

**PONTIFICIA UNIVERSIDAD
CATÓLICA DEL ECUADOR
SEDE AMBATO**

ESCUELA DE INGENIERÍA DE SISTEMAS

**DISERTACIÓN DE GRADO PREVIA LA
OBTENCIÓN DEL TÍTULO DE
INGENIERO DE SISTEMAS**

**“Portal de Servicios Académicos y Administrativos aplicado a la
P.U.C.E.S.A.”**

**Marjorie Lorena Cadena Pantoja
Mónica Noemí Manobanda Herrera**

DIRECTOR DE DISERTACIÓN: Ing. Janio Jadán G. M.Sc.

AMBATO, 2.001

**PONTIFICIA UNIVERSIDAD
CATÓLICA DEL ECUADOR
SEDE AMBATO**

ESCUELA DE INGENIERÍA DE SISTEMAS

**DISERTACIÓN DE GRADO PREVIA LA
OBTENCIÓN DEL TÍTULO DE
INGENIERO DE SISTEMAS**

**“Portal de Servicios Académicos y Administrativos aplicado a la
P.U.C.E.S.A.”**

DIRECTOR:

Ing. Janio Jadán G. M.Sc.

REVISORES:

Ing. Natasha Bayas

Ing. Pilar Urrutia

**Marjorie Lorena Cadena Pantoja
Mónica Noemí Manobanda Herrera**

AMBATO, 2.001

Dedicatoria

Este trabajo lo dedico a DIOS porque gracias a El he tenido la oportunidad de terminar mi carrera, me ha bendecido guiando mis pasos con sabiduría e inteligencia por el largo camino de las aulas, me ha dado dos modelos humanos; la abnegación y sacrificio de mi madre Chelita y la rectitud y disciplina moldeada en mi padre Jacinto, pero también me dio a mi compañera y confidente Cynthia, además recibí el amor y el apoyo incondicional de Marcelito, a todos ellos dedico esta obra que es la culminación de una etapa de mi carrera estudiantil y el inicio de mi vida profesional , puntales sin los cuales no hubiese alcanzado este peldaño mas de mi vida , porque todos necesitamos de una mano de amor que nos guíe y nos oriente . Además dedico a las futuras generaciones de la Pontificia Universidad Católica del Ecuador Sede Ambato, a fin de que ésta obra les sirva de guía para su formación ya que en ella está plasmada lo científico y lo humano pues combinando estas, podremos brindar un mejor aporte al crecimiento de nuestra Universidad y de la Comunidad.

Marjorie Lorena

Dedicatoria

Dedico esta tesis a quienes llenan mi vida de felicidad, ejemplo y comprensión, mis padres: María Herrera y Luis Manobanda, por ser fortalezas invalorables y brindarme su constante apoyo.

A mi familia, porque siempre confiaron en mí a lo largo de toda mi vida, en especial a mis hermanos quiénes me secundaron incondicionalmente para culminar mi carrera.

Mónica Manobanda

Agradecimiento

A la Pontificia Universidad Católica del Ecuador con su Sede en Ambato, a mi director de Tesis Ing. Janio Jadán, ya que él me ha brindado su guía incondicional y paciencia aportándome con su amplio conocimiento y experiencia; a las Ings. Natasha Bayas y Pilar Urrutia quienes fueron las impulsadoras para el desarrollo de este trabajo.

De igual manera agradezco a todas esas personas que fueron de gran apoyo moral e incluso intelectual para la culminación de mi Tesis.

Marjorie Lorena

Agradecimiento

En primer lugar agradezco a Dios y a la Virgen María, por ser guardianes de mi vida y alumbrar mi camino.

A mi Director de Tesis y revisores: Ing. Janio Jadán, Ing. Natasha Bayas e Ing. Pilar Urrutia, que han sido fuentes de conocimientos y experiencia.

De igual forma a todas aquellas personas que de una u otra manera me han apoyado para la culminación de este proyecto de tesis.

Mónica Manobanda

INDICE

INTRODUCCIÓN	1
---------------------------	---

CAPÍTULO I

REALIDAD Y PROYECCIÓN INSTITUCIONAL.

1.1. Introducción	3
1.1.1. Aspectos generales	4
1.1.2. Definición de Portales	4
1.1.3. Reseña Histórica	5
1.2. Influencia de los portales webs en la evolución de una entidad educativa ..	6
1.3. El futuro de las entidades educativas	7

CAPÍTULO II

INTRANETS INSTITUCIONALES

2.1. Fundamentos de una Intranet	10
2.1.1. Ventajas y características de una Intranet	12
2.1.2. Beneficios de una Intranet	13
2.1.3. Estructuración de datos de una Intranet	16
2.1.4. Seguridades en una Intranet	17
2.2. Usuarios en una Intranet	18
2.3. Servidores Webs	22
2.3.1. Tipos de Servidores World Wide Web (WWW)	22
2.3.2. Políticas para Servidores Webs	25
2.4. Red e Información de la P.U.C.E.S.A.	27

CAPÍTULO III**METODOLOGÍA PARA EL DISEÑO DE PÁGINAS WEB APLICADAS A ENTIDADES EDUCATIVAS.**

3.1. Creación de Páginas Webs	28
3.1.1. Herramientas de creación de páginas Webs	28
3.1.2. Lenguajes de Programación	29
3.1.3. Herramienta Auxiliares	30
3.2. Diseño de sitios webs interactivos	31
3.3. Introducción a las Webs Dinámicas	37
3.4. Aplicaciones Usuario-servidor	38
3.4.1. Aplicaciones ejecutadas en el cliente	40
3.4.1.1. Introducción a JavaScript	40
3.4.1.2. Introducción a los Applets	42
3.4.2. Aplicaciones ejecutadas en el servidor	44
3.4.2.1. Introducción al CGI (Common Gateway Interface)	45
3.4.2.2. Introducción al Hypertext Preprocessor (Php3)	47
3.4.2.3. Introducción a las Active Server Pages (Asp)	49
3.4.2.3.1. Declaración del Lenguaje	50
3.4.2.3.2. Aplicaciones de las páginas ASP	53
3.4.2.3.3. Requerimientos	53
3.4.2.3.4. Herramientas	54
3.4.2.3.5. Introducción a las Cookies (Galletas) con ASP	55

CAPÍTULO IV**COMERCIO ELECTRÓNICO APLICADO A PORTALES DE SERVICIOS ACADÉMICOS Y ADMINISTRATIVOS**

4.1. Introducción	58
4.2. Fundamentos del Comercio Electrónico	59

4.2.1. Elementos del Comercio Electrónico	60
4.2.2. Ventajas y Riesgos del Comercio Electrónico	62
4.2.3. Métodos de envíos y pago	67
4.3. Funcionamiento de un portal web	68
4.4. Gestión de tablas de impuestos (Cibertributación)	71
4.5. Análisis de redes de área extensa (WAN)	73
4.6. Herramientas de Internet aplicadas a portales webs	74
4.6.1. World Wide Web (WWW)	74
4.6.2. Correo electrónico	76
4.6.3. Sistema de nombres de dominios (DNS)	76
4.6.4. FTP (Protocolo de Transferencia de Archivos)	79
4.6.5. IRC (Internet Relay Chat).....	80
4.6.6. Videoconferencia	81
4.7. Portales Webs	81
4.7.1. ActiveX	81
4.7.2. Visual Basic Script (VBScript)	82

CAPÍTULO V

SEGURIDAD Y ENCRIPCIÓN EN UN PORTAL DE SERVICIOS

5.1. Introducción	83
5.2. Formas de Seguridad	84
5.2.1. Seguridad Interna	84
5.2.2. Seguridad Externa	86
5.3. Métodos Criptográficos	88
5.3.1. Métodos de Cifrado o Clave Secreta o Simétrica	89
5.3.2. Criptografía de Clave Pública o Asimétrica	90
5.4. Algoritmos de Destilación	92
5.5. Tarjetas débito y crédito (SSL & SET)	93
5.5.1. SSL (Secure Sockets Layer)	95

5.5.1.1. SSL HANDSHAKE	96
5.5.1.2. Límites del SSL	98
5.5.2. Transacciones electrónicas seguras (SET)	98
5.5.2.1. Problemas con las autoridades de certificación del SET	101
5.6. Firma electrónica	103
5.6.1. Autoridades de Certificación	104
5.7. Seguridad en los programas de Correo Electrónico	105
5.7.1. PGP (Pretty Good Privacy)	106
5.7.2. S/MIME (Secure Multipurpose Internet Mail Extension)	107
5.8. Soluciones a los problemas de seguridad	108
5.8.1. Certificados de usuario y de servidor seguros	109
5.8.2. Auditorías de seguridad	111

CAPÍTULO VI

PORTAL DE SERVICIOS ACADÉMICOS Y ADMINISTRATIVOS ORIENTADO AL USO DE LOS SERVICIOS ACADÉMICOS.

6. Análisis y Diseño	113
6.1. Descripción Global del Proyecto	113
6.2. Determinación de Requerimientos	116
6.2.1. Metodología para el desarrollo del sistema	116
6.2.2. Especificación de Requisitos	118
6.3. Análisis de software	119
6.3.1. Flujo de Información	119
6.3.2. Implementación del Portal de Servicios Académicos y Administrativos	121
6.3.2.1. Responsabilidades	122
6.4. Diseño del Sistema	123
6.4.1. Selección de Herramientas	123
6.4.1.1. Desarrollo de páginas webs dinámicas	123
6.4.1.1.1. ASP (Active Server Pages)	124

6.4.1.1.2. Requerimientos	124
6.4.1.1.3. Porqué Macromedia DreamWeaver UltraDev y ASP	125
6.4.1.1.4. Instalar DreamWeaver UltraDev	126
6.4.1.2. Servidor Web	126
6.4.1.2.1. Internet Information Server (IIS)	127
6.4.1.3. Base de datos	127
6.4.1.3.1. Microsoft SQL Server	128
6.4.1.4. Interfaz entre las aplicaciones y el gestor	130
6.4.1.5. Algoritmo de encriptación de datos	132
6.5. Refinamiento del Análisis	136
6.6. Representación del modelo global del sistema	143
6.6.1. Capas del Portal de Servicios Académicos y Administrativos	144
6.7. Diseño de Interfaz	144
6.7.1. Interfaz Cliente-servidor	144
6.7.2. Interfaz Gráfica	147
6.8. Implementación	160
6.8.1. Aplicación del sistema en una empresa	160
6.8.2. Análisis y Evaluación de la implementación	161
CONCLUSIONES	163
RECOMENDACIONES	166
GLOSARIO DE TÉRMINOS	167
BIBLIOGRAFÍA	182
ANEXOS	187

INTRODUCCION

La presencia en esta última década de la red internacional de información, Internet, se ha convertido en una auténtica revolución en términos tecnológicos y particularmente en cuanto a la manera de abordar y concretar las relaciones comerciales y comunicaciones en general. El mundo ha ido adoptando la nueva economía del Internet denominado Comercio Electrónico convirtiéndose así en la mejor estrategia para incrementar y potenciar las capacidades de las empresas para ingresar con éxito a la economía digital; esta nueva herramienta ha representando anualmente un rubro significativo para la economía de cada país.

La tecnología nos ofrece dar un paso importante en el emergente mercado del Comercio Electrónico, adaptando los procesos del negocio a la *Web* e integrándolos con avanzados sistemas de seguridad por lo cual nos motiva a desarrollar una investigación sobre una verdadera transacción comercial, para el efecto se propondrá como una futura aplicación en cuanto el Comercio Electrónico sea lícito en nuestro país, es decir que se integrará conjuntamente con el Portal de Servicios para ofrecer una adecuada promoción a nivel educativo.

A través de este proyecto, se desarrollará un servicio académico y administrativo con información comercial, orientado a adaptar los procesos del negocio a través de un sitio *Web*, permitiendo al usuario realizar transacciones con los servicios que brinda la

Pontificia Universidad Católica del Ecuador Sede Ambato (P.U.C.E.S.A.) en una forma rápida y segura, logrando de esta manera tener una audiencia empresarial activa.

Además, hay que destacar que se podrá dar oportunidad a los estudiantes de las diferentes escuelas para que a través de su nivel académico y su ingenio comercialicen sus creaciones y asuman nuevos retos; para así poder transformar nuestra entidad educativa en una ventaja competitiva que fortalezca el país.

Con todas estas ventajas, nos permitirá comercializar los servicios que la P.U.C.E.S.A. ofrece a los diferentes clientes potenciales, por lo tanto es necesario plantear proyectos en este sentido con la finalidad de aportar al crecimiento del sector educativo a través del comercio electrónico.

El Portal de Servicios Académicos y Administrativos de la P.U.C.E.S.A., así como las seguridades que se aplicarán en este proyecto serán el inicio de nuevas alternativas educativas y comerciales que están llamadas a crecer y consolidarse en aras de la tecnología, para que el Ecuador y nuestra entidad educativa abran las puertas al resto del mundo.

CAPÍTULO I

REALIDAD Y PROYECCIÓN INSTITUCIONAL

INTRODUCCION

Plantear un modelo de portal con éxito implica centrarse en la generación de tráfico (visitas recibidas) y comercio electrónico, para lo que se hace necesario potenciar los contenidos y la incorporación de servicios de valor añadido en general. Los portales contienen hoy en día generalmente un componente para formar comunidades y una sección con servicios populares, como clima, noticias, charlas interactivas, e-mail gratuito, directorios locales, foros etc.

La generación de negocios en los portales vendrá dada principalmente por dos factores relacionados entre sí: el tráfico y el comercio electrónico. Por un lado, la simple generación de tráfico en el portal puede suponer ingresos por publicidad, mejorables si se consigue fomentar realmente el comercio electrónico, hecho que hasta ahora no ha terminado de explotar en los portales como parecía preverse. Ello se debe a motivos como la desconfianza existente a usar tarjetas de crédito en Internet, cuando en realidad el fraude real en este aspecto es la décima parte del producido en el mercado tradicional [6].

Esa y otras barreras deben ser solventadas por aquellos portales que quieran participar del negocio que se prevee en el futuro.

1.1.1. ASPECTOS GENERALES

Se debe tratar de aprovechar las posibilidades de Internet, distinta de los sistemas, procesos y modelos tradicionales de negocio, para integrar contenidos y negocio de la forma más natural posible, permitiendo por ejemplo la posibilidad de que alguien realice una búsqueda y como resultado de ésta localice un producto interesante que pueda comprar con un simple click, poniéndoselo fácil al cliente que en un principio no pensaba comprar pero al que le ofrecemos algo que no conocía y ahora le resulta útil.

Un portal funcionará si se utilizan recursos para la generación de ideas de calidad, que diferencien nuestro producto del resto, con las que se consiga gran resultado con poco esfuerzo [7].

1.1.2. DEFINICION DE PORTALES

De forma simple podríamos definir portal como [8]: *Un punto de entrada a Internet donde se organizan sus contenidos, ayudando al usuario y concentrando servicios y productos, de forma que le permitan a éste hacer cuanto necesite en Internet sin tener que salir de dicho website.*

El objetivo pretende fidelizar a los usuarios para conseguir no solo que éstos coloquen dicha página en su *bookmark*, sino que dicha página sea la página de inicio del

navegador del usuario, con lo que se generará un tráfico en ese web que garantice la supervivencia en la red.

1.1.3. RESEÑA HISTORICA

Los primeros portales no fueron buscadores, eran las páginas de entrada de Netscape y Microsoft que permanecían por defecto como primera página de muchos usuarios de Internet al estar grabada en el navegador. El valor publicitario debido a la potencia de canalización de la navegación de los usuarios en la red hizo que Netscape fuera más valorado, más que nada por su portal de entrada que por sus productos, que eran realmente buenos. Este inmenso valor de poder guiar y canalizar a muchos millones de internautas (más de 160 millones de usuarios en este año) que ha hecho que se desate una carrera a ver quien consigue ofrecer el mejor servicio para conseguir atrapar a más usuarios. Esto unido a la característica ya comentada de la creación rápida y sólida de barreras de entrada en Internet, nos hace pensar que a lo largo del año 2001 se cimentará una de las pocas cosas que podemos pensar, será uno de los pilares definitivos de Internet, en un sector tan impredecible por lo nuevo y rápido, y que serán las puertas por las que los usuarios de la red entrarán a buscar su información.

Los portales evolucionarán de forma significativa, pero serán los que consigan establecerse como tales durante el año 2001. En el año 2002 si alguien quiere crear un portal, deberá preparar una inversión multimillonaria para intentar romper las barreras

de entrada que ya se están formando. Nuestra visión al respecto es que se consolidarán como portales internacionales con sus versiones regionales entre 5 y 7 grandes compañías, y como portales domésticos 2 o 3 por país desarrollado. Será el primer nivel de entrada todo tipo de servicios de información, accesos directos a buscadores temáticos, medios de comunicación, accesos a otros buscadores, servicios gratuitos, sección de compras, guías virtuales, comunidades virtuales, etc.

1.2. INFLUENCIA DE LOS PORTALES WEB EN LA EVOLUCION DE UNA ENTIDAD EDUCATIVA.

El objetivo principal de cualquier empresa que utilice el Word Wide Web es que los potenciales clientes visiten su Portal Web y cuantos más, mejor, porque aumentarán las posibilidades de vender o de mejorar su imagen de marca, es decir, que la influencia de *portales web* en una entidad educativa será de grandes beneficios como académicos y sociales.

Académicamente un Portal Web ofrece potenciales servicios a los diferentes usuarios que navegan en la red, por medio de aulas, seminarios virtuales, etc. Pero en este proyecto se destacará el ingenio y creatividad de los estudiantes para potenciar su nivel académico a través de proyectos que permitan incrementar el desarrollo de una comunidad empresarial. En lo social se brindará la mejor carta de presentación que una entidad educativa puede ofrecer al mundo, por medio de la publicidad en red y está se irá extendiendo más debido a la gran capacidad de segmentación que

proporciona y la posibilidad de abrir mercados en cualquier país sin tener que hacer una visita comercial o montar una delegación [8]. Pero es muy probable que el porcentaje de accesos a *sites* a través de buscadores se mantenga o incluso aumente en el futuro, según vaya creciendo el número de usuarios en el mundo, ya que el impacto publicitario de un Portal Web será la mejor imagen que una entidad educativa pueda transmitir en una red.

1.3. EL FUTURO DE LAS ENTIDADES EDUCATIVAS A TRAVES DE LA INCORPORACIÓN DE LA TECNOLOGÍA.

La tecnología en estos últimos años ha tenido un ascenso impresionante, por tal razón el mundo ha ido adaptando los recursos al crecimiento continuo de esta tecnología y tal es el caso que las entidades educativas deberán diseñar sistemas bajo estándares de Internet para que las soluciones en un corto y mediano plazo puedan integrarse a las plataformas de comercio electrónico.

Las entidades educativas se integrarán no solo en tecnología sino en servicios, permitiéndoles participar en el emergente mercado de los negocios electrónicos, para así poder difundir mejor el mercado nacional.

Para el futuro, las entidades educativas tendrán que regirse a los siguientes pasos. El primer paso requiere adaptar los procesos del negocio a la web e integrar los sistemas existentes de la tecnología de información; el segundo requiere aprovechar la

información para una toma de decisión rápida y estratégica; el tercero requiere implementar una tecnología que experimente un modelo de crecimiento continuo para la entidad y el cuarto requiere implementar un sistema administrativo que sea capaz de ejecutar de manera segura los complejos sistemas y redes de la tecnología de información [9].

De la misma forma y en contra de algunas opiniones, los avances tecnológicos y sobre todo la mayor penetración de la banda ancha y los nuevos servicios asociados a la misma (vídeo bajo demanda, v-mail, etc.) no terminará con la vigencia de los Portales (cuya misma estructura y definición les debe permitir integrar rápidamente dichos servicios), aunque si puede que este cambio tecnológico genere un nuevo reparto de fuerzas en Internet, en cuyo caso los Portales actuales deberán estar preparados para aprovechar esta nueva correlación de fuerzas si quieren mantener la supremacía [10].

Los Portales han experimentado un fuerte crecimiento en todos los aspectos durante 1998, configurándose como los principales sitios Internet por tráfico. La expansión de la base de usuarios y las nuevas tecnologías de acceso pensamos que servirán de soporte al mantenimiento y potencialización de los portales y a su transformación en plazas capaces de redirigir el tráfico hacia las zonas de servicios, productos/comercio y comunidad que seguirán siendo básicas para su funcionamiento. Según estadísticas del año 2000, una entidad educativa difundida bajo un Portal Web a través del comercio electrónico, se establecerá como un panorama empresarial con una buena administración tecnológica en donde se abarcará en la integración de los conceptos de

niveles de servicios, niveles de seguridad, manejo de disponibilidad y racionamiento; serán ejemplos claros de cómo la tecnología esta cambiando la manera de fomentar la educación a través del comercio electrónico.

CAPÍTULO II

2. INTRANETS INSTITUCIONALES

2. 1. FUNDAMENTOS DE INTRANET

Uno de los factores más importantes que buscan las empresas al construir una Intranet corporativa, es obtener mayor comodidad en el trabajo sin perder tiempo en localizar su información. Además, se puede compartir información a lo largo y ancho del mundo con sus clientes, visitarlos virtualmente y mantenerlos informados del modo más económico durante los 7 días de la semana y 24 horas del día.

Una Intranet podrá proveer a su organización o empresa de un nuevo concepto de trabajo más allá de los hábitos actuales. Con capacidad para organizar el escritorio de cada empleado de su compañía, publicación electrónica a través de la web reduciendo el consumo de papel y aquellos costes derivados de la impresión al mismo tiempo que elimina tiempos de presentación y entrega de información tanto a los empresarios como a los clientes.

Una Intranet es definida como [11]: *Una red de información de alcance local que fue diseñado con el fin de compartir datos entre computadoras a través de una red LAN (Local Area Network o Red de área local en español), este tipo de redes interconectadas entre sí forman lo que hoy se conoce como INTERNET.*

Se la puede relacionar como una red *TCP/IP* interna de una compañía. El concepto de **Intranet** está completamente relacionado al de Internet. Las empresas sirven en Internet la información pública y mantienen en la Intranet la información privada. La Intranet está basada en los estándares y protocolos abiertos desarrollados en Internet. Estos estándares abiertos soportan aplicaciones y servicios como correo electrónico, trabajo en grupo, servicios de directorio, seguridad, acceso a bases de datos, compartición de información y administración de sistemas.

A diferencia de los sistemas propietarios de Intranets como *BackOffice* de Microsoft o *Lotus Notes* de IBM, los estándares abiertos como el de Netscape (*SuiteSpot*) soportan múltiples plataformas y bases de datos, así como completa flexibilidad e independencia del proveedor. La Intranet se beneficia del esfuerzo de la industria entera y no de un sólo fabricante.

Las Intranets son fáciles de implementar porque trabajan a nivel de red sobre las máquinas, los sistemas operativos y los protocolos de red existentes. Por tanto, como no hay ningún sistema al que emigrar, los costes de implantación de una Intranet son muy reducidos. También se reducen costes y se aumenta la facilidad de desarrollo de aplicaciones ya que se crean una vez y funcionan para cualquier sistema.

Los servicios prestados por una Intranet se dividen en la parte del ordenador cliente, destinada al usuario, y la parte del servidor o de red, gestionada por un administrador de sistemas [12].

Dentro de los **Servicios de Usuario** tenemos:

- Compartir información y administración
- Comunicación y colaboración
- Navegación
- Aplicaciones

En los **Servicios de Red**, encontramos:

- Directorio
- Replicación
- Seguridad
- Administración

2.1.1. VENTAJAS Y CARACTERÍSTICAS DE UNA INTRANET

Dentro de las principales ventajas tenemos las siguientes:

- **Incrementa** la competitividad.
- **Ahorra** costes y tiempo.
- **Aumento** de la productividad.
- **Mejora** las comunicaciones y promueve la participación.

- **Permite** una relación directa con el cliente.
- **Contribuye** a la implantación y mantenimiento de la calidad.
- **Permite** desarrollar el Trabajo.

Las principales características son:

- **Sencillez** de funcionamiento para el usuario.
- **Flexibilidad** y permite una actualización permanente.
- Incorpora la tecnología **multimedia** e **interactiva**.
- Es una tecnología **cliente/servidor**.
- **Compatibilidad** con cualquier tipo de plataforma informática.

Una **Intranet** representa la parte “inteligente” de la organización y su objetivo es organizar el trabajo de cada una de las personas de la empresa a un mínimo coste, tiempo y esfuerzo con el único fin de llegar a ser más productiva, más rentable y más competitiva [13].

2.1.2. BENEFICIOS DE UNA INTRANET EN LA EMPRESA

Se debe tener claro un concepto fundamental, nunca debe tratarse como una plataforma de trabajo sino más bien como una herramienta de trabajo la cual aportará con múltiples beneficios:

- **Ahorro:** Adiós a documentos, formularios, manuales, tarifas, notas internas, bases de datos y demás documentación que obliguen al uso de papel y a la utilización de impresoras para la distribución de la información diaria de la empresa. Esta infraestructura necesaria puede dejar paso a páginas de texto HTML, sonidos, e incluso imágenes digitalizadas que tan sólo requieren un navegador para su consulta.
- **Control:** Los datos importantes de la organización no estarán tan sólo en la mesa de un directivo o en la de un mando intermedio. Se sabrá en cada momento cómo se encuentra un proyecto ya que la información en una Intranet se modifica y consulta en tiempo real.
- **Calidad:** Internet es la cantidad mientras que una Intranet es calidad. La Red está cargada de información importante, pero el tiempo que se debe emplear para su localización es a menudo demasiado para ofrecer soluciones rápidas a las dificultades diarias. En la Intranet el usuario encuentra todo lo que necesita ya que la información se encuentra mucho más organizada y seleccionada.
- **Comunicación:** El sistema de mensajería implementado puede ofrecer comunicaciones internas y externas, en tiempo real y diferido, e integrarlas completamente.
- **Colaboración:** Permiten aprovechar la experiencia intelectual individual de todos los empleados y tenerla disponible para su utilización global. Los usuarios pueden crear y manejar sus propios contenidos.

- **Efectividad:** Permite que no se dejen asuntos pendientes y que se acaben las excusas de falta de información para llevar a cabo un proyecto cualquiera. Además cada departamento genera y mantiene su propia documentación así como los datos que le pertenecen.
- **Eficiencia:** Una Intranet elimina en porcentajes muy altos los métodos de trabajo tradicionales y en ocasiones poco eficientes como el teléfono, el fax o las pequeñas reuniones de pasillo.
- **Facilidad:** Con el simple requerimiento de saber manejar un navegador, cualquier usuario corporativo podrá trabajar con una Intranet. Con algo más de conocimientos, no excesivos, podrá dotarla de toda su información y compartirla con el resto de los empleados de la organización.
- **Flexibilidad:** El trazado de puesta en marcha de una Intranet es algo que puede comenzar con un nivel relativamente simple e incrementar las prestaciones según las necesidades y las posibilidades de la empresa. El adecuado mantenimiento y la actualización posterior juegan un papel fundamental en el buen desarrollo del proyecto que se verá culminado con la adaptación al nuevo medio de todos los usuarios que componen la compañía.
- **Participación:** Un miembro de la organización en la que se monta una Intranet aporta la información que ha conseguido y la pone a disposición de todos los demás, que a su vez la pueden mejorar o implementar sus propios datos.

- **Rendimiento:** Todo el material que puede estar impreso en un catálogo, manual o libro, se puede implementar sin mucho esfuerzo en una Intranet.

2.1.3. ESTRUCTURACION DE DATOS EN UNA INTRANET

Una página de la Intranet que se cree es simplemente un documento hecho en lenguaje HTML. Varias de estas páginas HTML vinculadas pueden formar un sitio Intranet.

En ocasiones la avalancha de información crea un caos de estructura que hace muy difícil llegar a la información deseada. Para lo cual se debe tomar en cuenta lo siguiente:

- En la estructura **debe facilitarse la búsqueda** de cualquier información o recurso que se encuentre en la red.
- El servidor debe gobernar todo el tráfico de datos. El programa servidor Web es el que **debe manejar las solicitudes y las transmisiones de datos** de manera que cualquier computadora pueda utilizarlos en cualquier momento.
- **Cada departamento debe generar y mantener su propia documentación.** Los documentos se indexan y organizan mientras se publican, y pueden administrarse desde el escritorio, dentro del departamento y de forma centralizada, en un solo lugar, facilitando con ello la tarea de localización.

- Los índices y jerarquías de exploración se deben crear y mantener con la mayor facilidad posible. Por eso el diseño debe ofrecer **una interfaz de navegación**.

2.1.4. SEGURIDADES EN UNA INTRANET

Las Intranets aportan un valor sin precedentes a la distribución de la información, la automatización de los grupos de trabajo y el acceso a la información corporativa; pero no podían ser todo ventajas. La facilidad de acceso a la información que permiten las Intranets supone un aumento del riesgo de robo, pérdida o corrupción de esa información que ponemos a disposición en ella. Y eso es precisamente la que desde la Intranet de una empresa se debe evitar, para que la información no esté a disposición de quien no deba conocerla. Para ello existen mecanismos de seguridad que no se deben olvidar.

- Si la Intranet de una empresa carece de los controles de acceso adecuados, supone una invitación al borrado accidental o a la modificación de documentos. Por lo cual **la política de seguridad es algo que nunca debe dejarse de lado**.
- Es necesaria **toda la seguridad de que se pueda disponer**. Debemos decidir quién tiene acceso a cada documento, cuándo y desde dónde.

- Primero debe considerarse **la seguridad física de cada ordenador** (claves, cerrojos, cerraduras cifradas, etc.). **Después la seguridad electrónica**, evitando poner los datos en disposición de personal no autorizado y protegiendo convenientemente las transmisiones.
- **Un cortafuegos** es una estrategia de defensa que se podemos considerar ideal. Este sistema permite restringir y controlar el tráfico de datos de la Intranet pudiendo anular la acción de los curiosos.
- No hay que olvidar la **encriptación**, asegura los datos en las transmisiones que se realizan de equipo a equipo. Existe un sistema denominado PGP, de utilización libre, especial para este tipo de métodos de salvaguarda de datos.
- La regla de oro es **mantener la Intranet al día** en cuestiones de seguridad. Esto es un tema complejo que cambia tan rápido como la propia tecnología informática.

2. 2. USUARIOS DE UNA INTRANET

La tecnología Intranet permite a usuarios de una empresa trabajar de forma más eficiente facilitándoles el acceso a la información que precisan. A un nivel muy básico, la Intranet es el lugar común donde se puede poner toda la información que pueda necesitar cualquiera de sus empleados para llevar a cabo con éxito su labor diaria [18] . Con el apoyo de una red local, la Intranet es un vehículo gracias al cual se

reducen los tiempos de búsqueda de datos y se coordinan proyectos de trabajo ya que permite archivar el trabajo electrónicamente y volverlo a encontrar de manera muy rápida.

