	Yes
Telefono terminal	TELEFONO_TERMINAL	varchar(40)	No	Yes
Propietario terminal	PROPIETARIO_TERMINAL	varchar(32)	No	Yes
Responsable terminal	RESPONSABLE_TERMINAL	varchar(64)	No	Yes
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
Fecha crea	FECHA_CREA	datetime	No	Yes

## Tabla Transportista

<b>Nombre:</b>	Transportista
<b>Código:</b>	TRANSPORTISTA

Nombre	Código	Tipo	P	M
Cedula transportista	CEDULA_TRANSPORTISTA	varchar(10)	Yes	Yes
Nombre transportista	NOMBRE_TRANSPORTISTA	varchar(30)	No	Yes
Numero ruc	NUMERO_RUC	varchar(13)	No	Yes
Direccion transportista	DIRECCION_TRANSPORTISTA	varchar(64)	No	No
Telefonos transportista	TELEFONOS_TRANSPORTISTA	varchar(32)	No	No
Empleado crea	EMPLEADO_CREA	varchar(16)	No	Yes
fecha crea	FECHA_CREA	datetime	No	Yes

## 5.4. Modelo de control de accesos para @rsp



### 5.4.1. Información de tablas

#### Tabla LOG\_ACCESOS\_ARSP

<b>Nombre:</b>	LOG_ACCESOS_ARSP
<b>Código:</b>	LOG_ACCESOS_ARSP

Nombre	Código	Tipo	P	M
NOMBRE_PAGINA	NOMBRE_PAGINA	varchar(32)	Yes	Yes
FECHA_ACCESO	FECHA_ACCESO	datetime	Yes	Yes
CODIGO_USUARIO	CODIGO_USUARIO	varchar(16)	No	No
DESDE	DESDE	varchar(32)	No	No
OPERACIÓN	OPERACION	varchar(255)	No	No

#### Tabla PAGINA\_ARSP

<b>Nombre:</b>	PAGINA_ARSP
<b>Código:</b>	PAGINA_ARSP

Nombre	Código	Tipo	P	M
NOMBRE_PAGINA	NOMBRE_PAGINA	varchar(32)	Yes	Yes
URL	URL	varchar(255)	No	Yes

Nombre	Código	Tipo	P	M
NUM_ACCESOS	NUM_ACCESOS	integer	No	Yes
FECHA_CREACION	FECHA_CREACION	datetime	No	Yes
FECHA_ULTIMA_ACTUALIZACION	FECHA_ULTIMA_ACTUALIZACION	datetime	No	Yes
CREADA_POR	CREADA_POR	varchar(32)	No	Yes

### Tabla PERMISOS\_USUARIO\_ARSP

<b>Nombre:</b>	PERMISOS_USUARIO_ARSP
<b>Código:</b>	PERMISOS_USUARIO_ARSP

Nombre	Código	Tipo	P	M
NOMBRE_PAGINA	NOMBRE_PAGINA	varchar(32)	Yes	Yes
CODIGO_USUARIO	CODIGO_USUARIO	varchar(16)	Yes	Yes
A	A	integer	No	Yes
I	I	integer	No	Yes
S	S	integer	No	Yes
U	U	integer	No	Yes
D	D	integer	No	Yes

### Table USUARIO\_ARSPTabla USUARIO\_ARSP

<b>Nombre:</b>	USUARIO_ARSP
<b>Código:</b>	USUARIO_ARSP

Nombre	Código	Tipo	P	M
CODIGO_USUARIO	CODIGO_USUARIO	varchar(16)	Yes	Yes
NOMBRE_USUARIO	NOMBRE_USUARIO	varchar(32)	No	Yes
FECHA_CREACION	FECHA_CREACION	datetime	No	Yes
CREADO_POR	CREADO_POR	varchar(16)	No	No
PASSWORD	PASSWORD	varchar(16)	No	Yes
ESTADO	ESTADO	integer	No	Yes
FECHA_DESACTIVACION	FECHA_DESACTIVACION	datetime	No	No
DESACTIVADO_POR	DESACTIVADO_POR	varchar(16)	No	No

### 5.4.2. Triggers de control

```
/*
** TRIGGERS PARA LA BASE DE DATOS ARSP
** TRIGGERS PARTE #1 PROYECTO ARSP
*/
```

```
use arsp2000
go
```

```
dump tran arsp2000 with no_log
go
```

```
dump tran log_arsp with no_log
go
```

```
CREATE TRIGGER ti_usuario_arsp ON [USUARIO_ARSP]
```

```
/*
```

```
+-----+
| Nombre   : ti_usuario           |
| Descripcion : TRIGGER PARA MODIFICACION EN LA |
| TABLA USUARIO_ARSP            |
+-----+
| Tutor    : Carlos Javier Luna S. |
| Autor    : Fernando Sandoval Galárraga |
+-----+
| 1. Se dispara el momento de generar un nuevo usuario tabla |
| AUTOTANQUE de la BDD arsp2000. |
+-----+
| FECHA: DD/MM/YYYY             |
| Modificacion:                  |
+-----+
*/
```

```
FOR INSERT
```

```
AS
```

```
INSERT INTO PERMISOS_USUARIO_ARSP (NOMBRE_PAGINA,  
CODIGO_USUARIO)
```

```
SELECT NOMBRE_PAGINA,  
inserted.CODIGO_USUARIO
```

```
FROM PAGINA_ARSP,  
inserted
```

```
CREATE TRIGGER ti_pagina_arsp ON [PAGINA_ARSP]
```

```
/*
```

```
+-----+
| Nombre   : ti_pagina_arsp       |
| Descripcion : TRIGGER PARA MODIFICACION EN LA |
| TABLA PAGINA_ARSP             |
+-----+
| Tutor    : Carlos Javier Luna S. |
| Autor    : Fernando Sandoval Galárraga |
+-----+
| 1. Se dispara el momento de generar una nueva pagina tabla |
| AUTOTANQUE de la BDD arsp2000. |
+-----+
| FECHA: DD/MM/YYYY             |
+-----+
*/
```



## 5.5. Listado de Hardware y Software necesario

### 5.5.1. Software

#### Servidor

- Sistema Operativo, MS Windows NT Versión 4.0
- Windows NT Server Versión 4 Service Pack 3
- Windows NT Server Versión 4 Service Pack 4
- Windows NT Server Versión 4 Service Pack 5
- Internet Information Server Versión 4.0
- Internet Explorer 4.0
- Internet Explorer 4.01 Service Pack 1
- Modelador de Base de Datos, Power Designer Versión 6.5
- Gestor de Base de datos, MS SQL Server Versión 7.0
- MS Visual Interdev Versión 6.0
- MS Front Page 98

#### Cliente

- Sistema Operativo Windows 95
- Internet Explorer versión 4.0
- Internet Explorer 4.0 Service Pack 1

### 5.5.2. Hardware

#### Servidor

- 128 MB Memoria RAM
- Procesador Pentium II de 400 MHz de velocidad
- 4.3 GB disco duro
- Tarjeta de Video SVGA
- Tarjeta de Red

#### Estaciones

- 32 MB Memoria RAM
- Procesador de 200 MHz de velocidad
- 2.1 GB disco duro
- Tarjeta de Video SVGA
- Tarjeta de Red

#### Networking

- 1 Switch o Hub 10/100 Autosensing
- Tarjetas de Red 10/100 Mbps, tanto en el servidor como en las estaciones
- Cable UTP, categoría 5

## 5.6. Datos técnicos del sistema propuesto:

Arquitectura: Cliente / Servidor (2 capas)

Back End: MS SQL Server Versión 7.0

Sistema Operativo: Servidor Windows NT server 4.0

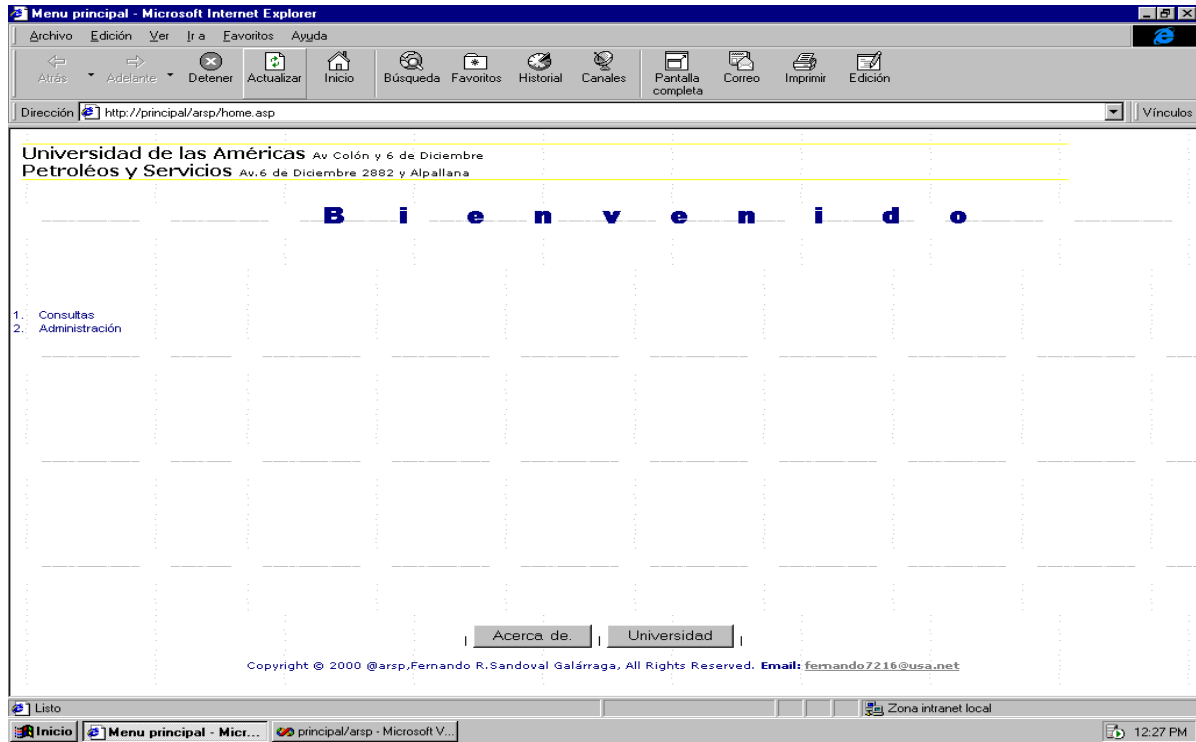


Front End: MS Internet Explorer 4.0  
Sistema Operativo: Clientes Win95

## 5.7. Presentacion de las pantallas

A continuacion se presenta las pantallas que fueron desarrolladas para administrar el proceso de facturacion y despachos en la compañía Petróleos y Servicios.

### Pantalla principal



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

1. Consultas

1. Clientes
2. Productos
3. Terminales
4. Bancos
5. Filial
6. Transportista
7. Autotanques

2. Administración

1. Conectarse

Acerca de. Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Zona intranet local

Inicio Menu principal - Mic... principal/arsp - Microsoft V... Sin título - Paint 12:30 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

**Cientes**

Hay 1 visitantes

1. Consultas

1. Clientes
2. Productos
3. Terminales
4. Bancos
5. Filial
6. Transportista
7. Autotanques

2. Administración

1. Conectarse

Código	Nombre	R.U.C	Dirección	Teléfonos	Propietario	Representante
01010001	ESPEJO	1704507696001	AV.ESPEJO S.N.CARCHI	[ 06-977460 ] - [ 06-974002 ]	CERVANTES GUIDO	CERVANTES GUIDO
01010003	LA MODERNA	1708722200001	PANAM. KM 1, VIA TULCAN QUITO	[ 06-290291 ] - [ 06-290291 ]	PALACIOS BLANCA	PALACIOS BLANCA
01010004	SAN ISIDRO	0400404659001	SAN ISIDRO-CARCHI	[ 06-974046 ] - [ 06-408505 ]	AUZ VINUEZA AGAPITO EFREN Y SR	AUZ VINUEZA AGAPITO EFREN Y SR
01010006	TAXIS COLON	0490002537001	PANAMERICANA KM 46 - MONTUFAR-	[ 06-290291 ] - [ 06-290317 ]	POZO DANIEL.	POZO DANIEL
01010008	URCUQUI	1702276401002	URCUQUI	[ 06-939228 ] - [ 06-447941 ]	QUILCA CALDERON LUIS ANIBAL Y	QUILCA CALDERON LUIS ANIBAL Y
01010009	JULIO ANDRADE	0400004545001	J. ANDRADE PANAM. NORTE	[ 06-973373 ] - [ 06-973753 ]	CASTRO QUELAL CARLOS HOMERO	CASTRO QUELAL CARLOS HOMERO
01010010	SERVICENTRO CARCHI	0400185500001	AV.VEINTIMILLA TULCAN	[ 06-980515 ] - [ 06-981424 ]	CORDOVA BERTHA JOSEFINA	CORDOVA BERTHA JOSEFINA
01010016	AUTO, PANAMERICANA	1000205544001	AMAZONAS Y PANAMERICANA ESQ.	[ 06-910224 ] - [ 06-910193 ]	RUIZ JAIME TARQUINO	RUIZ JAIME TARQUINO
01010018	SIND. CH. DE MONTUFAR	0490038531001	PANAM. SUR. KM 54, EL	[ 06-291427 ] - [ 06-291427 ]	POZO PERDOMO	POZO PERDOMO MARCO