El propio servidor de red de la LAN (*Red de Area Local*), puede ser el equipo encargado de manejar el tráfico de los datos en código HTML, depositados en su propio disco duro, para que mediante un navegador Web todos los usuarios puedan acceder a la información organizada como si de una Internet interna se tratase. Hay que tener en cuenta que existen varios niveles dentro de la Intranet, los cuales se corresponden al perfil de usuario:

- **Gestor de Sistemas Informáticos:** Se encargaría de diseñar la estructura informática de la organización, planificar y realizar instalaciones de sistemas operativos y aplicaciones muy específicas, programar aplicaciones, etc.
- **Gestor de Información:** Sus funciones serían la de crear el Sistema de Información, diseñar y mantener la estructura de Bases de Datos y servidores de Información, diseñar aplicaciones para la gestión de información, etc.
- **Usuario final:** Utiliza los recursos informáticos e informativos para el desarrollo de su trabajo, en conjunción con los miembros de la organización.

En lo referente al campo comercial, una Intranet tiene una gran ventaja, ya que el usuario potencial de está son las empresas y el entorno comercial. Algunos ejemplos del uso de la Intranet en las diferentes áreas de una empresa son:

- **Administración y Operaciones:** Independientemente del giro industrial, comercial o de servicios de la empresa, las áreas de Administración y Operaciones interactúan constantemente con todos los empleados lo que generalmente involucra una gran cantidad de papeleo para la realización de trámites, seguimiento de pedidos, proyectos especiales, etc., sobre los cuales es necesario mantener permanentemente informados a los empleados y ejecutivos involucrados.
- **Comunicación Interna:** Una de las primeras áreas de trabajo de una empresa en donde debe implementarse Intranet es en el área de Comunicación Corporativa ya que es un medio altamente efectivo y económico para la establecer una red de información permanentemente actualizada hacia todo el personal de una organización, tanto si se encuentra ubicado en una misma localidad como si se encuentra geográficamente disperso. A través de la Intranet se disemina fácil y rápidamente la información, se difunden las nuevas directrices de la organización y se distribuyen las ultimas versiones de los todos los documentos corporativos que los ejecutivos y empleados puedan necesitar.

- ***Finanzas y Jurídico:*** La Intranet se convierte en una eficiente herramienta de monitoreo del estado legal y financiero de las relaciones de la corporación con clientes, proveedores y empleados, permitiendo consultar en cualquier momento el estado que guardan cada una de esas relaciones, pagos pendientes, cuentas atrasadas, procesos legales, etc. Asimismo, a través del Web se pueden difundir rápida y eficientemente nuevos procesos y requerimientos hacia el interior de la organización.
- ***Area de Sistemas:*** El uso de Intranet en el área de Sistemas permite obtener un mejor aprovechamiento de sus recursos tecnológicos y mayor eficiencia en el suministro de soporte técnico a los usuarios. Colocando la información y recursos adecuados en la red, el personal del área puede centrarse en la solución de problemas críticos y la implementación de nuevos desarrollos en vez de tener que dedicar gran cantidad de tiempo en la atención individual de los usuarios proporcionándoles respuestas que, además, suelen ser rutinarias.
- ***Ventas y Mercadotecnia:*** Para el área comercial de la empresa la Intranet se constituye en un recurso invaluable a través del cual se distribuyen una gran variedad de documentos y material de ventas a los que pueden tener acceso inmediato sus agentes de ventas y personal relacionado tanto el que se encuentra ubicado en la misma localidad como el que se localiza en diferentes

sucursales o viajando y si se desea, se puede proveer acceso también a distribuidores, proveedores e incluso consumidores.

2.3. SERVIDORES (WORLD WIDE WEB)

A un servidor web se lo define como: *"Un programa que está permanentemente escuchando las peticiones de conexión de los clientes mediante el protocolo HTTP (HyperText Transfer Protocol)"* [20].

Funciona de la siguiente manera: si encuentra en su sistema de ficheros el documento HTML solicitado por el cliente, lo envía y cierra la conexión; en caso contrario, envía un código de error y cierra la conexión. También se ocupa de controlar los aspectos de seguridad, comprobando si el usuario tiene acceso a los documentos.

2.3.1. TIPOS DE SERVIDORES WEBS

Tenemos los siguientes:

- **Servidores HTTP de libre distribución y versiones Shareware:** Protegidos por derechos de autor, generalmente ofrecen todo lo que usted necesita para tener una Intranet operativa.

- **Servidores Comerciales:** De gama media incorporan herramientas de monitorización y mantenimiento del Web mientras que los de gama alta, implementan excelentes medidas de seguridad, recursos de criptografía para transacciones seguras y hasta enlaces con bancos de datos corporativos.

El **control de acceso** al servidor web puede ser de dos tipos. Normalmente se definen distintos *niveles de acceso* caracterizados por los permisos otorgados sobre la información contenida en el servidor. Este tipo de control es similar a la distribución de derechos para los usuarios de la red. Esto es lo que se llama filtrado de IP (**Internet Protocol**) o nombre de huésped, ya que algunas direcciones IP poseen los permisos necesarios para acceder a determinadas páginas en el servidor. Además, existe también un método de verificación en el ámbito de usuario o *acceso controlado por contraseña* a las páginas webs.

Una vez planificado y estructurado el contenido real, debe ser preparado para su **almacenamiento en la Web**. Esto significa que debe ser codificado con un lenguaje de programación de hipertexto o usar alguna herramienta automatizada diseñada para tal fin.

Es posible crear documentos con lenguaje HTML (**HyperText Markup Language**) directamente, emplear herramientas de traducción de documentos en otros formatos a HTML, utilizar un sistema automatizado de generación de código o usar un banco de datos de documentos existentes que ofrece una traducción HTML automatizada en

tiempo real para usuarios web. Entre los servidores web mayormente difundidos en el mundo tenemos (**Tabla 2.1**):

Tabla 2.1: Principales Servidores webs

Alibaba	AOLserver
AOLserver	Apache
Apache	Avenida
Avenida	Domino Go Webserver
GoAhead	Enterprise for NetWare
Jigsaw	First Class
Lotus Domino	Microsoft IIS v4.0
Microsoft IIS v5.0	NCSA HTTPd
Microsoft PWS	Netscape Enterprise
Microsoft Site Server	Netscape FastTrack
RapidSite	OmniHTTPd Pro
Roxen Challenger	Savant
Roxen Web Server	Servotec Internet Server
Sambar Server	SimpleServer:WWW
Stronghold	vqServer
Tcl Web Server	Web Commander
URL Live!	WebSite Pro
WebSTAR	Xitami
ZBServer	Zeus Web Server

La P.U.C.E.S.A. posee 3 tipos de servidores webs, los cuales son: *Netscape Enterprise Server* (SUN SOLARIS), *Microsoft Internet Server* (ITS/WINDOWS), *Apache Web Server* (LINUX)

2.3.2. POLITICAS PARA SERVIDORES WEBS

Para obtener la mejor difusión de información en un servidor web, se deben tomar en cuenta las necesidades prioritarias de una entidad. Hay dos consideraciones principales en la construcción de un Servidor Web:

- ¿Cuánto tráfico se espera utilizar?
- ¿Puede un sistema crecer mientras que las necesidades crecen?

La capacidad de un sistema debe corresponder con la cantidad de tráfico que se espera utilizar. Si se está ejecutando un servidor de Internet, la respuesta a las peticiones del cliente son cruciales; un servidor lento hace una impresión pobre. Hay que especificar las necesidades futuras y seleccionar un camino óptimo para incrementar la potencia y la rapidez del Servidor, pero para ello hay que iniciar planteándose las siguientes interrogantes:

a. ¿Que plataforma y sistema operativo se debería comprar?

Generalmente no existen sistemas operativos o plataformas que sean una mala opción para un Servidor Web, la elección debe basarse en las siguientes consideraciones:

- ¿Qué sistema operativo utiliza y goza actualmente?
- ¿Qué puede la empresa permitirse?

- ¿Qué otras clases de software se desea para que se ejecute las bases de datos en lo referente a lo comercial?

A continuación las plataformas de un Servidor web más utilizadas (**Tabla 2.2**)

Tabla 2.2: Plataformas de un servidor

FreeBSD Novell NetWare Red Hat Linux Windows NT Server 4.0	Mac OS X OpenLinux Sun Solaris Windows 2000 Server
---	---

b. Consideraciones para elegir hardware en un servidor web

Las consideraciones para elegir **Hardware** de un servidor web son: (Ver **Tabla 2.3**)

Tabla 2.3: Hardware para Servidores Web

Arquitectura	Intel , AMD, POWER PC
Tarjeta Madre	PCI/ISA
Controlador de Disco	SCSI-PCI, IDE
Discos	SCSI +CDROM SCSI
Dispositivos de almacenamiento	Tape Backup SCSI/ CD-WRITE
Tarjeta de Red	PCI 10/100 MPS
Memoria	Mínima 674 y optima 118
Sistema operativo de red	Novell Linux, NT ,Solaris

2.4. RED E INFORMACIÓN DE LA P.U.C.E.S.A.

Los servicios brindados por la P.U.C.E.S.A. se encuentran clasificados dentro de las siguientes categorías:

- Nivel Administrativo:
- Académico:
- Y Red Informática (**Ver Anexo A**)

CAPÍTULO III

3. METODOLOGÍA PARA EL DISEÑO DE PÁGINAS WEBS APLICADAS A ENTIDADES EDUCATIVAS

3.1. CREACIÓN DE PÁGINAS WEBS

Antes de crear una serie de páginas webs, es conveniente realizar un diseño previo en dónde se especifique la estructura que van a tener las páginas y el contenido de cada una de ellas. Este diseño estará condicionado por factores tales como el tipo y la cantidad de información que se quieren colocar en las páginas y el perfil de los visitantes de las páginas. Una vez realizado el diseño, se debe considerar tres alternativas a la hora de crear las páginas:

- Herramientas de creación de páginas web
- Lenguajes de programación
- Herramientas auxiliares

3.1.1. HERRAMIENTAS DE CREACIÓN DE PÁGINAS WEBS

Son herramientas diseñadas de manera específica para la construcción de páginas webs. Normalmente consisten en un entorno gráfico con una serie de menús y barras de herramientas a través de las cuales el usuario puede crear los distintos elementos de

la página web: textos, imágenes, tablas, listas, etc. Estas herramientas permiten crear páginas webs de una manera rápida y simple. Entre estas herramientas podemos citar las siguientes:

- **Editores de HTML:** Permiten introducir elementos HTML mediante una cómoda interfaz gráfica. Entre ellos se encuentran el *Composer* (Netscape), *FrontPage Express* (Microsoft) y el *Amaya* (Web Consortium).
- **Entornos de desarrollo Web:** Son herramientas más completas porque crean y mantienen sitios web completos con múltiples páginas enlazadas entre sí, como el *ColdFusion Studio* (Allaire), *Front Page* (Microsoft), *PageMill* (Adobe) y el *Dreamweaver* (Macromedia).
- **Salida en formato HTML de aplicaciones estándar:** Muchas aplicaciones permiten actualmente archivar sus documentos en formato HTML. De esta manera se pueden crear páginas web con un simple procesador de textos o una hoja de cálculo. Entre estas aplicaciones podemos citar paquetes integrados (suites) como *Office* (Microsoft), programas gráficos como *CorelDraw* (Corel) o *Photoshope* (Adobe) y de autoedición como *PageMaker* (Adobe).

3.1.2. LENGUAJES DE PROGRAMACIÓN

El lenguaje en el que están escritas las páginas web es el **HTML**. Es un lenguaje bastante simple, por lo que una forma de crear páginas web consiste en escribir

directamente su código HTML, utilizando para ello un editor de texto como, por ejemplo, el *Wordpad* (editor de texto incluido en el sistema operativo Windows). El escribir directamente el código HTML es una alternativa a tener en cuenta para la creación de páginas web ya que permite colocar cualquier tipo de elemento en la página con un mayor control sobre el efecto final que cualquier herramienta de creación. Este método puede utilizarse de forma independiente o como complemento de alguna de las herramientas mencionadas en el apartado anterior para aquellos elementos que no estén contemplados en dichas herramientas.

Además del lenguaje HTML, también se utilizan otros lenguajes para la construcción de páginas webs, como: **ASP (*Active Server Pages*)**, **Javascript**, **Java**, **Applets**, etc. Con ellos se pueden conseguir páginas web interactivas y ofrecer contenidos más complejos, aunque también resulta más compleja la creación de las páginas.

3.1.3. HERRAMIENTAS AUXILIARES

Además de las herramientas mencionadas anteriormente, existen otras herramientas que nos pueden ayudar en la preparación de la información que se va a colocar en la página web. Entre ellas se pueden citar las siguientes:

- **Analizadores de vínculos**, para comprobar los enlaces entre las páginas, muy útil cuando su número es elevado.

- **Editores gráficos**, para la creación de iconos e imágenes o el retoque de fotografías (*Microsoft Paint, PaintShop Pro, Adobe Photoshop, Corel PhotoPaint*).
- **Editores de mapas**, para crear mapas sensibles (*Mapedit*).
- **Editores de gráficos animados**, para animaciones (*GIF Construction Set*).
- **Convertidores de formatos gráficos y de texto**, para incorporar a un documento HTML documentos realizados con otros programas y almacenados en diferentes formatos (*Graphics Workshop*).

3.2. DISEÑO DE SITIOS WEBS INTERACTIVOS

El proceso de diseño relaciona diversos factores que deben ser tomados en cuenta a la hora de crear un sitio web interactivo, dentro de los principales factores tenemos los siguientes:

a. Propósito:

- Proporcionar una interfaz de usuario para un servicio
- Vender productos o servicios
- Presentar información a una audiencia interesada
- Establecer las intenciones claramente cuando se inicie el proceso, y tenerlo en cuenta mientras evoluciona el producto

- Proporcionar una colección de enlaces

b. Audiencia:

- Ancho de banda de la conexión a Internet
- Antes de iniciar el proceso de diseño, intentar definir la audiencia
- Contestar las preguntas “¿Quién usará las páginas?”, “¿Qué problema esta intentado resolver el usuario?”
- Sopesar cuidadosamente las ventajas y desventajas de usar las características de un visor en particular, e intentar hacer sus documentos útiles y utilizables para un amplio número de lectores

c. Enlaces:

- Escribir sobre su tema como si no hubiera enlaces en el texto
- Seleccionar palabras o frases significativas para los enlaces
- Seleccionar un ancho apropiado para el texto del enlace
- Crear el contexto para un enlace
- Seleccionar sus enlaces para que den soporte a su contenido y estructure el concepto
- Intentar coincidir el texto del enlace que el usuario selecciona con el título de la página resultante

- Iluminar el texto que es diferente
- No cambiar el color del texto de los enlaces

d. Largo de la página:

- Para presentaciones que deben atraer la atención de la gente, no hacer la página más larga que la ventana
- Algunos contenidos deben ser presentados en una pantalla, ya que el usuario no puede saber si hay más que ver debajo del fin de la ventana
- Si se necesita presentar segmentos de información cortos y claros, se debe intentar mantener las páginas cortas para que la gente no se pierda de cosas que están al final de la página
- Si las páginas presentan texto que la gente querrá leer completo, es correcto usar texto largo
- Como una regla general, intentar hacer la mayoría de las páginas no más largas que una y media pantalla de texto
- Para imprimir o guardar, proporcionar un enlace al documento completo
- Usar páginas cortas para hacer el sitio más manejable

e. Gráficas:

- Usar gráficas relacionadas al contenido de tu página

- Limitar las grandes imágenes que son usadas únicamente como atractivo visual
- Conservar el tamaño total de todas las imágenes usadas en una página en menos de 30K
- Usar los trucos disponibles en la tecnología para minimizar el tiempo de acceso al contenido
- Advertir a la audiencia si un enlace conduce a una imagen muy grande
- Minimizar el número de colores que usa una imagen e incluir texto alternativo.
- Usar imágenes transparentes para una mejor integración con el documento
- No usar gráficas referenciadas desde otro sitio
- Usar gráficas de viñetas con un propósito, no porque luzcan novedosas
- Usar en forma discriminada las barras gráficas
- Usar un conjunto pequeño de viñetas o gráficas en forma repetida, más que usar un gran número solamente una vez
- Revisar las imágenes en varias combinaciones de hardware y visores

f. Navegación:

- Si se usan gráficas como botones de navegación, usar adicionalmente etiquetas de texto descriptivas
- Proporcionar texto alternativo para los botones gráficas de navegación
- Si es apropiado, agregar una breve tabla de contenido al inicio de la página
- Colocar un encabezado en cada página

- Seleccionar un título que refleje el contenido de la página
- Proporcionar un mecanismo de búsqueda
- Considerar duplicar los encabezados de navegación al final de las páginas

g. Mapas de imágenes:

- Delimitar claramente las áreas que son enlaces en mapa
- Si es posible, hacer que las áreas que se pueden seleccionar parezcan botones
- Proporcionar enlaces de texto adicionales al mapa de imagen

h. Seguridad:

- No publicar información registrada
- Conservar información confidencial de la compañía detrás de un Firewall
(*Muro de seguridad*)
- Cuidado con los robots (*Agentes de búsqueda*)

i. Calidad:

- Verificar cada enlace
- Verificar la sintaxis y construcción en HTML
- Conservar las páginas actualizadas

- Verificar la ortografía
- Fechar las páginas
- Colocar un enlace a un mecanismo de comentarios en todas las páginas
- Responder a la gente que hace comentarios de las páginas

j. Cortesía:

- No insultar u ofender a la gente
- No publicar información registrada sin el permiso del autor
- Cuidado con el uso de marcas
- No publicar enlaces a otra página a menos que el autor desee ser publicitado

k. Contenido:

- Colocar tanto contenido al inicio de la de jerarquía como sea posible
- Proporcionar contenido útil en cada página vista por tu audiencia
- Proporcionar información que haga que los usuarios coloquen la página en sus marcadores
- Proporcionar enlaces en el contexto para satisfacer las necesidades de la audiencia
- Proporcionar enlaces a la naturaleza dinámica del contenido
- No asumir que todos los usuarios usarán el mismo visor y características

I. Ventas:

- Minimizar el esfuerzo requerido para aprender sobre el producto
- Optimizar el uso de páginas cortas
- Proporcionar una forma sencilla de obtener información
- Proporcionar una ruta para hacer una compra
- Pensarlo dos veces antes de ofrecer enlaces a sitios de competidores

3.3. INTRODUCCION A LAS WEBS DINAMICAS

En sus inicios las páginas webs se comportaban de forma estática, es decir una vez cargadas en la ventana del navegador, la información mostrada permanecía inalterable. Esto no suponía ningún inconveniente para el uso al que estaban destinadas que era básicamente el de compartir información a través de la red. Sin embargo; a medida que fueron surgiendo nuevas aplicaciones para las páginas webs surgió también la necesidad de dotarlas de un mayor dinamismo, permitiendo que su contenido se modificara de forma autónoma o como resultado de la interacción con el usuario.

Es así, que el usuario no se limita a buscar y encontrar la información de un modo pasivo, sin intervenir, por lo tanto la mayor innovación de las páginas webs se traduce en una sola palabra "*Interactividad*". Dentro de las aplicaciones mayormente utilizadas de las páginas webs dinámicas tenemos las siguientes:

- Actualizar el contenido de una base de datos.
- Mostrar el contenido de una base de datos, basándose en la información que solicita un usuario a través de un formulario de web.
- Mejorar la interacción entre el usuario y el sitio web.
- Generar páginas webs de contenido estático.

A una Página Web Dinámica, se la define como [47]: *"Se conoce con el nombre de página web dinámica a aquella, cuyo contenido se genera a partir de lo que un usuario introduce en un web o formulario. El contenido de la página no está incluido en un archivo HTML (HyperText Markup Language) como en el caso de las páginas webs estáticas"*.

3.4. APLICACIONES USUARIO-SERVIDOR

El concepto **usuario-servidor** surge de la necesidad de distribuir carga de procesamiento entre varios procesadores a fin de mejorar el tiempo de respuesta de las aplicaciones. El concepto involucra los siguiente elementos:

- **Servidor:** Aplicación que se encarga de procesar la petición que recibe del cliente. Una vez procesada la solicitud, se envía al cliente, quién la procesa a fin de mostrarla en un formato compresible para el usuario.

- **Cliente:** Aplicación que se encarga de formar una solicitud válida para enviarla al servidor.
- **Conexión entre el cliente y el servidor:** Medio que permite la comunicación entre el cliente y el servidor.
- Para que cliente y servidor se entiendan deben tener un lenguaje en común, un **protocolo.**

En la **Figura 3.1**, se muestra las principales aplicaciones usuario-servidor aptas para el desarrollo de portales webs, las cuales se encuentran clasificados dentro de dos categorías que son las siguientes:

- Páginas con aplicaciones ejecutadas en el cliente.
- Páginas con aplicaciones ejecutadas en el servidor.

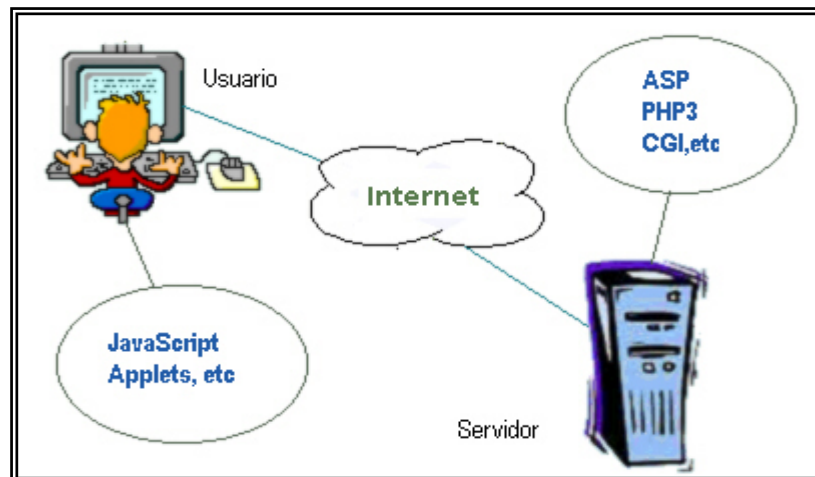


Figura 3.1: Aplicaciones Usuario-Servidor

3.4.1. APLICACIONES EJECUTADAS EN EL CLIENTE.

Estas páginas webs se encuentran en el navegador del usuario. Podemos nombrar como aplicaciones que funcionan en el cliente a: JavaScript, Applets (Java) y todos los plug-ins o ActiveX que nuestro navegador posea, como cuando se ve una animación en Flash, un mundo virtual VRML (*lenguaje modelado de realidad virtual*). A continuación se realizará una breve descripción de los más importantes:

3.4.1.1. INTRODUCCIÓN A JAVASCRIPT

Netscape tendió un puente entre las tecnologías HTML y Java; para ello se puso a trabajar en un nuevo lenguaje de órdenes que pudiera ocupar el vacío entre éstos y que, a la vez, fuera lo suficientemente potente como para enlazar ambas tecnologías. Así nace LiveScript, el cual fue introducido de inmediato en el navegador más popular de Netscape, para conseguir que la comunidad de Internet lo adoptara cuanto antes. Poco después Netscape y Sun se unieron para ayudar a que LiveScript se estableciera como el lenguaje estándar de Internet para la escritura de órdenes basada en la web. Pero, LiveScript tenía una sintaxis muy similar a la de Java, por lo que ambas compañías decidieron rebautizar su nuevo producto para que pudiera ser identificado mejor, y lo llamaron **JavaScript**.

JavaScript fue creado como un lenguaje de órdenes, fácil de utilizar, abierto, de plataforma cruzada, capaz de enlazar objetos y recursos propios tanto de HTML como

de Java, tiene la particularidad de haber sido diseñado para integrarse con HTML, además ofrece su capacidad de reducir el tráfico de red, permitiendo la realización local de las tareas más simples. Es decir, en lugar de encomendar esas tareas al servidor y que este pase los resultados al navegador, el navegador puede realizar algunas de esas tareas a nivel local, con lo que el usuario, además, obtiene sus respuestas en un tiempo más corto.

A JavaScript se lo define como [46]: *"Un lenguaje de scripts, compacto basado en objetos, interpretado en el cliente por el navegador al momento de cargarse la página, cuyo código se incluye directamente en el mismo documento HTML. Es multiplataforma, es decir, que el código se puede ejecutar en cualquier máquina (Windows, Machintosh. etc.), lo único que se necesita es un visor web "*.

Para que el navegador reconozca que un archivo contiene funciones escritas en JavaScript, dichas funciones se han de colocar entre dos etiquetas especiales "**<script> </script>**". Entre estas dos etiquetas se colocaran las funciones que luego el navegador reconocerá cuando cargue la página, las cuales tienen atributos como **LANGUAJE="JavaScript"**.

Dentro de las principales **aplicaciones de JavaScript** tenemos: realización de cálculos en tiempo real, responder a eventos locales dentro de la página, validación de formularios dentro de una página, personalización de la página por el usuario, inclusión de datos del propio sistema (hora y fecha), animaciones, etc.

3.4.1.2. INTRODUCCIÓN A LOS APPLETS

Java es un lenguaje de programación orientado a objetos diseñado para una rápida ejecución y protección contra errores de tipos. Fue desarrollado por la compañía Sun Microsystems, basándose en el lenguaje C++ aunque es también un lenguaje de carácter general. Java, cuya denominación original fue Oak en 1991, fue diseñado para programar dispositivos electrónicos de consumo.

Java se parece a JavaScript porque es multiplataforma; pero de éste los programas Java que se ejecutan en el web denominados **Applets**, no están incluidos dentro de la página sino que viajan por separado y el resultado de su ejecución en la máquina del usuario se presenta en la página. Su principal característica es la de ser independiente de cualquier plataforma, lo que le hace ser muy adecuado para ser utilizado en Internet, ya que puede ejecutarse en cualquier ordenador que tenga un navegador compatible con Java. Esto quiere decir que el mismo programa se puede utilizar, sin ningún cambio, en un PC, Mac o máquina Unix. Esto es así porque un programa Java no corre directamente en el ordenador, sino que lo hace en una máquina virtual (Máquina Virtual Java) quedando, además, confinado dentro de ella, lo que hace que sea un lenguaje seguro, ya que no puede acceder a otros recursos de nuestro ordenador. Con el lenguaje de programación Java es posible incrustar una aplicación multiplataforma dentro de una página Web con los llamados applets. Es necesario utilizar un navegador o browser compatible con Java como Sun, Hot_Java, Netscape 2.x, Internet Explorer 3.0 o superiores.

A los Applets, se les definen como [40]: "*Pequeños programas ejecutables escritos en lenguaje Java, que podemos colocar en nuestro servidor, junto con el resto de ficheros que componen un sitio del Web (documentos HTML, ficheros de imagen, sonido, etc.)*".

Si en una página hemos incrustado un applet, cuando un usuario cargue la página, recibirá del servidor dicho applet (al igual que ocurre con una imagen o sonido), y se ejecutará en su navegador. Pero para que esto ocurra así, es condición indispensable que el usuario esté utilizando un navegador compatible con Java.

Para colocar un applet en una página web dinámica, es necesario tener el **programa** del applet, los cuales tienen extensión *.class*, bajo el siguiente formato: "`<applet code =nombre del applet> </applet>`"

Hay que tomar en cuenta que estos programas tienen la extensión *.class* y, respetar escrupulosamente la disposición de las mayúsculas y minúsculas en su nombre (por ejemplo *SineText.class* y no *sinetext.class*).

Dentro de las principales **aplicaciones de los Applets** tenemos: Se pueden conseguir efectos visuales y sonoros (*incluso ambos a la vez*), textos en movimiento, utilidades (*por ejemplo los relojes*), pequeños programas educativos, juegos interactivos, presentaciones multimedia, etc. En definitiva, cualquier cosa que se pueda conseguir

con un programa pequeño, claro está que no hay ninguna limitación teórica en el tamaño de estos programas. La razón de que sean pequeños es la misma por la que no es razonable colocar en una página gigantescos ficheros de imagen o sonido, es decir, no hay que alargar en exceso su tiempo de carga.

3.4.2. APLICACIONES EJECUTADAS EN EL SERVIDOR

La programación en el servidor es mucho más potente, ya que no estamos dependiendo del poder de procesamiento. La norma CGI, fue la primera tecnología en aparecer, permitiendo que un programa realizado en cualquier lenguaje (C/C++, Pascal, Basic, etc.) pudiera transformarse en un programa para la web. Sin embargo, el lenguaje que mayor aceptación tuvo dentro de esta plataforma fue el Perl. En la actualidad han ido apareciendo en el mercado nuevas tecnologías mayormente utilizadas por los programadores, tal es el caso del ASP y el PHP.

Cada uno de estos tipos tiene sus ventajas y desventajas, algunos ocasionan una mayor carga al servidor, aumentan el tiempo de espera, páginas más grandes, el código puede ser copiado, no se tiene control del funcionamiento, etc.; y a la hora de programar hay que tener en cuenta esta clasificación para algunas situaciones. Una de las grandes ventajas de la programación en el servidor es que es casi invisible a los ojos del usuario. A continuación se realizará una breve descripción de las aplicaciones anteriormente citadas:

3.4.2.1. INTRODUCCIÓN AL COMMON GATEWAY INTERFACE (CGI)

La plataforma WWW ha evolucionado progresivamente y pasó de ser una aglomeración de documentos con información estática a un ambiente donde se pueden implementar potentes aplicaciones cliente-servidor accesibles desde un cliente web o browser como el Netscape Navigator o el Microsoft Internet Explorer. La tecnología pionera en esta rama fue **CGI**.

El **CGI** (*Por sus siglas en inglés "Common Gateway Interface"*), cambió la forma de manipular la información en el web. En sí, es un método para la transmisión de información hacia un compilador instalado en el servidor. Su función principal es la de añadir una mayor interacción a los documentos web que por medio del HTML se presentan de forma estática. Esta tecnología tiene la ventaja de correr en el servidor cuando el usuario lo solicita por lo que es dependiente del servidor y no de la computadora del usuario.

Según la definición de la NCSA (*National Center for Supercomputing Applications*), el CGI es [41]: *"Un documento HTML es estático, lo que significa que existe en un estado constante; es un archivo de texto que no cambia. Un script CGI por otro lado, es ejecutado en tiempo real, lo que permite que regrese información dinámica."*

Los programas que maneja el **CGI** pueden estar compilados en diferentes lenguajes de programación. El más popular para el desarrollo de contenidos Web es el lenguaje Perl de distribución gratuita, aunque también podemos mencionar: C, C++ y Java.

El funcionamiento de esta tecnología es muy sencillo. Los scripts residen en el servidor, donde son llamados, ejecutados y regresan información de vuelta al usuario.

Hay que tomar muy en cuenta que existen dos formas de enviar información; siendo estas por medio de **GET** y **POST**.

a. GET: Envía la información dentro del URL separando los campos con signos de interrogación '?' antes de la información, como por ejemplo:

<http://www.maestrosdelweb.com/cgi-bin/ejemplo.cgi?nombre=Cristian&cargo=Webmaster>

Esta forma presenta varias desventajas, ya que no permite manejar grandes cantidades de información y por ser una dirección, los Caches de los navegadores pueden guardar los resultados, lo que dificulta el poder acceder nuevamente a la aplicación, pero simplifica el uso de los scripts con solo utilizar una dirección URL.

b. POST: El cual envía la información directamente al servidor, haciéndolo invisible en el URL y permitiendo cualquier cantidad de información, como el envío de archivos.

Las diferencias entre **GET** y **POST** son primordiales para adaptar una aplicación y hacerla funcionar.

Dentro de las **aplicaciones del CGI** tenemos: contadores, motores de búsquedas, formularios, generadores de email automático, foros de discusión, chats, comercio electrónico, rotadores y mapas de imágenes, juegos en línea, tratamiento de formularios introducidos en el cliente, consulta y/o modificación de bases de datos remotas, estadísticas de acceso a una determinada página Web, animaciones con gráficos, etc.

3.4.2.2. INTRODUCCIÓN AL HYPERTEXT PREPROCESSOR (PHP)

El PHP, es un lenguaje interpretado de alto nivel en páginas HTML y ejecutado en el servidor. Nace como una modificación a Perl escrita por **Rasmus Lerdorf**, siendo su función la de mantener un control sobre quien visitaba su curriculum en su web. En los siguientes tres años, se fue convirtiendo en lo que se conoce como PHP/FI 2.0. Esta forma de programar abarcó a muchos usuarios, pero no llenó las expectativas, hasta que **Zeev Surasky** y **Andi Gutmans** le incluyeron nuevas características (1997), que dio por resultado el PHP 3.0. La versión 4 es la más reciente.

Según la definición del FAQ de PHP.net [42]: *"El PHP es un lenguaje de script incrustado dentro del HTML. La mayor parte de su sintaxis ha sido tomada de C,*

Java y Perl con algunas características específicas de sí mismo. La meta del lenguaje es permitir rápidamente a los desarrolladores la generación dinámica de páginas”.

Dentro de las **aplicaciones del PHP** podemos mencionar las siguientes: básicamente se puede hacer todo lo que se hace con el CGI, procesamiento de información en formularios, foros de discusión, manipulación de cookies y páginas dinámicas. Las aplicaciones dinámicas para el Web son frecuentes en los sitios comerciales (e-commerce), donde el contenido visualizado se genera de la información alcanza en una base de datos u otra fuente externa.

Una de sus características más potentes es su soporte para gran cantidad de bases de datos, entre las cuales se pueden mencionarse a InterBase, mSQL, MySQL, Oracle, Informix, PostgreSQL, etc. **PHP** ofrece una solución simple y universal para las paginaciones dinámicas del Web de fácil programación. Su diseño elegante lo hace perceptiblemente más fácil de mantener y ponerse al día con el código. Como producto de código abierto, **PHP** goza de la ayuda de un gran grupo de programadores, permitiendo que los fallos de funcionamiento se encuentren y se reparan rápidamente. El código se pone al día continuamente con mejoras y extensiones de lenguaje para ampliar las capacidades de PHP. El **PHP** es la opción natural para los programadores en máquinas con Linux que ejecutan servidores web con Apache, pero funciona igualmente bien en cualquier otra plataforma de UNIX o de Windows, con el software de Netscape o del web server de Microsoft. PHP también

utiliza las sesiones de HTTP, conectividad de Java, expresiones regulares, LDAP, SNMP, IMAP, protocolos de COM (bajo Windows).

3.4.2.3. INTRODUCCIÓN A LAS ACTIVE SERVER PAGES (ASP)

Active Server Pages (ASP), es una tecnología propietaria de Microsoft. Se trata básicamente de un lenguaje de tratamiento de textos (scripts), basado en Basic, y que se denomina VBScript (*Visual Basic Script*) o JavaScript de Netscape. Se utiliza casi exclusivamente en los servidores Web de Microsoft (*Internet Information Server* y *Personal Web Server*). Los *scripts* ASP se ejecutan, por lo tanto, en el servidor y puede utilizarse conjuntamente con HTML y Javascript para realizar tareas interactivas y en tiempo real con el cliente.

Este servicio es soportado por los siguientes servidores [Microsoft]:

- Microsoft *Internet Information Server* 3.0 para Windows NT *Server*.
- Microsoft *Peer Web Services* para Windows NT *Workstation* .
- Microsoft *Personal Web Server* para Windows 95/98.

Según la definición de Microsoft [43]: "*Las Active Server Pages son un ambiente de aplicación abierto y gratuito en el que se puede combinar código HTML, scripts y componentes ActiveX (Objetos de tecnología de Microsoft) del servidor para crear soluciones dinámicas y poderosas para el web*".

3.4.2.3.1. DECLARACIÓN DEL LENGUAJE

Para insertar instrucciones ASP dentro del código HTML se incluye encerrado entre "<% %>". Estos comandos son los que procesa el servidor antes de enviar la página al navegador. Como ocurre en otros lenguajes de programación, en ASP existe una sentencia de declaración opcional del lenguaje a utilizar.

```
<%@ LANGUAGE="VBScript" %>
```

Esta declaración se pone al principio del archivo, antes de cualquier otra expresión.

Un ASP *script* comienza a ejecutarse cuando el cliente solicita un fichero .asp. Inmediatamente el servidor *web* llama a la ISAPI que da servicio a las ASP, e interpreta el fichero y devuelve la página HTML resultante al *browser*. También tiene la ventaja principal de las tecnologías del lado del servidor que radica en la seguridad que tiene el programador sobre su código, ya que éste se encuentra únicamente en los archivos del servidor que al ser solicitado a través del web, es ejecutado, por lo que los usuarios no tienen acceso más que a la página resultante en su navegador.

Para explicar mejor el funcionamiento del ASP se presenta la siguiente gráfica:



Figura 3.1: Funcionamiento del ASP

Dentro del ASP se implementaron cinco objetos que facilitan la programación de los *scripts*. Éstos son:

- **Session:** En este objeto se almacenan valores que pueden ser accedidos por todas las páginas que estén dentro de una sesión. Una sesión comienza cuando el usuario accede por primera vez al directorio donde se encuentran los ficheros .asp y solicita uno de éstos. Este objeto es muy útil para guardar valores comunes a varias páginas como por ejemplo el nombre del usuario, el tipo de gráficos que soporta su hardware, entre otras cosas.
- **Application:** Brinda la posibilidad de compartir información entre todos los usuarios que se encuentran dentro de una sesión. Tanto **Application** como **Session** pueden guardar números, cadenas, arreglos y controles ActiveX.

- **Request:** Permite el acceso a los datos mandados por el usuario desde una *forma* del HTML.
- **Response:** Es el encargado de escribir información en la página que se desea formar dinámicamente.
- **Server:** Brinda la posibilidad de acceder a métodos y propiedades del servidor.

El ASP tiene una serie de controles ActiveX cuyas interfaces permiten acceder a bases de datos y conocer las características del *browser* que está accediendo en ese momento, entre otras funciones. Estos también pueden ser guardados en objetos del sistema como **Session**.

Existe un archivo especial que se coloca en el directorio ASP nombrado *Global.asa* donde se definen funciones que se ejecutan bajo distintas condiciones:

- **Application_OnStart:** Cuando comienza el servicio www. Los objetos que se crean en esta función existen durante toda el período de tiempo que el servidor está funcionando.
- **Application_OnEnd:** Al terminar el servicio www.
- **Session_OnStart:** Cada vez que comienza una sesión. Los objetos que se crean en esta función existen durante toda la sesión.
- **Session_OnEnd:** Al terminar cada sesión.

3.4.2.3.2. APLICACIONES DE LAS PÁGINAS ASP

- La facilidad para conectar con una base de datos y extraer datos de la misma dinámicamente visualizándolos en el navegador es la utilidad más practicada de las páginas ASP.
- Puede conectarse a gestores de Base de datos SQL, Access, Oracle, o cualquier otro motor que disponga de driver ODBC (*Open Database Connectivity*).
- Comercio electrónico, portales, sedes personalizables y todas aquellas aplicaciones en las que el protagonista es la información dinámica.
- Envío de correo electrónico, creación dinámica de gráficos, etc.

Básicamente, muchas cosas que se realizan con el CGI (*Common Gateway Interface*) se pueden realizar con el ASP, puesto que resulta tan eficiente como escribir código directamente a la interfaz de la aplicación del servidor, además, toma como ventaja la arquitectura multitareas ya que el ASP corre como un servicio en el servidor, mientras que el CGI depende de un compilador.

3.4.2.3.3. REQUERIMIENTOS

Para procesar una página ASP no existe ninguna restricción especial en el lado del cliente, por lo que es indiferente la utilización del navegador Internet Explorer o Netscape Communicator. Sin embargo, en el lado del servidor, es necesario un servidor Web de Microsoft. Se utiliza el archivo ASP.DLL para interpretar el código, siendo el

servidor más extendido *Internet Information Server* (IIS). El IIS es una aplicación gratuita que puede conseguirse en el Option Pack del NT.

Estos son los servidores de contenidos ASP posibles para plataformas Microsoft

- Internet Information Server 3.0 o superior (para sistema operativo NT 4.5x o superior)
- Personal Web Server (para Windows 95 y Windows 98)

Para plataformas Unix es necesario añadir un software que actúe de intérprete siendo algunos de los más conocidos: Chilisoft e Instant ASP.

La mayoría de proveedores de Hosting pagado con plataformas NT tienen acceso a esta tecnología en sus servidores. El código puede ser trabajado en cualquier editor HTML o de texto. Existen en el mercado varias herramientas para trabajar profesionalmente el ASP en modo visual como lo son: DreamWeaver (*Macromedia*), Drumbeat 2000 y el Visual Interdev de Microsoft.

3.4.2.3.4. HERRAMIENTAS

ASP, VBScript y Javascript son lenguajes de programación comunes, luego su sintaxis es implementada en código ASCII, por lo que para poder crear, editar y modificar dicho código, sólo es necesario utilizar un simple y común editor de textos, como

puede ser el "edit" del *DOS*, el "Notepad" o el "Wordpad" de los entornos *Windows*, o cualquiera de los múltiples editores de texto que existen en los entornos Linux (Emacs, vi, joe, jed, etc.), así como en los *Mac*.

Macromedia, ha tenido la referencia de crear un editor profesional para la creación y administración de sitios y páginas Webs, denominado *UltraDev*; el mismo que incorpora herramientas de diseño de páginas y administración de sitios de *Dreamweaver*. Además, *UltraDev* puede crear aplicaciones basadas tanto en tecnologías *Active Server Pages* (ASP), ColdFusion o *JavaServer Pages* (JSP).

3.4.2.3.5. INTRODUCCIÓN A LAS COOKIES (GALLETAS) CON ASP

Las cookies son el mecanismo que nos permite **guardar información relativa a un usuario a lo largo de sus distintos accesos a nuestras páginas** [45]. Se almacenan en los equipos de los clientes, esto hay que tenerlo en cuenta por las posibles faltas de integridad de datos que pudieran ocurrir. ASP implementa la posibilidad de usar cookies para crear o destruir información que se almacena en los equipos de los clientes.

Permite integrar funcionalidades como: Personalización de opciones de cliente, personalización en función de las características del cliente, cestas de compra, etc. Las cookies se transmiten en las cabeceras cuando se realiza la comunicación http y es el

navegador el encargado de almacenarlas. Se implementan como una colección y se usan mediante los objetos integrados **Request** y **Response**.

Se debe poner la caducidad de las cookies de otro modo caducarían inmediatamente después de haberse creado. Es importante saber que las cookies tienen una duración igual a la sesión, es decir, a menos que lo especifiquemos, el archivo texto generado se borrará desde el momento en que el usuario haya abandonado el sitio por un tiempo prolongado (generalmente unos 20 minutos) o que el navegador haya sido cerrado. Podemos arreglar este supuesto inconveniente mediante la propiedad **Expires** (*Establece el día de caducidad de una cookie*). Existen dos métodos que se pueden usar para poner la caducidad de las cookies:

- Poner la fecha exacta en que va a expirar, en este caso va a expirar el primero de enero del 2010:

```
<% Response.Cookies("nombre_de_la_cookie").Expires=#January 01, 2010# %>
```
- Poner la cantidad de días que la Cookie va a estar activa apartir de que se crea, en este caso 5 días:

```
<% Response.Cookies("nombre_de_la_cookie")=Date+5
```

Para **escribir una Cookie**: El valor de la cookie puede ser una variable, un numero o una cadena delimitada por comillas. Ejemplos:

```
<% Response.Cookies("nombre_de_la_cookie")=Value %>
```

En la siguiente línea se creará una cookie con el nombre de "visitante" y con el valor "juan": `<% Response.Cookies("visitante")="juan" %>`

En la siguiente línea se creará una cookie con el nombre de "visitante" y el valor se tomará de una forma: `<% Response.Cookies("visitante")=Request.form("nombre") %>`

Para **leer las cookies**, nada más fácil que usando el objeto Request de la siguiente forma: `<%Request.Cookies("nombre_de_la_cookie") %>`

Es común que el valor de una cookie se mande a una variable, en el siguiente ejemplo se le asigna el valor de la cookie "visitante" a una variable llamada "var":

```
<% var=Request.Cookies("visitante") %>
```

A lo largo de este capítulo se han estudiado varias tecnologías y herramientas aplicadas al desarrollo de proyectos webs, las mismas que serán seleccionadas de acuerdo a las diferentes necesidades de cada proyecto web.

En el caso particular de ésta tesis, se ha creído conveniente utilizar la tecnología ASP (*Active Server Pages*), debido a que cubre las necesidades que implican en el desarrollo del Portal de Servicios Académicos y Administrativos para la P.U.C.E.S.A.

CAPÍTULO IV

4. COMERCIO ELECTRONICO APLICADO A PORTALES DE SERVICIOS ACADEMICOS Y ADMINISTRATIVOS

4.1. INTRODUCCIÓN

La formidable revolución que se está produciendo en la actualidad con el Comercio Electrónico, es la consecuencia de la aceptación masiva que ha tenido el fenómeno de Internet como medio de comunicación rápido y barato entre grupos muy amplios de la población y las empresas. Dada la globalidad y la facilidad de acceso a las redes telemáticas en las que se basa, también puede constituir una eficaz herramienta para reducir desequilibrios regionales y un instrumento clave de competitividad en cualquier campo.

La nueva economía del Internet denominado Comercio Electrónico ha logrado posesionarse vertiginosamente en la economía digital, es así que se ha convertido en una verdadera estrategia para incrementar y potenciar las capacidades de un ente empresarial y por ende conseguir un rubro significativo para la economía de cada país. No obstante, el Comercio Electrónico también se ha extendido a otros campos diferentes del empresarial, tal es el caso que en el campo educacional se pueden realizar transacciones electrónicas en beneficio de la entidad educativa. Esta tecnología, cubre las preocupaciones del comprador (*mayor empleo de tiempo, realización de las compras en un horario determinado, selección limitada de*

productos y servicios, etc.) y las del vendedor (*Necesidad de capital y recursos, coste de las operaciones en aumento, presión mayor de la competencia, etc.*).

4.2. FUNDAMENTOS DEL COMERCIO ELECTRÓNICO

Actualmente, existen muchas acepciones de cómo definir el Comercio Electrónico, una de las primeras que se creó en 1992, constituye la más acertada; pero que no por antigua ha perdido vigencia sino más bien lo contrario [34]. "*El Comercio Electrónico consiste en la utilización de la Informática y las telecomunicaciones para canalizar los flujos de información y transacciones de negocio existentes entre una empresa y sus interlocutores de negocio habituales (clientes, proveedores, entidades financieras, transportistas, etc.)*".

En un precepto amplio, el comercio electrónico es reconocido como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet, por lo que, el comercio electrónico no sólo incluye la compra y venta electrónica de bienes, información o servicios, sino también el uso de *la Red* para actividades anteriores o posteriores a la venta, como son:

- Publicidad.
- Búsqueda de información sobre productos, proveedores, etc.
- Negociación entre comprador - vendedor sobre precios, forma de entrega, etc.

- Atención al cliente antes y después de la venta
- Cumplimiento de trámites administrativos relacionados con la actividad comercial
- Colaboración entre empresas con negocios comunes (*a largo plazo o sólo de forma circunstancial*)

La **Figura 4.1** ilustra un posible camino de implantación gradual de comercio electrónico, desde el caso más simple de la publicidad no interactiva a través de Internet, hasta el caso completo donde todos los pasos, incluido el pago, se hacen de forma electrónica.

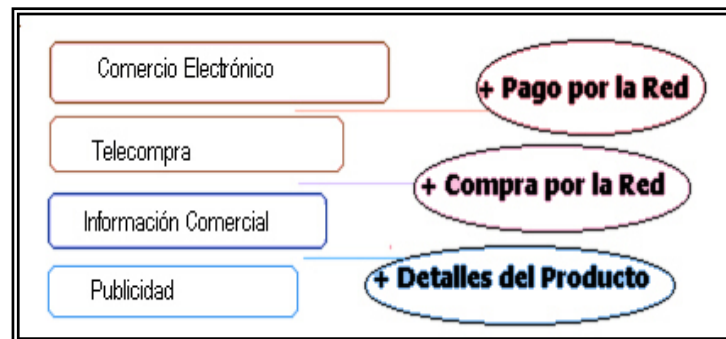


Figura 4.1: Implantación gradual del Comercio Electrónico

4.2.1. ELEMENTOS DEL COMERCIO ELECTRÓNICO

En el comercio electrónico participan como actores principales las empresas, los consumidores y las administraciones públicas. Así se distinguen normalmente tres tipos básicos de comercio electrónico como se distingue en la **Figura 4.2**:

- Entre empresas o B2B (*business to business*)
- Entre empresa y consumidor o B2C (*business to consumers*)
- Entre empresa y administración o B2A (*business to administrations*)
- Entre consumidor y administración o C2A (*consumers to administrations*)

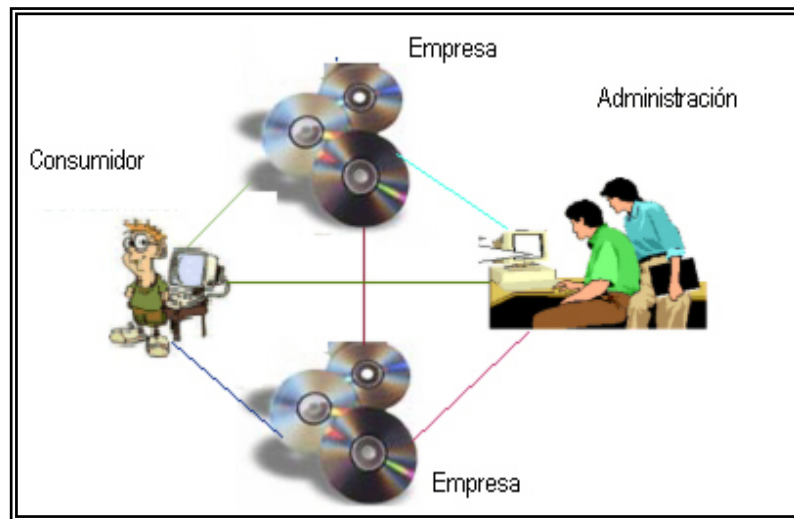


Figura 4.2: Actores y tipos de Comercio Electrónico

- **La categoría empresa–empresa:** Se refiere a una empresa que hace uso de una red para hacer ordenes de compra a sus proveedores, recibir facturas y realizar los pagos correspondientes. Esta categoría ha sido utilizada por muchos años, particularmente haciendo uso de EDI (*Electronic Data Interchange*) sobre redes privadas o redes de valor agregado (*Value added Networks-VAN*).
- **La categoría empresa–consumidor:** Se puede comparar con la venta al detalle de manera electrónica. Esta categoría ha tenido gran aceptación y se ha ampliado sobre manera gracias al WWW, ya que existen diversos centros comerciales (*del*

Inglés malls) por todo Internet ofreciendo toda clase de bienes de consumo, que van desde pasteles y vinos hasta computadoras.

- **La categoría empresa-administración:** Se refiere a todas las transacciones llevadas a cabo entre las empresas y las diferentes organizaciones de gobierno. Por ejemplo en Estados Unidos cuando se dan a conocer los detalles de los requerimientos de la nueva administración a través de Internet, las empresas pueden responder de manera electrónica. Se puede decir que por el momento esta categoría esta en sus inicios pero que conforme el gobierno empiece a hacer uso de sus propias operaciones, para dar auge al Comercio Electrónico, está alcanzará su mayor potencial. Cabe hacer mención que también se ofrecerán servicios de intercambio electrónico para realizar transacciones como el regreso del IVA y el pago de impuestos corporativos.
- **La categoría consumidor-administración:** Aún no ha nacido, sin embargo, después del nacimiento de las categorías B2C y B2A, el gobierno hará una extensión para efectuar interacciones electrónicas como serían pagos de asistencia social y regreso de pago de impuestos.

4.2.2. VENTAJAS Y RIESGOS DEL COMERCIO ELECTRÓNICO

Dentro de las principales ventajas del comercio electrónico para los **clientes** tenemos:

- **Permite el acceso a más información:** La naturaleza interactiva del Web y su entorno hipertexto permiten búsquedas profundas no lineales que son iniciadas y

controladas por los clientes, por lo tanto las actividades de mercadeo mediante el Web están más impulsadas por los clientes que aquellas proporcionadas por los medios tradicionales.

- **Facilita la investigación y comparación de mercados:** La capacidad del Web para acumular, analizar y controlar grandes cantidades de datos especializados permite la compra por comparación y acelera el proceso de encontrar los artículos.
- **Abarata los costos y precios:** Conforme aumenta la capacidad de los proveedores para competir en un mercado electrónico abierto se produce una baja en los costos y precios, de hecho tal incremento en la competencia mejora la calidad y variedad de los productos y servicios.

Las ventajas para las **empresas** son:

- **Mejoras en la distribución:** El Web ofrece a ciertos tipos de proveedores (industria del libro, servicios de información, productos digitales) la posibilidad de participar en un mercado interactivo, en el que los costos de distribución o ventas tienden a cero. Por poner un ejemplo, los productos digitales (software) pueden entregarse de inmediato, dando fin de manera progresiva al intermediarismo. También compradores y vendedores se contactan entre sí de manera directa, eliminando así restricciones que se presentan en tales interacciones. De alguna forma esta situación puede llegar a reducir los canales de comercialización,

permitiendo que la distribución sea eficiente al reducir sobrecosto derivado de la uniformidad, automatización e integración a gran escala de sus procesos de administración. De igual forma se puede disminuir el tiempo que se tardan en realizar las transacciones comerciales, incrementando la eficiencia de las empresas.

- **Comunicaciones de mercadeo:** Actualmente, la mayoría de las empresas utiliza el Web para informar a los clientes sobre la empresa, a parte de sus productos o servicios, tanto mediante comunicaciones internas como con otras empresas y clientes. Sin embargo, la naturaleza interactiva del Web ofrece otro tipo de beneficios conducentes a desarrollar las relaciones con los clientes. Este potencial para la interacción, que actualmente es asíncrono, facilita las relaciones de mercadeo así como el soporte al cliente, hasta un punto que nunca hubiera sido posible con los medios tradicionales. Un sitio Web se encuentra disponible las 24 horas del día bajo demanda de los clientes. Las personas que realizan el mercadeo pueden usar el Web para retener a los clientes mediante un diálogo asíncrono que sucede a la conveniencia de ambas partes. Esta capacidad ofrece oportunidades sin precedentes para ajustar con precisión las comunicaciones a los clientes individuales, facilitando que éstos soliciten tanta información como deseen. Además, esto permite que los responsables del área de mercadeo obtengan información relevante de los clientes con el propósito de servirles de manera eficaz en las futuras relaciones comerciales. Los sitios Web más sencillos involucran a los clientes mediante botones para enviar mensajes de correo electrónico a la

empresa. En otros centros más sofisticados, los clientes rellenan formularios, con el objeto de que desarrollen una relación continua con la empresa, cuyo fin es informar tanto sobre los productos y servicios como obtener información sobre las necesidades que los clientes tienen sobre los mismos. De esta manera, se obtiene publicidad, promoción y servicio al cliente a la medida. El Web también ofrece la oportunidad de competir sobre la base de la especialidad, en lugar de hacerlo mediante el precio, ya que desde el punto de vista del mercadeo, rara vez es deseable competir tan sólo en función del precio. El mercadeo intenta satisfacer las necesidades de los clientes en base a los beneficios que buscan, lo que quiere decir que el precio depende de la valorización del cliente, y no de los costos; tales oportunidades surgen cuando lo ofrecido se diferencia por elementos de mercadeo distintos al precio, lo cual produce beneficios cargados de valor, como por ejemplo, la comodidad producida por el reparto directo mediante la distribución electrónica de software.

- **Beneficios operacionales:** El uso empresarial del Web reduce errores, tiempo y sobrecostos en el tratamiento de la información. Los proveedores disminuyen sus costos al acceder de manera interactiva las bases de datos de oportunidades de ofertas, enviar éstas por el mismo medio, y por último, revisar de igual forma las concesiones; además, se facilita la creación de mercados y segmentos nuevos, el incremento en la generación de ventajas en las ventas, la mayor facilidad para entrar en mercados nuevos, especialmente en los mercados geográficamente remotos, y alcanzar con mayor rapidez el mercado. Todo esto se debe a la

capacidad de contactar de manera sencilla y a un costo menor a los clientes potenciales, eliminando demoras entre las diferentes etapas de los sub-procesos empresariales.

Como medio comercial el Web presenta las siguientes **Deficiencias o Riesgos**, derivadas tanto de su tecnología como de su naturaleza interactiva:

- **Entorno empresarial y tecnológico cambiante:** Empresas y clientes desean tener flexibilidad para cambiar, según su voluntad, de socios comerciales, plataformas y redes. No es posible evaluar el costo de esto, pues depende del nivel tecnológico de cada empresa, así como del grado deseado de participación en el comercio electrónico. Como mínimo una empresa necesitará una computadora personal con sistema operativo Windows o Machintosh, un módem, una suscripción a un proveedor de servicios de Internet, una línea telefónica. Una compañía que desee involucrarse más, deberá prepararse para introducir el comercio electrónico en sus sistemas de compras, financieros y contables, lo cual implicará el uso de un sistema para el intercambio electrónico de datos (EDI) con sus proveedores y/o una Intranet con sus diversas sedes.
- **Privacidad y seguridad:** La mayoría de los usuarios no confía en el Web como canal de pago. En la actualidad, las compras se realizan utilizando el número de la tarjeta de crédito, pero aún no es seguro introducirlo en Internet sin conocimiento alguno. Cualquiera que transfiera datos de una tarjeta de crédito mediante el Web,

no puede estar seguro de la identidad del vendedor. Análogamente, éste no lo está sobre la del comprador. Quien paga no puede asegurarse de que su número de tarjeta de crédito no sea recogido y sea utilizado para algún propósito malicioso; por otra parte, el vendedor no puede asegurar que el dueño de la tarjeta de crédito rechace la adquisición. Resulta irónico que ya existan y funcionen correctamente los sistemas de pago electrónico para las grandes operaciones comerciales, mientras que los problemas se centren en las operaciones pequeñas, que son mucho más frecuentes.

- **Cuestiones legales, políticas y sociales:** Existen algunos aspectos abiertos en torno al comercio electrónico: validez de la firma electrónica, no repudio, legalidad de un contrato electrónico, violaciones de marcas y derechos de autor, pérdida de derechos sobre las marcas, pérdida de derechos sobre secretos comerciales y responsabilidades. Por otra parte, deben considerarse las leyes, políticas económicas y censura gubernamentales.

4.2.3. MÉTODOS DE ENVÍOS Y PAGO

El comercio electrónico para medios de pagos tiene las siguientes características:

- Compra-venta de productos y servicios a través de redes abiertas (Internet, Infovía, etc.).
- Compra de productos y servicios de forma remota.

- La orden de pago puede ser realizada por varias vías (contra reembolso, tarjetas, transferencia, etc.).
- En caso de realizar el pago con Tarjeta, no exige la presentación física de la misma.

En este tipo de Comercio se debe tener muy presente lo siguiente:

- *Autenticación de las partes:* Se debe asegurar a los participantes en la transacción que los otros agentes que intervienen están autorizados a operar.
- *Privacidad de la información:* Se trabaja en redes abiertas en dónde pueden ser interceptados los mensajes. Se debe asegurar que la información transmitida, tanto en la orden de pedido como la orden de pago, sólo sea leída por el destinatario autorizado.
- *Integridad de los mensajes:* Se debe asegurar que no se alteren los datos del mensaje durante su transmisión

4.3. FUNCIONAMIENTO DE UN PORTAL WEB ORIENTADO A LA PROMOCIÓN DE SERVICIOS ACADÉMICOS Y ADMINISTRATIVOS

Antes de realizar el proceso de funcionamiento de un portal web de servicios académicos y administrativos; se tratará de explicar sus bases de formación. El **Portal de Servicios Académicos y Administrativos aplicado a la P.U.C.E.S.A.**, constituye

un software orientado al comercio electrónico, mediante el cual se podrá comercializar (*cursos/productos/servicios*) de la universidad hacia los usuarios, y tiene como lineamientos los siguientes puntos:

- Información actualizada y confiable de los diferentes (servicios/productos/servicios).
- La reservación de un (curso/servicio/producto) en un tiempo límite (3 días).
- Comprobar si el servicio/producto se encuentra en stock.
- Verificación del depósito.
- Mecanismo de encriptación y seguridades para datos.

El proceso manual comúnmente realizado por la gran mayoría de empresas, que ocurre desde que un usuario (*empresa compradora*) detecta la necesidad de reaprovisionar cierto bien (producto/servicio/curso), que ofrece una entidad educativa (*empresa proveedora*) hasta que dicho producto se halla físicamente ubicado en su hogar o depósito, resulta poco alentador. Todo el proceso se resume en ineficiencias, uso de papel, teléfono y fax en grandes cantidades, propensión a errores, pérdidas de tiempo que implican stocks más grandes, etc.

El proceso anterior, utilizando las técnicas de comercio electrónico en su máxima extensión se reduciría a:

- a. El usuario podrá comprar un bien (servicio/producto/curso) que desee, mediante formularios web, sin necesidad de visitar la institución.
- b. Mediante el uso de las redes de telecomunicación (pudiendo ser la red Internet una de ellas), el usuario anterior enviaría un pedido electrónico, sin papel, a la aplicación de gestión de pedidos de la empresa proveedora.
- c. En dicha empresa proveedora, el pedido electrónico se integraría directamente en el sistema informático para la recepción de pedidos, sin necesidad de intervención humana.
- d. Desde dicho sistema, también de forma automática, podrían lanzarse notificaciones electrónicas a los procesos contables, pagos, de facturación y de almacén, además de comunicar telemáticamente también al operador logístico la información necesaria para el transporte de la mercancía desde origen a destino.

Como se puede apreciar, se han reducido tiempos drásticamente en todo el proceso; así como la posibilidad de errores, ineficiencias, etc. En definitiva, se ha aumentado la competitividad de la empresa proveedora. Una vez visto este pequeño análisis, enfocaremos un modelo de portal de servicios académicos y administrativos aplicados a una institución educativa (P.U.C.E.S.A.), como se muestra en la **Figura 4.3**.