Acerca de. Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Listo Zona intranet local

Inicio Menu principal - Mic... principal/arsp - Microsoft V... opcionesarsp - Paint 12:31 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ira Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp

---

Universidad de las Américas Av Colón y 6 de Diciembre  
Petrolés y Servicios Av.6 de Diciembre 2882 y Alpillana

**B i e n v e n i d o**

---

**Productos**

Hay 1 visitantes

Código	Descripción
0101	EXTRA
0103	SUPER
0104	DIESEL 2
0107	DIESEL 1
0121	DIESEL PREMIUN

1. Consultas  
 1. Clientes  
 2. **Productos**  
 3. Terminales  
 4. Bancos  
 5. Filial  
 6. Transportista  
 7. Autotanques  
 2. Administración  
 1. Conectarse

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Listo Zona intranet local

Inicio Menu principal - Micr... principal/arsp - Microsoft V... 3clientes - Paint 12:33 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ira Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp

---

Universidad de las Américas Av Colón y 6 de Diciembre  
Petrolés y Servicios Av.6 de Diciembre 2882 y Alpillana

**B i e n v e n i d o**

---

**Terminales**

Hay 1 visitantes

Código	Nombre	Ciudad	Teléfono	Propietario	Responsable
02	BEATERIO	QUITO	692-695 691-357	PETROCOMERCIALRAMIRO RUIZ	
04	AMBATO	AMBATO	03 849-173 09 703-119	PETROCOMERCIALSEGUNDO CACERES	
05	RIOBAMBA	RIOBAMBA	09 703-120 03 944-104	PETROCOMERCIALDANIEL VILLAGOMEZ	
06	CHAULLABAMBA	CUENCA	09 725-711 09 703-194	PETROCOMERCIALCRISTIAN PEREZ	
07	ESMERALDAS	ESMERALDAS	06 728-807 09 584-319	PETROCOMERCIALKELLOAG SALAS	
08	BARBASQUILLO	MANITA	05 629-399 05 611-559	PETROCOMERCIALMAURICIO MENDOZA	
09	LA LIBERTAD	LALIBERTAD	04 784-058	PETROCOMERCIALHEVIN LOPEZ	
13	PASCUALES	GUAYAQUIL	04 893-637 04 892-804	PETROCOMERCIALLINDA MENDOZA	
15	CHIGUILPE	SANTO DOMINGO	09 703-231	PETROCOMERCIALNORALMA PAREDES	
16	LA TOMA	LA TOMA	07 677-855	PETROCOMERCIALOTTO LOAIZA	
22	SHUSHUFINDI	NUEVA LOJA	677-428 EXT 693 QUITO	PETROCOMERCIALPETROCOMERCIAL	
42	ITULCACHI	QUITO	X	ITULCACH S.A.	MARCELO ALMAGRO

1. Consultas  
 1. Clientes  
 2. Productos  
 3. **Terminales**  
 4. Bancos  
 5. Filial  
 6. Transportista  
 7. Autotanques  
 2. Administración  
 1. Conectarse

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Listo Zona intranet local

Inicio Menu principal - Micr... principal/arsp - Microsoft V... 4productos - Paint 12:33 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ira Favoritos Ayuda

Altrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

**Bancos**

Hay 1 visitantes

1. Consultas

1. Clientes
2. Productos
3. Terminales
4. Bancos
5. Filial
6. Transportista
7. Autotanques

2. Administración

1. Conectarse

Código	Descripción
31	Filanbanco
32	Pacífico
35	Pichincha
36	Internacional
41	Tungurahua

Última actualización: 06/27/00

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Listo

Inicio Menu principal - Micr... principal/arsp - Microsoft V... Terminales - Paint Zona intranet local 12:33 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ira Favoritos Ayuda

Altrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

**Filiales**

Hay 1 visitantes

1. Consultas

1. Clientes
2. Productos
3. Terminales
4. Bancos
5. Filial
6. Transportista
7. Autotanques

2. Administración

1. Conectarse

Filial	Nombre
PCE	PETROL CENTRO
PSH	PETRO SHYRIS
PYS	PETROLEOS Y SERVICIOS

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Zona intranet local 12:34 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

Filiales

Hay 1 visitantes

Filial	Nombre
PCE	PETROL CENTRO
PSH	PETRO SHYRIS
PYS	PETROLEOS Y SERVICIOS

1. Consultas

- Cientes
- Productos
- Terminales
- Bancos
- Filial
- Transportista
- Autotanques

2. Administración

- Conectarse

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Zona intranet local

Inicio Menu principal - Mic... principal/arsp - Microsoft V... Ebancos - Paint 12:34 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección http://principal/arsp/home.asp Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

Autotanques

Hay 1 visitantes

Transportista	Placa	Marca	Capacidad
PEJA CASTRO MANUEL AGUSTIN	AAJ983	MERCEDES BENZ	9000
MOLINA FLORES GERMAN BOLIVAR	AAM087	MERCEDES BENZ	10500
YANEGAS LEON LAUTARO H.	AAI142	MERCEDES BENZ	4000
PEJA CASTRO MANUEL AGUSTIN	AAI192	WESTERN STAR	9000
DE LA TORRE LOPEZ MIGUEL E.	ABA805	SCANIA BAVIS	6000
AROCA ORTIZ GERMAN EDUARDO	ABC233	HINO	4001
ASTUDILLO JORGE	ABC313	NN	6000
ESCUDERO JARAMILLO JORGE LUIS	ABC360	HINO	4000
HUGO MUÑOZ MARIO RAFAEL	ABC539	M. BENZ	4000
MENDEZ ALTAMIRANO ANGEL OLMEDO	ABC852	MERCEDES BENZ	6000
VILLASIS CALLE NELLY CARMEN	ABD113	M. BENZ	6000
VILLASIS CALLE NELLY CARMEN	ABD114	M. BENZ	6000
MEDINA JACHO MANUEL CRISTOBAL	ABE112	SCANIA BAVIS	6000
HIDALGO FARFAN ARTURO BALTAZAR	ABE157	SCANIA	4000
SIND. CHOFERES DEL AZUAY	ABE200	M. BENZ	10000
SIND. CHOFERES DEL AZUAY	ABE201	M. BENZ	6000
FLORES ORTEGA MARIA ANGELA	ABE991	MERCEDES BENZ	6000
GONZALEZ FLORES WILSON ROBERTO	ABF340	MERCEDES BENZ	4000

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Listo Zona intranet local

Inicio Menu principal - Mic... principal/arsp - Microsoft V... Transportista - Paint 12:35 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

---

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

**Información confidencial Pys**

1. Consultas  
2. Administración

1. Conectarse

Si usted necesita ver información de la comercializadora, rápida y oportunamente logrará acceder, otorgándole seguridad y eficiencia en las consultas.

Si usted posee una cuenta en Petróleos y Servicios, ingrese su usuario y clave.

Usuario:   
Clave:

Aceptar Cancelar

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Zona intranet local

Inicio Menu principal - M... principal/arsp - Micros... 1adm\_clave - Paint http://principal/arsp/a... http://principal/arsp/a... http://principal/arsp/u... 12:38 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

---

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

@rsp Menú de Administración

1. Consultas  
2. Administración

1. Conectarse

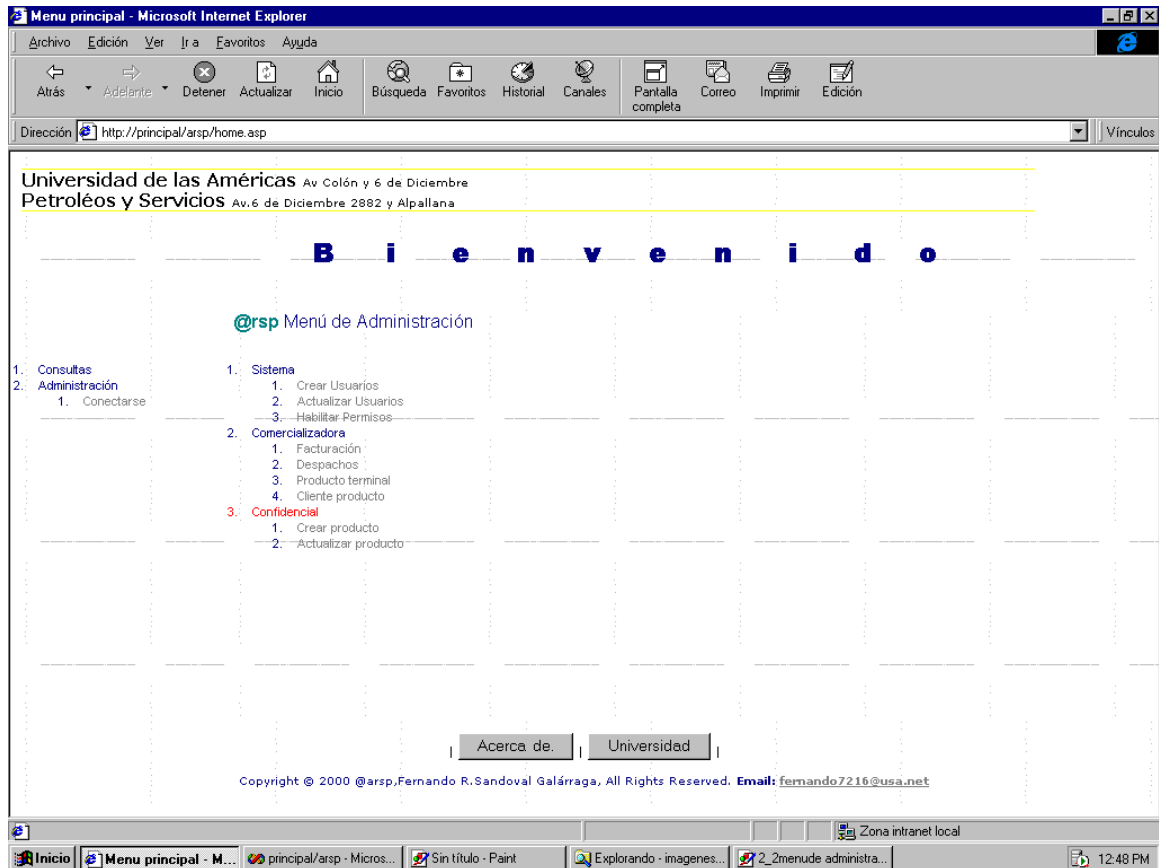
1. Sistema  
2. Comercializadora  
3. Confidencial

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Zona intranet local

Inicio Menu principal - M... principal/arsp - Micros... Sin título - Paint Explorando - imagenes... 1adm\_clave - Paint 12:47 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petrolés y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

@rsp Menú de Administración

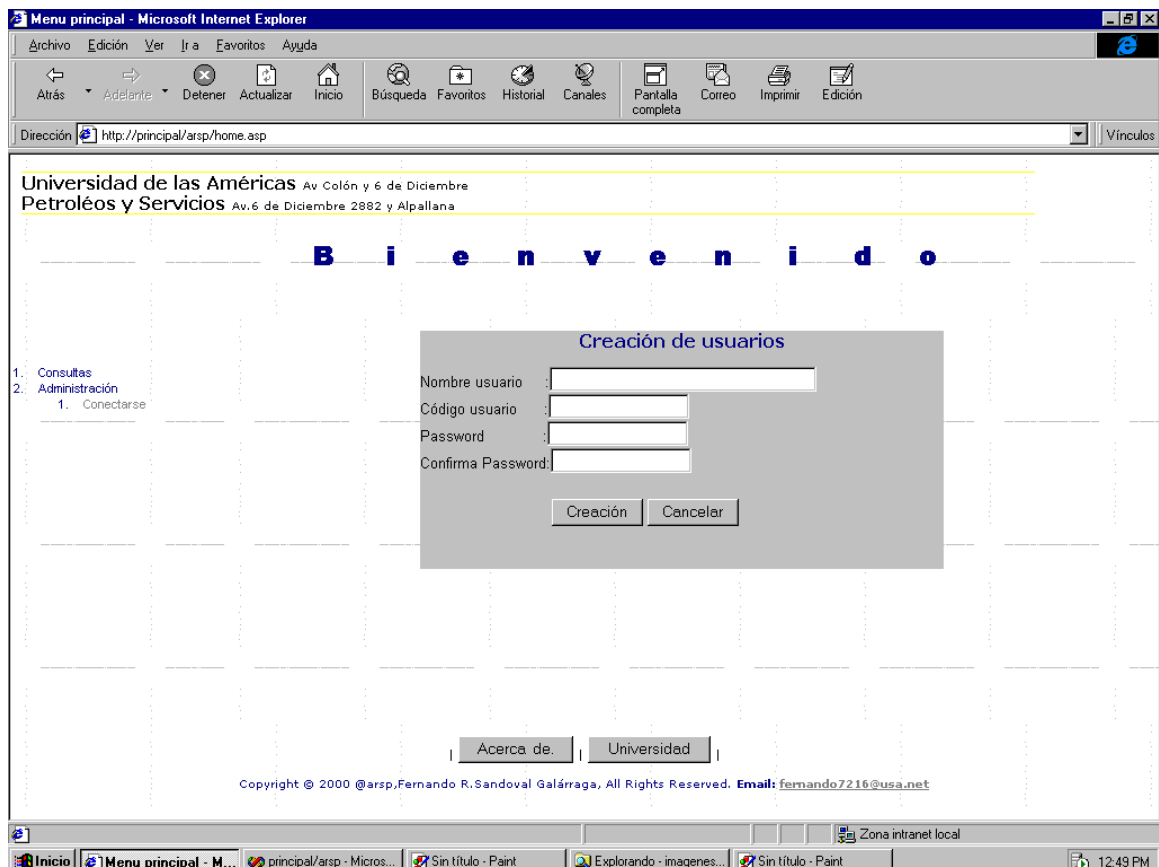
- 1. Consultas
- 2. Administración
  - 1. Conectarse
- 1. Sistema
  - 1. Crear Usuarios
  - 2. Actualizar Usuarios
  - 3. Habilitar Permisos
- 2. Comercializadora
  - 1. Facturación
  - 2. Despachos
  - 3. Producto terminal
  - 4. Cliente producto
- 3. Confidencial
  - 1. Crear producto
  - 2. Actualizar producto

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Zona intranet local

Inicio Menu principal - M... principal/arsp - Micros... Sin título - Paint Explorando - imagenes... 2\_2menude administra... 12:48 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petrolés y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

Creación de usuarios

Nombre usuario :

Código usuario :

Password :

Confirma Password:

Creación Cancelar

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Zona intranet local

Inicio Menu principal - M... principal/arsp - Micros... Sin título - Paint Explorando - imagenes... Sin título - Paint 12:49 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

---

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleo y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

**Actualización de usuarios**  
Por favor digite el código de usuario

1. Consultas  
2. Administración  
    1. Conectarse

Código usuario:

Actualizar Cancelar

Acerca de Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Lista Zona intranet local

Inicio Menu principal - M... principal/arsp - Micros... Sin título - Paint Explorando - imagenes... 2\_2creacionusuarios - ... 12:49 PM

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

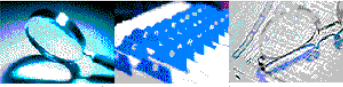
Dirección <http://principal/arsp/home.asp> Vínculos

---

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleo y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

1. Consultas  
2. Administración  
    1. Conectarse



**Facturación de Combustibles**

Fecha de inicio: año  mes  día

Fecha de finalización: año  mes  día

Código cliente :(01010001)

Consultar Cancelar

Acerca de Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Lista Zona intranet local

Inicio Menu principal - M... principal/arsp - Micros... Sin título - Paint Explorando - imagenes... 2\_2actualizausuarios - ... 12:50 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

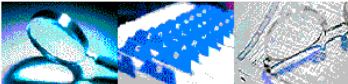
Dirección <http://principal/arsp/home.asp> Vínculos

---

Universidad de las Américas Av Colón y 6 de Diciembre  
Petróléos y Servicios Av.6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

1. Consultas  
2. Administración  
    1. Conectarse



**Despachos de Combustibles**

Fecha de inicio: año 1995 mes Junio día 27

Fecha de finalización: año 2000 mes Junio día 27

Código cliente :(01010001) 01010001

Consultar Cancelar

Acerca de Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

---

Universidad de las Américas Av Colón y 6 de Diciembre  
Petróléos y Servicios Av.6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

**PERÍODO:** Jun/27/1995 - Jun/27/2000      **CLIENTE:** 01010001  
Estación de Servicio ESPEJO

Cliente	Terminal	Factura	Fecha Factura	Comprobante	Fecha Comprobante	Producto	Cantidad	Autotanque
ESPEJO	BEATERIO	31930099	9/10/99	02659659	9/10/99	EXTRA	3000	CB6685

[Regresar a consultar](#)

Acerca de Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Listo Zona intranet local

Inicio Menu principal... principal/arsp - Mi... 2\_despachosco... Explorando - imag... 2\_3facturacion - P... Entorno de progra... 12:52 PM

Menu principal - Microsoft Internet Explorer

Dirección: http://principal/arsp/home.asp

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

Producto Terminal

Hay 1 visitantes

Producto	Terminal	Ciudad	Teléfono
EXTRA	BEATERIO	QUITO	692-695 691-357
EXTRA	AMBATO	AMBATO	03 849-173 09 703-119
EXTRA	RIOBAMBA	RIOBAMBA	09 703-120 03 944-104
EXTRA	CHAULLABAMBA	CUENCA	09 725-711 09 703-194
EXTRA	ESMERALDAS	ESMERALDAS	06 728-807 09 584-319
EXTRA	BARBASQUILLO	MANA	05 629-399 05 611-559
EXTRA	LA LIBERTAD	LALIBERTAD	04 784-058
EXTRA	PASCUALES	GUAYAQUIL	04 893-637 04 892-804
EXTRA	CHIGUILPE	SANTO DOMINGO	09 703-231
EXTRA	LA TOMA	LA TOMA	07 677-855
EXTRA	SHUSHUFINDI	NUOVA LOJA	677-428 EXT 693 QUITO
SUPER	BEATERIO	QUITO	692-695 691-357
SUPER	AMBATO	AMBATO	03 849-173 09 703-119
SUPER	CHAULLABAMBA	CUENCA	09 725-711 09 703-194
SUPER	ESMERALDAS	ESMERALDAS	06 728-807 09 584-319
SUPER	PASCUALES	GUAYAQUIL	04 893-637 04 892-804
SUPER	CHIGUILPE	SANTO DOMINGO	09 703-231
SUPER	LA TOMA	LA TOMA	07 677-855

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Inicio | Menu principal... | principal/arsp - M... | 2\_despachos... | Explorando - imag... | 2\_3facturacion - P... | Entorno de progra... | 12:53 PM

Menu principal - Microsoft Internet Explorer

Dirección: http://principal/arsp/home.asp

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

Producto Cliente

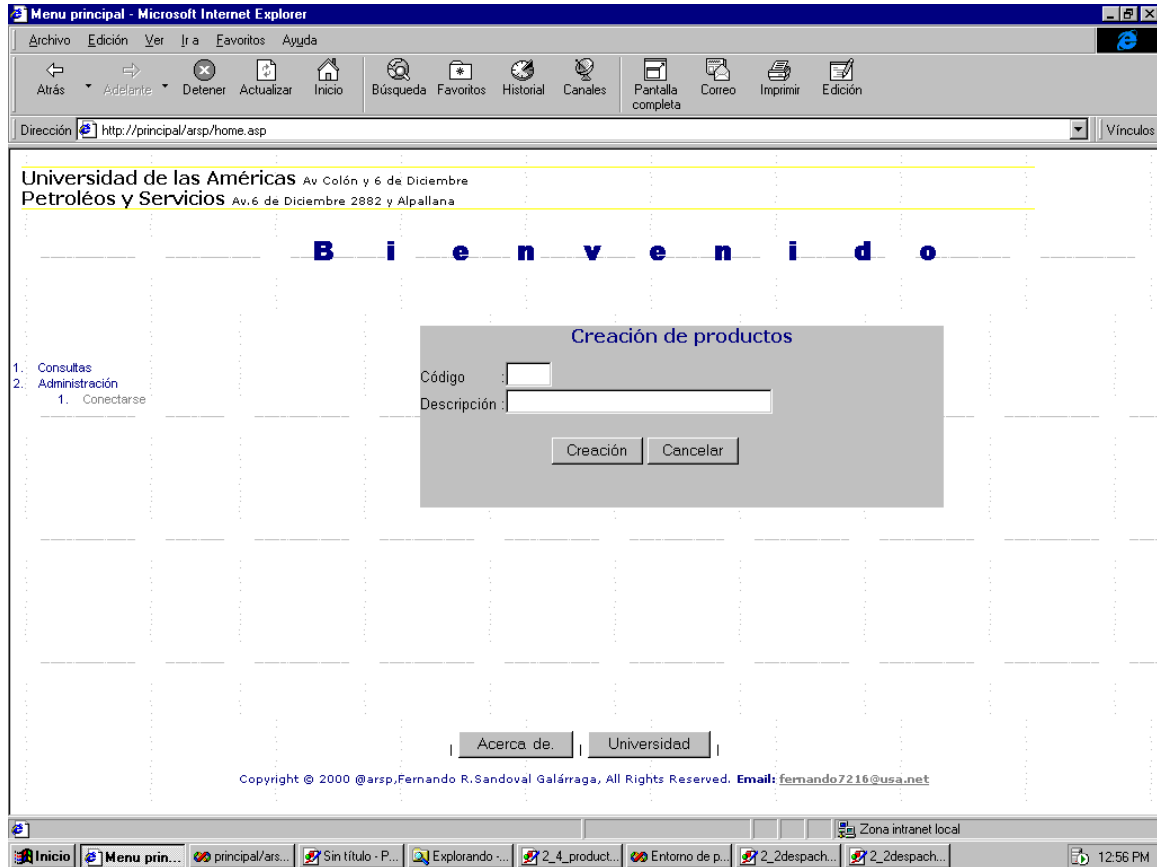
Hay 1 visitantes

Código	Estación de servicio	Dirección	Producto
01010001	ESPEJO	AV.ESPEJO S.N.CARCHI	EXTRA
01010001	ESPEJO	AV.ESPEJO S.N.CARCHI	DIESEL 2
01010004	SAN ISIDRO	SAN ISIDRO-CARCHI	EXTRA
01010004	SAN ISIDRO	SAN ISIDRO-CARCHI	DIESEL 2
01010006	TAXIS COLON	PANAMERICANA KM 46 -MONTUFAR-	EXTRA
01010006	TAXIS COLON	PANAMERICANA KM 46 -MONTUFAR-	DIESEL 2
01010008	URCUQUI	URCUQUI	EXTRA
01010008	URCUQUI	URCUQUI	DIESEL 2
01010009	JULIO ANDRADE	J.ANDRADE PANAM. NORTE	EXTRA
01010009	JULIO ANDRADE	J.ANDRADE PANAM. NORTE	DIESEL 2
01010010	SERVICENTRO CARCHI	AV.VEINTIMILLA TULCAN	EXTRA
01010010	SERVICENTRO CARCHI	AV.VEINTIMILLA TULCAN	SUPER
01010010	SERVICENTRO CARCHI	AV.VEINTIMILLA TULCAN	DIESEL 2
01010016	AUTO.PANAMERICANA	AMAZONAS Y PANAMERICANA ESQ.	EXTRA
01010016	AUTO.PANAMERICANA	AMAZONAS Y PANAMERICANA ESQ.	DIESEL 2
01010018	SIND.CH. DE MONTUFAR	PANAM.SUR KM 54, EL CAPULI	EXTRA
01010018	SIND.CH. DE MONTUFAR	PANAM.SUR KM 54, EL CAPULI	DIESEL 2
01010020	SUPER.EST. LOS OLIVOS	PANAMERICANA NORTE KM.1	EXTRA

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Inicio | Menu prin... | principal/ars... | 2\_4despach... | Explorando - ... | 2\_4\_product... | Entorno de p... | 2\_2despach... | 2\_2despach... | 12:55 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petroléos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

1. Consultas  
2. Administración  
1. Conectarse

**Creación de productos**

Código :   
Descripción :

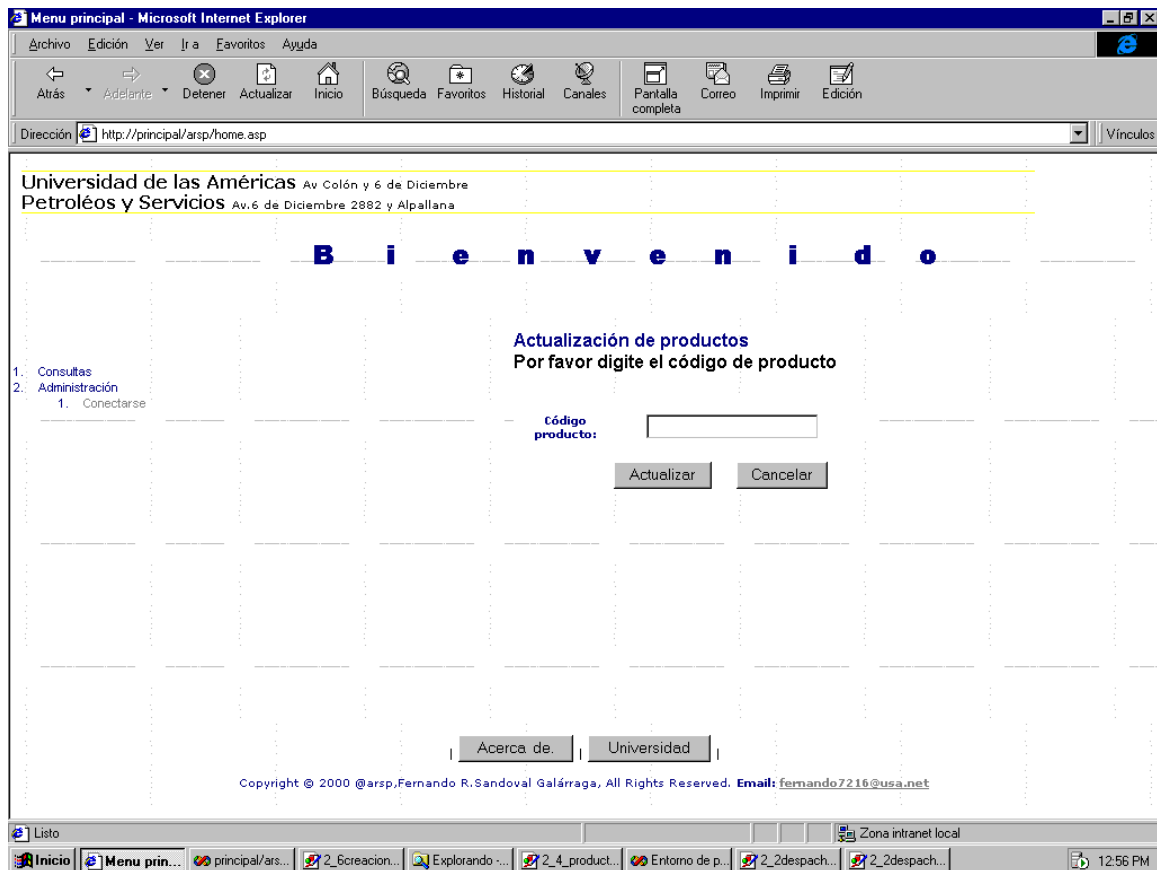
Creación Cancelar

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Zona intranet local

Inicio Menu prin... principal/ars... Sin título - P... Explorando ... 2\_4\_product... Entorno de p... 2\_2despach... 2\_2despach... 12:56 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petroléos y Servicios Av. 6 de Diciembre 2882 y Alpallana