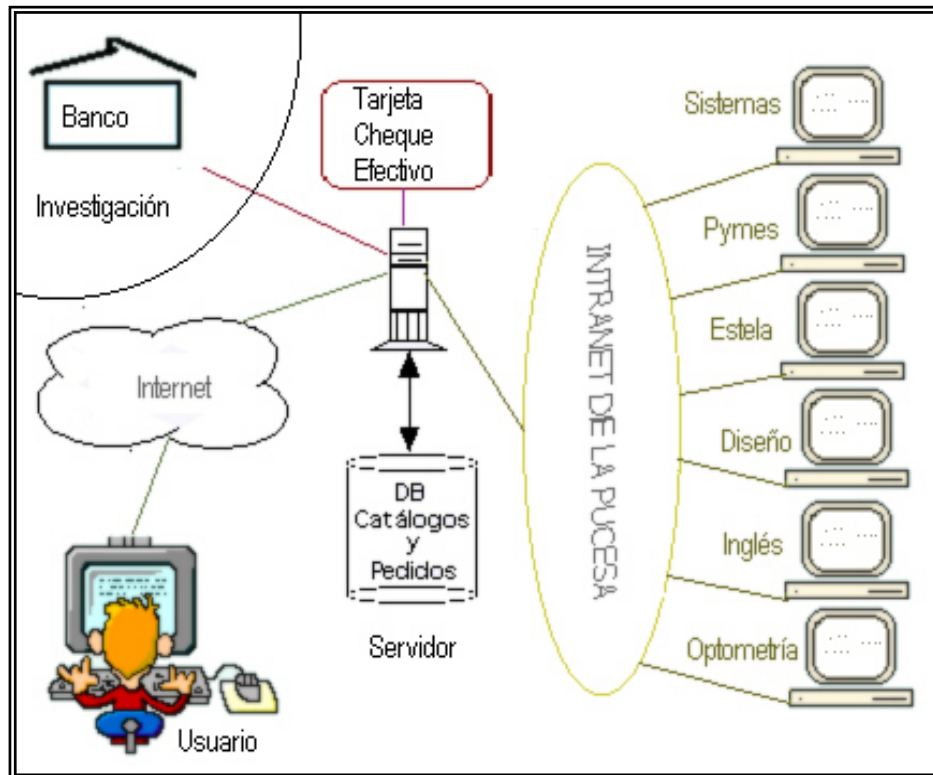


Figura 4.3: Portal de Servicios Académicos y Administrativos aplicado a la P.U.C.E.S.A.

4.4. GESTIÓN DE TABLAS DE IMPUESTOS (CIBERTRIBUTACIÓN)

Existe consenso en reconocer las enormes posibilidades y ventajas que representa la utilización de plataformas digitales en el desarrollo de estrategias comerciales que ayuden a la máxima explotación del sector educativo, y específicamente en el desarrollo y aplicación del comercio electrónico, de su enorme y creciente impacto en economías desarrolladas y en desarrollo del significativo y constante aumento de los volúmenes transados por dicha vía, de su eficiencia y enorme ahorro de tiempo,

recursos humanos y financieros, y de su cualidad como factor de integración del Ecuador con el resto de las economías del mundo. Es así como, nuestro país no puede quedarse atrás en esta realidad, dada su actual integración al comercio mundial. Retrasarnos en el desarrollo de esta modalidad haría que el país pierda mucho terreno en el comercio exterior y en los mercados que con tanto esfuerzo ha logrado abrir para sus productos.

No obstante lo anterior, y dadas las múltiples y aceleradas expectativas respecto de Internet y de la rápida inundación de innovaciones tecnológicas, pareciera existir confusión sobre lo que constituye un acercamiento responsable al comercio electrónico, entendiendo para este trabajo por comercio electrónico todas aquellas, transacciones realizadas por medios electrónicos sea que se trate de bienes, servicios, información y fondos de dinero, en redes abiertas o cerradas, a través de computadores interconectados entre sí por medio de los servicios de telecomunicaciones normales. Importante resulta para salvar esta confusión el reconocer la necesidad de crear un marco legal que de seguridad y certeza jurídica a las partes que están en relación contractual, y de reconocer como principio básico que, "transacciones aseguradas y respaldadas legalmente", son los elementos que constituyen la primera piedra del ejercicio del comercio electrónico.

Por consiguiente, la *Corporación Ecuatoriana de Comercio Electrónico* (C.O.R.P.E.C.E.), ha elaborado el presente "**Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos**" (Ver Anexo B), que

pretende de manera general en esta primera etapa, avanzar en la búsqueda de soluciones a las problemáticas impuestas al interior de nuestro país, como consecuencia del desarrollo y ejercicio del comercio electrónico [39]. Dicha ley regula la eficacia y el valor jurídico de los documentos electrónicos, el uso de firmas electrónicas, la prestación de los servicios de certificación, el manejo de bases de datos y la protección a los usuarios del comercio electrónico. Por lo tanto, se tendrán como base para la creación del Portal de Servicios Académicos y Administrativos aplicado a la P.U.C.E.S.A.

4.5. ANÁLISIS DE REDES DE ÁREA EXTENSA (WAN)

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN (*Red de Area Local o Local Area Network*). A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Los componentes importantes de cualquier red lo forman la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales (DBP en Alemania o British Telecom en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como *Frame Relay* y *SMDS-Synchronous Multimegabit Data Service*) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de

banda ancha. Se prevee que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

Redes de Área Amplia (WAN: *Wide Area Network*) [2]: "*Son cables de comunicaciones que unen redes locales separadas por grandes distancias. Son más lentas que las Redes Locales, y sólo se pueden instalar por empresas especializadas en Telecomunicaciones.*"

4.6. HERRAMIENTAS DE INTERNET APLICADAS A PORTALES WEB

Los beneficios que se pueden obtener al utilizar la Internet son muchos y muy variados, y así de variadas también son las herramientas necesarias para explotar todo el potencial que le ofrece el estar conectado a la red de computadoras más grande del mundo. Actualmente existen en el mercado, varias herramientas para la manipulación de portales web, por lo que analizaremos las más utilizadas dentro de este ámbito.

4.6.1. WORLD WIDE WEB (WWW)

La WWW, es considerado como un sistema de publicación y distribución electrónica de información basado en Hipertexto, la herramienta de más potencia para el acceso a la red Internet. Desde su aparición, se ha generado una extraordinaria actividad económica alrededor del WWW. Fue creada en 1989-90 por un grupo de científicos en el CERN (*Consejo Europeo para la Investigación Nuclear*) en Génova, con un

objetivo muy concreto: "**Compartir información de manera flexible, sencilla y distribuida**".

Uno de los principales responsables es *Tim Berners Lee* para quien la WWW es [33]:
"Un sistema de información multimedial distribuido, heterogéneo y colaborativo".

- **Es multimedial**, Maneja textos, imágenes estáticas y actualmente imágenes dinámicas (video o animación) y sonido.
- **Es distribuido**, No hay un gran punto central donde la información está concentrada, sino que la Web cubre todo el globo con miles de servers, cada uno conteniendo algo de información organizada como un gran hipertexto.
- **Es heterogéneo**, Incluye varios servicios de Internet que la precedieron, y distintos del de la Web, como por ejemplo Gopher, FTP, Newsgroups, etc.
- **Es colaborativo**, Permite que cualquiera pueda agregar nueva información y la misma esté disponible rápidamente para todos los demás.

Algunos de los conceptos fundamentales de la World Wide Web son:

- **HiperText Markup Language** (*lenguaje de Mercado de Hipertextos*): Permite expresar toda esta información multimedial y que el cliente la interprete para nosotros, simples humanos.)

- **HiperText Transfer Protocol (Protocolo de Transferencia de Hipertextos):**
Permite pasar hipertexto entre clientes y servidores.
- Los **estándares**: Permiten el avance gracias a los acuerdos en común.
- **Arquitectura cliente-servidor**: Permite este tipo de operación descentralizada.

4.6.2. CORREO ELECTRÓNICO (ELECTRONIC MAIL)

Permite mandar mensajes que contengan texto a cualquier parte del mundo en tan sólo unos instantes, tal como si enviásemos una carta normal, sólo que es extremadamente rápido. Tiene otra ventaja sobre el correo ordinario, y es que permite mandar archivos adjuntos al texto, lo que lo convierte en una poderosa herramienta de trabajo. Toda dirección electrónica se compone de un **nombre de usuario** y de un **dominio**, unidos con el símbolo @ denominado arroba o "at". Para manejar el correo electrónico, existen programas como el Eudora o el Pegasus, Nail, Netscape o similares que están especializados en esta tarea. Sin embargo, es más cómodo usar un navegador como Netscape o Internet Explorer, puesto que incorporan la posibilidad de gestionar el correo en el propio navegador.

4.6.3. SISTEMA DE NOMBRES DE DOMINIOS (DNS)

La identificación de todos los ordenadores en la Red se realiza a través de su **número IP**. Este número consta de cuatro bloques de uno, dos o tres números cada uno,

separados por un punto como por ejemplo (160.233.9.52). Como recordar esos números es una tarea complicada se creó un sistema de nombres más sencillo denominado **DNS**. Estos nombres de dominio están formados por dos palabras separadas por un punto. Por ejemplo: “*miweb.ec*”, consta de las palabras *miweb* y *ec*. La primera, es el nombre que nos identifica, que puede ser el nombre de nuestra empresa, una marca o nuestro nombre de pila. La segunda representa la actividad o la procedencia territorial.

4.6.3.1. DOMINIOS GENÉRICOS

Dentro de los dominios genéricos mayormente conocidos tenemos los que se muestran en la **Tabla 4.1**:

Tabla 4.1: Dominios Genéricos

<p>'.com', para empresas comerciales, es actualmente el más popular.</p> <p>'.org', para organizaciones sin fines de lucro.</p> <p>'.net', para empresas relacionadas con Internet.</p> <p>'.mil', para instituciones militares.</p> <p>'.int', para instituciones internacionales.</p> <p>'.edu', para instituciones educativas.</p> <p>'.gov', para organizaciones gubernamentales.</p>
--

Todos estos dominios los gestiona la organización **InterNIC** en Estados Unidos.

4.6.3.2. DOMINIOS TERRITORIALES

Los dominios territoriales o geográficos los gestiona cada país. Por ejemplo en nuestro país Ecuador el organismo que los mantiene se llama **EcuNet** y al dominio se le asigna el sufijo **'ec'**. Todos los dominios territoriales tienen dos letras, **'ar'** (Argentina), **'uk'** (Reino Unido) son algunos de ellos.

El gran desarrollo y masificación de los dominios genéricos, en especial **'com'**, ha propiciado que se vayan a crear otros siete dominios genéricos nuevos que se muestran en la **Tabla 4.2**:

Tabla 4.2: Dominios Territoriales

<p>'firm', dedicados a empresas comerciales.</p> <p>'shop', para puntos de venta.</p> <p>'info', para puntos de información.</p> <p>'web', para páginas en Internet.</p> <p>'rec', para actividades recreativas.</p> <p>'arts', para actividades artísticas y culturales.</p> <p>'nom', para páginas personales.</p>

Para registrar un dominio lo que tenemos que hacer es pensar varios nombres, por si el que queremos utilizar ya está registrado, y decidir el tipo de dominio que deseamos. Después hemos de comprobar, a través de alguna empresa autorizada para registrar un dominio como por ejemplo **www.interdomain.org**, que no existe el que queremos

crear y, cuando lo hayamos comprobado hemos de reservarlo para que nadie pueda adelantarse. Para continuar con el proceso debemos contar con dos máquinas que sean servidores de nombres para ponerlas una como servidor primario y otra como secundario. Las direcciones de estas máquinas las suele proporcionar el proveedor que vaya a alojar nuestras páginas web. Con esas direcciones ya podemos registrar el dominio que teníamos reservado.

4.6.4. FTP (FILE TRANSFER PROTOCOL)

FTP, es **el Protocolo de Transferencia de Ficheros de la Internet**, Es un conjunto de reglas o procedimientos (**protocolo**) que determina cómo se copiarán archivos de una máquina a otra.

La Transferencia de Archivos, tiene la función de facilitar el intercambio de archivos a través de Internet por medio de la instalación de servidores públicos o privados que contienen en forma ordenada y jerarquizada los archivos, y que dependiendo de los privilegios del usuario, le permiten transmitirlos hacia su computadora.

Como todas las aplicaciones de la Internet, FTP utiliza la tecnología **cliente/servidor**. Es un servicio comúnmente usado en Internet para transferir programas y documentos de una computadora a otra.

Se puede usar para:

- Download (**descargar**) o traer archivos a nuestra máquina desde una computadora en Internet. (generalmente programas)
- Upload (**cargar**) Enviar nuestra información a otra máquina en Internet.

A lo largo de la **Internet** existen miles de servidores de **FTP** a los que se puede acceder anónimamente, es decir, no hay necesidad de estar autorizado para acceder a estos servidores. Este servicio se llama **FTP Anónimo**. Mediante el servicio **FTP Anónimo** se puede obtener software para todo tipo de ordenadores, documentos y manuales, archivos de gráficos y sonido, etc.

Para descargar software o información desde servidores FTP, se deben abrir los sitios al igual que para la Web pero usando el protocolo **ftp://** en vez de **http://**. Los links a sitios ftp funcionan igual que los http. Al hacer clic sobre un link, éstos se abren automáticamente. Una diferencia es que un sitio FTP puede estar ocupado si el cupo de usuarios conectados a la vez se llena.

4.6.5. IRC (INTERNET RELAY CHAT)

Nos permite entablar una conversación en tiempo real con una o varias personas por medio de texto. Todo lo que escribimos en el teclado aparece en las pantallas de los que participan de la charla. También permite el envío de imágenes u otro tipo de ficheros mientras se dialoga.

4.6.6. VIDEOCONFERENCIA

Son las últimas aplicaciones que han aparecido para Internet. Nos permiten establecer una conexión con voz entre dos personas conectadas a Internet desde cualquier parte del mundo sin tener que pagar el coste de una llamada internacional. Algunos de estos servicios incorporan no sólo voz, sino también imagen. A esto se le llama **Videoconferencia**.

4.7. PORTALES WEB

Mediante la incorporación de scripts dinámicos se puede realizar funciones específicas de acuerdo a las necesidades del usuario y de la empresa, con lo cual se obtendrá mayor aceptación y competitividad del portal comercial. Dentro de los portales web tenemos: ActiveX y el lenguaje VBScript (Diseño Gráfico)

4.7.1. INTRODUCCIÓN A LOS ACTIVE-X

ActiveX es el nombre que Microsoft ha dado a un grupo de tecnologías y herramientas "estratégicas" orientadas a objetos. Su principal tecnología es el Modelo de Objeto Componente (*Component Object Model*, COM). Al usarlo en una red con un directorio y apoyo adicional, el COM se convierte en el Modelo Distribuido de Objetos Componentes (*Distributed Component Object Model*, DCOM). El principal objeto que

uno crea al escribir un programa ejecutable en el entorno ActiveX es un componente, un programa autosuficiente que puede ejecutarse en cualquier sitio en la red ActiveX (que es actualmente una red que consta de sistemas tanto Windows como Macintosh). Este componente se conoce como un Control ActiveX.

4.7.2. INTRODUCCIÓN A VISUAL BASIC SCRIPT (VBSCRIPT)

VBScript, también conocido como Visual Basic Script es un nuevo lenguaje de scripts empaquetado con Microsoft Internet Explorer 3.0. Tiene fama por la sencillez de su aprendizaje, es decir, no diferencia entre mayúsculas y minúsculas y asegura poseer un único tipo de datos. Este lenguaje es el utilizado por Microsoft para todos sus productos y, claro está, no podía faltar en el Internet Explorer. La necesidad de estudiarlo viene casi más por su inclusión en muchas utilidades Microsoft y algunas no Microsoft (CorelScript es muy similar) y, especialmente, por la programación de *Active Server Pages* (ASP) en los servidores Web Microsoft. Sin embargo, los VBScript dependiendo de la aplicación dispondrán de una jerarquía de objetos diferente y adaptada a dicha aplicación para poder interactuar con ella [3]. La sintaxis de VBScript está basada sobre Visual Basic, aunque VBScript ofrece una mayor y simple fijación de comandos al trabajar con él. VBScript es usado para validar la forma de datos, crea nuevas páginas webs al vuelo y lleva a cabo otras operaciones como el que utiliza entradas. VBScript se asemeja al objeto orientado JavaScript.

CAPÍTULO V

5. SEGURIDAD Y ENCRIPCIÓN EN UN PORTAL DE SERVICIOS

5.1. INTRODUCCION

Nadie tiene una seguridad absoluta en Internet, tanto los proveedores como los compradores tienen un riesgo, sin embargo, la tecnología ofrece medios de transacciones cada vez más seguros. Las técnicas de encriptación de datos pueden convertir al comercio electrónico en más seguro que el comercio tradicional basado en tarjetas de crédito. La dificultad estriba en convencer al consumidor digital de que nuestro sitio es realmente seguro así como que el comercio electrónico también lo es.

Cuando se realiza una transacción por Internet y se envían los datos personales (nombre, dirección, número de tarjeta de crédito, etc.) deberíamos plantearnos si pueden ser interceptados durante la transmisión (entre comprador y vendedor) por alguien que no sea el vendedor. Ese alguien, ¿podría utilizar estos datos para suplantar nuestra identidad?. Igualmente el vendedor quiere asegurarse de que los datos que recibe son verdaderos, es decir, necesita saber que el comprador es quien dice ser. Es por estas razones que se han desarrollado los sistemas de transacciones seguras. La firma digital no es más que un tipo de encriptación, en la cual se realiza un control sobre el flujo de información (por ejemplo de un contrato, de un número de tarjeta de crédito, etc.) Se usan para verificar al proveedor de una determinada información y

que la información firmada (el pedido, el número de tarjeta, etc.) no ha sido alterada.

5.2. FORMAS DE SEGURIDAD

Los sistemas abiertos de comunicaciones tienden a emular la organización, estructura y comportamiento de las sociedades a las que sirven. Así, al igual que en las empresas, en los sistemas de información habrá diversos niveles de acceso a los contenidos. Estas políticas de seguridad suelen dividirse en: Seguridades Internas y Externas

5.2.1. SEGURIDAD INTERNA

En el nivel interno, el objetivo es **mantener privados y accesibles sólo a usuarios autorizados aquellos datos confidenciales o sensibles de la compañía.**

Se habla muy poco de los problemas de seguridad interna, puesto que no se denuncian o no se llegan siquiera a descubrir, pero lo cierto es que la mayoría de los incidentes de seguridad se producen en el seno de las organizaciones. En la práctica, la seguridad interna de las empresas se basa en la utilización de lo siguiente:

- Contraseñas
- Cifrado de determinados materiales
- Certificación para acceder a los contenedores de información.

Limitarse al uso de **Contraseñas** (*en sus distintas modalidades: clave de acceso, nombre de usuario y pin, contraseñas cruzadas, etc.*) no es sino el nivel más básico de seguridad. Basta con que alguien conozca esa clave para que acceda a todos los datos. Hay que recordar, además, que en muchas empresas no resulta extraño encontrar las contraseñas anotadas en *post-it* (*papelitos*) sobre el monitor u oír cómo se pasan en voz alta entre los empleados.

Las contraseñas se emplean mas bien para reforzar o dar acceso a un mayor nivel de seguridad, como el que aportan los **Sistemas de Cifrado** (Ver literal 5.3.). Sin embargo, podemos apuntar que se trata de *sistemas que codifican la información con unos algoritmos que la hacen ilegible al usuario no autorizado*. Existen varios grados de cifrado. Uno de los más potentes es el denominado Triple DES.

Los sistemas de cifrado conviven con los de **Certificación Electrónica** (Ver Literal 5.6.). Como indica el propio término, *estos sistemas son una especie de notarios electrónicos que certifican la identidad del usuario, evitando que otro lo suplante*. Con la equiparación legal de la firma electrónica y la manuscrita, estas tecnologías, que se presentan en distintas modalidades (*monederos electrónicos de software, tarjetas chip, etc.*), se extienden poco a poco, aportando un elevado nivel de seguridad tanto en el ámbito interno como en el externo.

Las compañías que requieren un nivel de seguridad alto están sumando a todas estas fórmulas los denominados **Sistemas Biométricos**, *sistemas de reconocimiento físico*

de los usuarios por voz, huellas dactilares e incluso iris ocular. Estos sistemas, que todavía suenan a misión imposible, se están abaratando hasta tal punto que incluso se llegan a implantar en teléfonos móviles.

En Internet ocurre lo mismo, es cuestión de adaptar estos sistemas para delimitar distintas áreas de acceso al servidor web, según se trate de una red Intranet (*de uso exclusivo de la firma*), Extranet (*una red privada ampliada a socios y proveedores*) o de un simple web con accesos privados para determinados usuarios.

5.2.2. SEGURIDAD EXTERNA

La seguridad externa puede parecer más compleja de controlar, aunque en realidad no lo es tanto. En principio, los usuarios ajenos a la compañía carecen de acceso al sistema, a menos que ésta se lo conceda explícitamente, en calidad de usuarios registrados o de visitantes. Con todo, las acciones de *hackers (Intrusos)*, capaces de irrumpir en los sistemas Internet de grandes empresas bloqueando sus accesos o modificando los contenidos de sus páginas, son motivo de alarma. Ciertamente, es imposible mantenerse a salvo al 100%, pero existen herramientas la mayoría de ellas incorporadas al sistema operativo de sus servidores y estaciones de trabajo que impiden la entrada de extraños en todos los niveles de nuestras comunicaciones por Internet.

Para empezar, existe una primera barrera que aísla la red interna de la externa. Se

construye mediante los denominados **Cortafuegos** (*firewalls*), *unas sofisticadas herramientas de hardware, software o combinaciones de ambos, que ejercen control sobre el tipo de tráfico que circula, su origen y destino*. Más allá de los cortafuegos, habrá que establecer sistemas de seguridad en cada una de las aplicaciones de nuestro entorno Internet.

La seguridad de los programas de correo electrónico, por ejemplo, puede complementarse con mecanismos de cifrado de datos y firma electrónica, como los mencionados en el apartado de seguridad interna. En este ámbito, los más extendidos son el **Protocolo S/MIME** (*Extensiones Multipropósito para Correo en Internet*) y el **Sistema de Cifrado PGP** (*Intimidad bastante buena*) (Ver literal 5.7.).

Pero donde la seguridad está preocupando verdaderamente es en las transacciones económicas. El arranque del comercio electrónico B2C (*business to consumers*) ha despertado las alarmas de comerciantes y consumidores que, de modo progresivo, van exigiendo mayores niveles de seguridad en sus comunicaciones por la red. El sistema más utilizado para protegerlas es el del cifrado, mediante los protocolos **SSL 3.0** (*Secure Socket Layer Protocol*) o **SET** (*Secure Electronic Transaction*) (Ver literal 5.5.). Con el uso de estos protocolos puede hablarse de entornos plenamente fiables. Sin embargo, perdura todavía la resistencia de los usuarios a facilitar datos como el número de la tarjeta de crédito. Por ello, muchas de las transacciones siguen combinando la transmisión electrónica de datos y el teléfono, así como los sistemas de pago contra reembolso.

Por último, los usuarios que acceden desde el exterior y que requieren acceso a los servicios internos de la organización pueden utilizar las denominadas **Redes Privadas Virtuales (VPN)**, canales de comunicación cifrados dentro de la propia Internet.

5.3. MÉTODOS CRIPTOGRÁFICOS

Tienen su origen en la Segunda Guerra Mundial; se utilizaban sistemas criptográficos para enviar mensajes con el fin de que el enemigo no pudiese obtener información, tenía un fin exclusivamente militar. Al finalizar la guerra, las transmisiones cifradas de datos comenzaron a difundirse para otras finalidades de carácter no bélico.

La criptografía es, pues, *un sistema o método de transformación de cualquier tipo de mensaje de datos para volverlo ininteligible (de manera aparente) y, poder más tarde, recuperar el formato original* [49]. Normalmente, se utilizan algoritmos matemáticos para cifrar o "criptar" los datos. Tiene la finalidad de que solamente las personas que posean decodificadores o las claves correspondientes puedan tener acceso a la información que envía el emisor del mensaje de datos.

Los sistemas criptográficos se pueden dividir en dos grandes grupos:

- Sistemas de criptografía simétrica (se incluye el tradicional "cifrado")
- Sistemas de criptografía asimétrica (se incluye la firma digital)

5.3.1. CRIPTOGRAFÍA DE CLAVE SECRETA O SIMÉTRICA

Consisten en la utilización de una clave común y conocida por todas las partes. Esta clave es la que permite la codificación o cifrado de los datos, así como el descifrado del mensaje de datos. Las posibilidades de vulneración son muy escasas si la clave se mantiene secreta; si la protección es deficiente y terceros pueden acceder a la misma, la información ya no será segura. De entre los algoritmos matemáticos más importantes que se suelen utilizar en el sistema de cifrado, destacan: DES (*Data Encryptions Standard*), RC4, IDEA (*International Data Encryption Algorithm*), FEAL (*Fast Encryption Algorithm*), RC5, etc.

Este método criptográfico tiene ventajas e inconvenientes.

Entre las **ventajas** se encuentra la confidencialidad que comporta tanto al iniciador como al destinatario del mensaje de datos, puesto que sólo ellos conocen la clave para acceder al mensaje de datos. Otra ventaja del sistema de claves secretas es que proporciona integridad, en el sentido de que si al descifrar el mensaje con la clave correcta, aparece desvirtuado, significará que ha sido interceptado por terceros no autorizados. La tercera ventaja radica en la autenticación del mensaje de datos inter partes, en cuanto que los únicos conocedores de la clave son emisor o signatario y receptor del mensaje.

El **inconveniente** principal de los sistemas simétricos de cifrado, radica en el mantenimiento en secreto de la clave. Ésta se debe transmitir por medios seguros, con el fin de evitar manipulaciones de los mensajes de datos. A este problema, hay que añadir que "no ofrece todos los servicios de seguridad necesarios para cumplir las exigencias legales: ofrece, como hemos visto, autenticación e integridad entre las dos partes que comparten la clave secreta, pero no frente a terceros". Esto significa que, frente a un tercero, bien el signatario como el destinatario pueden rechazar la autoría del mensaje atribuyéndolo a la otra parte; y que un tercero, que acceda fraudulentamente a la clave secreta, podrá engañar a una de las partes haciéndose pasar por la otra.

5.3.2. CRIPTOGRAFÍA DE CLAVE PÚBLICA O ASIMÉTRICA

A partir de los años setenta comienza a desarrollarse este nuevo sistema de cifrado, denominado sistema de clave asimétrica o pública. Se trata de un método más complejo que el sistema de clave simétrica.

Estos sistemas asimétricos se basan en la utilización de dos claves en una única operación criptográfica, es decir: una clave pública que sirva para cifrar o encriptar el mensaje de datos, y una clave privada para descifrarlo. De esta manera, un mensaje codificado con una clave pública determinada, solamente podrá descodificarse con la clave privada correspondiente, y viceversa.

Ambas claves están relacionadas entre sí por operaciones matemáticas. Al inicio se trataba de simples operaciones aritméticas (generalmente operando con números primos), más tarde con operaciones algebraicas más complicadas y en la actualidad se investigan técnicas de encriptación o cifrado que utilizan un sistema de curvas elípticas. En relación con la clave privada, es absolutamente necesario mantenerla en secreto para que solo, única y exclusivamente, pueda utilizarla el titular de la misma.

En la práctica, casi nunca el mismo titular de la clave privada la conoce; se suele mantener en una tarjeta electrónica, y se accede la clave mediante un PIN (*Personal Identification Number*) típico ejemplo de las tarjetas de los teléfonos móviles; o en algunos casos, se usan dispositivos más seguros de tipo biométrico, como puede ser el reconocimiento de huellas digitales o de la voz. La clave pública es accesible a cualquier persona, no necesita ni debe mantenerse oculta.

El sistema de cifrado asimétrico más conocido es el RSA (*Rivest, Shamir, Adleman nombres de los creadores*); un dato anecdótico es que éste es el sistema utilizado por el Netscape Navigator y que todavía no se ha realizado uso fraudulento del mismo, no se ha "pirateado". Este sistema, mucho más reciente que el de clave secreta, es la primera solución a la que se ha llegado en estos momentos para poner remedio a la necesidad existente en el ordenamiento respecto a la confidencialidad, autenticación, integridad y no rechazo en origen del mensaje de datos (*estos tres últimos los proporciona directamente la firma digital creada por el método asimétrico*).

5.4. ALGORITMOS DE DESTILACIÓN

Además de estos algoritmos de encriptación asimétrica existen otros algoritmos de compresión necesarios para conseguir que la firma digital tenga los mismos efectos que la manuscrita. Se trata de los algoritmos de compresión **hash** que se aplican sobre un determinado texto en cuestión (*por ejemplo el contrato on-line*). Son algoritmos que aplican funciones de no retorno. Estas funciones que realizan son peculiares en el sentido de que no es necesario la tenencia de una clave, ya que aplican funciones matemáticas sencillas para cifrar, pero para poder descifrar los cálculos matemáticos a realizar serían prácticamente imposibles de encontrar. Luego nadie, ni si quiera la persona que cifra el texto, podría llegar al documento original.

La compresión crea un texto limitado y reducido de entre 128 y 160 bits, el cual representa de forma fehaciente la integridad del documento, ya que si cambiamos un solo bit del documento original el resultado obtenido al volver a aplicar la función hash sería totalmente diferente. Además de estas peculiaridades nos encontramos con que las probabilidades para que dos textos distintos tuviesen el mismo hash serían prácticamente nulas. Estos algoritmos también son conocidos como algoritmos de destilación, algoritmos de huella digital o algoritmos de función resumen, los cuales son vitales y necesarios para la introducción de la firma digital en la sociedad de la información. El algoritmo de destilación más conocido es el MD5 que es utilizado para encriptar datos del login y password.

5.5. TARJETAS DE DÉBITO Y CRÉDITO (SSL & SET)

Los mecanismos de encriptación **SSL** (*Secure Socket Layer Protocol*) y **SET** (*Secure Electronic Transaction*), permitirán realizar transacciones comerciales seguras dentro del Comercio en Internet. Actualmente, son las más utilizadas como medio de pago en el Comercio Electrónico, las tarjetas de crédito y débito tradicionales han permitido la realización de transacciones comerciales en el nuevo medio a través de la utilización de los procedimientos de liquidación y pago preestablecidos.

Si se realiza una compra en Internet utilizando una tarjeta de crédito como medio de pago, la transacción comercial se ordena en la red, pero la validación y la realización efectiva del pago se efectúa a través de los circuitos tradicionales de procesamiento de operaciones con tarjeta de crédito.

En el esquema más general, intervienen en este proceso los siguientes actores:

- El comprador.
- El vendedor (*merchant*).
- El banco emisor (*issuer*) de la tarjeta de crédito o débito que presenta el cliente.
- El banco que en nombre del vendedor recibe la transacción (*acquirer*) y en él reside la cuenta en la que a éste se le va a liquidar el pago.

- La red de medios de pago (*scheme*) como VISA o MasterCard.

El proceso de pago es como sigue:

- a. Una vez realizado el pedido, el comprador proporciona su número de tarjeta al vendedor a través de la red.
- b. El centro servidor donde reside el vendedor envía la transacción al banco "acquirer" o directamente a la red de medios de pago. Este envío suele producirse fuera de la red pública y se realiza de forma análoga a como se efectuará desde una *terminal punto de venta* (TPV) físico que existiese en una tienda real.
- c. El banco receptor pide autorización al banco emisor a través de la red de medios de pago.
- d. Si la transacción se autoriza, la liquidación del pago (**transferencia de dinero desde la cuenta del comprador en el banco emisor hasta la cuenta del vendedor en el banco receptor**) se realiza a través de la red tradicional de medios de pago.