**B i e n v e n i d o**

1. Consultas  
2. Administración  
1. Conectarse

**Actualización de productos**  
Por favor digite el código de producto

Código producto:

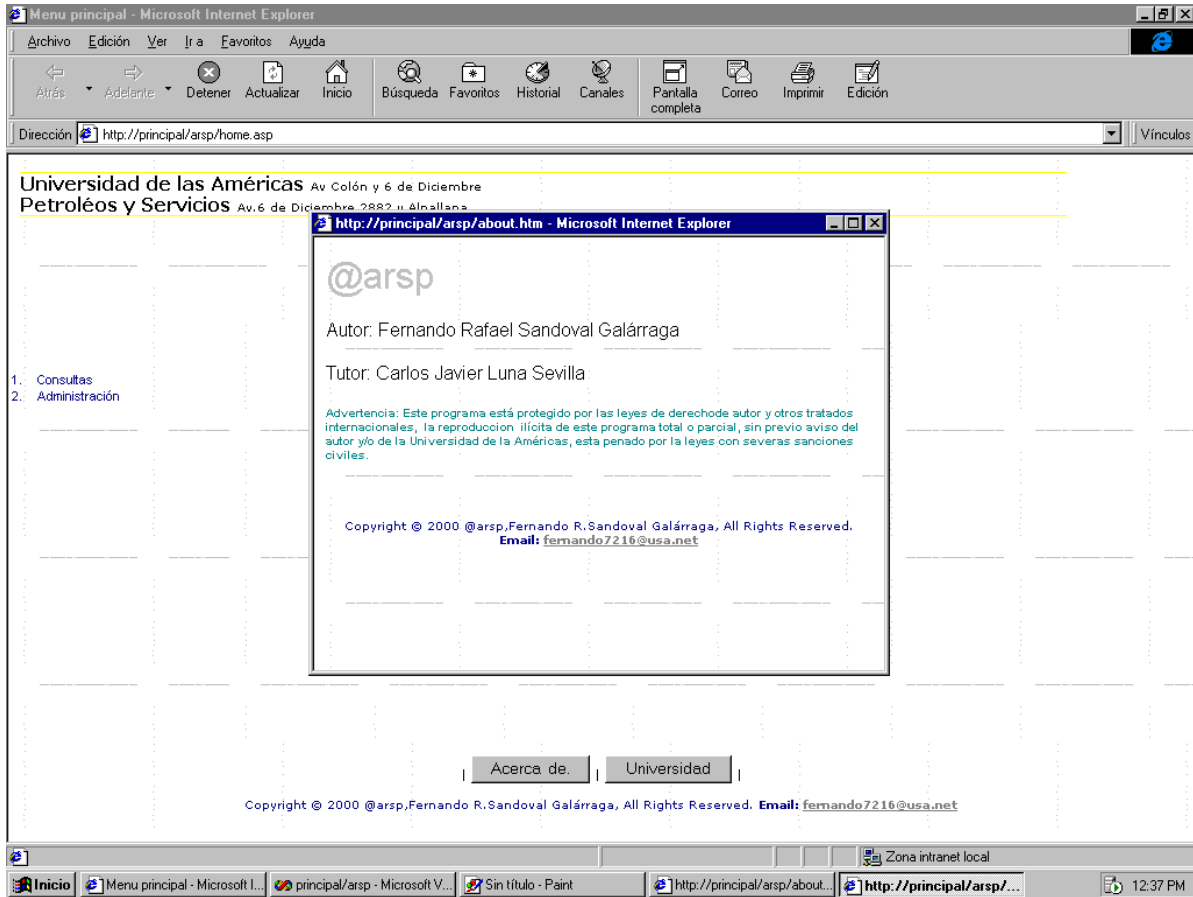
Actualizar Cancelar

Acerca de. Universidad

Copyright © 2000 @arsp,Fernando R.Sandoval Galárraga, All Rights Reserved. Email: fernando7216@usa.net

Zona intranet local

Listo Menu prin... principal/ars... 2\_6creacion... Explorando ... 2\_4\_product... Entorno de p... 2\_2despach... 2\_2despach... 12:56 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Canales Pantalla completa Correo Imprimir Edición

Dirección <http://principal/arsp/home.asp> Vínculos

Universidad de las Américas Av. Colón y 6 de Diciembre  
Petróleos y Servicios Av. 6 de Diciembre 2882 u. Elmallasa

**@arsp**

Autor: Fernando Rafael Sandoval Galárraga

Tutor: Carlos Javier Luna Sevilla

Advertencia: Este programa está protegido por las leyes de derechos de autor y otros tratados internacionales. La reproducción ilícita de este programa total o parcial, sin previo aviso del autor y/o de la Universidad de las Américas, está penada por la ley con severas sanciones civiles.

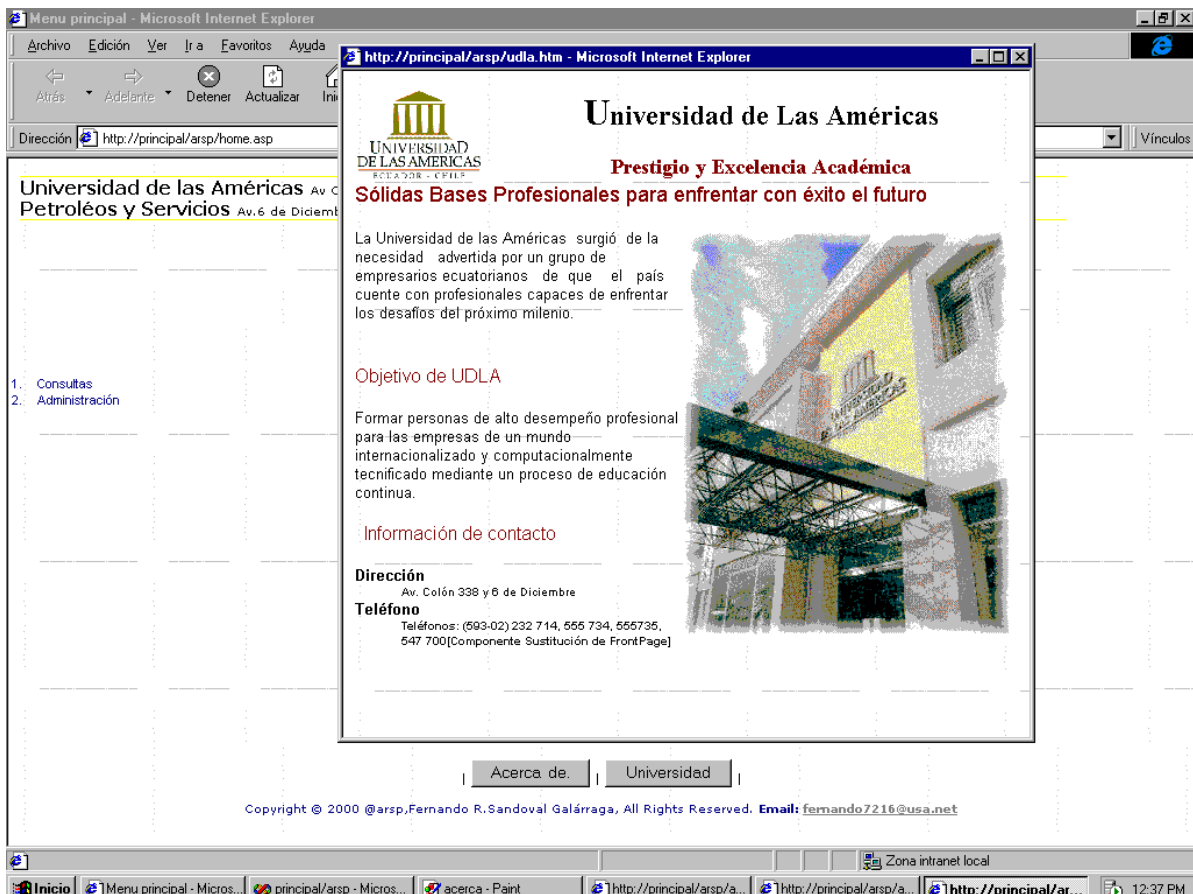
Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved.  
Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Zona intranet local

Inicio Menu principal - Microsoft I... principal/arsp - Microsoft V... Sin título - Paint http://principal/arsp/about... http://principal/arsp/... 12:37 PM



Menu principal - Microsoft Internet Explorer

Archivo Edición Ver Ir a Favoritos Ayuda

Atrás Adelante Detener Actualizar Ini Dirección <http://principal/arsp/home.asp> Vínculos

Universidad de las Américas Av. C  
Petróleos y Servicios Av. 6 de Diciem

**Universidad de las Américas**  
UNIVERSIDAD DE LAS AMÉRICAS  
ECUADOR - CHILE

**Prestigio y Excelencia Académica**  
**Sólidas Bases Profesionales para enfrentar con éxito el futuro**

La Universidad de las Américas surgió de la necesidad advertida por un grupo de empresarios ecuatorianos de que el país cuenta con profesionales capaces de enfrentar los desafíos del próximo milenio.

**Objetivo de UDLA**

Formar personas de alto desempeño profesional para las empresas de un mundo internacionalizado y computacionalmente tecnificado mediante un proceso de educación continua.

**Información de contacto**

**Dirección**  
Av. Colón 338 y 6 de Diciembre

**Teléfono**  
Teléfonos: (593-02) 232 714, 555 734, 555735, 547 700[Componente Sustitución de FrontPage]

Acerca de Universidad

Copyright © 2000 @arsp, Fernando R. Sandoval Galárraga, All Rights Reserved. Email: [fernando7216@usa.net](mailto:fernando7216@usa.net)

Zona intranet local

Inicio Menu principal - Micros... principal/arsp - Micros... acerca - Paint http://principal/arsp/a... http://principal/arsp/a... http://principal/ar... 12:37 PM

## 6. Conclusiones

En mi opinión, hay dos razones claves en nuestro retraso en la adopción de las tecnologías de la información y particularmente de Internet: la falta de una cultura de la información y del uso de la informática, por un lado, y la ausencia de un tejido empresarial volcado hacia el negocio de las nuevas tecnologías digitales, por otro.

Vayamos al primer punto: la falta de educación tecnológica, los empresarios ecuatorianos piensan que invertir en informática significa acumular ordenadores. Yo diría que eso no sólo hay que aplicárselo a los empresarios sino a las principales estructuras dominantes en casi todos los ámbitos de nuestro país, y entre ellas a los responsables educativos.

Quisiera hacer especial énfasis en el tipo de educación porque es clave para que los estudiantes se adapten a un mercado en el que el valor principal no es la mano de obra ni el capital, sino el conocimiento. En la medida en que la Universidad introduzca Internet, y la dinámica de trabajar en red, en sus hábitos, no sólo se conseguirá tener profesionales mejor dotados, sino, exportar conocimiento.

También voy a indicar que, algunos directivos y ejecutivos ven en la Internet, como un arma para apoyar de manera eficiente a sus empresas. Pero en ocasiones olvidan que a final de cuenta los administradores de dicha tecnología son los que la harán exitosa o no dentro de una empresa. La tecnología por sí sola no nos producirá logros o descalabros, sino el administrador de la misma, es el que nos dará los resultados. Una buena inversión en esta campo proporcionará a la empresa un dividendo en un futuro próximo.

Si observamos introspectivamente y haciendo uso de las Intranets, dicha tecnología proporcionará el beneficio para las que Pymes mejoren su comunicación interna; dando así un impacto a lo que llamamos, la cultura corporativa de una forma muy positiva. Además de esto, ayudará a la correcta utilización de herramientas que busquen proporcionar una eficiencia operacional y facilitará que las herramientas de trabajo y las personas que las utilizan sean capaces de tomar decisiones debido al acceso compartido de información sin que medien fronteras geográficas.

Cabe destacar que, la Intranet es una excelente herramienta para promover la visión, misión y los valores corporativos y así lograr la sinergia necesaria en este mundo de alta competitividad e indiscutible camino hacia la globalización total.

Finalmente se debe mencionar como el World Wide Web está modificando el modo en el que los usuarios acceden a la información convirtiéndose de manera creciente en la vía preferida para la transmisión y acceso a la información, información que a veces será sensible desde el punto de vista comercial. Por ello se plantea la necesidad de dotar a WWW de los mecanismos para manejar datos de manera similar a como lo haríamos, por ejemplo, en un entorno de red local.

En este ámbito, las sedes Web se están convirtiendo en auténticas aplicaciones. La funcionalidad de este sistema requiere que las sedes Web se diseñen adecuadamente, utilizando un cierto modelo de aplicación y nuevas técnicas de desarrollo. Para este trabajo tecnológico, se introdujo el escenario en el que la aplicación Web va a residir en un servidor

Microsoft Internet Information Server sobre Windows NT Server 4.0, los mecanismos de programación van a girar alrededor de las páginas activas de servidor (Active Server Pages) y en el que la herramienta de desarrollo va a ser Microsoft Visual Interdev. Se eligió a Microsoft por su alto grado de uso, así como su compatibilidad y la adquisición de la mayoría de empresas con estos sistemas.

Retomando el tema, uno de los aspectos que se refleja más directamente en la funcionalidad de la sede Web, es el aspecto de las páginas que la integran. De nada servirá diseñar una sede Web extraordinariamente potente si sus contenidos no se presentan de un modo lo suficientemente atractivo como para que el usuario que visite la sede no encuentre de manera sencilla y amable la información que solicita.

Ahora bien, en lo que respecta a la infraestructura (hardware y seguridades) necesaria para que todo la aplicación ARSP pueda ser accesada en forma segura, podemos anotar los diferentes equipos de distintos fabricantes que dan soluciones SSL (equipos SSL que hacen el trabajo de encriptar y desencriptar la información como los NETStructure de Intel), soluciones firewall-VPN (Shiva LanRover VPN Gateway), firewall-routers (Cisco, Intel, 3Com, etc.), tunneling, etc.; pero el motivo de este trabajo de investigación, como se lo introdujo tanto en el resumen ejecutivo como en la introducción, se centra en elaborar la aplicación ARSP, que es en sí, lo fundamental del acceso remoto para PYMES, así como el dar los conceptos necesarios para comprender la tecnología de Internet, de manera que posteriores trabajos de investigación, puedan completar de una manera más estricta la aplicación y su uso.

De esta manera, se ha entregado al aparato productivo ecuatoriano, una solución de Tecnologías de la Información, que genera una herramienta competitiva para introducir a las PYMES ecuatorianas en el ámbito tecnológico actual y poder generar mayores economías de escala y más riqueza para un país, en dónde una diferencia de tecnología, podría ser la clave para el mantenimiento o el reapuntamiento de las empresas y de las personas que en él habitan.

## **Bibliografía**

Inside Microsoft Visual InterDev. Ken Miller y otros. Microsoft Press

Windows NT 4 Web Development Sanjana Hettihewa. SAMS Publishing

Build your own Web Site. Louis Kahn y Laura Logan. Microsoft Press

Running Microsoft Internet Information Server. Leon Braglinski, Mathew Powell.  
Microsoft Press

EOI-EPN, "Material de apoyo del Master Executive en Gestión de las Comunicaciones  
y Tecnologías de la información", España-Ecuador, 1999.

Hanh, Harley 1994. "**Internet, manual de referencia**", Madrid, McGrawHill,  
Interamericana

Lemay, Laura. 1995. "**Aprendiendo HTML para Web en una semana**", México D.F,  
Prentice Hall Hispanoamericana.

## **Webliografía**

Otras fuentes de información multimedia o en el WWW:

<http://www.matisse.net/files/glossary.html>

<http://www.hispan.com/eltaller/vinterdev>

<http://www.microsoft.com/vinterdev/>

<http://www.action-links.com/windows/miscfree.htm>

<http://www.asdj.com/>

<http://www.aspdeveloper.net/>

<http://www.microsoft.com/iis>

[http://www.maestrosdelweb.com/tutoriales/asp/usuarios\\_activos.asp](http://www.maestrosdelweb.com/tutoriales/asp/usuarios_activos.asp)

<http://www.globalnet.com.mx/intranet/>

<http://www.uan.mx/~juan/tesis/hp.html>

<http://www.ub.es/personal/impacto.htm>

[http://metro.inter.edu/progacad/educ/facultad/elopateg/net\\_educ.htm](http://metro.inter.edu/progacad/educ/facultad/elopateg/net_educ.htm)

<http://www.uco.es/webuco/si/ccc/glosario/glosario.html>

<http://www.microsoft.com/latam/technet/hoy/intranet/art09/art091.asp>

<http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html>

<http://www.frlp.utn.edu.ar/jornada97/sistemas/lan/sld009.htm>

<http://terra.es/informatica/que-es/extranet.cfm>

<http://www.diarioti.com/noticias/not25081997c.htm>

<http://www4.uji.es/~al019803/Tcpip.htm>

## Anexos

### Glosario

#### A

##### Administración remota

Administración de una computadora por parte de un administrador situado en otra computadora y conectado a la primera a través de la red.

##### Administrador

Una persona responsable de la configuración y administración de la red. El administrador generalmente configura la red, asigna contraseñas y permisos, y ayuda a los usuarios. Para usar las Herramientas administrativas, como por ejemplo el Administrador de servidores, un administrador debe tener una cuenta de usuario con privilegio de Administrador.

##### Administrador de servidores

En Windows NT Server, aplicación utilizada para ver y administrar los dominios, grupos de trabajo y computadoras.

##### Administrador de usuarios

Herramienta de Windows NT Workstation que permite administrar la seguridad de una computadora. Administra el plan de seguridad, los grupos y las cuentas de usuario.

##### Administrador de usuarios para dominios

Herramienta de Windows NT Server que permite administrar la seguridad de un dominio o de una computadora individual. Administra el plan de seguridad, los grupos y las cuentas de usuario.

##### Agente

En SNMP, la información de los agentes está formada por comentarios acerca del usuario, la ubicación física de la computadora (ordenador) y los tipos de servicio, y se utiliza para generar informes de la configuración de la computadora.

##### Alertas administrativas

Las alertas administrativas están relacionadas con el uso de los servidores y los recursos, y advierten acerca de posibles problemas en áreas tales como la seguridad y el acceso, las sesiones de usuario, el cierre del servidor debido al corte de suministro eléctrico (cuando se dispone de un SAI), la duplicación de directorios y la impresión. Cuando una computadora genera una alerta administrativa, se envía un mensaje a una lista predefinida de usuarios y computadoras. Vea también servicio de Alerta.

##### AppleShare

Software para el cliente que se incluye con todas las computadoras Macintosh y con el software para el servidor de Apple Computer. Con Servicios para Macintosh, las computadoras Macintosh usan el software de cliente original de AppleShare para conectarse a las computadoras que ejecutan Windows NT Server que tienen Servicios para Macintosh.



## AppleTalk

Arquitectura y protocolos de redes de Apple Computer. Una red que cuenta con clientes Macintosh y una computadora que ejecuta Windows NT Server con Servicios para Macintosh funciona como una red AppleTalk.

## Archivo de comandos de inicio de sesión

Generalmente es un archivo por lotes que se ejecuta automáticamente cada vez que un usuario inicia una sesión. Puede utilizarse para configurar el entorno de trabajo de un usuario cada vez que inicie una sesión y permite al administrador modificar el entorno de los usuarios sin necesidad de administrar todos los aspectos del mismo. El archivo de comandos de inicio de sesión puede asignarse a una cuenta de usuario o a varias.

## Archivo HOSTS

Un archivo de texto local con el mismo formato que el archivo /etc/hosts de UNIX 4.3 Berkeley Software Distribution (BSD). Este archivo asigna nombres de host a direcciones IP. En Windows NT, este archivo se almacena en el directorio \raíz\SYSTEM32\DRIVERS\ETC.

## Archivo de información de programa (PIF)

Archivo que proporciona información sobre el modo en que Windows NT deberá ejecutar una aplicación no basada en Windows NT. Los archivos PIF contienen datos tales como el nombre del archivo, el directorio de inicio y las opciones de multitarea para aquellas aplicaciones que se ejecuten en el modo extendido del 386.

## Archivo de intercambio

Archivo especial del disco duro. Cuando se utiliza la memoria virtual en Windows NT, parte del código de los programas y otra información adicional se mantiene en la memoria RAM, mientras que el resto se transfiere temporalmente a la memoria virtual. Cuando dicha información se necesita nuevamente, Windows NT vuelve a extraerla y la transfiere a la RAM y, si es necesario, realiza el intercambio de otro bloque de información a la memoria virtual. También se denomina archivo de paginación.

## Archivo LMHOSTS

Un archivo de texto local en el que se asignan direcciones IP a los nombres NetBIOS de las computadoras (ordenadores) de red Windows fuera de la subred local. En Windows NT, este archivo se almacena en el directorio \raíz\SYSTEM32\DRIVERS\ETC.

archivo de paginación

## Archivo PostScript encapsulado (EPS)

Archivo que se imprime con la máxima resolución que admita la impresora. Un archivo EPS puede imprimirse más rápido que otras representaciones gráficas. Algunas aplicaciones gráficas basadas en Windows NT y no basadas en Windows NT pueden importar archivos EPS.

## Autenticación:

Validación de la información de inicio de sesión de un usuario. Cuando un usuario inicia una sesión utilizando una cuenta en una computadora con Windows NT, dicha computadora realiza la autenticación.

**Acceso conmutado:**

una conexión de red que puede ser creada y desechada rápidamente. La forma más sencilla son los enlaces de marcado por línea telefónica. SLIP o el PPP son protocolos generalmente usados para este tipo de conexiones.

**Address:**

dirección de un usuario del sistema, como en el caso del e-mail (requerida para que el mensaje enviado pueda dirigirse a una determinada persona) o la dirección de un sitio en la red.

**AFS:**

grupo de protocolos, similar al NFS, que permite el uso de archivos localizados en otra máquina de la red como si se encontrasen localizados en su propia máquina. De tal manera, en vez de utilizar el FTP para transferir un archivo a su computadora, se puede leer, escribir o editar en él desde la máquina remota. Se usan los mismos comandos que se usarían localmente.

**Analogous loopback:**

moderno test que evalúa el origen del módem o la frecuencia de la respuesta.

**Analogous signal:**

señal analógica. Ondas continuas pero variadas, como en el caso de los tonos de voz transmitidos por la línea telefónica.

**ANSI:**

American National Standards Institute o Instituto Americano de Estándares Nacionales, responsable de aprobar los estándares de diversas áreas.

Ancho de banda: diferencia expresada en hertz entre la más alta y la más baja frecuencia de un canal de transmisión. Usualmente se utiliza para describir la cantidad de tráfico a través de un newsgroup o conferencia.

**Anonymous FTP:**

FTP Anónimo. Permite al usuario recobrar archivos desde otro sitio en Internet sin tener que establecer una identificación de usuario y password en el sistema.

Aplicación: una pieza de software que ejecuta una determinada función. Por ejemplo, una aplicación de correo electrónico.

**Arj:**

para crear una copia comprimida de un archivo o grupo de archivos, usando el programa de comprensión ARJ. Actualmente es poco común su uso pero se pueden encontrar archivos en este formato que se envían por Internet.

**Archie:**

sistema para encontrar en Internet archivos de dominio público para FTP.

Archive: archivo o grupo de archivos que han sido comprimidos para formar otro archivo más pequeño. Dependiendo del programa utilizado para comprimir, el resultado será un archivo con extensión.lha.zip.arc.

**ARPA:**

Advanced Research Projects Agency o Agencia de Proyectos de Investigación de Avanzada. Es una sección del Departamento de Defensa de los Estados Unidos.

**ARPAnet:**

Red experimental de los años '70 en la cual se basó Internet.

**ARQ:**

Automatic Repeat Request o Demanda Automática de Repetición. Un protocolo de control contra errores utilizado por los módems Miracom.

**ASCH:**

American Standard Code for Information Interchange o Código Americano Estándar para Intercambio de Información. Un código que casi todas las computadoras soportan para producir caracteres especiales o letras y números.

**Asynchronous:**

forma de transmisión de datos que permite enviar información a intervalos irregulares.

**B**

**Barra de estado**

Línea de información relacionada con la aplicación contenida en la ventana. Generalmente suele aparecer en la parte inferior de la ventana. No todas las ventanas incluyen una barra de estado.

**Barra de herramientas**

Grupo de botones de método abreviado que proporciona acceso rápido a los comandos. Generalmente está situada inmediatamente debajo de la barra de menús. No todas las ventanas disponen de una barra de herramientas.

**Barra de unidades:**

Permite cambiar de unidad seleccionando uno de los iconos de unidad.

**Base de datos de SAM**

Base de datos que incluye información de seguridad (como los nombres de cuenta de usuario y las contraseñas), así como la configuración del plan de seguridad. En Windows NT Workstation, la base de datos de SAM se administra mediante el Administrador de usuarios. En los dominios de Windows NT Server, la administración de la base de datos la realiza el Administrador de usuarios para dominios.