Como puede observarse el punto crítico de este proceso se produce cuando el comprador envía su número de tarjeta al vendedor a través de una red pública potencialmente insegura como Internet. El estándar que se utiliza en Internet para asegurar esta transferencia de datos es el SSL.

5.5.1. SSL (SECURE SOCKETS LAYER)

El SSL, o *Secure Sockets Layer*, es un método de encriptación desarrollado por Netscape para proveer de seguridad en Internet. Soporta diversos protocolos de encriptación diferentes y proporciona autenticación de cliente y servidor. El SSL opera en el nivel de transporte, crea un canal seguro de datos encriptados, y así puede encriptar sin costuras datos de muchos tipos. Con el uso del SSL [51]:

- El comprador tiene garantía de que el vendedor es quien dice ser y que, por tanto, no está entregando su número de tarjeta a un posible impostor.
- La información que envía el comprador se cifra, impidiendo el acceso a la misma por alguien distinto al vendedor.
- Se garantiza la no manipulación de los datos entre el comprador y el vendedor.
- La versión 3 de SSL permite la autenticación del comprador, que debe recibir sus claves previamente de una autoridad de certificación.

Para la realización de una transacción utilizando SSL se requiere de dos elementos:

1. Que el vendedor se haya certificado con una organización reconocida por las partes, lo que supone un procedimiento administrativo y el pago de unas tarifas de alta, así como la renovación de tal certificación.
2. Que el comprador utilice un visor o navegador ("browser") compatible como SSL.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos:

- a. Primero se debe hacer una solicitud de seguridad.
- b. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como SSL Handshake.
- c. 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.
- d. Tan pronto como la transacción ha sido completada, se termina SSL.

5.5.1.1. SSL HANDSHAKE.- Consta de los siguientes pasos:

- **Client Hello** o también llamado *saludo de cliente*, tiene por objetivo informar al servidor que algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.
- **Server Hello:** El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.
- **Aprobación del Cliente:** El cliente verifica la validez del identificador digital o certificado enviado por el servidor.

- **El siguiente paso es el de verificación:** Ambas partes se envían una copia de las anteriores transacciones encriptadas. Si ambas partes confirman la validez de las transacciones, el handshake se completa, de lo contrario se reinicia el proceso.
- **Intercambio de datos:** Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos.
- **Finalmente, la 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. En la **Figura 5.4**, se resume el proceso que sigue el SSL Handshake en una comunicación privada:

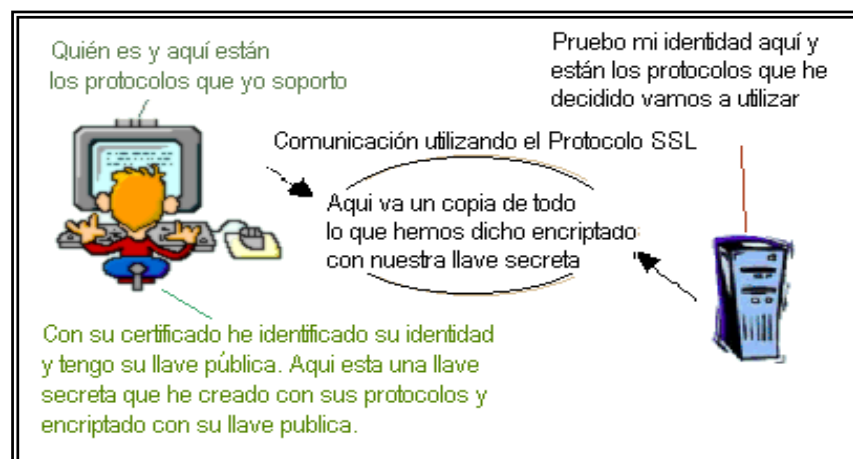


Figura 5.4: Proceso del SSL Handshake

Los dos últimos mensajes ya se realizaron haciendo uso del protocolo SSL, lo que quiere decir que se realizó una comunicación privada.

Según lo antes dicho, el SSL comete dos pequeños errores: Utilizar únicamente clave pública y no exigirle verificación al cliente.

5.5.1.2. LÍMITES DEL SSL

Lo que SSL no garantiza es el aspecto económico de la transacción, de tal manera que sólo con proporcionar un número de tarjeta válido con saldo suficiente cualquier persona podría intentar comprar electrónicamente de forma fraudulenta, sobre todo si no existe una entrega física de los bienes en sí con una autoridad de certificación. Ante ésta limitante, en 1995 se constituyeron dos grupos de trabajo liberado respectivamente por VISA y MasterCard, que comenzaron a definir dos estándares incompatibles para asegurar las transacciones dentro de Internet. Afortunadamente, a principios de 1996 debido a la presión del mercado (consumidores, vendedores, y fabricantes de tecnología) ambos grupos se fusionaron para la definición del estándar SET (*Secure Electronic Transactions*) en el que participan además de VISA y MasterCard, empresas como Microsoft, Netscape, IBM, Terisa, GTE, SAIC, VeriSign y otras compañías tecnológicas.

5.5.2. TRANSACCIONES ELECTRÓNICAS SEGURAS (SET)

Es un protocolo estandarizado y respaldado por la industria, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas, incluyendo

Internet. El estándar SET fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, VeriSign y otras. En este punto se mostrará su arquitectura. SET resuelve las siguientes necesidades [51]:

- Confidencialidad de los datos, tanto económicos, como respecto a la naturaleza de los bienes comprados.
- Integridad de los datos en la transacción, sin la posibilidad de modificaciones intermedias.
- Autenticación del comprador como legítimo usuario de un medio de pago.
- Autenticación del comercio como poseedor de una cuenta de liquidación con un banco vendedor.
- Compatibilidad entre múltiples plataformas "hardware" y "software".

Antes de poder realizar una transacción SET, el cliente debe poseer un medio de pago y recibir un certificado de la institución financiera emisora que incluye la firma digital de esa institución y una fecha de expiración. De igual manera, cada comercio debe también certificarse con la institución financiera donde posee la cuenta de liquidación. Así, cada uno de los agentes (comprador, vendedor, banco emisor, banco adquiriente) de una transacción posee una firma digital emitida por una autoridad de certificación SET.

En un sistema SET se agrega un "gateway" de pago diferente del servidor de transacción. Las diferencias principales con respecto a la arquitectura servidor de Web con orden de pedido son respecto al manejo de la orden de pedido y la forma de manejar las comunicaciones relacionadas con el pago. En su forma simple, la arquitectura SET adquiere la orden de pedido del servidor vendedor en el momento que el pago por tarjeta de crédito es apropiado. El servidor vendedor incorpora un modulo SET vendedor en lugar de conectarse directamente a una red de autorización de tarjetas de crédito. Cuando el módulo SET es llamado para manejar el pago, los siguientes pasos ocurren:

- a. El modulo vendedor envía un mensaje al "wallet" SET ubicado en la computadora del comprador, conteniendo una descripción de la orden y del precio total.
- b. El comprador utiliza el "wallet" SET para seleccionar una tarjeta de pago y para aprobar la compra.
- c. El "wallet" SET se comunica a través de la computadora vendedora con el "gateway" de pago con SET ubicado en el banco que en nombre del vendedor recibe la transacción.
- d. El "gateway" de pago se conecta a una red financiera tradicional para autorizar la transacción.
- e. La computadora vendedor almacena el "acknowledgment" y envía un recibo al comprador.

En la **Figura 5.5** se muestra un diagrama que muestra la disposición de esta arquitectura.

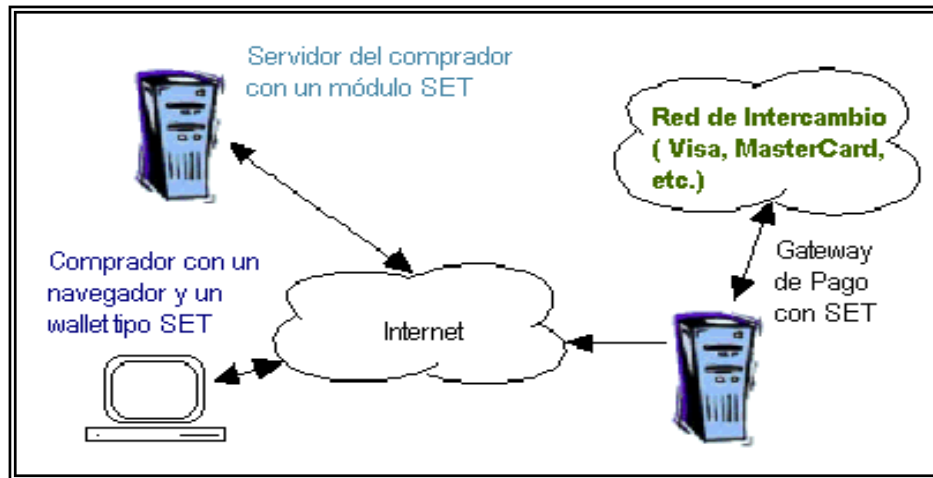


Figura 5.5: Arquitectura SET

5.5.2.1. PROBLEMAS CON LAS AUTORIDADES DE CERTIFICACIÓN SET

Uno de los puntos conflictivos que supone SET es la jerarquía de estas autoridades de certificación, en la que VISA y MasterCard están en el primer nivel y certifican autoridades de nivel inferior: geopolíticas, bancos, y clientes (vendedores o compradores), donde cada escalón supone un elemento de costo en la transacción. Por ejemplo, cuando un cliente emite un pedido, el proceso es el siguiente:

- a. El cliente recibe la firma digital de la tienda y verifica su validez
- b. El cliente envía (firmados digitalmente por él) al comercio la siguiente información:

- El pedido, de una forma tal que sólo puede leerlo el comercio.
 - La orden de pago, de tal manera que sólo puede verla el banco.
 - La relación entre el pedido y la orden de pago, que los liga indisolublemente.
- c. El comercio recibe el pedido y verifica la validez de la firma digital del cliente.
- d. El comercio pasa, con su firma digital, al banco la información de la orden de pago que él no ha podido leer.
- e. El banco autoriza la transacción.

En la liquidación de pago, al igual que sucede en una compra tradicional, el vendedor no percibe el importe total, sino que se produce un descuento que se reparten los bancos emisor, adquirente y la red de medios de pago.

El porcentaje de descuento, que en el comercio tradicional depende fundamentalmente del sector de actividad del vendedor, es muy alto en el comercio electrónico, al no haber presentación física de la tarjeta con el consiguiente riesgo de fraude.

Se puede preveer que el uso de SET supondrá una disminución del riesgo y, consecuentemente, del porcentaje de descuento de este tipo de transacciones. En cualquier caso, los costos asociados a una transacción comercial mediante tarjeta de crédito o débito hacen que este medio de pago no sea posible para importes inferiores a 10 o 15 dólares, lo que se conoce como micropagos.

5.6. FIRMA ELECTRÓNICA

La firma electrónica “ordinaria” es una tecnología de seguridad que podemos emplear en nuestros documentos para dejar constancia de nuestra voluntad de identificarnos y obligarnos a lo que en ellos estipulemos. Esta definición, funcionalmente equivalente a la firma de un documento físico, se cumple en Internet acudiendo a diversos elementos:

- Una clave secreta que sólo posee el firmante
- Una clave pública que conoce todo el mundo
- Programas que son capaces de firmar y comprobar firmas, y, muy importante
- Un certificado que garantiza que el poseedor de una determinada clave secreta correspondiente a una clave pública es una persona concreta.

Un **Certificado digital** constituye un documento digital emitido por una entidad y para un tercero. Dicha entidad (*Autoridad de Certificación CA*), garantiza los datos contenidos en el citado documento relativos a una persona, ya sea física o jurídica (empresas). En la actualidad existe un solo tipo de certificado digital corporativo ya sea para entidades educativas o para empresas comerciales.

La firma digital consiste en la utilización de un método de encriptación llamado **Asimétrico o de Clave Pública**, el cual consiste en establecer un par de claves asociadas a un sujeto, una pública, conocida por todos los sujetos que intervienen en el

sector, y otra privada, sólo conocida por el sujeto en cuestión. De esta forma cuando quiera establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo.

La expresión, firma digital es definida como [48]: "*La firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad)*"

5.6.1. LAS AUTORIDADES DE CERTIFICACIÓN

Si todos estos medios de seguridad están utilizando el procedimiento de encriptación asimétrico, habrá que garantizar tanto al emisor como al receptor la autenticación de las partes, es decir, que éstas son quienes dicen ser, y sólo a través de una autoridad de certificación (**CA *Certification Authority***) podrá corregirse dicho error, certificando e identificando a una persona con una determinada clave pública. Estas autoridades emiten certificados de claves públicas de los usuarios firmando con su clave secreta un documento, válido por un período determinado de tiempo, que asocia el nombre distintivo de un usuario con su clave pública.

Una autoridad de certificación es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actuaría como una especie de notario

electrónico que extiende un certificado de claves, el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Los certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona, evitando que alguien utilice una clave falsa para suplantar la personalidad de otro.

El mercado ecuatoriano de autoridades de certificación está todavía en desarrollo. Para la contratación on-line existen varias autoridades certificadoras, de las que cabe destacar por su importancia y esfuerzo realizado a **VERISIGN** que proporciona firmas para cualquier servidor SSL (*servidor seguro*) y efectúa estrictas comprobaciones de identidad (Es la más conocida). Los certificados cuestan entre USD 349 y 995.

5.7. SEGURIDAD DE LOS PROGRAMAS DE CORREO ELECTRÓNICO

La seguridad de los programas de correo electrónico, por ejemplo, puede complementarse con mecanismos de cifrado de datos y firma electrónica. En este ámbito, los más extendidos son el protocolo S/MIME y el sistema de cifrado PGP (*Pretty Good Privacy*). El problema que ha tenido la firma digital es que no se ha convertido en un estándar global debido a razones políticas (debido a que debe tener el mismo peso legal que una firma normal), además, todavía no se ha masificado el software necesario.

5.7.1. PGP (PRETTY GOOD PRIVACY)

El PGP ó "*Intimidad bastante Segura*", de Phil's Pretty Good Software, es una aplicación informática de criptografía de alta seguridad para MS-DOS, Unix, VAX/VMS y otros ordenadores. Utiliza criptografía de clave pública (*PKI/Public Key Infrastructure*) para proteger el correo electrónico y los ficheros de datos. Además, se puede comunicar con seguridad con personas a las que nunca se ha visto, sin necesidad de canales seguros para intercambiar claves[52].

El PGP combina la comodidad del criptosistema de clave pública de *Rivest-Shamir-Adleman* (RSA) con la velocidad de la criptografía convencional, es rápido y ofrece muchas prestaciones, entre ellas una completa gestión de claves, resúmenes de mensajes para firmas digitales, compresión de datos antes de encriptar y un buen diseño ergonómico. Por otra parte, PGP realiza las funciones de clave pública con más rapidez que la mayoría de las demás implementaciones informáticas. PGP es criptografía de clave pública para todos. PGP no lleva incorporada comunicación por módem. Para ello debe utilizarse otro programa distinto.

Permite intercambiar ficheros y mensajes con intimidad (*sólo podrán leer el mensaje aquellos a quienes va dirigido*), autenticación (*los mensajes que parecen ser de alguien sólo pueden venir de esa persona en particular*) y comodidad (*no se necesitan canales seguros para intercambiar claves entre usuarios*).

PGP es tan seguro que es prohibido en países, donde sus gobiernos alegan que sería un método de proteger las transmisiones de los delincuentes evitando la vigilancia policial.

5.7.2. S/MIME (SECURE MULTIPURPOSE INTERNET MAIL EXTENSION)

El estándar S/MIME ó (*Extensiones Multipropósito para Correo en Internet*), está definido en la RFC 1521 y se ha desarrollado para poder transmitir mensajes multimedia a través de las redes IP. Es pues una ampliación de e-mail para la transmisión de información multimedia, que convierte en texto cualquier clase de información y que la regenera al formato original en el destino [52].

S/MIME es una aplicación para el correo electrónico que firma y comprueba firmas, permitiendo a los particulares comunicarse entre sí de forma segura. También se emplea en pedidos comerciales por correo. Fue creado en junio de 1992 por IETF (*Internet Engineering Task Force*). El objetivo de S/MIME es permitir a los clientes de correo electrónico enviar y recibir mensajes de texto plano y, también, textos con formatos y figuras, ficheros ejecutables, sonidos, imágenes, etc. El protocolo anterior a S/MIME, SMTP (*Simple Mail Transfer Protocol*), estaba limitado al juego de caracteres ASCII americano, y causaba problemas a los usuarios de otros países que necesitaban caracteres con tilde y símbolos especiales.

Sin embargo, con S/MIME los mensajes de correo electrónico pueden contener: Múltiples objetos en un mensaje simple, texto de longitud ilimitada, conjuntos de caracteres (distintos de ASCII); permitiendo lenguajes diferentes al Inglés, mensajes con fuentes múltiples, archivos binarios o de aplicación específicos, mensajes con imágenes, audio, vídeo y multimedia y campos de encabezado.

Por lo que S/MIME es, actualmente, el protocolo más utilizado para enviar textos con formato no ASCII a través de Internet.

Antes de que se estableciera S/MIME no era posible crear ni leer mensajes que no fueran de texto de una manera fácil; la única posibilidad era codificar los mensajes en un formato propietario, perdiéndose la información no textual si las pasarelas intermedias en la Red no lo soportaban. Con MIME se conserva todo tipo de información y se muestra íntegramente el contenido al receptor.

5.8. SOLUCIONES A LOS PROBLEMAS DE SEGURIDAD

Hoy no se puede decir que la conexión a Internet o a cualquier otra red abierta no se pueda realizar de forma segura, existen las herramientas y la mayoría de ellas seguro que se encuentran incorporadas en el sistema operativo de sus servidores y estaciones de trabajo. Las consecuencias de un mal diseño de red y de seguridad, de la no utilización de herramientas adecuadas y el desconocimiento de lo que le puede estar pasando a nuestra red, son los peores enemigos de cualquier sistema.

Es muy recomendable e incluso imprescindible contar con empresas especializadas en seguridad, para el análisis de necesidades y el mantenimiento y control de los niveles de seguridad. Al ser un tema tan amplio y que evoluciona muy rápidamente, solo las personas que se especializan en estos temas conocen y siguen el día a día de su evolución. Las soluciones a los problemas de seguridad son [48]:

1. Certificados de usuario y de servidores seguros
2. Auditorías de seguridad

5.8.1. CERTIFICADOS DE USUARIO Y DE SERVIDORES SEGUROS

Estos sistemas proporcionan un mecanismo de firma simple y seguro que está basado en los estándares de los navegadores de Internet, Navigator y Explorer (S/MIME). Son procesos optimizados de autenticación de documentos, en los que los mensajes encriptados con la clave pública del destinatario sólo pueden ser descifrados (descifrados) usando la clave privada de éste. Los mecanismos basados en estas fórmulas públicas sólo se pueden utilizar en una única dirección irreversible, sin posibilidad de violar la confidencialidad de los datos que viajan por Internet. La clave privada nunca abandona la máquina del usuario y no se transmite por Internet. Sólo el usuario (es decir, su ordenador) dispone de dicha clave privada. Ésta no podría ser interceptada, y menos aún se podrá descifrar por observadores indeseados.

Gracias a estos sistemas de seguridad las empresas pueden poner en marcha servicios

de transacciones electrónicas, para los cuales sus clientes deben asegurar su identificación mediante certificados digitales. Todas las transacciones que se realicen, ya sea usando un servidor web o mediante e-mail, y que incluyan el envío de datos, pueden llevar incorporadas la firma electrónica y la encriptación del usuario para asegurar el origen e integridad de los datos.

Los certificados de servidor y usuario son emitidos por autoridades certificadoras como IPS Seguridad. Una autoridad certificadora no es más que una entidad que proporciona el certificado después de haber realizado una serie de comprobaciones sobre la identidad del peticionario. Las autoridades certificadoras pueden ser **comerciales** (aquellas que emiten el certificado después que el usuario ha pagado), utilizadas para el acceso seguro del público o de los navegantes a redes web, y **autoridades de tipo interno corporativo** que aseguran el acceso de los empleados a los servidores de la organización.

Este mecanismo automático y transparente no sólo puede certificar la seguridad de un usuario, sino también la del servidor. Los navegadores disponen de un mecanismo de petición de certificados que se activa automáticamente al conectarse a una página web habilitada especialmente, donde se recogen los datos de identificación del usuario. A continuación se generan un par de claves: una privada (que queda residente en la máquina desde la que se hizo la petición) y otra pública (que se envía automáticamente a la autoridad certificadora). Por último, se verifican los datos y se genera el certificado. Al igual que en cualquier transacción inmobiliaria acudimos al despacho

de un notario para que certifique la autenticidad de los documentos presentados, los sistemas avanzados de autenticación electrónica constituyen una Notaría Digital que, como una tercera persona, puede verificar, autenticar y certificar la identidad de los usuarios. Este sistema permite resguardar la confidencialidad e integridad de la información en los nuevos medios abiertos, como Internet, que ofrecen grandes posibilidades para el ocio y el comercio, con las debidas condiciones de seguridad.

5.8.2. AUDITORÍAS DE SEGURIDAD

Las empresas deberían conocer todos los puntos débiles de su seguridad, para darles una solución global, y que, además, puedan ser complementadas con una Auditoría de Seguridad. Las auditorías son actividades muy comunes en estos entornos empresariales, especialmente las realizadas por personal externo, y permiten conocer el nivel de seguridad y las acciones a emprender para corregir los posibles fallos. El hecho de que en general las auditorías las realicen personas externas, permite mantener un nivel de objetividad que muchas veces no se da entre el personal propio, por razones obvias. Una auditoría puede durar, en función del tamaño del sistema, desde unos pocos días, hasta varias semanas. En general siguen normas estrictas y protocolos extensos y requieren fuertes compromisos de apoyo de los recursos internos de la organización en cuestión. Pueden, sin embargo, ser más flexibles.

IPS Seguridad, creó un nuevo servicio de **Análisis de Seguridad para Pymes**. Este nuevo tipo de auditoría permitirá a las empresas que no cuenten con los recursos

económicos o técnicos que exige una auditoría a mayor escala realizar un análisis exhaustivo y suficiente de su seguridad. Es evidente que el peligro no acecha sólo a las grandes corporaciones y que no sólo este tipo de negocios son los negocios importantes, menos aún para los propietarios de los negocios amenazados, por pequeños que sean. El desarrollo de Internet es espectacular y las posibilidades del comercio electrónico son ilimitadas. Lamentablemente, los chicos malos también se multiplican y la libertad de la red se convierte en el paraíso de los traviesos o de los peligrosos que disfrutan rompiendo, robando o haciendo daño.

La auditoría de seguridad es uno de los servicios llamados a un mayor desarrollo en los próximos años. El proceso comienza con un análisis de las amenazas potenciales que enfrentan a una organización. Examina sistemas, políticas y prácticas de la organización para identificar sus vulnerabilidades. El análisis continúa con una valoración de riesgo y concluye con un informe de valoración y una serie de recomendaciones. Con respecto a los costes de la seguridad se puede pensar que son elevados, y en muchos casos los son, especialmente cuando se trata de una auditoría convencional, aunque evidentemente existen diferencias entre las necesidades de cada caso, que se relacionan de forma directa con el coste.

CAPÍTULO VI

6. PORTAL WEB ORIENTADO AL USO DE LOS SERVICIOS ACADÉMICOS Y ADMINISTRATIVOS DE LA PUCESA.

6. ANÁLISIS Y DISEÑO DEL SISTEMA

En éste capítulo se presenta el análisis y diseño del Portal de Servicios Académicos y Administrativos; el mismo que se efectuará basándose en las distintas actividades que se relacionan con este proyecto, las cuales son:

- Necesidades y características del nuevo sistema
- Análisis del flujo de información
- Diseño interior y exterior
- Diseño arquitectónico.

6.1. DESCRIPCIÓN GLOBAL DEL PROYECTO

Durante el proceso de investigación que se ha venido realizando durante el desarrollo de los capítulos anteriores, se ha establecido el propósito del presente proyecto, el cual es desarrollar un software denominado “Portal de Servicios Académicos y Administrativos”, mediante el cual un usuario podrá realizar compras de bienes (cursos/productos/servicios) por Internet que ofrecen las distintas Escuelas de la

P.U.C.E.S.A. (*Pontificia Universidad Católica del Ecuador Sede Ambato*); utilizando como diseñador del sitio web la Tecnología ASP (*Active Server Pages*), MS SQL Server como motor de la base de datos y para la seguridad, el algoritmo de encriptación de datos (MD5).

Se estableció un cuestionario de preguntas (**Ver Anexo C**), el cual fue emitido para cada uno de los Directores de las diferentes Escuelas que forman la P.U.C.E.S.A., para posteriormente mediante entrevistas realizadas con los mismos, se determinase el área o áreas más relevantes que entrarían en el proceso de automatización, las cuales son:

- Productos
- Servicios
- Cursos

En la **Figura 6.1.** se resumen los procesos a seguir para la reservación de los módulos anteriormente señalados:

1. El cliente a través de la red Internet accede al Portal de Servicios Académicos y Administrativos éste se encuentra establecido en el servidor de la Universidad para realizar la reserva de algún Curso, Producto o Servicio; en esta fase al momento de publicar la factura se le indica la forma de Pago adicionándole el Número de la cuenta corriente de ProduBanco.

2. En esta etapa, el cliente se acerca al Banco para realizar la cancelación del Curso, Producto o Servicio; en donde recibe el comprobante de depósito.
3. Posteriormente, el Banco envía la lista de los depositantes a la Universidad, en donde, en la sección administrativa del Portal el administrador comprueba la información del cliente que se encuentra almacenada en las Base de Datos ; se compara con la información enviada por el Banco , esta puede ser : Nombre del Cliente , Forma de Pago y Numero de cédula .
4. Finalmente se le envía una confirmación por correo electrónico, dándole la bienvenida al curso o indicándole el retiro del servicio o producto.

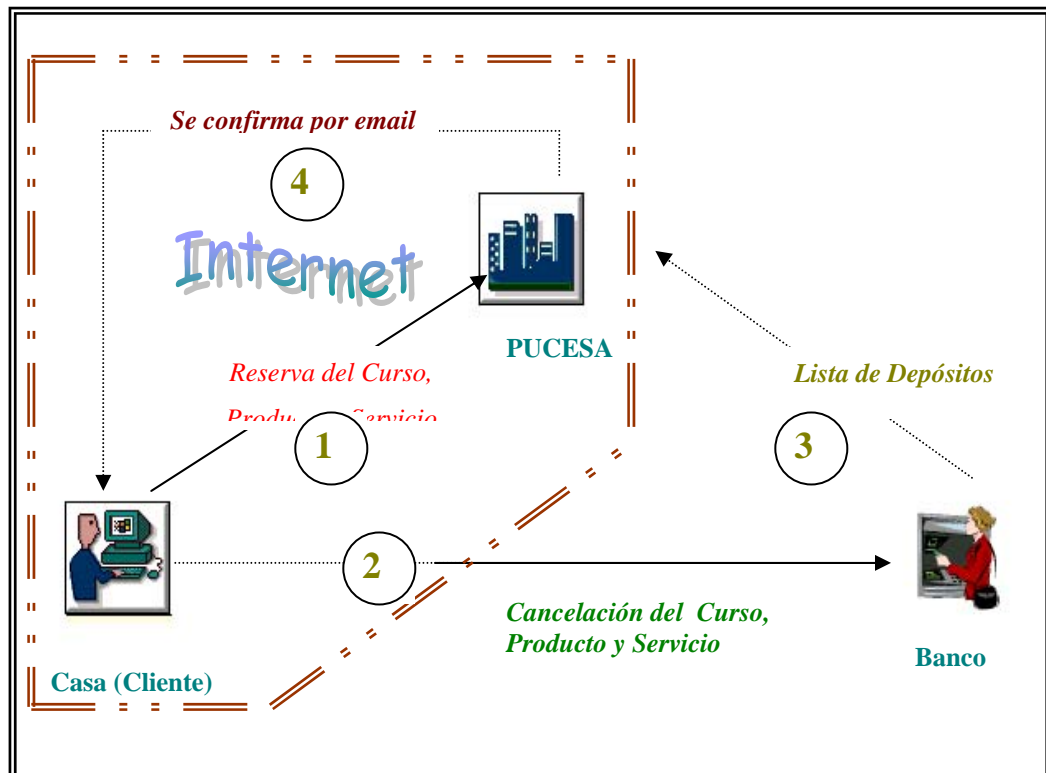


Figura 6.1: Procesos para dar solución a una necesidad de Automatización

6.2. DETERMINACIÓN DE REQUERIMIENTOS

Luego de haber enfocado el proyecto de manera general, proseguiremos en este punto a establecer los requerimientos necesarios para el desarrollo del Software e identificar el Hardware.

6.2.1. METODOLOGÍA PARA EL DESARROLLO DEL SISTEMA

Para la elaboración del presente proyecto, hemos considerado sustentarnos en algunas metodologías existentes que han sido aplicadas en el desarrollo del Portal de Servicios Académicos y Administrativos y de acuerdo a la realidad y necesidades que enfrenta la P.U.C.E.S.A. A continuación se describen los diferentes procesos que se tomarán en cuenta en la presente investigación:

a. Proceso de Pre-Desarrollo: En esta fase se realiza un estudio de las actividades, estructura y características que identifican a cada una de las Escuelas de la P.U.C.E.S.A.; lo que significa recabar la mayor información posible de la misma, que nos permita establecer anomalías que forman parte de una crítica, que a partir de ella se proponen alternativas que resuelvan dicho problema y se realiza un estudio sobre el perfil que tendrá el nuevo sistema en base a la documentación generada. Para el efecto se diseña el flujo de información; las entradas y salidas de los procesos del proyecto, creando así la documentación correspondiente. Finalmente en este proceso se realizan

los estudios de factibilidad para la división del sistema en subsistemas y posterior a esto se realiza el diseño de la estructura e interfaz del mismo.

b. Escogitamiento de la herramienta o lenguaje de programación: En esta fase se realiza un estudio sobre la herramienta de programación seleccionada con el afán de conocer sus ventajas y desventajas. Adicionalmente se presenta la codificación del proyecto.

c. Proceso de Desarrollo: En este literal se determina qué información se debe obtener, en dónde se debe obtener, así como la estructuración de datos y algoritmos a utilizar para la elaboración del portal, llegar a implementarlos, y por último desarrollar el tipo de interfaz. Este proceso tiene tres sub-procesos, los cuales son:

- **Proceso de Requerimientos:** Se definen las características o requerimientos que debe cumplir el software.
- **Proceso de Análisis y Diseño:** Este proceso tiene mayor relevancia, puesto que se establece un estudio de necesidades, las mismas que sirven de inicio para definir el software que las satisfaga, para luego proceder a diseñar la estructura y arquitectura del software. Terminado el análisis y diseño correspondiente se procede a codificar el software.
- **Proceso de Implementación:** El proceso de análisis y diseño anteriormente señalado, se convierte en el software propuesto, elaborado en un lenguaje de programación (ASP) que tenga la capacidad de crear objetos y controles para el

carrito de compras. En este proceso también se genera el código fuente del software con su respectiva documentación.

6.2.2. ESPECIFICACIÓN DE REQUISITOS

Los requisitos de un sistema son **condiciones o características** que debe tener un sistema para satisfacer la necesidad, también se convierten en estándares para su desarrollo y de control de calidad. En este punto, como su nombre lo indica, se describe la especificación de requisitos del software, precisando las capacidades que debe tener un sistema, los procedimientos mediante los cuales se determina si se cumplen o no los requisitos funcionales, de rendimiento y de interfaz del software, de esta manera definimos los entornos de operación y de soporte. A continuación se detallan los requisitos funcionales, de rendimiento y de interfaz:

- a. Requisitos Funcionales:** Especifica la función que debe ser capaz de realizar un sistema, subsistema o componente del sistema.
- b. Requisitos de Rendimiento:** Se especifica las características numéricas, tanto estáticas y dinámicas que debe tener el sistema o subsistema.
- c. Requerimientos de Interfaz:** Se determina características que el sistema o subsistema debe soportar para cada interfaz humana del producto; es decir la interfaz de usuario, así como las características lógicas que debe disponer el sistema, más conocida como interfaz de hardware.

Dentro de este requisito se debe tomar en cuenta la interfaz con otros sistemas, como el navegador, el sistema de base de datos, el sistema operativo, programa para manejo de correo electrónico, y otros productos de software que pudiese utilizar la empresa.

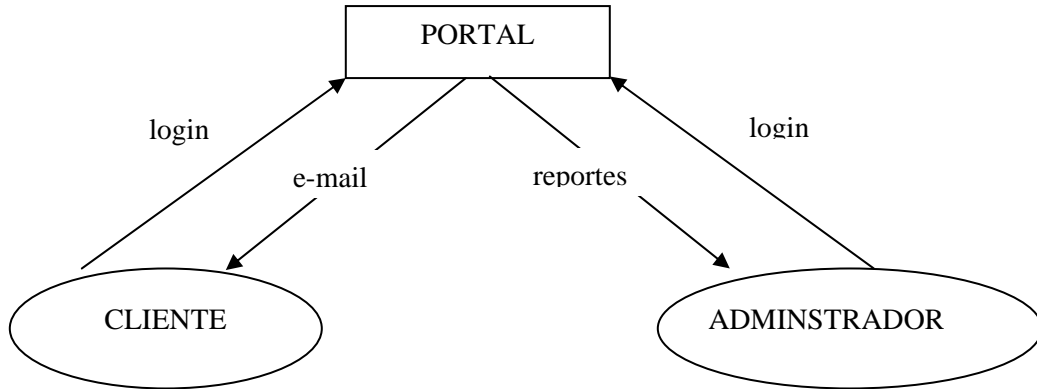
6.3. ANÁLISIS DEL SOFTWARE

En esta etapa se realiza un estudio de cada una de las actividades que la conforman como: el flujo de la información y las responsabilidades; que formarán parte del nuevo sistema.

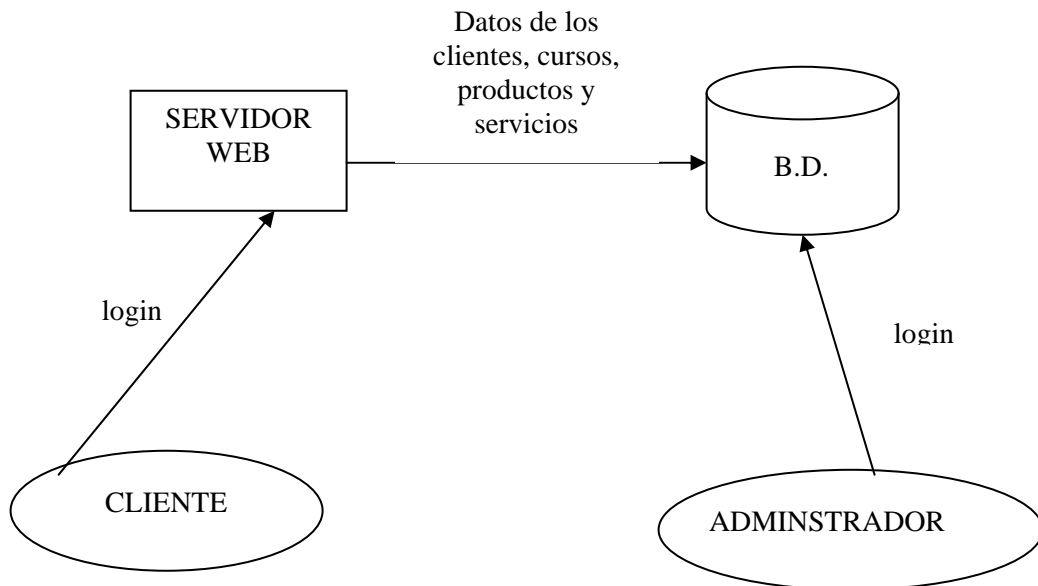
6.3.1. FLUJO DE INFORMACIÓN

El estudio del flujo de información, nos permite tener una idea clara de la creación, utilización y manejo de la información, que permiten realizar el proceso de control de inventarios. Para el diseño del flujo de información, se basó en los requerimientos del nuevo sistema, el mismo que se presentara gráficamente definiendo todos aquellos elementos que involucran los procesos del portal de servicios académicos y administrativos, que se muestran en la **Figura 6.2**.

Nivel 0



Nivel 1



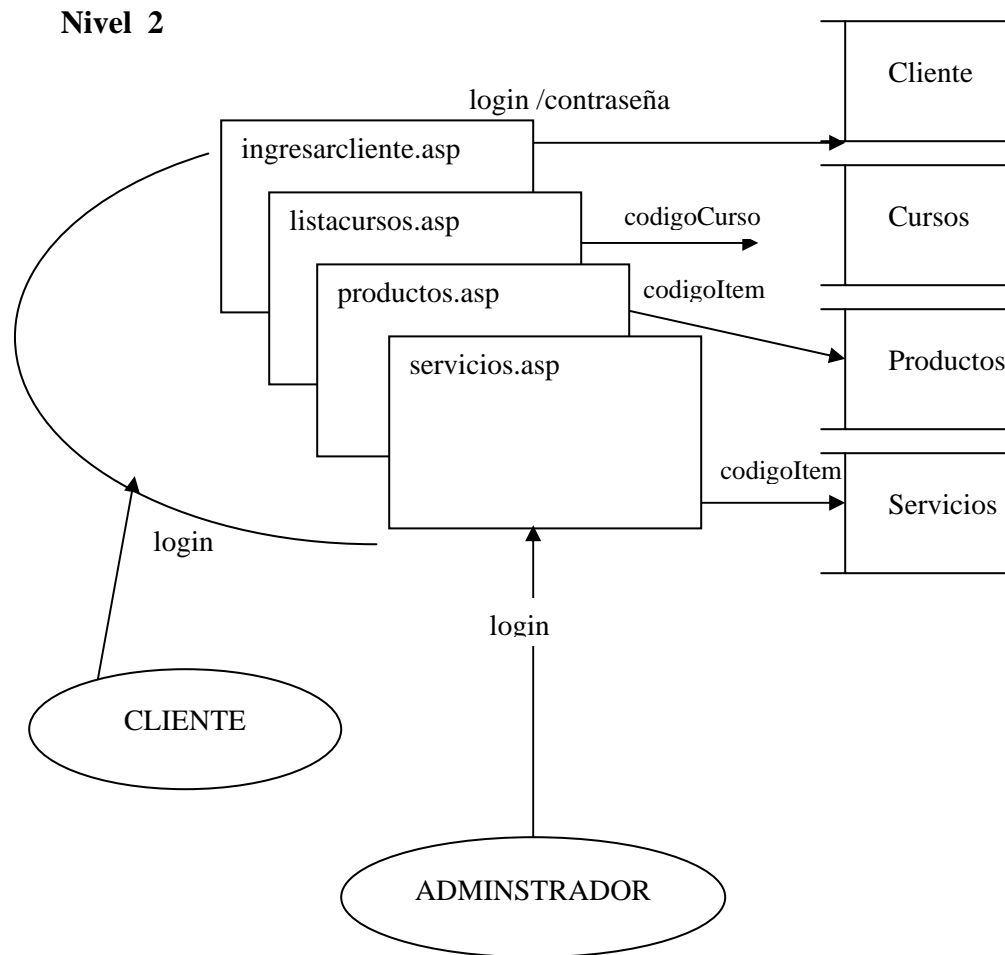


Figura 6.2: Información de los DFD del Portal con los niveles de Implosión

6.3.2. IMPLEMENTACION DEL PORTAL DE SERVICIOS ACADEMICOS Y ADMINISTRATIVOS

Una vez que se han determinado los procesos que se siguen en el análisis y desarrollo de un software en términos generales se va a detallar la aplicación de estos procesos en la elaboración del Portal de Servicios Académicos y Administrativos.

6.3.2.1. RESPONSABILIDADES

En esta fase se determinan las obligaciones que tienen cada una de las entidades involucradas en el Portal de Servicios Académicos y Administrativos, con la finalidad de mostrar la función específica de cada una de ellas.

En la **Tabla 6.1** se resumen las responsabilidades de las entidades que intervienen en el Portal de Servicios Académicos y Administrativos de la P.U.C.E.S.A.

Tabla 6.1: Responsabilidades de las entidades del Portal de Servicios

Entidades	Responsabilidad
Escuela	<ul style="list-style-type: none">• Controlar la información de las diferentes Escuelas
Curso	<ul style="list-style-type: none">• Comprobar si existe• Comprobar precio• Comprobar cupo• Receptar Cursos• Emitir Cursos
Ítem	<ul style="list-style-type: none">• Controlar datos del Ítem• Receptar Servicios, Productos• Emitir Servicios, Productos
Cliente	<ul style="list-style-type: none">• Controlar datos sobre clientes• Petición de Productos y Servicios
Administrador	<ul style="list-style-type: none">• Controlar datos sobre la sección administrativa
Auditoría	<ul style="list-style-type: none">• Obtener datos sobre los diferentes administradores activos.
Variables	<ul style="list-style-type: none">• Controlar el Iva y el descuento.

6.4. DISEÑO DEL SISTEMA

En esta etapa se define al diseño del sistema como un croquis del mismo; se lo divide en tres etapas, las cuales son: diseño externo, diseño arquitectónico y diseño detallado.

6.4.1. SELECCIÓN DE LAS HERRAMIENTAS

Para el desarrollo del presente Portal de Servicios Académicos y Administrativos para la P.U.C.E.S.A., se ha realizado un exhaustivo análisis a cerca de las herramientas de programación que existen en nuestro medio, referente a las siguientes categorías:

6.4.1.1. DESARROLLO DE PÁGINAS WEB DINÁMICAS

Php3, JavaScript, Aplets, CGI, y ASP constituyen los lenguajes mayormente utilizados para el diseño de sitios web dinámicos de carácter comercial, eje principal de nuestro proyecto. Posteriormente, de evaluar la capacidad de soportar tecnología de comercio electrónico, también se analizó, la interfaz de desarrollo que estas herramientas presentan, la velocidad del compilador, la potencia del lenguaje, su complejidad, y su facilidad.

Luego del análisis de las herramientas anteriormente citadas, se decidió utilizar la tecnología **ASP** (*Páginas de Servidor Activas*).

6.4.1.1.1. ASP (ACTIVE SERVER PAGES)

Es una tecnología que trabaja con un lenguaje de tratamiento de textos (scripts), basado en Basic, llamado VBScript (*Visual Basic Script*) o un lenguaje llamado JavaScript. Se utiliza casi exclusivamente en los servidores Web de Microsoft. Las razones para su elección son las siguientes:

- La facilidad para conectar con una base de datos y extraer datos de la misma, dinámicamente visualizándolos en el navegador es la utilidad mas practicada de las páginas ASP.
- Puede conectarse a gestores de bases de datos MS SQL Server, Access, Oracle, o cualquier otro motor que disponga de driver ODBC.
- Es aplicable en el Comercio electrónico, portales, sedes personalizables y todas aquellas aplicaciones en las que el protagonista es la información dinámica.
- Envío de correo electrónico
- Creación dinámica de gráficos
- El servidor web de la P.U.C.E.S.A. está en plataforma Windows.

6.4.1.1.2. REQUERIMIENTOS

Para procesar una página ASP no existe ninguna restricción especial en el lado del cliente, por lo que es indiferente la utilización del navegador Internet Explorer o

Netscape Communicator. Sin embargo, en el lado del servidor, es necesario un servidor Web de Microsoft. Se utiliza el archivo ASP.DLL para interpretar el código, siendo el servidor más extendido Internet Information Server (más conocido como IIS).

La mayoría de proveedores de Hosting pagado con plataformas NT tienen acceso a esta tecnología en sus servidores. El código puede ser trabajado en cualquier editor HTML o de texto. Existen en el mercado dos herramientas para trabajar profesionalmente el ASP en modo visual como: Dreamweaver UltraDev 4, Drumbeat 2000 y el Visual Interdev de Microsoft.

Aunque también existan muchos otros factores, como temas de utilización, documentación, soporte, etc. hemos creído conveniente que lo antes anotado es suficiente para haber elegido ASP.

6.4.1.1.3. POR QUÉ MACROMEDIA DREAMWEAVER ULTRADEV Y ASP

UltraDev es un entorno profesional de creación de aplicaciones Web, facilita la creación, administración y edición de páginas Web para múltiples plataformas y navegadores. Puede crear sus propios objetos, comandos y comportamientos de servidor, modificar menús y métodos abreviados de teclado, e incluso escribir secuencias de comandos para ampliar UltraDev con nuevas acciones, comportamientos e inspectores de propiedades. La habilidad de fusionarse con el ASP nos ayuda a simplificar las tareas de creación de páginas dinámicas, la codificación

manual de secuencias de comandos de servidores, la escritura de comportamientos de servidor personalizados y la creación de conexiones de base de datos.

6.4.1.1.4. INSTALAR DREAMWEAVER ULTRADEV

Para ejecutar Dreamweaver UltraDev, es preciso disponer del hardware y el software siguiente:

Para Microsoft Windows:

- Un procesador Intel Pentium o equivalente a 166 MHz o más rápido que ejecute Windows 95, Windows 98, Windows Me, Windows NT 4.0 con Service Pack 5 o Windows 2000.
- 64MB de memoria de acceso aleatorio (RAM), además de 170 MB de espacio libre en el disco duro.
- Macromedia Flash Player para ver las Visitas guiadas y las Lecciones. El CD incluye un archivo instalador de Flash Player.

6.4.1.2. SERVIDOR WEB

Para hacer una rápida mirada a este tema, podemos mencionar que existen dos sistemas operativos dominantes del mercado de los servidores web, Unix y Windows

NT. Los servidores web más utilizados son Apache Server e Internet Information Server (IIS) respectivamente.

6.4.1.2.1. INTERNET INFORMATION SERVER (IIS)

En lo más elemental, un servidor de Web como IIS es un servicio que recibe solicitudes de información, en la forma de URLs, desde los exploradores y devuelve páginas en HTML. Al crecer más los sitios Web y el contenido dinámico se vuelve más popular, los servidores de Web han expandido su rango de funcionalidad más allá de sólo dar servicio a las solicitudes de http.

IIS, por ejemplo, ofrece: Soporte para la administración de un sitio, así como su publicación, seguridad y comunicación de bases de datos además de servicios de HTTP, FTP y gopher.

6.4.1.3. BASE DE DATOS

Un sistema de administración de Bases de Datos *RDBMS (Relational Data Base Management System)*, es una colección de datos relacionados y un conjunto de programas para acceder a estos datos, nos permite almacenar información relacionada, y poder consultarla en forma eficiente. El objetivo es proporcionar un ambiente eficiente para almacenar y recuperar datos en la base de datos.

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, Interbase, Oracle o Paradox*, etc.

Particularmente en nuestra aplicación, hemos optado por Microsoft SQL Server 7.0; ya que está plagado de nuevas características.

6.4.1.3.1. MICROSOFT SQL SERVER

Es un sistema administrador para Bases de Datos relacionales basadas en la arquitectura Cliente / Servidor (RDBMS) que usa Transact-SQL para mandar peticiones entre un cliente y el SQL Server.

Requerimientos mínimos de hardware

SQL Server 7.0 requiere el siguiente hardware como mínimo:

- **Computadora:** DEC Alpha AXP y sistemas compatibles, Intel o compatibles (Pentium 166 MHz o superior, Pentium PRO, o Pentium II).

- **Memoria:** 32 MB de RAM.
- **Unidad de Disco:** Un CD-ROM, más un disco duro con al menos 80 MB de espacio libre en disco para la instalación mínima.

En la **Tabla 6.2** se muestra la cantidad mínima de espacio disponible en disco que requieren las diferentes instalaciones:

Tabla 6.2: Cantidad mínima de espacio en disco

Opción de Instalación	Espacio en Disco
Completa	210 MB
Típica	185 MB
Herramientas de administración	90 MB
Mínima	80 MB

SQL fue escogido por los siguientes aspectos:

- SQL Server ofrece un conjunto de capacidades diseñadas para facilitar la construcción, el despliegue y la gestión de aplicaciones *cliente/servidor* distribuidas.

- Simplifica la creación y gestión de aplicaciones Internet e Intranet.
- La habilidad de trabajar juntos con Internet Information Server para generar páginas dinámicas de HTML.
- Asegura la integridad de la base de datos bajo grandes cargas de transacciones y actualizaciones.
- Mantenimiento de servicios de distribución de datos entre múltiples computadoras.
- Mantenimiento de aplicaciones orientadas a transacciones.
- Contribución a reducir el tiempo del desarrollo el sitio Web para sitios con gran volumen de datos relacionados al aprovechar la base de datos en segundo plano para crear unas pocas plantillas de HTML cuyos datos deberán ser vaciados en cientos o aún miles de páginas estáticas de HTML.

6.4.1.4. 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 a 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* (*manejador*) 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 podremos hacer referencia en *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.

Además de estos beneficios, IIS y SQL Server están estrechamente integrados unos con otro y con Windows NT® y Windows® 2000 Server. Tanto IIS como SQL Server están diseñados para aprovechar las ventajas de la seguridad, análisis del rendimiento y las funciones de registros de sucesos de Windows NT y Windows 2000. **Internet**

Database Connector (IDC) y Active Server Pages proporcionan un acceso a SQL Server desde IIS. Esta adherencia permite al desarrollador enfocarse en la funcionalidad de la aplicación en lugar de desarrollar las rutas de comunicación entre el sistema operativo, el servidor Web y la base de datos.

6.4.1.5. ALGORITMO DE ENCRIPCIÓN DE DATOS

Para las seguridades del Portal, se escogió el algoritmo de encriptación de datos MD5 realizado en JavaScript y; para el login con la clave de acceso del cliente se aplicó un sencillo algoritmo de encriptación-desencriptación de datos.

6.4.1.5.1. ALGORITMO DE ENCRIPCIÓN DE DATOS (MD5)

El algoritmo MD5 es una función de cifrado tipo *hash* que acepta una cadena de texto como entrada, y devuelve un número de 128 bits. Las ventajas de este tipo de algoritmos son la imposibilidad (computacional) de reconstruir la cadena original a partir del resultado, y también la imposibilidad de encontrar dos cadenas de texto que generen el mismo resultado.

Esto nos permite usar el algoritmo para transmitir contraseñas a través de un medio inseguro. Simplemente se cifra la contraseña, y se envía de forma cifrada. En el punto de destino, para comprobar si el password es correcto, se cifra de la misma manera y se comparan las formas cifradas.

Posteriormente se utilizó un sistema de codificación de tarjetas de crédito, débito y otras. El algoritmo que se describe en esta fase es válido para la mayor parte de tarjetas, no solo las de crédito o débito, sino la de grandes centros comerciales; este algoritmo se aplicó para controlar la validez de la tarjeta de crédito.

Descripción del Número de Tarjeta

El número se compone de tres partes principales:

- a. Los cuatro primeros dígitos componen el identificador del banco que cede la tarjeta.** Hay un número diferente para cada banco pero estos números no son los mismos de acuerdo al continente en que se esté. Según esto el número de CITIBANK en E.E.U.U. es el 4013, mientras que en Europa es el 4539.
- b. El quinto dígito es el tipo de tarjeta e indica que entidad financiera gestiona ese plástico.** Las más importantes son: Visa, American Express y MasterCard. Los diez dígitos siguientes componen el número de usuario e identifican a éste de manera única. El dígito de control es el último número y se obtiene aplicando un algoritmo al resto del número. El formato es el siguiente: **1111 2333 3333 3334**

Donde:

- El identificador esta representado por **1111** el cual es un número de cuatro dígitos siendo cada dígito un número del 0 al 9.

- El tipo esta representado por el 2 el cual es un número de un solo dígito siendo cualquier número del 0 al 9.
- El número de usuario esta representada por 333 3333 333 el cual es un número de diez dígitos siendo cada dígito un número del 0 al 9.
- El dígito de control esta representado por el 4 el cual es un único número del 0 al 9.

c. El identificador del Banco

- Cada banco o entidad financiera que distribuye tarjetas lleva un número de cuatro dígitos que lo identifica.
- *Tipo de Tarjeta*

El 5° dígito identifica al tipo de tarjeta de acuerdo a los valores; que se muestra en la **Tabla 6.3**.

Tabla 6.3: Tipo de tarjeta de acuerdo a los valores

Tipo	Entidad Financiera
3	American Express
4	Visa
5	Master Card
6	Discover

6.4.1.5.2. ALGORITMO DE CODIFICACIÓN DEL NÚMERO

La codificación del número de la tarjeta se realiza en tres pasos:

- Se multiplican por dos todos los dígitos de las posiciones impares y aquellos mayores de 9 se suman los dos dígitos.
- Después de calcular los nuevos números de las posiciones impares se suman entre sí todos los dígitos.
- Si el resultado es múltiplo de 10 entonces el número de tarjeta es valido.
Resultado MOD 10 = 0

Ejemplo:

Si tenemos el número de tarjeta 4539 4512 0398 7356 y queremos comprobar que es un número válido:

1ro. Multiplicar por dos los números de las posiciones impares (4 - 3 - 4 - 1 - 0 - 9 - 7 - 5) y dejarlos con un solo dígito:

$$4 \times 2 = 8$$

$$3 \times 2 = 6$$

$$4 \times 2 = 8$$

$$1 \times 2 = 2$$

$$0 \times 2 = 0$$

$$9 \times 2 = 18 \rightarrow 1 + 8 = 9$$

$$7 \times 2 = 14 \rightarrow 1 + 4 = 5$$

$$5 \times 2 = 10 \rightarrow 1 + 0 = 1$$

Los últimos tres, como dieron más de 9 se los sumó entre sí.

2do. Sumar los dígitos de las posiciones pares y los nuevos de las posiciones impares.

$$5 + 9 + 5 + 2 + 3 + 8 + 3 + 6 + 8 + 6 + 8 + 2 + 0 + 9 + 5 + 1 = 80$$

3ro. 80 es múltiplo de 10 por lo que el número de tarjeta es válido.

6.5. REFINAMIENTO DEL ANÁLISIS

Una vez analizado el sistema, se realizará su refinamiento, esto es realizando el diseño arquitectónico del mismo (Ver **Figura 6.3**), el diseño de la base de datos y por ultimo sus respectivas relaciones (Ver **Figura 6.4**).

- **Diseño Arquitectónico**

En esta fase se establece un bosquejo real de la forma estructural del Portal de Servicios Académicos y Administrativos de la P.U.C.E.S.A.

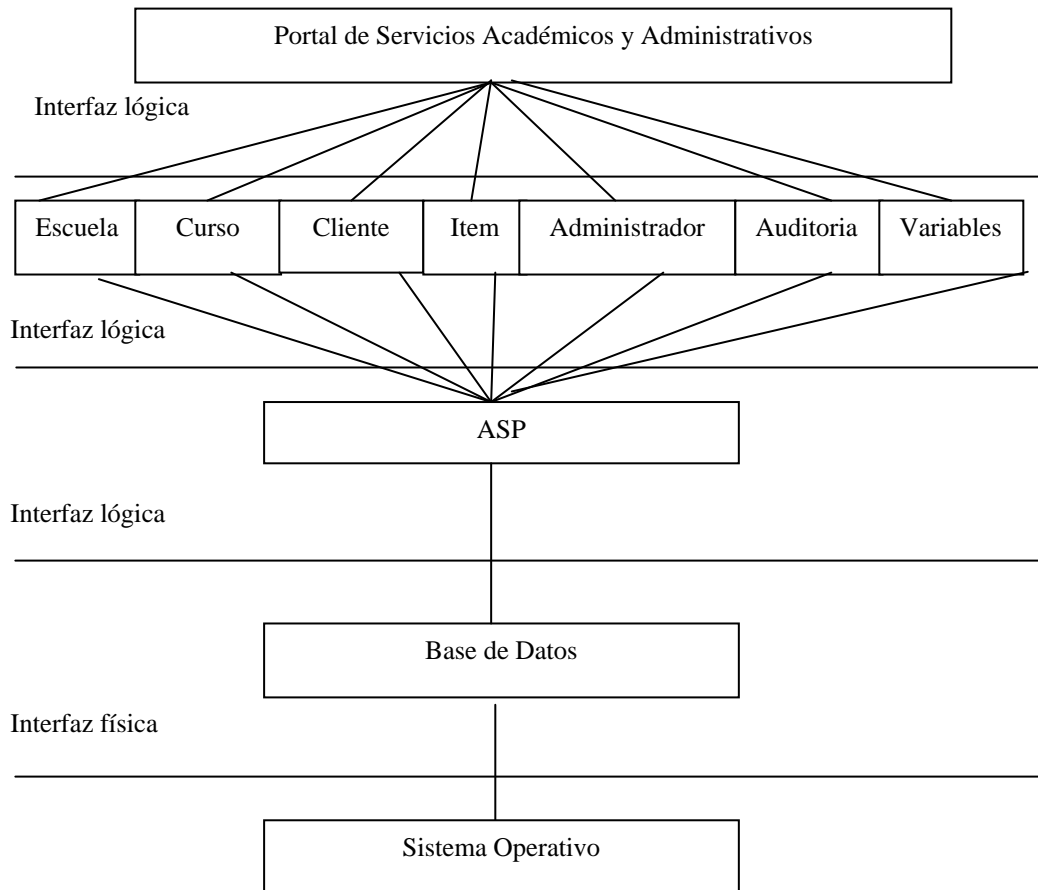


Figura 6.3: Diseño Arquitectónico

- **Diseño de la base de datos**

Definición de tablas

1. En esta tabla se almacena toda la información a cerca de las diferentes escuelas de la P.U.C.E.S.A. (Ver **Tabla 6.4**)

Tabla 6.4: Almacena Información de las Escuelas

<i>Base de Datos : PUCE</i>			
<i>Tabla : Escuela</i>		<i>Función: Almacena Información de las Escuelas</i>	
Campo	Tipo	Longitud	Descripción
codigoEscuela	Int	4	Código de la Escuelas
Nombre	Varchar	50	Nombre de la Escuelas
Telefono	Varchar	8	Teléfono de la Escuelas
Dirección	Varchar	50	Dirección de la Escuelas

2. Esta tabla tiene la función de almacenar los diferentes datos de los cursos que van a estar dentro del Portal. (Ver **Tabla 6.5**)

Tabla 6.5: Almacena datos de los cursos

<i>Base de Datos: PUCE</i>			
<i>Tabla: Curso</i>		<i>Función: Almacena datos de los cursos</i>	
Campo	Tipo	Longitud	Descripción
codigoCurso	int	4	Código del curso
codigoEscuela	int	4	Código de la escuela
Nombre	varchar	30	Nombre del curso
duracionHoras	int	4	Duración en horas del curso
fechaInicio	datetime	8	Fecha de Inicio del curso
fechaFinal	datetime	8	Fecha de Finalización del curso
Horario	varchar	30	Horario del curso
Dirigido	varchar	60	A que público esta dirigido
Profesor	varchar	30	El profesor que expone el curso
Costo	money	8	Costo del curso
Cupo	int	4	Cupo de alumnos participantes
Foto	varchar	60	Fotografía del curso
Estado	char	1	El curso esta Disponible o no

3. En esta tabla se guarda el detalle de los cursos que van a estar expuestos dentro del Portal. (Ver **Tabla 6.6**)

Tabla 6.6: Guarda el detalle de cada curso

<i>Base de Datos : PUCE</i>			
<i>Tabla:</i> MovimientoCurso	<i>Función:</i> Guardar detalle de los cursos		
Campo	Tipo	Longitud	Descripción
nVentaCurso	varchar	60	Numero de la venta del curso
codigoCurso	int	4	Código del curso
Cantidad	int	4	Existencia de cursos
costoUnitario	money	8	Costo unitario del curso
Iva	money	8	Impuesto

4. En esta tabla se almacena Información acerca de las ventas de los cursos. (Ver **Tabla 6.7)**

Tabla 6.7: Almacena información de las ventas de los cursos

<i>Base de Datos : PUCE</i>			
<i>Tabla :</i> VentaCurso	<i>Función:</i> Almacena Información de las ventas de los cursos		
Campo	Tipo	Longitud	Descripción
nVentaCurso	varchar	60	Número de la venta del curso
codigoCliente	int	4	Código del cliente
fechaVenta	datetime	8	Fecha en que se hizo la venta
descuento	varchar	10	Valor de descuento
nTarjeta	varchar	30	Número de la Tarjeta
nombreTarjeta	varchar	30	Nombre de la tarjeta

5. Esta tabla guarda el detalle de los colaboradores del administrador, otorgándoles los permisos correspondientes a cada uno de ellos. (Ver **Tabla 6.8)**

Tabla 6.8: Guarda el detalle de los colaboradores del administrador

<i>Base de Datos : PUCE</i>			
<i>Tabla :</i> Auditoria	<i>Función:</i> Guardar detalle de los administradores		
Campo	Tipo	Longitud	Descripción
codigoAdministrador	int	4	Código del administrador
fechaCreación	datetime	8	Fecha de Ingreso del Administrador
Opcion	varchar	60	Los permisos otorgados

6. En esta tabla se almacena la información de los clientes que ingresan a nuestro Portal. (Ver **Tabla 6.9**)

Tabla 6.9: Almacena datos de los clientes

<i>Base de Datos:</i> PUCE			
<i>Tabla:</i> Cliente		<i>Función:</i> Almacena datos de los clientes	
Campo	Tipo	Longitud	Descripción
codigoCliente	int	4	Código del cliente
Nombre	varchar	30	Nombre del cliente
Apellido	varchar	30	Apellido del cliente
Cedula	varchar	11	Cédula del cliente
fechaIngreso	datetime	8	Fecha de Ingreso
Ciudad	varchar	30	Ciudad del cliente
Provincia	varchar	30	Provincia del cliente
Dirección	varchar	30	Dirección del cliente
Telefono	varchar	8	No. Telefónico del cliente
Email	varchar	60	Correo electrónico
Ncompras	int	4	Código de la compra

7. En esta tabla se almacena los datos de los diferentes Servicios y Productos que ofrece el Portal. (Ver **Tabla 6.10**)