**Base de información de gestión (MIB)**

Un conjunto de objetos que representan varios tipos de información acerca de un dispositivo, utilizado por SNMP para administrar los dispositivos. Debido a que se utilizan distintos servicios de administración de red para diferentes tipos de dispositivos o protocolos, cada servicio tiene su propio conjunto de objetos. El juego completo de objetos que utiliza un servicio o protocolo se conoce como su MIB.

**Bifurcación**

Segmento del árbol de directorios que representa un directorio y todos los subdirectorios que éste contiene.

### Bit de modificación

Los programas de copia de seguridad emplean el bit de modificación para marcar los archivos en el momento de realizar la copia de seguridad de los mismos, tanto con el método normal como con en el progresivo.

### Búfer:

Área para el almacenamiento temporal de información.

### Búfer de pantalla

Área de memoria reservada para mostrar información en el símbolo del sistema.

### Bang Path:

sistema antiguo de dirección electrónica UUCP.

### Baseband:

técnica de señalización digital usada en las redes de área local de Ethernet.

### Baud:

al transmitir datos, el baud, como unidad de medida, representa el número de veces que cambia el "estado" del medio de transmisión en un segundo. Cada cambio debe portar más de un bit de información.

### BBS:

Bulletin Board System.

### Bit:

unidad de medida que representa un carácter de dato. El bit es la más pequeña unidad de almacenamiento de una computadora.

### BITNET:

red académica de computadoras de base IBM. BITNET es también un acrónimo inglés para "Because It's Time, Network", que significa: "Porque ya es tiempo, a las redes!".

### Bits por segundo (bps):

velocidad a la que se transmiten los bits en un medio de una comunicación.

### Bounce: Rebote.

Cuando un mensaje e-mail retorna debido a una falla en la distribución.

### Bridge:

dispositivo que conecta dos o más redes físicas y sirve para transmitir paquetes entre ellas.

### BTW:

abreviatura utilizada en el correo electrónico para significar "By The Way" que significa "Por cierto".

### C

cabecera

Los datos introducidos al principio de un paquete que contienen información de control. En un paquete TCP, la cabecera contiene el identificador de puerto, la suma de comprobación, el número de secuencia y otros datos.

#### Captura

En SNMP, un bloque discreto de datos que indica que ha fallado la autenticación de la petición. El servicio SNMP puede enviar una captura cuando recibe una petición de información que no contiene el nombre de comunidad correcto y que no coincide con un nombre de host aceptado para el servicio. Los destinos de las capturas son los nombres o las direcciones IP de hosts para los cuales el servicio SNMP debe enviar capturas con nombres de comunidad.

#### Canalización con nombre

Mecanismo de comunicación entre procesos que permite a un proceso comunicarse con otro proceso local o remoto.

#### Cargador de inicialización

Define la información necesaria para iniciar el sistema, tal como la ubicación de los archivos del sistema operativo. Windows NT crea automáticamente la configuración correcta y comprueba esta información cada vez que se inicia el sistema.

#### Chooser Pack:

Una colección de archivos, algunos de los cuales contienen información PostScript. Cuando una computadora Macintosh envía una tarea de impresión a una impresora PostScript, la impresora utiliza un archivo Chooser Pack para interpretar los comandos PostScript de la tarea de impresión.

#### Clases de dirección

Agrupaciones predefinidas de direcciones Internet, donde cada clase define redes de determinado tamaño. El rango de números que se puede asignar para el primer byte de la dirección IP se basa en la clase de dirección. Las redes de clase A (valores 1–126) son las mayores, con más de 16 millones de hosts por red. Las redes de clase B (128–191) pueden tener un máximo de 65.534 hosts por red y las de clase C (192–223) pueden tener un máximo de 254 hosts por red.

#### Cliente

Computadora que accede a recursos compartidos de red proporcionados por otra computadora (denominada servidor).

#### Cola de espera

Software que acepta los documentos enviados por un usuario para su impresión y después almacena dichos documentos y los envía, uno por uno, a la(s) impresora(s) disponible(s).

#### Compactación

El proceso de limpieza de la base de datos de WINS.

#### Compartir

Poner los recursos, como directorios, impresoras y páginas del Portafolio, a disposición del resto de los miembros de la red.

#### Compartir impresión:

La capacidad de una computadora con Windows NT Workstation o Windows NT Server para compartir una impresora conectada localmente para su uso en la red. Esto se realiza mediante el Administrador de impresión o utilizando el comando net share.

#### Computadoras de Importación

En la duplicación de directorios, se denomina así a los servidores o estaciones de trabajo que reciben las copias del conjunto maestro de directorios de un servidor de Exportación.

#### Conexión

Un enlace de software entre un cliente y un recurso compartido, como por ejemplo, una impresora o un directorio compartido en un servidor.

#### Conector lógico

Una canalización bidireccional para los datos de entrada y salida entre computadoras conectadas en red. La API de Windows Sockets es una API de conectividad en red utilizada por los programadores en la creación de aplicaciones de conector lógico basadas en TCP/IP.

#### Configurar:

Cambiar los valores iniciales establecidos en un cliente, un volumen accesible a Macintosh, un servidor o una red.

#### Contraseña:

Cadena de caracteres exclusiva que debe introducirse antes de que se autorice el inicio de una sesión o el acceso a un sistema. Se trata de una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los sistemas y recursos de la computadora.

#### Contraseñas codificadas

Contraseñas desordenadas para que sean menos vulnerables a los "rastreadores de redes", que pueden usarse para disolver la seguridad de una red.

#### Contraseñas de texto simple

Contraseñas que no están codificadas y por lo tanto son más susceptibles a "rastreadores de redes".

#### Contraseña de usuario

La contraseña almacenada en la cuenta de cada usuario. Generalmente cada usuario tiene una contraseña diferente y debe escribir dicha contraseña al iniciar una sesión o acceder al servidor.

#### Controlador de dispositivo

Programa que permite a un determinado elemento de hardware (dispositivo) comunicarse con Windows NT.

#### Controlador de dispositivo de red

Software que coordina la comunicación entre la tarjeta adaptadora de red y el hardware de la computadora, así como con otro software, controlando el funcionamiento físico de las tarjetas adaptadoras de red.

#### Controlador de dominio

En los dominios de Windows NT Server, el controlador principal de dominio o el controlador de reserva que realiza la autenticación de inicio de sesión en el dominio y mantiene el plan de seguridad y la base de datos maestra de un dominio.

#### Controlador de protocolo

Un controlador de dispositivo de red que ejecuta un protocolo, comunicándose entre Windows NT Server y uno o más controladores de tarjetas adaptadoras de redes. Con Servicios para Macintosh, la pila del protocolo de AppleTalk se ejecuta como un controlador de protocolo de NDIS y está enlazada a uno o más controladores de tarjetas adaptadoras de redes.

#### Controlador de reserva

En los dominios de Windows NT Server, computadora que recibe una copia del plan de seguridad y la base de datos maestra del dominio, y que realiza la autenticación de los inicios de sesión en la red.

#### Controlador de tarjetas adaptadoras de red

Un controlador de dispositivo para red que funciona directamente con la tarjeta adaptadora de red, actuando como un intermediario entre la tarjeta y el controlador del protocolo. Con Servicios para Macintosh, la pila del protocolo AppleTalk del servidor se ejecuta como un controlador de protocolo y está enlazado a uno o más controladores de tarjetas adaptadoras de redes.

#### Controlador principal de dominio

En los dominios de Windows NT Server, la computadora que realiza la autenticación de los inicios de sesión en el dominio y mantiene el plan de seguridad y la base de datos maestra de un dominio.

#### Creador de archivos

Una secuencia de cuatro caracteres que indica a Finder de Macintosh el nombre de la aplicación que creó un archivo. Con Servicios para Macintosh, puede crear asociaciones según el tipo de extensión que proyectan extensiones de los nombres de archivos de computadoras PC a los creadores de archivos y tipos de archivos de Macintosh. Estas asociaciones permiten que los usuarios de computadoras Macintosh y PC compartan los mismos archivos de datos en el servidor.

#### Cuadro de lista

En un cuadro de diálogo, se trata de un tipo de cuadro en el que se muestra una lista de opciones disponibles (por ejemplo, una lista de todos los archivos de un directorio). Si en el cuadro de lista no caben todas las opciones disponibles, aparecerá también una barra de desplazamiento.

#### Cuadro del menú Control

Icono situado a la izquierda de la barra de título. Este icono abre el menú Control de una ventana.

#### Cuenta de usuario

Consta de toda la información que define a un usuario para Windows NT. Ello incluye aspectos tales como el nombre del usuario y la contraseña necesaria para iniciar una sesión, los grupos a los que pertenece la cuenta de usuario, y los derechos y permisos de que dispone el usuario para la utilización del sistema y para el acceso a los recursos del mismo.

#### Cuenta de usuario desactivada

Cuenta de usuario que no permite el inicio de una sesión. Las cuentas que se encuentren en esta situación aparecerán en la ventana del Administrador de usuarios y podrán reactivarse siempre que se desee.

#### Cuenta global

En Windows NT Server, es la cuenta de usuario normal en el dominio base de un usuario. La mayoría de las cuentas de usuario son cuentas globales. En caso de que existan varios dominios en la red, se obtienen mejores resultados si cada usuario dispone de una sola cuenta en un solo dominio y el acceso de cada usuario al resto de los dominios se realiza estableciendo relaciones de confianza entre dominios.  
cuenta local

#### Carrier:

señal de frecuencia continua capaz de ser modulada con otra señal de información.

#### Charla IRC:

servicio donde son posible grandes conversaciones por Internet.

#### CIM:

CompuServe Information Manager o Administración de Información de CompuServe. Es el lector off-line autorizado oficialmente y navegador del sistema de CompuServe.

#### CIX:

Commercial Internet Exchange o Intercambio Comercial en Internet. Acuerdo entre proveedores de la red para llevar la contabilidad del tráfico comercial.

Cliente: aplicación de software que permite a un usuario obtener un servidor localizado en la red.

#### CNT:

Comisión Nacional de telecomunicaciones. Organismo oficial que en la Argentina está encargado de regular el mercado de las telecomunicaciones.

#### Compress:

programa individual que se envía a un grupo de interés de Usenet.

#### Comunicado:

artículo individual que se envía a un grupo de interés de Usenet.

#### Conexión o tiempo de conexión:



palabra utilizada para indicar el tiempo o espacio de tiempo que el usuario se encuentra conectado on-line a Internet.

**CREN:**

fusón de BITNET Y CSNET dio por resultado la CREN o Corporation for Research and Educational Networking (Corporación para la Investigación y Educación en Redes).

**CTS:**

Clear To Send o Listo para Enviar. Una señal RS-232c que significa básicamente que todo está preparado para la transmisión de datos.

**D**

**Daemon**

Un programa de conectividad en red que se ejecuta en segundo plano.

**Datagrama:**

Un paquete de datos y otra información de entrega que se encamina a través de una red de conmutación de paquetes o que se transmite por una red de área local.

**Derecho**

Autoriza a un usuario a realizar ciertas acciones en el sistema. Los derechos son válidos en todo el sistema y son diferentes de los permisos, que son válidos para objetos específicos.

**Desplazar**

Moverse por un texto o un gráfico (hacia arriba, abajo, izquierda o derecha) para ver las partes del archivo que no quepan en la pantalla.

**Dirección IP**

Se utiliza para identificar un nodo en una red y para especificar la información de encaminamiento en un conjunto de redes. Todos los nodos del conjunto de redes deben tener asignada una única dirección IP, que está formada por el identificador de red y un único identificador de host asignado por el administrador de la red. En Windows NT, se puede configurar la dirección IP de forma estática en la computadora o de forma dinámica mediante DHCP.

**Dirección MAC**

La dirección de un dispositivo tal como está identificado en la capa de control de acceso a medios en la arquitectura de la red.

**Directorio**

Parte de la estructura de organización de los archivos en disco. Un directorio puede contener archivos y otros directorios (denominados subdirectorios).

**Directorio compartido**

Directorio al que pueden conectarse los usuarios de la red.

**Dispositivo**

Cualquier pieza de equipo que se puede conectar a una red; por ejemplo, una computadora, una impresora o cualquier otro dispositivo periférico. Con AppleTalk Phase 2, los dispositivos se pueden asignar a zonas.

#### Dominio

En una red Windows NT Server, grupo de computadoras que comparten una misma base de datos de dominio y un plan de seguridad. Cada dominio cuenta con un nombre único.

#### Duplicación de directorios

Copia de un conjunto maestro de directorios desde un servidor (denominado servidor de Exportación) a varios servidores o estaciones de trabajo especificados (denominadas computadoras de Importación) en el mismo dominio o en otros diferentes. La duplicación simplifica la tarea de mantener conjuntos de directorios y archivos idénticos en varias computadoras, ya que basta con mantener una sola copia maestra de los datos. Los archivos se duplican cuando se agregan a un directorio exportado y cada vez que se guarda una modificación en un archivo.

#### Duplicación de discos:

Establecer una copia espejo en un disco con un controlador diferente.

#### Duplicador de extracción

Un servidor WINS que extrae duplicaciones de las entradas de la base de datos de su duplicador de inserción solicitándolas y después aceptando las réplicas insertadas.

#### Duplicador de inserción

Un servidor WINS que envía mensajes de notificación de actualización a su duplicador de extracción cuando cambia su base de datos WINS. Cuando su interlocutor responde a la notificación con una petición de duplicación, el duplicador de inserción envía una copia de su base de datos WINS actual al interlocutor.

#### Duración máxima de contraseña

Intervalo de tiempo durante el que puede utilizarse una contraseña sin que el sistema solicite al usuario que la modifique.

#### Duración mínima de contraseña

Intervalo de tiempo durante el que debe usarse una contraseña hasta que el usuario pueda cambiarla.

#### DARPA:

Defense Advanced Research Projects Agency o Agencia de Investigaciones en Proyectos de Defensa Avanzada, responsable del desarrollo de ARPANET, basamento inicial del cual surgió Internet.

#### Datagrama:

paquete de información que es enviado de una computadora a otra sin previo aviso. El concepto se asemeja a un telegrama. Los datagramas se utilizan en aplicaciones con pequeñas cantidades de información a transmitir.

#### DDN:

Defense Data Network o red de Datos de Defensa. Una parte de Internet que ésta en conexión con las bases militares de los Estados Unidos y sus contratistas. Se utiliza en comunicaciones que no necesitan de una seguridad especial.

DECnet:

grupo de protocolos de red que utilizan los sistemas operativos de los equipos de una compañía Digital Equipment Corporation, en lugar del típico TCP/IP, no compatible con Internet.

Desencriptado:

volver a su formato original los datos codificados bajo encriptación.

DFS:

otro nombre dado a AFS, El DFS es, más específicamente , una implementación de AFS, parte del Distributed Computing Environment o ambiente de computación distribuida de la Open Foundation.

Down:

se usa para indicar que un sistema no trabaja, como el caso del mensaje "the BBS is down".

E

Editor de perfiles de usuario

Herramienta de Windows NT Server que permite crear, editar y guardar perfiles personales de usuario, perfiles obligatorios de usuario y el perfil predeterminado de usuario, así como el perfil predeterminado del sistema.

Encaminador

Software que transmite información de encaminamiento, como por ejemplo, direcciones de la red y conexiones que el encaminador ha establecido y responde a las solicitudes de encaminamiento de las computadoras de la red. El encaminador también mantiene un registro y dirige los paquetes de datos a otras redes.

Encaminador de inicialización:

Un encaminador en una red AppleTalk que inicialmente define el número (o números) y la zona (o zonas) de una red. Los servidores de Servicios para Macintosh pueden funcionar como encaminadores de inicialización; también es posible usar encaminadores de hardware creados por otras compañías como encaminadores de inicialización.

Encaminador de interred

Un dispositivo que conecta redes y dirige información de la red a otras redes, generalmente eligiendo la ruta más eficaz a través de otros encaminadores.

Encaminamiento

El proceso de reenvío de paquetes a otras pasarelas hasta que el paquete se entrega finalmente a una pasarela conectada al destino especificado.

## Enlaces

Un proceso que establece el canal de comunicación entre un controlador de protocolo y un controlador de adaptador de red.

## Entorno heterogéneo

Una interred formada por servidores y estaciones de trabajo de distintos fabricantes, que utilizan distintos sistemas operativos y protocolos de transporte.

## Escritorio

Fondo de la pantalla, sobre el que aparecen las ventanas, iconos y cuadros de diálogo. espacio de nombres de dominio La estructura de base de datos utilizada por el Sistema de nombres de dominio (DNS).

## Especificación de interfaz de controlador de red (NDIS)

En las redes Windows, la interfaz para los controladores de adaptadores de red. Todos los controladores de transporte llaman a la interfaz NDIS para acceder a las tarjetas adaptadores de red.

## Estación de trabajo

En general, computadora de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. En Windows NT, las computadoras en las que se ejecuta el sistema operativo Windows NT Workstation se denominan estaciones de trabajo, para distinguirlas de aquéllas en las que se ejecuta Windows NT Server y que se conocen como servidores. estaciones de trabajo de inicio de sesión

## Ethernet

Un tipo de medio de comunicación de redes. (También un protocolo de enlace de datos adoptado por IEEE como un estándar).

## EARN:

European Academic Research Network o Red Europea de Investigaciones Académicas.

## EMACS:

uno de los editores más comunes que se encuentran en sistemas on-line.

## e-mail:

electronic mail o correo electrónico, uno de los recursos más usados de Internet. Es un método práctico para el envío de mensajes vía computadora que aventaja en varias cualidades al sistema terrestre de mensajería.

## Encriptado:

método para codificar datos y prevenir el acceso desautorizado, comúnmente utilizado en Internet para proteger al mensaje e-mail de miradas curiosas.

## Enrutador:

sistema que transfiere información entre dos redes que utilizan el mismo protocolo pero pueden diferir en sus características físicas.

## F

**FDDI (Interfaz de fibra óptica para datos distribuidos)**

Un tipo de medio de comunicación de red diseñado para su uso con cableado de fibras ópticas.

**FAQ:**

Frequently Asked Questions o Preguntas de Frecuente Aparición. Se trata de una pregunta o grupo de preguntas de común aparición, y sus respuestas. Se encuentran en toda Internet, ya sea en Usenet Newgroups, mailing list, FTP, Gopher y sitios WWW. Generando listas de FAQ, los usuarios no pierden tiempo contestando cada una, cada vez que aparece.

**Firewall: cortafuegos.**

Dispositivo de seguridad que ayuda a proteger una red privada de hackers o crackers de Internet. Es una máquina con dos interfases de red configurada para restringir que pueden ser usados y la dirección IP interna que puede ser mostrada al exterior de Internet.

**Firma:**

archivo de unas cinco líneas anexadas al final de un mensaje e-mail o de artículos Usenet donde los usuarios informan nombre, domicilio de correo electrónico, etc. Pueden contener fotos y otras informaciones.

**Flame:**

ataque personal, abusivo y virulento que se dirige contra el autor de un mensaje en Usenet.

**Flame relay:**

instrumento que se emplea en determinadas oportunidades como proveedor de enlaces de alta velocidad a Internet, en todos los casos mayor a 56 Kbps.

**FTP:**

File Transfer Protocol o Protocolo de Transferencia de Archivos. Establece como transferir archivos en distintas computadoras. Existen FTP anonymous y otros a los cuales se accede vía password.

**G**

**Gopher:**

servidor que provee información a través de un sistema de menús, rastreando datos a través de la red.

**Grupo de trabajo de ingeniería Internet (IETF)**

Un consorcio que introduce procedimientos de nueva tecnología en Internet. Las especificaciones de IETF se publican en documentos denominados Peticiones de comentarios (RFC).

**H**

## Host

Cualquier dispositivo conectado a un conjunto de redes y que utilice TCP/IP.

## HPFS

Siglas en inglés de sistema de archivos de alto rendimiento (HPFS), utilizado fundamentalmente en el sistema operativo OS/2 versión 1.2 y posteriores. Admite nombres de archivo largos, pero no dispone de funciones de seguridad.

## Hackers:

alguien que explora los sistemas computarizados generalmente en forma ilegal.

## HTML:

HyperText Mark-up Language. Lenguaje base de armado de hipertexto, utilizado para la construcción de los documentos de la World Wide Web.

## HTTP:

HyperText Transfer Protocol. Uno de los más importantes protocolos Internet utilizados en la comunicación World Wide Web.

## I

### ID de host

La parte de la dirección IP que identifica una computadora dentro de un determinado ID de red.

### Identificador de puerto

El método que utilizan TCP y UDP para especificar qué aplicación que se está ejecutando en el sistema está enviando o recibiendo los datos.

### Identificador de red

La parte de la dirección IP que identifica un grupo de computadoras y dispositivos ubicados en la misma red lógica.

### ID de seguridad

Nombre exclusivo que identifica ante el sistema de seguridad a los usuarios que han iniciado una sesión. Los identificadores de seguridad (SID) permiten identificar a un usuario o a un grupo de usuarios.

### Intercambio dinámico de datos

Tipo de comunicación entre procesos (IPC) implementado en la familia de sistemas operativos Microsoft Windows. Dos o más programas que dispongan de funciones de intercambio dinámico de datos (DDE) pueden intercambiar información y comandos.

### Interfaz de controlador de transporte (TDI)

En las redes Windows, la interfaz común para los componentes de la red que se comunican en la capa de sesiones.

### Interred

Dos o más redes conectadas a través de uno o más encaminadores para formar una red más grande.

Los usuarios de las redes de una interred pueden compartir información y dispositivos de redes.

#### IP de línea serie (SLIP)

Un estándar de la industria que forma parte de RAS de Windows NT para asegurar la interoperatividad con software de acceso remoto de otros fabricantes.

#### IPX/SPX

Protocolos de transporte utilizados en las redes NetWare de Novell. En Windows NT, se utiliza NWLink para implantar este protocolo.

#### Íconos emocionales:

son gráficos que condensan estados de ánimo o frases economizando la cantidad de palabras que requerirían si se escribiesen. Se leen apoyando la cara en el hombro izquierdo. Por ejemplo: smiley utilizado para indicar "sonriente".

#### Internet:

cuando se utiliza con mayúsculas se refiere a la red de redes que usa en su interconexión el protocolo TCP/IP. La acepción en minúscula indica cualquier conjunto de redes, que tenga un funcionamiento único.

#### Internet Society:

conocida también como ISOC: cuyo fin es dar soporte a los emprendimientos de Internet, brinda asesoramiento a los usuarios y promueve la investigación. El capítulo argentino, denominado Internet Society Chapter Argentino, se fundó en 1995 como una asociación civil sin fines de lucro que sigue los lineamientos de la idea internacional impulsando el desarrollo de Internet a nivel nacional.

#### IP:

Internet Protocol o Protocolo Internet en el cual se basa Internet. Es el más importante de los protocolos a través de los cuales se intercomunican las computadoras en Internet.

#### IRC:

Internet Relay Chat o Difusoras de Charlas en Internet, la cual permite mantener conversaciones en tiempo real a través de Internet.

#### L

#### Línea de interrupción requerida (IRQ)

Línea de interrupción requerida (IRQ) es una línea de hardware a través de la cual un dispositivo puede enviar señales para recabar la atención del procesador cuando dicho dispositivo esté preparado para aceptar o enviar información. Por lo general, cada uno de los dispositivos conectados a la computadora utiliza una línea IRQ diferente.

#### Llamada a procedimiento remoto

(RPC) Función de transmisión de mensajes que permite a una aplicación distribuida llamar a los servicios disponibles en diversas computadoras de una red. Se utiliza durante la administración remota de computadoras.

#### LAN:

**Local Area Network o Red de Area Local.** Un tipo de red que interconecta computadoras en un radio de alcance restringido. Generalmente este alcance no supera la distancia de algunos kilómetros.

**Línea conmutada:**

un tipo de conexión que se establece empleando un emulador de terminal y un módem.

**Línea dedicada:**

una línea telefónica permanentemente conectada a la computadora para la transferencia de datos. En Internet se utiliza para diferenciarla del servicio estándar basado en un módem y una línea telefónica que transfiere datos en forma discontinua según el contrato estipulado con la empresa proveedora del servicio.

**Listserv:**

sistema de distribución automática de información vía correo electrónico.

**Login:**

sistema de identificación del usuario para el ingreso a un sistema computarizado, previo al password o palabra clave.

**M**

**Máscara de subred**

Un valor de 32 bits que permite al destinatario de paquetes IP distinguir en la dirección IP la parte de identificador de red de la parte de identificador de host.

**Mail gateway:**

máquina que transfiere archivos entre dos o más sistemas de e-mail.

**Mailing list:**

grupo de discusión cuyos mensajes son distribuidos por e-mail.

**MAN:**

Metropolitan Area Network o Red de Area Metropolitana. Tipo de red, de alcance intermedio entre una LAN y una WAN que permite, como su nombre lo indica, interconectar sistemas a nivel urbano.

**Módem:**

Modulador/DEModulador/o Modulador/DEModulador. Dispositivo que habitualmente interconecta una computadora con una línea telefónica para la transferencia de datos. Convierte señales binarias en señales analógicas.

**Mosaic:**

examinador de la Word Wide Web que está preparado para asimilar los sistemas de hipermedia.

**N**



## NetBIOS sobre TCP/IP

El módulo de conectividad en red que proporciona la funcionalidad para soportar el registro de nombres NetBIOS y su resolución.

### Nivel de privilegios

Una de tres configuraciones (Usuario, Administrador o Invitado) asignada a cada cuenta de usuario. El nivel de privilegios que tiene una cuenta de usuario determina las acciones que el usuario puede realizar en la red. Vea también privilegio de Administrador, privilegio de Invitado y privilegio de Usuario.

### Nombre de computadora

Nombre exclusivo, con una longitud máxima de hasta 15 caracteres, que identifica a una computadora en la red. Este nombre no puede ser igual al de ninguna otra computadora o dominio de la red.

### Nombre de dominio

Nombre que identifica al dominio en la red.