Tabla 6.10: Almacena datos de los Servicios y Productos

<i>Base de Datos:</i> PUCE			
<i>Tabla:</i> Item		<i>Función:</i> Almacena datos de los Servicios y Productos	
Campo	Tipo	Longitud	Descripción
codigoItem	int	4	Código del Item
codigoEscuela	int	4	Código de la Escuelas
Nombre	varchar	60	Nombre del Item
Tipo	varchar	30	Servicio / Producto
Existencia	int	4	Existencia de Servicio/ Producto
Detalle	varchar	120	Detalle de Servicio/ Producto
Precio	money	8	Precio Servicio/ Producto
Foto	varchar	60	Fotografía de los Items
Eliminado	char	1	Si esta eliminado algún Item

8. Esta tabla tiene la función de guardar el detalle de los Servicios y Productos. (Ver **Tabla 6.11**)

Tabla 6.11: Guardar detalle de los Items

<i>Base de Datos</i> : PUCE			
<i>Tabla:</i> MovimientoItem		<i>Función:</i> Guardar detalle de los Items	
Campo	Tipo	Longitud	Descripción
NVentaItem	varchar	60	Numero de la venta de Items
CodigoItem	int	4	Código del Item
Cantidad	int	4	Existencia de Items
costoUnitario	money	8	Costo unitario del Item

9. La función de esta tabla es la de almacenar la información del administrador del Portal. (Ver **Tabla 6.12**)

Tabla 6.12: Almacena la información del administrador del Portal

<i>Base de Datos</i> : PUCE			
<i>Tabla:</i> Administrador		<i>Función:</i> Almacena Información del administrador	
Campo	Tipo	Longitud	Descripción
CodigoAdministrador	int	4	Código del administrador
Nombre	varchar	30	Nombre del administrador
Email	varchar	60	Correo electrónico
Clave	varchar	15	Clave del administrador
fechaCreación	datetime	8	Fecha de Creación del Administrador

10. La función principal de esta tabla es la de almacenar la información del Iva y del descuento. (Ver **Tabla 6.13**)

Tabla 6.13: Almacena Información del Iva y del Descuento

<i>Base de Datos</i> : PUCE			
<i>Tabla</i> : Variable		<i>Función:</i> Almacena Información del Iva y del Descuento	
Campo	Tipo	Longitud	Descripción
codigoVariable	int	4	Código de la Variable
Iva	money	8	Valor del iva
Descuento	money	8	Valor del descuento
fechaIngreso	datetime	8	Fecha de Ingreso de las variables

- **Relación entre las tablas**

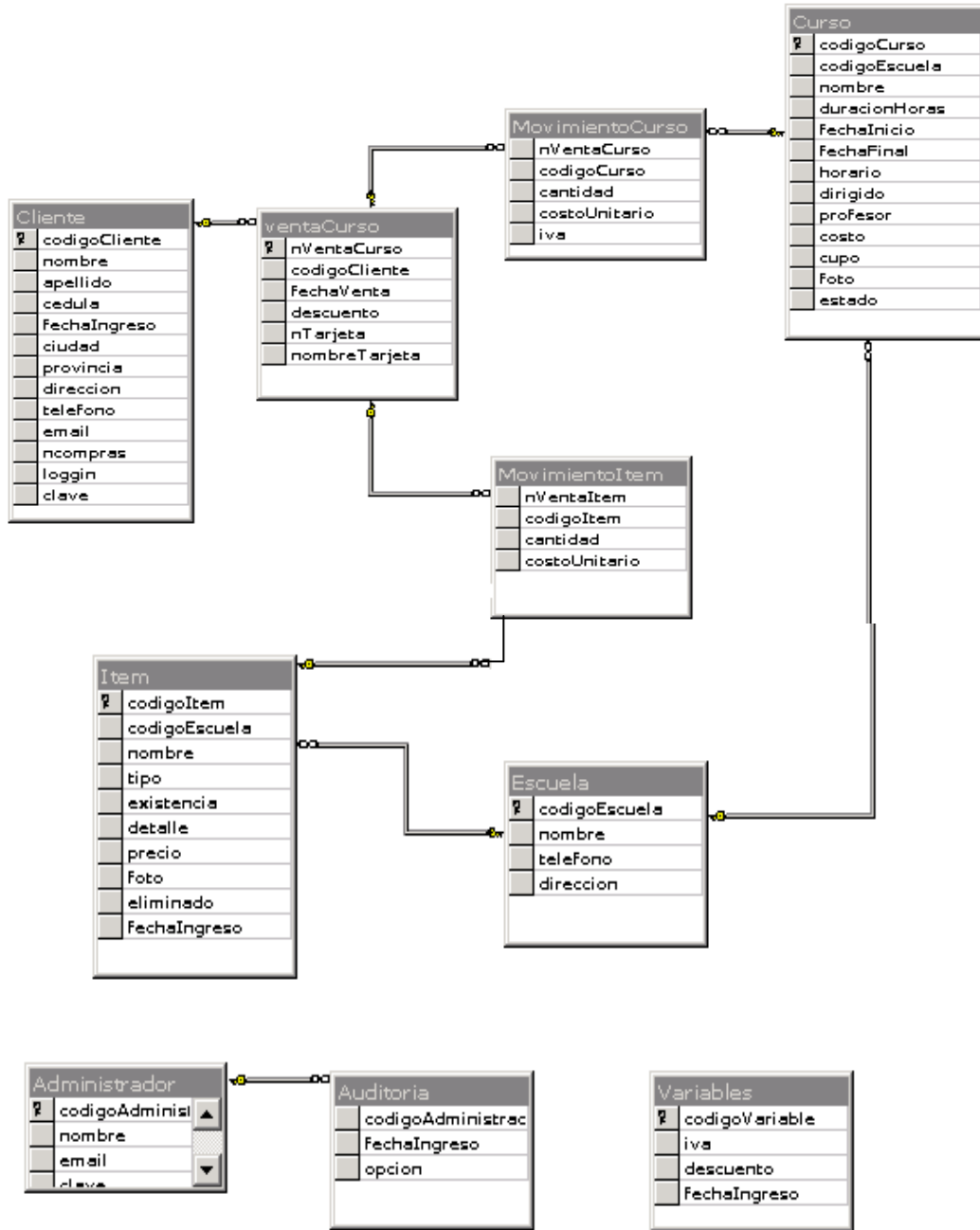


Figura 6.4: Relaciones entre las Tablas

6.6. REPRESENTACIÓN DEL MODELO GLOBAL DEL SISTEMA

La **Figura 6.5** representa en forma global el sistema identificando las respectivas jerarquías de las entidades, las cuales van a fusionar en la ejecución del Portal.

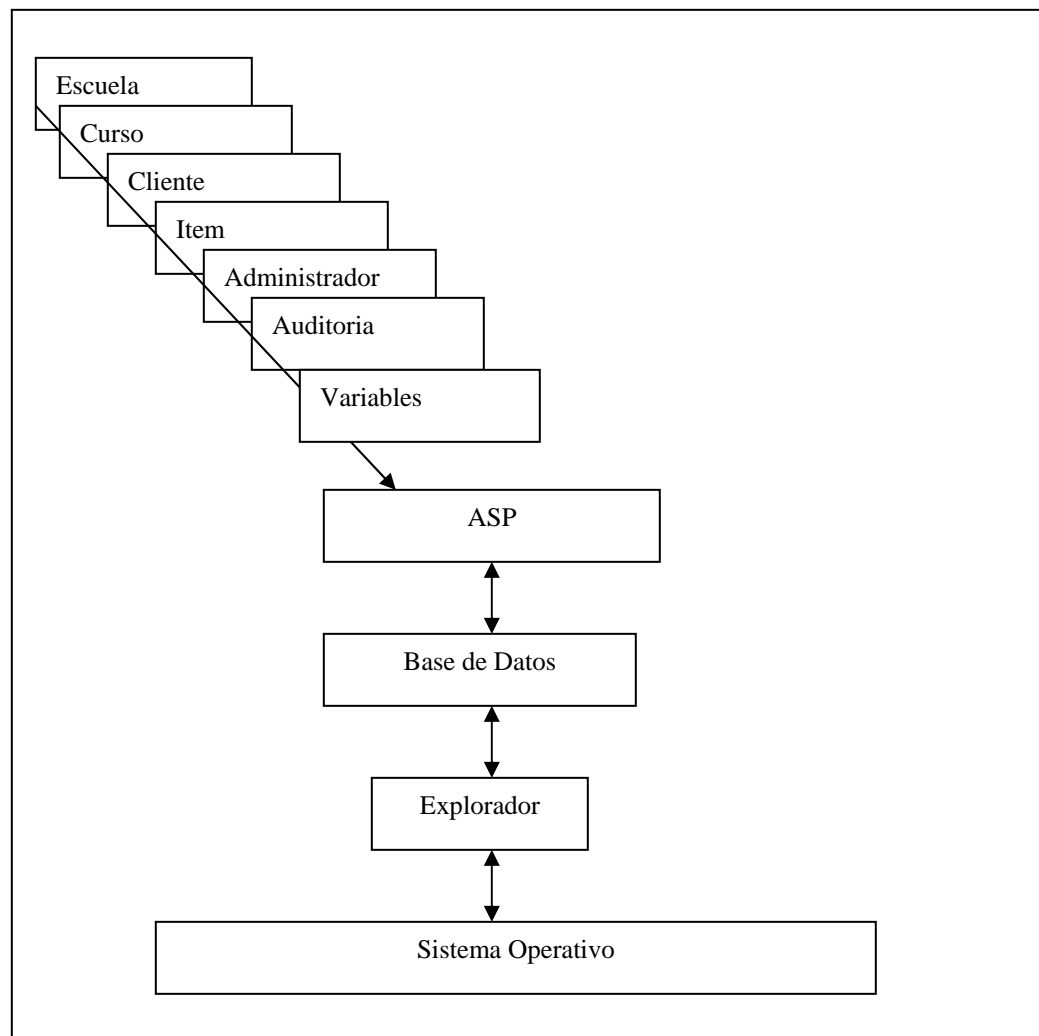


Figura 6.5: Jerarquía de Entidades

6.6.1. CAPAS DEL PORTAL DE SERVICIOS

En esta Figura se identifica las diferentes capas que conforman el Portal tomando en cuenta que el Portal consta de cinco capas como se muestra en la **Figura 6.6**.

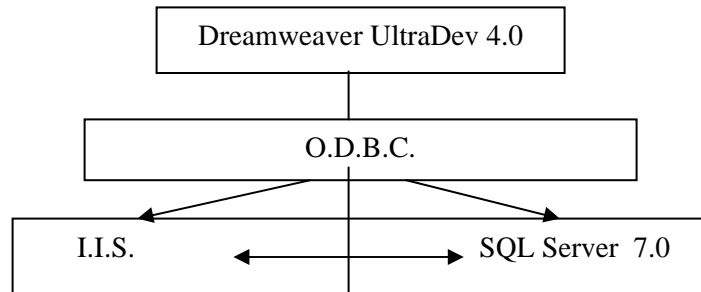


Figura 6.6: Capas del Portal de Servicios Académicos y Administrativos

6.7. DISEÑO DE INTERFAZ

Para establecer prioridades hemos empezado a edificar la interfaz cliente – servidor con las siguientes características:

6.7.1. INTERFAZ CLIENTE-SERVIDOR

- **Características del Cliente-Servidor**

En las siguientes tablas se listan las diferentes características para el Cliente – Servidor. **Tabla 6.14 y 6.15**

Tabla 6.14: Características del Cliente

Sistema Operativo	Browser
Windows 95	Internet Explorer 3.0
Windows 98	Internet Explorer 4.0
Windows 2000	Internet Explorer 4.0

Tabla 6.15: Características del Servidor

Internet Information Server
Windows 2000 server
SQL Server
ODBC

- **Procesos del Cliente –Servidor**

En la **Tabla 6.16** se muestra los diferentes procesos que se ejecutan tanto en el Cliente como en el Servidor.

Tabla 6.16: Procesos del Cliente–Servidor

CLIENTE	<u>SERVIDOR</u>
Registrarse	Agregar Usuarios de administración del Sistema
Reservar Cursos	Agregar Cursos, Productos, Servicios
Adquirir Productos	Eliminar Cursos, Productos, Servicios
Obtener Servicios	Modifica Cursos, Productos, Servicios
Pago confiable	Establece seguridades

- **Procesos de encriptación**

a. Encriptación de la Contraseña

- 1) El cliente ingresa el login
- 2) Luego ingresa la contraseña y se mostrará con (*****)
- 3) Al presionar INGRESAR, en la contraseña se aplica el proceso de encriptación (MD5) y posteriormente este código encriptado se guarda en la Base de Datos. (Ver **Figura 6.7**)

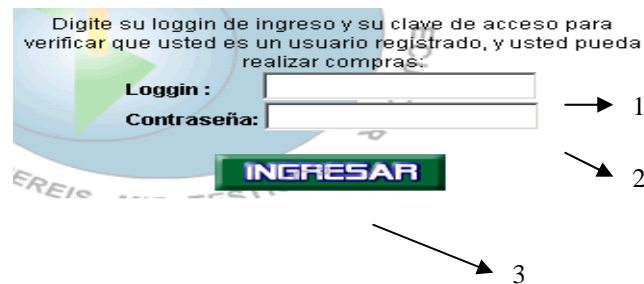


Figura 6.7: Encriptación del login y la contraseña del cliente

b. Encriptación de la Tarjeta de Crédito

- 1) El cliente ingresa la tarjeta de Crédito
- 2) Se verifica si el número de la tarjeta es real.

- 3) En el momento que presionamos Facturar Comprar el número de la tarjeta de crédito se encripta aplicando un algoritmo de seguridad y posteriormente este código encriptado se guarda en la Base de Datos, como se muestra en la siguiente **Figura 6.8**

1

Tarjeta de Crédito: 6

Número de Tarjeta: 12344343414234

2

Tarjeta de crédito: Mastercard Internacional

Detalle					
Nombre del Curso	Inicia	Finaliza	Duración(h)	Horario	Costo (USD)
aaaa	01/09/2001	01/10/2001	20	7h30 a 12h30	20

Subtotal: 20
Descuento: 0
IVA (14%): 2.8
(USD) Total a pagar : 22.8

Facturar Compra

Continuar Comprando

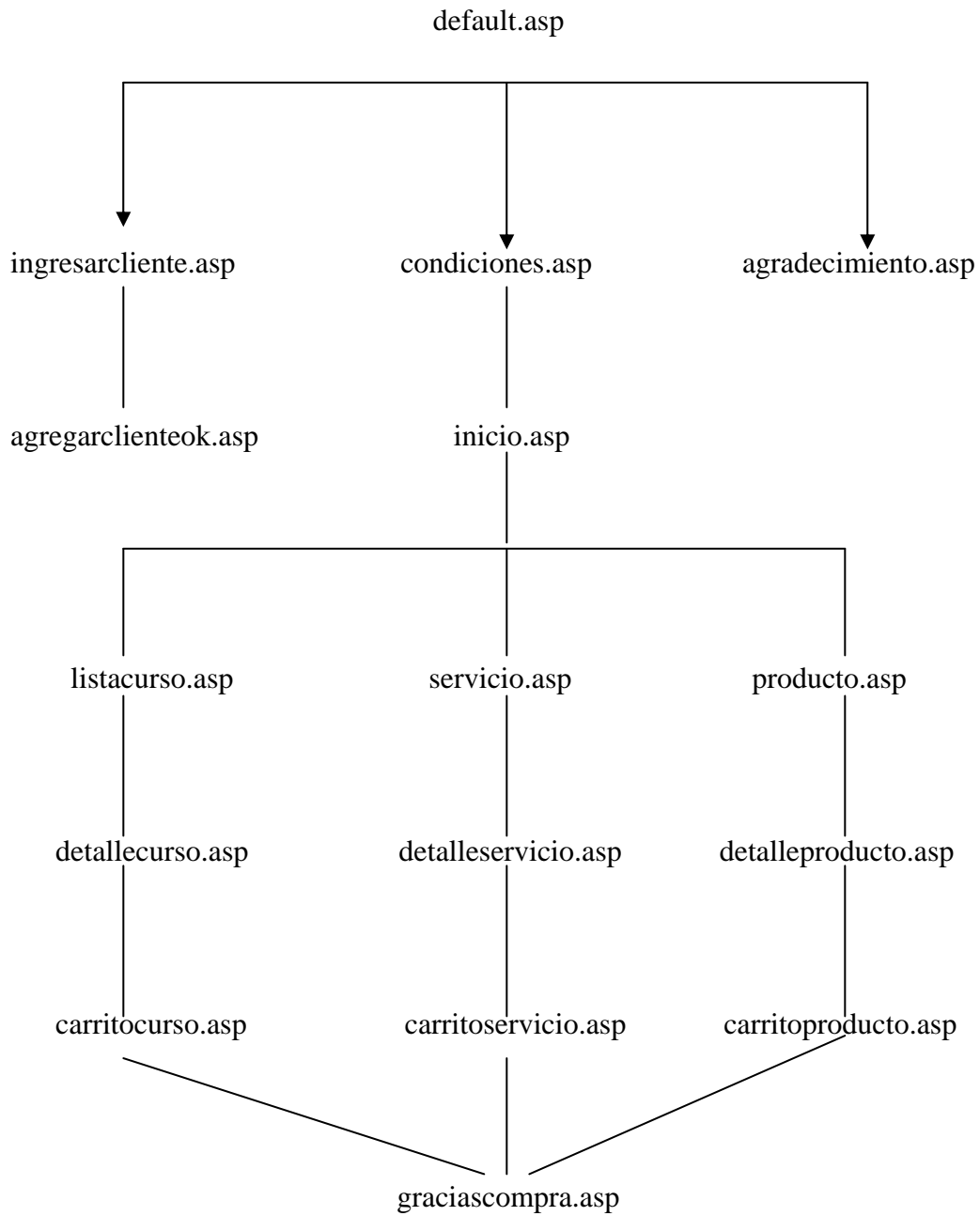
Imprimir

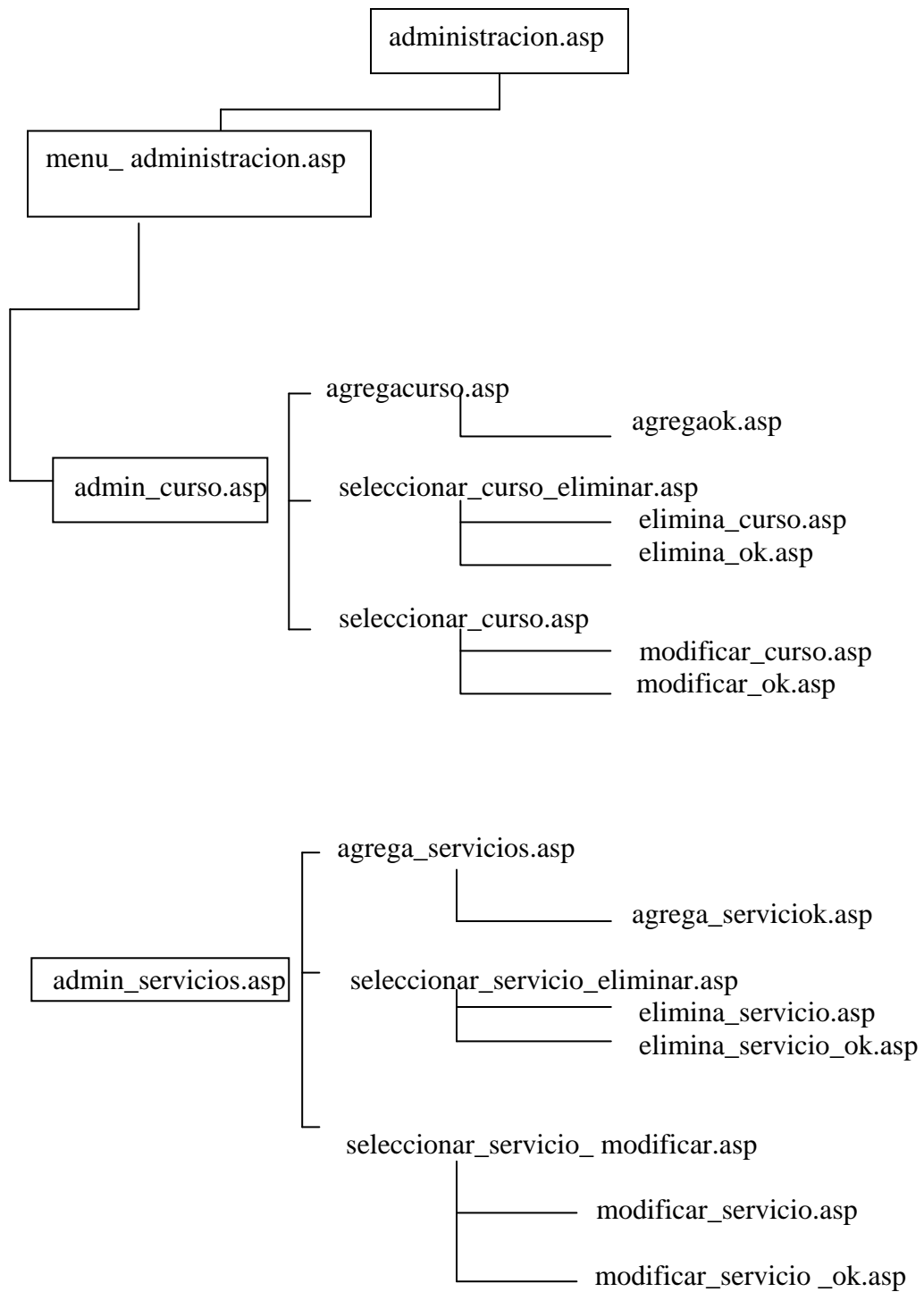
3

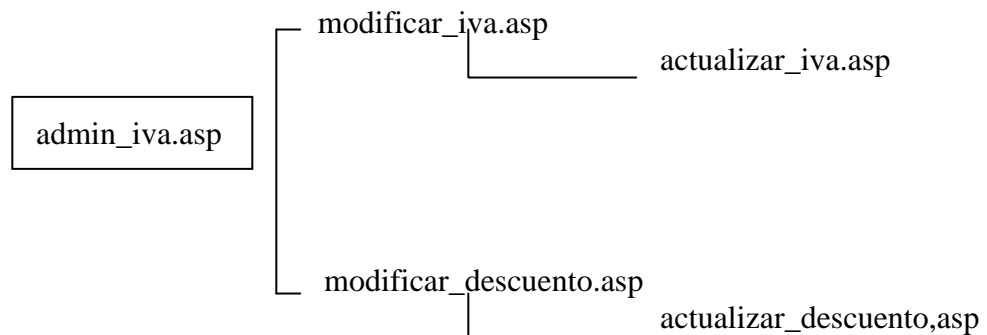
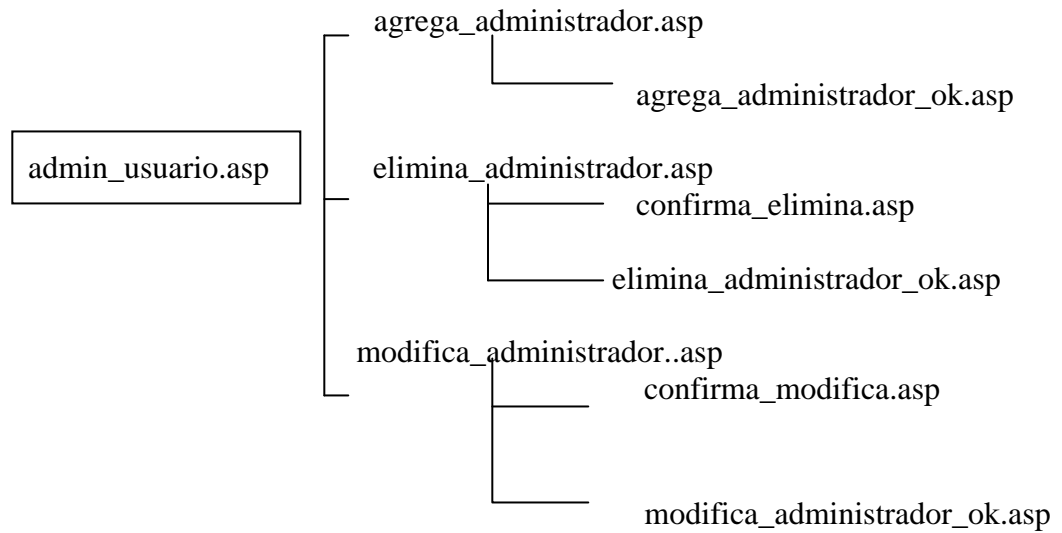
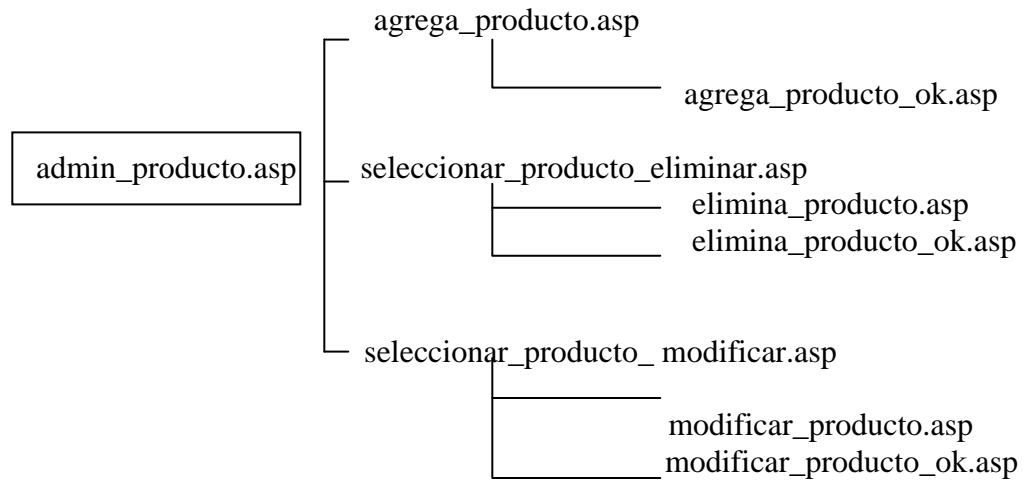
Figura 6.8: Encriptación de la Tarjeta de Crédito

6.7.2. INTERFAZ GRAFICA

Para diseñar la Interfaz gráfica nos basamos en las herramientas que nos ofrece Flash 4 y Dreamweaver UltraDev 4, en el siguiente esquema de interfaz se muestra los enlaces de cada una de las pantallas. **Figura 6.9**







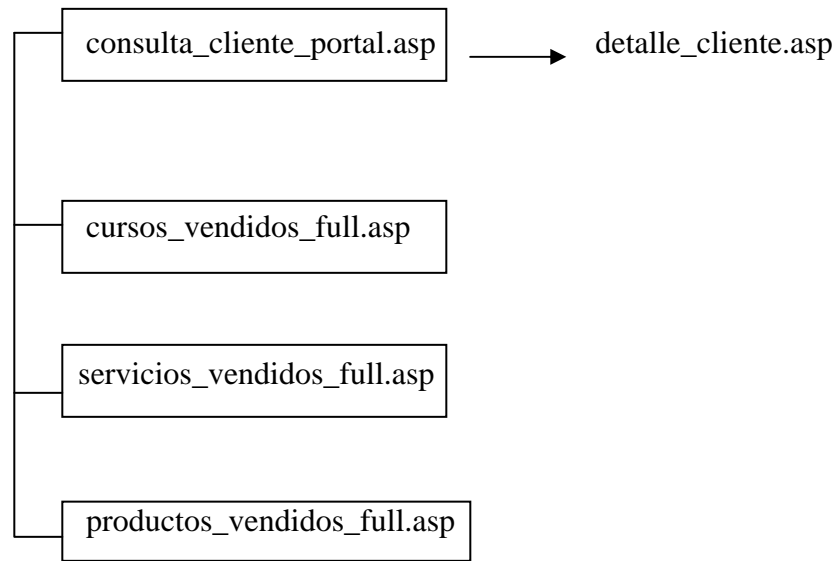


Figura 6.9. Enlaces de las Pantallas

A continuación se explicara el objetivo principal que tiene cada pantalla:

1) En esta pantalla se muestra la Introducción del Portal, brindando una publicidad de los diferentes cursos, productos y servicios a través de la combinación de colores, movimientos ,tipos de letra e imágenes que nos ofrece Flash Versión 4. (Ver **Figura 6.10)**



**Figura 6.10: Pantalla Introdutoria del Portal de Servicios Académicos y
Administrativos para la P.U.C.E.S.A.**

2) En esta pantalla se muestra la bienvenida al cliente e invitándole a visitar nuestro Portal , se le indica al cliente que debe ingresar el Login y la Contraseña y si es un usuario nuevo debe registrarse previamente . **(Ver Figura 6.11)**

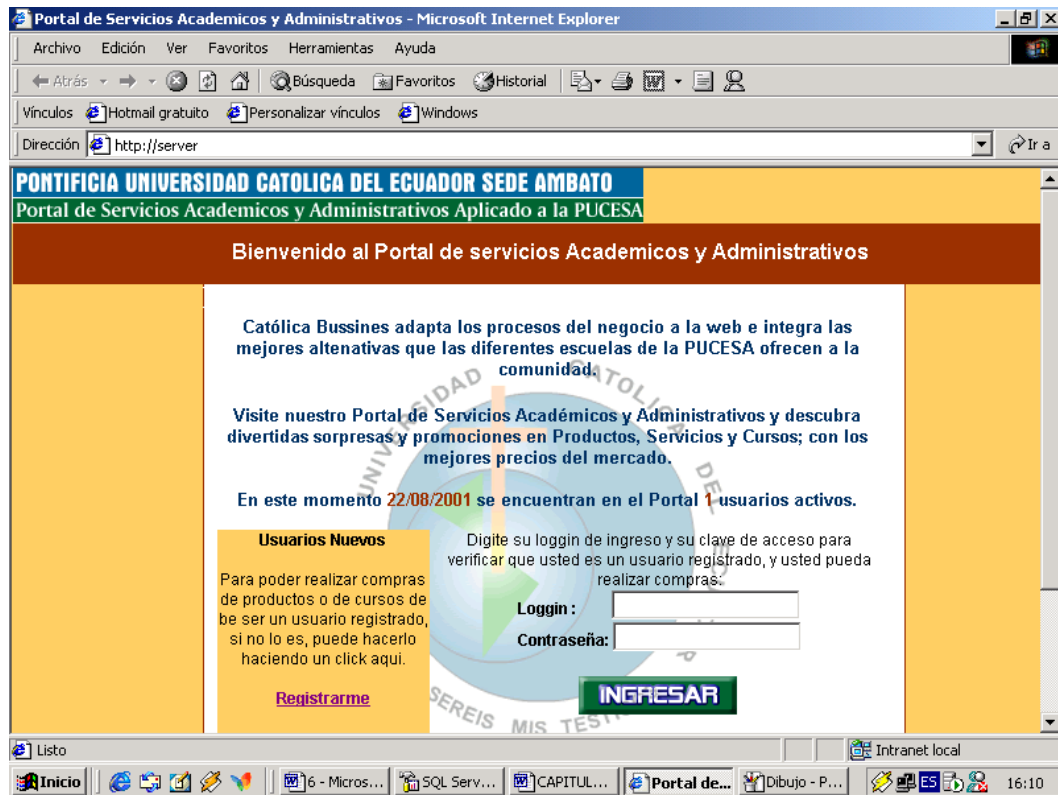


Figura 6.11: Tecnología ASP para el control de la pantalla de inicio (server)

3) Esta pantalla muestra las reglas que el cliente debe seguir para obtener un buen servicio del Portal (Ver **Figura 6.12**)

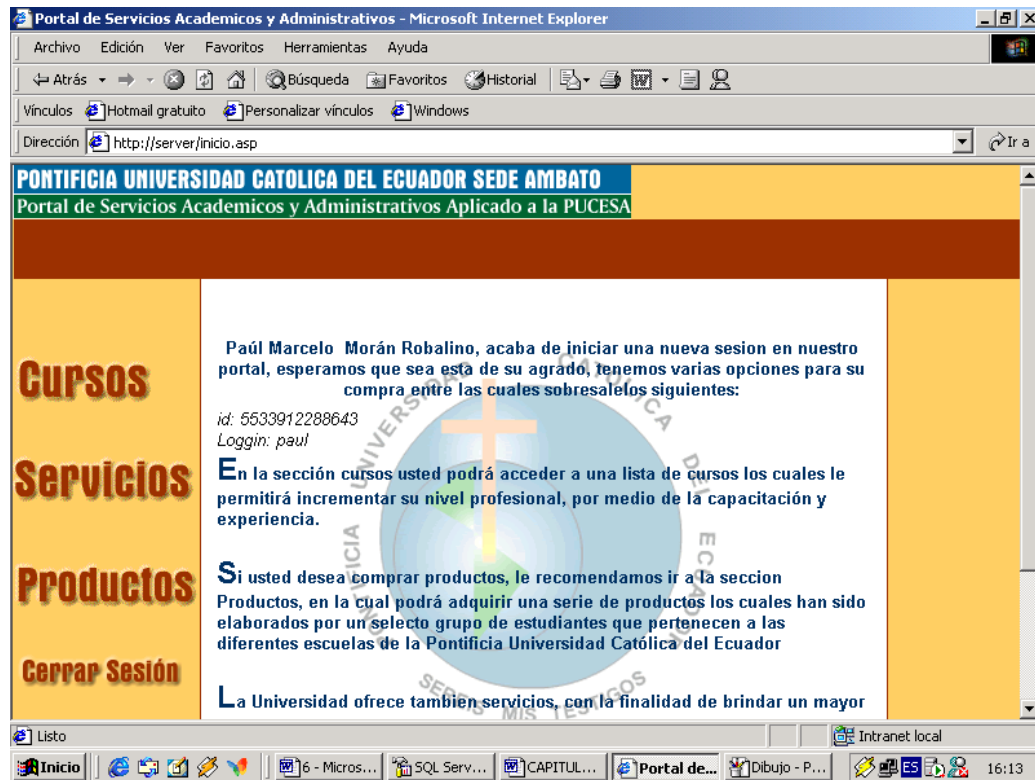


Figura 6.12: Tecnología ASP para el menú del sistema

(inicio.asp)

4) En esta pantalla se despliega los diferentes cursos que ofrecen las diferentes Escuelas de la PUCESA, se muestra las características principales que tiene cada curso dándole oportunidad al cliente que escoja el curso de una manera sencilla y práctica.