### Nombre de grupo Internet

En las redes Windows NT, es un nombre registrado por el controlador del dominio que contiene una lista de las direcciones concretas de los sistemas que han registrado su nombre. El nombre tiene el carácter número 16 con el valor 0x1C.

### Nombre de host

El nombre de un dispositivo en un conjunto de redes. Para un dispositivo en una red Windows, puede ser el mismo nombre que el de la computadora, pero puede ser diferente. El nombre de host tiene que estar en la tabla de host o estar reconocido en algún servidor de DNS para que otra computadora pueda encontrarlo cuando intente comunicarse con él.

### Nombres de comunidad

Un grupo de hosts al que pertenece el servidor que ejecuta el servicio SNMP. El nombre de comunidad se introduce en el paquete SNMP cuando se envía una captura. Normalmente, todos los hosts pertenecen a "public", que es el nombre estándar para la comunidad general de todos los hosts.

### NTFS

Sistema de archivos avanzado diseñado para su utilización específica en el sistema operativo Windows NT. Incorpora funciones de recuperación de archivos del sistema, medios de almacenamiento de tamaño muy grande y diversas funciones para el subsistema POSIX. Asimismo, incluye aplicaciones orientadas a objetos, tratando a todos los archivos como objetos que cuentan con atributos definidos por el usuario y definidos por el sistema.

### O

#### Off-line:

no conectado a un sistema on-line.

#### On-line:

conexión directa entre dos computadoras a través de módems en tiempo real, Por ejemplo, el Bulletin Board System es un sistema on-line.

## P

#### Partición

Parte de un disco físico que actúa como si se tratase de una unidad físicamente independiente.

#### Pasarela

Se utiliza indistintamente con el término encaminador IP para describir un sistema conectado a varias redes físicas TCP/IP, que es capaz de encaminar o entregar paquetes IP entre ellas.

#### Pasarela predeterminada

El dispositivo intermedio de la red local que conoce los identificadores de las demás redes del sistema de redes interconectadas, de forma que puede reenviar paquetes a otras pasarelas hasta que el paquete se entregue finalmente a la pasarela que está conectado al destino especificado. En general, las pasarelas son computadoras dedicadas denominadas encaminadores.

#### Permiso

Regla asociada a un objeto (generalmente un directorio, archivo o impresora) para regular los usuarios que pueden acceder al objeto y el modo en que se realiza este acceso.

#### Pertenencia a grupos:

Grupos a los que pertenece una cuenta de usuario. Los permisos y derechos concedidos a un grupo se conceden también a sus miembros.

#### Peticiones de comentarios (RFC)

Los documentos oficiales del Grupo de trabajo de ingeniería de Internet (IETF) que especifican los detalles de los protocolos incluidos en la familia TCP/IP.

#### Pila de protocolo

La ejecución de una familia de protocolos específica en una computadora u otro nodo en la red.

#### Plan de auditoría

Define el tipo de sucesos de seguridad que se desea registrar para los servidores de un dominio o para una computadora individual.

#### Plan de cuentas

Controla el modo en que las cuentas de usuario de un dominio o de una computadora individual deben utilizar las contraseñas.

## Plan de derechos de usuario

Administra la asignación de derechos a los grupos y cuentas de usuario.

### Protocolo

Software empleado para comunicarse a través de una red, como NetBEUI, TCP/IP y NWLink. Un conjunto de normas y convenios mediante los cuales dos computadoras se intercambian mensajes a través de la red.

### Protocolo de administración de red simple (SNMP)

Un protocolo utilizado por las consolas y los agentes SNMP para comunicarse. En Windows NT, el servicio SNMP se utiliza para obtener y definir información de estado acerca de un host en una red TCP/IP.

### Protocolo de configuración dinámica de host

Un protocolo para la configuración automática de TCP/IP que proporciona gestión y asignación de direcciones estáticas y dinámicas.

### Protocolo de control de transmisión (TCP)

Un protocolo Internet basado en la conexión, responsable de la división de los datos en paquetes, que el protocolo IP envía a través de la red. Este protocolo asegura una secuencia de comunicación fiable y ordenada en el conjunto de redes.

### Protocolo de control de transmisión/Protocolo Internet (TCP/IP)

Los protocolos Internet que se utilizan para conectar una interred mundial de universidades, laboratorios de investigación, instalaciones militares y empresas. TCP/IP incluye estándares sobre las comunicaciones entre las computadoras y convenios para la conexión de redes y el encaminamiento del tráfico.

### Protocolo de datagramas de usuario (UDP)

Un complemento de TCP que ofrece un servicio de datagramas sin conexión que no garantiza ni la entrega ni orden correcto de los paquetes entregados. Las sumas de verificación opcionales de datos de UDP pueden validar la cabecera y los datos, pero no existen confirmaciones obligatorias, dejándolas a las aplicaciones.

### Protocolo de inicio (BOOTP)

Un protocolo entre redes utilizado para configurar sistemas a través de redes interconectadas. DHCP es una ampliación de BOOTP.

### Protocolo de información de encaminamiento (RIP)

Un protocolo entre encaminadores que soporta el encaminamiento dinámico. En esta versión, Microsoft TCP/IP no soporta este protocolo.

### Protocolo de mensajes de control Internet (ICMP)

Un protocolo de mantenimiento del conjunto TCP/IP, necesario en todas las implantaciones de TCP/IP, que permite a dos nodos de una red IP compartir información de estado y de error IP. La utilidad ping utiliza ICMP para determinar la disponibilidad de un sistema remoto.

### Protocolo de resolución de direcciones (ARP)

Un protocolo de la serie TCP/IP que proporciona una resolución de direcciones IP a control de acceso a medios (MAC) para los paquetes IP.

#### Protocolo de transferencia de archivos (FTP)

Un servicio que soporta la transferencia de archivos entre sistemas locales y remotos que utilizan este protocolo. FTP ofrece varios comandos que permiten la transferencia bidireccional de archivos binarios y ASCII entre los sistemas. El Servicio Servidor FTP se puede instalar en Windows NT pero no se incluye de forma predeterminada debido a consideraciones de seguridad. El cliente FTP se instala con las utilidades de conectividad de TCP/IP.

#### Protocolo Internet (IP)

El protocolo de mensajería de TCP/IP, responsable del direccionamiento y del envío de paquetes en la red.

#### Protocolo punto a punto (PPP)

Un estándar de la industria que forma parte de RAS de Windows NT para asegurar la interoperatividad con software de acceso remoto de otros fabricantes.

#### Proxy

Una computadora que escucha las difusiones de consulta de nombres y responde a los nombres que no estén en la subred local. El proxy de WINS se comunica con el servidor de nombres para resolver los nombres y luego los mantiene en su memoria caché durante un intervalo de tiempo.

#### Puerto

Conexión o enchufe utilizado para conectar un dispositivo, por ejemplo una impresora, un monitor o un módem, a su computadora. La información se envía desde la computadora al dispositivo a través de un cable.

#### Paquete:

conjunto de información. En Internet los datos se transfieren por paquetes, cada uno de ellos puede oscilar entre 40 y 32 bytes de tamaño de información.

#### Postmaster:

maestro de correo. La persona responsable de la administración y distribución de información que llega a una computadora vía electrónica.

#### PPP:

Protocolo Punto a Punto. Es un protocolo que hace posible que una computadora pueda emplear los protocolos TCP/IP, utilizando para ello la línea telefónica y un módem.

#### Protocolo:

instrucciones a partir de las cuales dos computadoras establecen su comunicación con la cual se transferirán datos. El protocolo que utiliza Internet es TCP/IP.

Proveedor: organización que ofrece el servicio Internet o parte de él.

R

### Rastreadores de redes.

Una herramienta de diagnóstico de hardware y software que también puede usarse para descifrar contraseñas, lo cual podría resultar en un acceso no autorizado a cuentas de redes. Las contraseñas de texto simple son susceptibles a los rastreadores de redes.

### Recurso

Cualquier elemento de un sistema de computadora o de una red, tal como una unidad de disco, una impresora o la memoria, que se puede asignar a un programa o a un proceso durante su ejecución.

### Registro de seguridad

Registra los sucesos de seguridad. Ello facilita el seguimiento de los cambios en el sistema de seguridad y la identificación de las posibles transgresiones de la misma. Por ejemplo, si la configuración de auditoría del Administrador de usuarios así lo establece, los intentos de iniciar sesiones en el sistema pueden anotarse en el registro de seguridad.

### Relación de confianza

Las relaciones de confianza son vínculos entre dominios que permiten la autenticación cruzada, de forma tal que cada usuario tenga cuenta únicamente en un dominio y pueda acceder a toda la red. Las cuentas de usuario y grupos globales definidos en un dominio en el que se confía pueden obtener derechos y permisos de acceso a recursos en el dominio que confía, aunque esas cuentas no existen en la base de datos del dominio en el que se confía. Los dominios de confianza dan por válidas las autenticaciones de inicio de sesión de los dominios en los que confían.

### Resolucionadores

Cientes de DNS que consultan a los servidores DNS para la resolución de nombres en las redes.

### Resolución de nombres

Un servicio proporcionado por un servidor de nombres DNS o un servidor de nombres NetBIOS (NBNS) para asignar nombres de computadoras DNS o NetBIOS a direcciones IP. En una red Windows, un servidor WINS es un servidor NBNS.

### Router:

sistema que transfiere información entre dos redes que usan el mismo protocolo.

## S

### SAI

Sistema de alimentación ininterrumpida alimentada por baterías conectado a una computadora con el fin de mantener el sistema en funcionamiento durante las interrupciones del suministro eléctrico.

### SAM

Siglas en inglés de Administrador de cuentas de seguridad. Subsistema protegido de Windows NT que mantiene la base de datos de SAM y proporciona la interfaz de programación de aplicaciones (API) para el acceso a la base de datos.

## Seguridad

Una manera de asegurar que solamente los usuarios autorizados pueden acceder a los archivos compartidos.

## Selector

El accesorio de escritorio de Macintosh a través del cual los usuarios seleccionan el servidor y las impresoras de la red que desean usar.

## Servicio

Proceso que realiza una función específica del sistema y que a menudo proporciona una interfaz de programación de aplicaciones (API) que es llamada por otros procesos.

## Servicio de acceso remoto (RAS)

Un servicio que proporciona conectividad en red para trabajadores autónomos, empleados desplazados y administradores de sistemas que supervisan y administran los servidores de varias sucursales. Los usuarios de RAS en una computadora Windows NT pueden acceder de forma remota (mediante marcación) a los servicios de red que tengan disponibles: compartición de archivos e impresoras, correo electrónico, planificación y acceso a bases de datos SQL.

## Servicio de información de red (NIS)

Un servicio para los sistemas de proceso distribuido que proporciona un sistema de base de datos distribuido para los archivos de configuración comunes.

## Servicio de nombres Internet de Windows (WINS)

Un servicio de resolución de nombres que resuelve los nombres de computadoras en una red Windows a direcciones IP en un entorno encaminado. Un servidor WINS gestiona los registros de nombres, las consultas y las liberaciones.

## Servidor de nombres NetBIOS (NBNS)

El servidor implantado según las RFCs 1001/1002 para proporcionar servicios de resolución de nombres para los nombres de computadora NetBIOS.

## Serial cable:

cable serial. El cable usado para conectar dispositivos a través del puerto serial de la computadora.

## Serial port:

el puerto que transmite y recibe datos asincrónicos. Dispositivos periféricos como impresoras y módems utilizan serial port.

## Server:

programa que hace posible que una computadora preste a otra sus servicios. También se utiliza para designar a la computadora donde corre dicho software.

## SLIP:

Serial Line IP o Línea Serial IP. Protocolo que permite a una computadora utilizar los protocolos de Internet usando una línea telefónica estándar.

## TCP:

**Transmission Control Protocol o Protocolo de Control de Transmisión.** Uno de los protocolos en los cuales se basa Internet.

**telnet:** protocolo de Internet que permite loguearse con otro sistema de la red.

**UNIX:**

sistema operativo comúnmente utilizado en Internet. Sin embargo, no es necesario saber UNIX para operar Internet.

**URL:**

Uniform Resource Locator. Intento por estandarizar la locación o detalles de dirección d las fuentes de Internet. Actualmente se lo utiliza en relación con la Word Wide Web.

**Usenet:**

grupo informal de sistemas para el intercambio, el debate y la conversación en Internet, al modo de los newsgroups.

**UUCP:**

Unix to Unix Copy. Instrumento para el copiado de archivos entre dos o más sistemas UNIX.

**Verónica:**

instrumento que, como Archie, forma parte del Gopher. Permite buscar información en los servidores Gopher.

**WAIS:**

Wide Area Information Server o Servidores de Información de Area Ancha. Utilizados para la búsqueda de bases de datos indizadas a través de Internet.

**WAN:**

Wide Area Network o Redes de Area Ancha. Tipo de red que interconecta computadoras con un espectro amplio de cobertura, en el ámbito de un país o grupo de países. Internet puede considerarse como la más eficaz WAN actualmente existente.

**White pages:**

listados de usuarios de Internet a los cuales se puede acceder a través de la misma Intenet.

**World Wide Web:**

sistema de base hipertextual que se convierte en la fuente de información más difundida de Internet en la actualidad.

**Yellow pages:**

Páginas amarillas. Listado de direcciones electrónicas correspondientes a distintos tipos de instituciones de Internet.