(Ver **Figura 6.13**)

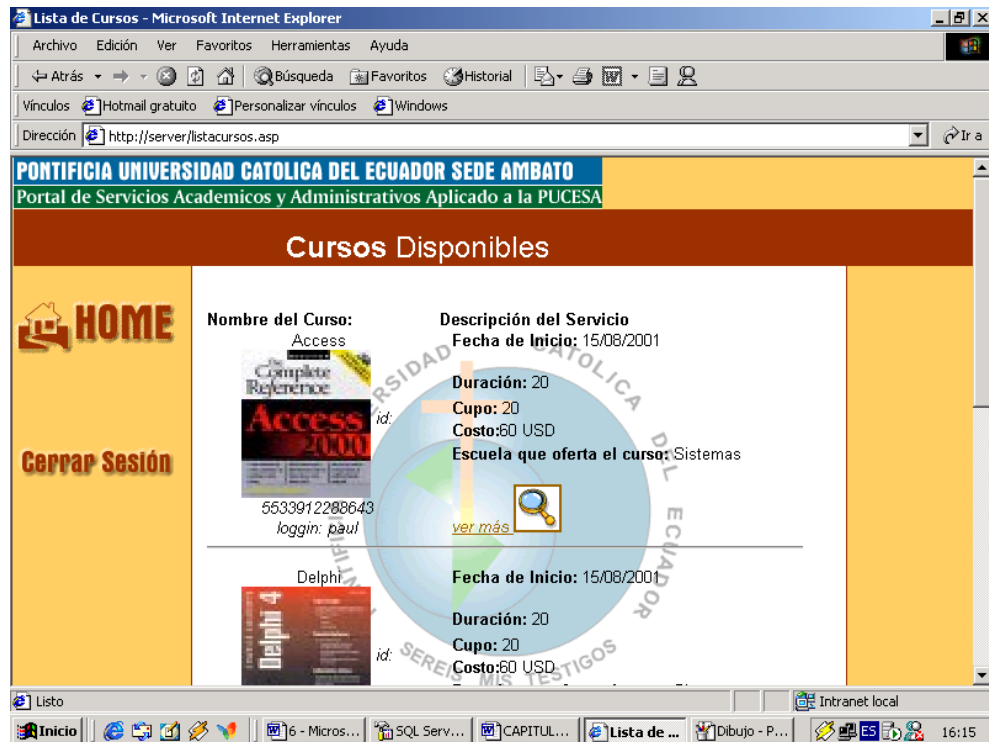


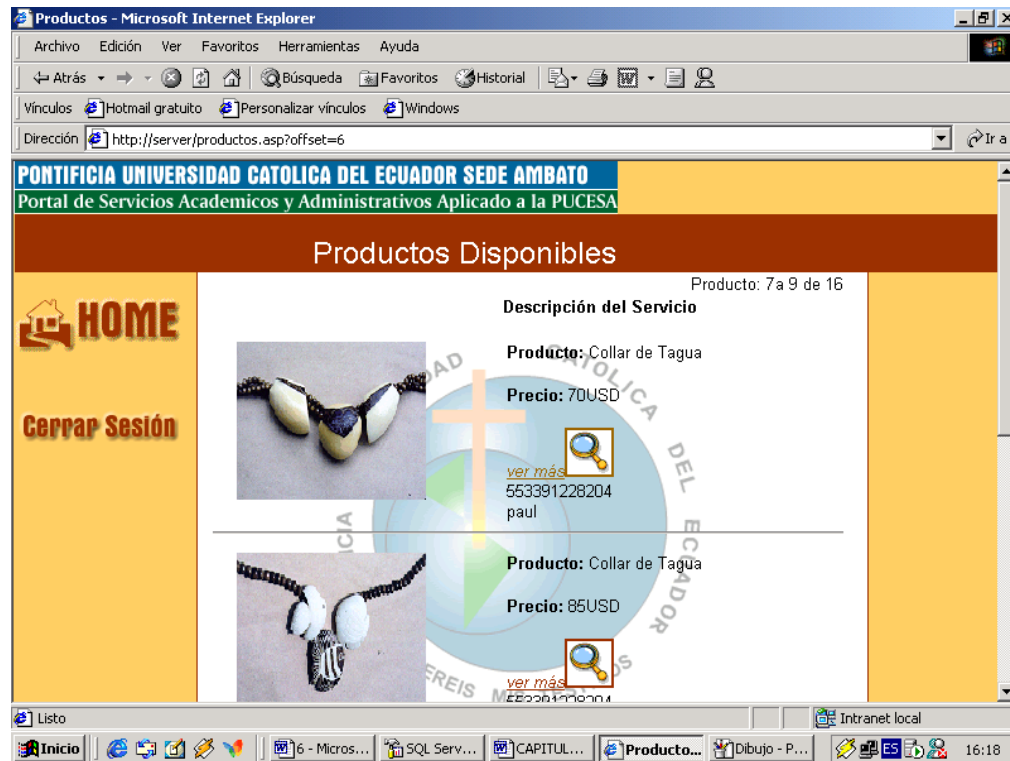
Figura 6.13: Tecnología ASP para el control de la lista de cursos (listacursos.asp)

5) En esta pantalla se despliega los diferentes servicios que ofrecen las escuelas de la PUCESA, se muestra las características principales que tiene cada servicio. (Ver **Figura 6.14**)



**Figura 6.14: Tecnología ASP para el control del detalle de los servicios
(detalleservicio.asp)**

6) En esta pantalla se despliega los diferentes servicios que han aportado las escuelas de la PUCESA, se muestra las características principales que tiene cada servicio. (Ver **Figura 6.15)**



**Figura 6.15: Tecnología ASP para el control de los productos
(productos.asp)**

7) En esta pantalla se muestra la factura de compra en la cual se despliega las compras obtenidas por el cliente , además se le permite imprimir para tener mayor referencia de los valores a pagar. (Ver **Figura 6.16**)

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO
Portal de Servicios Académicos y Administrativos Aplicado a la PUCESA

Factura de Venta

Adquiere: Paúl Marcelo Morán Robalino **Fecha:** 07/09/2001
Dirección: Ficoa **Cédula de Identidad:** 180233568-7
Teléfono: 82345611 1123843503880
paul

Forma de Pago

Efectivo: Puede cancelar su factura en el Banco Produbanco, en la cuenta corriente #0108000297-6
Cheque:
Tarjeta de Crédito: Número Tarjeta:
Nombre Tarjeta: Mastercard Internacional

Detalle

Nombre del Servicio	Costo Unitario	Cantidad	Subtotal (USD)
Alquiler de computadoras	3	2	6

Subtotal: 6
Descuento: 0
(USD) Total a pagar : 6

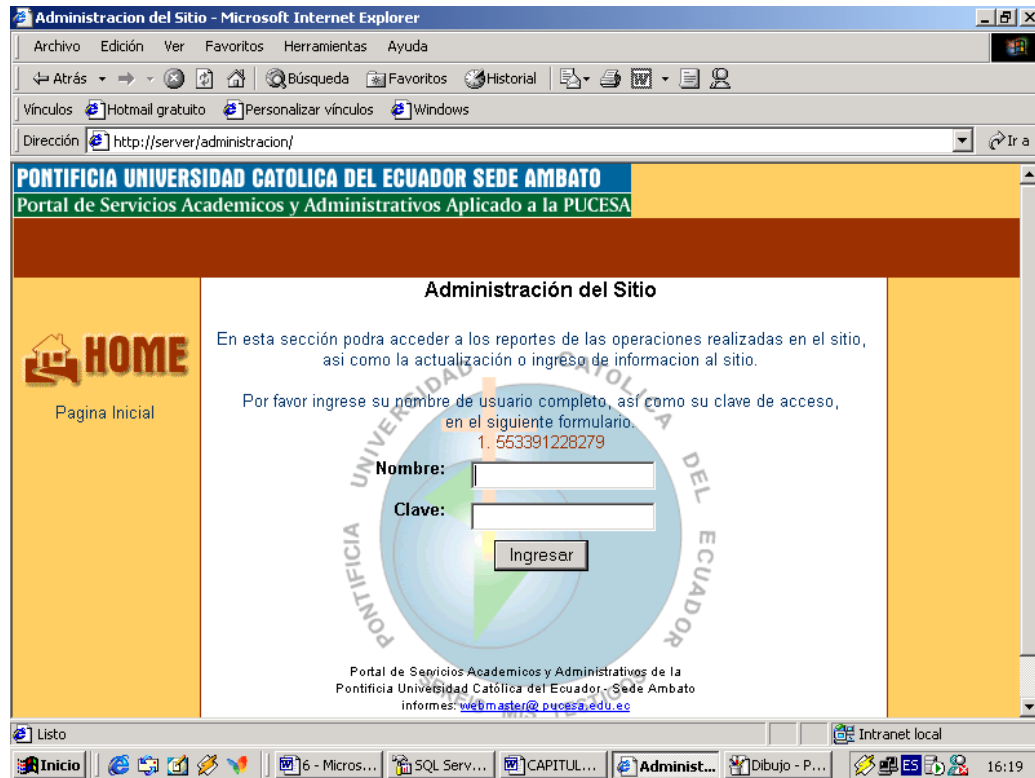

Imprimir

Si no desea completar la factura puede hacer un click aquí para [Cerrar esta Sesión](#), para ir a la Página de Bienvenida.

Portal de Servicios Académicos y Administrativos de la
Pontificia Universidad Católica del Ecuador - Sede Ambato
informes: webmaster@pucesa.edu.ec
© Reservados todos los derechos
Ambato - Ecuador
2001

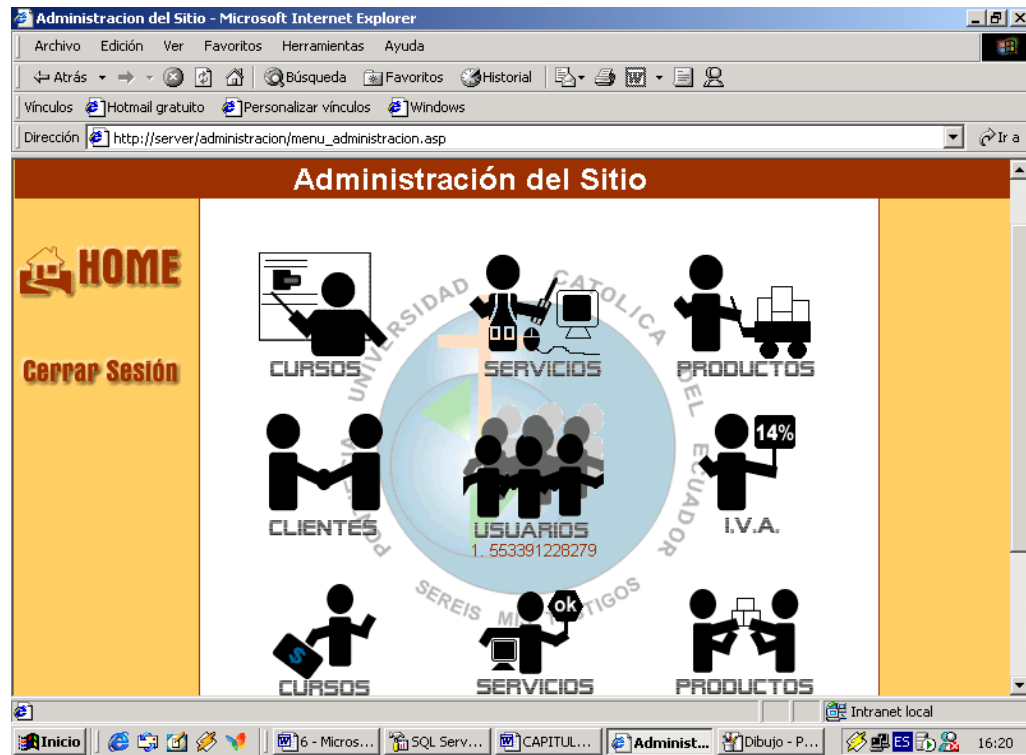
Figura 6.16: Tecnología ASP para desplegar la factura

8) Esta pantalla sólo ingresarán personal administrativo del sistema, en donde deberán digitar el nombre y la contraseña asignada por el Administrador. (Ver **Figura 6.17**)



**Figura 6.17: Tecnología ASP para el control de administración del sitio
(administración)**

9) Esta pantalla se muestra el menú de la sección administrativa con la finalidad de agregar, modificar e eliminar algún curso, servicio o producto , también se podrá obtener información acerca de los cursos ,servicios y productos vendidos. (Ver **Figura 6.18.**)



**Figura 6.18: Tecnología ASP para el control del menú de administración
(menu_administración.asp)**

6.8. IMPLEMENTACIÓN

Se realizará la prueba de fuego, esto es a la implementación del Portal de Servicios Académicos y Administrativos en la P.U.C.E.S.A y el carrito de compras en ASP.

6.8.1. APLICACIÓN DEL SISTEMA EN UNA EMPRESA

Para la implementación del sistema tuvimos que realizar varias pruebas, estas se las realizó en una Pentium III, 550 MHz ,128 RAM y un disco duro de 15 Gb con

Windows 2000 (Milenum) como Servidor y un Cliente con las siguientes características: Pentium II de 500 Mz con 64 Mb de RAM y un disco duro de 8.5 Gb con Windows 98.

6.8.2. ANÁLISIS Y EVALUACIÓN DE LA IMPLEMENTACIÓN

Después de un sinnúmero de pruebas en lo referente al portal de comercio electrónico, se procedió a su análisis; el mismo que se detalla a continuación:

La integración de la tecnología Dreamweaver UltraDev 4.0 con HTML, Windows 2000 e Internet Explorer es de buena calidad, resultado de esta integración es la estabilidad de todo el sistema y el tiempo de respuesta aceptable, además de proveer una interfaz y funcionalidad de los formularios.

Active Server Pages (ASP), es una tecnología que trata básicamente de un lenguaje de tratamiento de textos (scripts), basado en Basic, y que se denomina VBScript (Visual Basic Script). Se utiliza casi exclusivamente en los Servidores Web de Microsoft (*Internet Information Server* y *Personal Web Server*). Con ASP se pueden realizar fácilmente páginas de consulta de bases de datos, funciones sencillas como obtener la fecha y la hora actual del sistema servidor, cálculos matemáticos simples, etc.

Se utilizó un algoritmo de encriptación denominado MD5, el cual encripta la clave de acceso y la guarda en la base de datos encriptada. asegurando la información que se

maneja en el portal. Además, se empleó un algoritmo propuesto para implementar la seguridad de la tarjeta, primero se establece la verificación de la tarjeta, posteriormente este algoritmo tiene la función de encriptar el número de la tarjeta y se lo guarda en la Base de Datos. Finalmente se realizó la evaluación del sistema en base a la cantidad de cursos, productos y servicios que se incorporaron en el Portal de Servicios Académicos y Administrativos del la P.U.C.E.S.A., los cuales se muestran en la **Tabla 6. 17.**

Tabla 6. 17: Evaluación del sistema en base a la cantidad de cursos, productos y servicios

Curso	39
Cliente	56
Productos	34
Servicios	25

Los resultados que se obtuvieron a través de la ejecución de toda esta información y por las pruebas realizadas, se dio como a conocer que la aplicación estaba lista para ser ejecutada e implantada en el sitio Web de la Pontificia Universidad Católica del Ecuador Sede Ambato.

7. CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

- Los Portales de Comercio Electrónico constituyen la mejor herramienta de marketing y estrategia comercial para las pequeñas y grandes empresas, otorgan prestigio a las mismas frente a sus competidores que todavía no gozan de presencia en Internet.
- Una de las razones de que Internet y los portales de comercio electrónico sean tan populares, es que permite a los negocios tomar pedidos electrónicos para sus productos, alcanzar un mayor número de clientes e incrementar el número de transacciones de su negocio.
- El Portal de Servicios Académicos y Administrativos ayudará a crear y promover la identidad de la P.U.C.E.S.A. en Internet, posesionando nuestra marca ante una audiencia potencial de millones de clientes, estableciendo un punto de contacto, un lugar donde potenciales clientes pueden comprar y obtener información sobre los productos/servicios/cursos de nuestra entidad educativa.
- Mediante el uso de portales de Comercio Electrónico la P.U.C.E.S.A. podrá optimizar sus procesos y las relaciones con sus interlocutores comerciales mediante la aplicación de las tecnologías en las transacciones comerciales que fluyen entre ellas.
- Existe una cantidad de ventajas técnicas y tácticas para implementar el Portal de Servicios aplicado a la P.U.C.E.S.A, incluyendo:

- Fácil implementación y mantenimiento, lo que se traduce en ahorros de tiempo y costos.
- La habilidad para dar servicio a usuarios independientes de su ubicación física.
- En el portal tanto las escuelas o empleados de la P.U.C.E.S.A. pueden publicar información, datos; de forma fácil, rápida. y evitando costos por papel o tinta
- El incorporar acceso directo a bases de datos en el Portal de Servicios Académicos y Administrativos ofrece beneficios adicionales:
 - Un servidor de bases de datos relacional puede optimizar el tráfico de red al devolver sólo los datos que requiere una aplicación.
 - Los costos de *hardware* pueden minimizarse. Debido a que los datos no se almacenan en cada cliente, los clientes no requieren tener un espacio de disco dedicado a almacenar los datos. Los clientes tampoco necesitan procesar la capacidad de administrar localmente los datos y el servidor no requiere dedicar un poder de procesamiento para mostrar los datos.
 - Las tareas de mantenimiento como hacer copias de seguridad y recuperar los datos se simplifican.
 - Las reglas de empresa y de seguridad para todos los usuarios pueden definirse una sola vez, para todos, en el servidor.
- La tecnología de servidor ASP (*Active Server Pages*), brinda la posibilidad de crear páginas dinámicas robustas para un Portal Web, facilita la conexión con la base de datos, corre como un servicio en el servidor, tomando ventaja de la arquitectura de multitareas.

- UltraDev es un editor profesional para la creación y administración de sitios y páginas Web, dado que incorpora las herramientas de diseño de páginas y administración de sitios de Dreamweaver, UltraDev facilita la creación, administración y edición de páginas Web para múltiples plataformas y navegadores.
- Los requisitos concretos dependen de si utiliza UltraDev para crear aplicaciones ASP (*Active Server Pages*), aplicaciones ColdFusion o aplicaciones JavaServer Pages (JSP).
- Internet es una red insegura para todo tipo de operaciones. La única forma de poder hacer transacciones seguras es imponiéndole mecanismos de seguridad a cada una de ellas.
- El MD5 forma parte de los algoritmos hash, los mismos que son considerados como algoritmos matemáticos unidireccionales (*lo encriptado no se puede desencriptar*), el cual permitirá encriptar los datos del login y password asegurando así que los mismos no puedan ser interceptados por intrusos que hagan mal uso de la información, por lo tanto el usuario tendrá mayor confianza al realizar compras en el Portal de Servicios de la P.U.C.E.S.A.
- Al momento de finalizar la compra se envía los datos personales y la forma de pago (efectivo, cheque, número de tarjeta de crédito), el algoritmo de encriptación y des-encriptación de bits es el encargado de proteger su información de pedido y los números de tarjeta de crédito.

7.2. RECOMENDACIONES

- Debido a que en nuestro país, Ecuador, no existe una ley reguladora para el manejo del Comercio Electrónico, no ha sido posible implementar el algoritmo de des-criptación en el portal, sin embargo se lo ha desarrollado para una aplicación futura dentro de los parámetros legales y se recomienda que se afilie a una empresa internacional, la cual pueda emitir las seguridades que mejor convengan a la Universidad.
- Las transacciones comerciales entre el portal y una entidad bancaria para la verificación de la tarjeta de crédito no se ha podido realizar; se recomienda se realice un convenio Banca – Universidad.
- Debido a que este portal comprende la parte comercial que oferta la P.U.C.E.S.A., se recomienda se integre el actual nombre de dominio que la identifica.
- Los estudiantes a través de su nivel académico e ingenio podrán tener la oportunidad de darse a conocer por este medio, con sus proyectos y creaciones.
- Se recomienda utilizar JavaScript para el desarrollo de este tipo de aplicaciones.
- Recomendamos utilizar las herramientas de Flash 4 ya que estas dan la oportunidad de crear un ambiente dinámico para un sitio Web.

GLOSARIO DE TÉRMINOS

A

- ACTIVEX (CONTROL)** Programa autosuficiente que puede ejecutarse en cualquier sitio en la red ActiveX
- ACCESO ALEATORIO** Operación de almacenamiento y recuperación de la información en la que el sistema accede directamente a la memoria en base a un parámetro preestablecido.
- ACCESO DIRECTO** Técnica por la cual los diferentes periféricos del ordenador acceden a la memoria de éste sin control de la CPU.
- API** (*Application Program Interface*). Conjunto de convenciones internacionales que definen cómo debe invocarse una determinada función de un programa desde una aplicación.
- APLICACIÓN** Programa informático que proporciona servicios de alto nivel al usuario, generalmente usando otros programas más bajos que se sitúan por debajo.
- APPLETS** Pequeñas aplicaciones escritas en Java y que se difunden a través de la red para ejecutarse en el visualizador cliente.
- ASCII** (*American Standard Code of Information Exchange*).

Estándar que recoge 128 caracteres, letras, números y símbolos utilizados en procesadores de textos y algunos programas de comunicaciones.

ASÍNCRONO

Que no tiene un intervalo de tiempo constante entre cada evento.

ASP

(*Active Server Pages*) o páginas activas de servidor. Como su nombre lo indica son páginas activas las cuales son analizadas por el servidor modificando el código HTML según las necesidades

AUI

(*Attachment Unit Interface*). Interfaz de unidad de conexión. Conector usado con la Ethernet de alambre grueso.

AUDITORÍA

Servicio estadístico válido para conocer el éxito de un sitio web.

AUTENTIFICACIÓN

Procedimiento de seguridad por el que se verifica el reconocimiento y validación de un usuario de Internet.

B

BANNER

Anuncios. Elemento rectangular gráfico que se utiliza como anuncio o información.

BASE DE DATOS

Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la

posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc.

BIT Es la unidad de información más pequeña. Puede tener sólo dos valores o estados: 0 o 1, encendido o apagado.

BPS Es el acrónimo de bits por segundo, medida estándar de velocidad con que se transmiten datos mediante un módem.

BROWSER Aplicación para visualizar documentos WWW y navegar por Internet.

BUSCADOR Los buscadores son sitios webs, especializados en localizar información a través de Internet.

C

CARRITO DE COMPRAS Es utilizado para elegir y almacenar temporalmente los productos que compran los clientes.

CERN (*Centro Europeo de Física de Partículas*) en Ginebra, Suiza; grupo que inventó la WWW.

CERTIFICADO DIGITAL Documentos emitidos por entidades generalmente públicas que aseguran la validez de las transacciones realizadas por las partes en Internet.

CGI *Common Gateway Interface*. Interfaz de puerta de acceso común que permite a un usuario de Internet interactuar con la World Wide Web.

CHAT	Conversación interactiva en tiempo real, en Internet.
CIBERESPACIO	Todo el universo de información que está disponible en la red.
COOKIE	<i>Galleta.</i> Archivo de texto en la memoria del cliente del que se valen los servidores Web para guardar información acerca del visitante de un sitio.
CRIPTOGRAFÍA	Ciencia que estudia algoritmos informáticos que codifican la información para posibilitar la realización de transmisiones seguras en la red.
CLAVE DE ACCESO	Es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.
CLIENTE	Aplicación que se encarga de formar una solicitud válida para enviarla al servidor
CLIENTE/SERVIDOR	Modelo lógico de una forma de proceso cooperativo, independiente de plataformas hardware y sistemas operativos. .
CODIGO	Se refiere a las instrucciones contenidas en un programa, y entendibles por el ordenador.
COMANDO	Orden dada al ordenador para que realice una acción determinada.

CORTAFUEGOS Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala.

CRACKER Hacker cuya ocupación es buscar la forma de entrar en sistemas y encontrar los fallos de seguridad de programas.

D

DATO Unidad mínima de información, sin sentido en sí misma, pero que adquiere significado en conjunción con otras precedentes de la aplicación que las creó.

DNS Es el acrónimo de *Domain Name System* (Sistema de Nombres de Dominio), que se emplea para identificar a un servidor.

DIRECCIÓN IP Dirección de protocolo de Internet. Número especial que se asigna a cada ordenador que forma parte de Internet, aunque sea de manera temporal.

DOWNLOAD Transmisión de ficheros desde la red al PC del usuario.

E

E-BUSINESS Conjunto de líneas de negocio canalizadas a través de Internet.

EDI *Electronic Data Interchange*. Formatos electrónicos que permiten el intercambio de información en las transacciones realizadas entre

empresas a través de redes electrónicas.

ENCRIPtar Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor.

E-MAIL Intercambio de mensajes entre personas conectadas a una red de manera similar al correo tradicional.

EXPLORER Navegador diseñado por Microsoft para su uso con Windows95. Actualmente está disponible para otros sistemas operativos.

F

FORMULARIO Serie de redes de seguridad que sirven para controlar y filtrar el acceso a servicios web.

FRAME Capacidad de un documento HTML para subdividirse en diferentes ventanas independientes.

FTP *File Transfer Protocol*. Protocolo de transferencia de archivo que se utiliza para transferir un archivo de un ordenador desde un lugar a otro.

G

GIF *Graphic Interchange Format*. Intercambio gráfico empleado en los anuncios en banners y en la mayoría de imágenes Web.

GUI (*Interfaz gráfica de usuario*). Término aplicado a la representación gráfica de

la manipulación de los comandos de un programa.

H

- HARDWARE** Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un ordenador, incluidos sus periféricos.
- HERRAMIENTA** Aplicación empleada para la construcción (de ahí su nombre) de otros programas o aplicaciones.
- HIPERMEDIOS** Grupo de documentos en el que cada uno puede contener texto, gráficos, fragmentos de vídeo y audio, así como referencias a otros documentos.
- HIPERTEXTO** Texto vinculado electrónicamente con otros documentos, a los que se puede acceder haciendo click en la palabra que sirve de vínculo.
- HIPERVÍNCULO** Enlace. Son referencias entre varias páginas que se encuentran en la red Internet o Intranet.
- HOST** Utilizado a veces como sinónimo de mainframe, en realidad identifica al ordenador central en un sistema informático complejo.
- HOSTING** Servicio mediante el cual una empresa se encarga de gestionar las páginas web de otras empresas, incluyendo el hardware, el software y las comunicaciones.

HTML	<i>Hyper Text Markup Language</i> . Formato de texto electrónico caracterizado por poder vincular otros textos a través de enlaces.
HOME PAGE	Define lo que se conoce como página de inicio o principal (la primera que aparece cuando se accede a un servidor de páginas Web).
HTTP	Protocolo de transporte de hipertexto (<i>Hipertext Transport Protocol</i>). Conjunto de reglas pactadas entre sistemas para la transmisión de hipertextos.

I

ICONO	Un gráfico pequeño que representa una función o acción.
IDE	(<i>Integrated Development Environment</i>). Entorno de desarrollo integrado. Conjunto de programas que se ejecuta a partir de una única interfaz de usuario.
INDEXAR	Se usa en las aplicaciones de bases de datos para indicar la operación de ordenar los registros contenidos en ella de manera especial, en función de unos parámetros definidos previamente.
INFORMACIÓN	Elemento fundamental que manejan los ordenadores en forma de datos binarios.
INFOVÍA	Lugar de encuentro entre usuario y ordenador. Por ejemplo, la interfaz de un ordenador es su pantalla.
INTERFAZ	Conexión e interacción entre hardware, software y el usuario.

- INTERNET** Red electrónica mundial que interconecta a miles de redes y millones de usuarios de ordenadores.
- INTRANET** Red de comunicaciones interna y privada que permite a todas las personas de una empresa u organización tener acceso a información y transmitir documentos de una manera similar a la que se aplica en Internet o en la WWW.
- IMAGE MAP** Imágenes interactivas que incluyen distintos enlaces, que se activan apuntando a distintas partes de la imagen.
- ISAPI** Interfaz de programación de aplicaciones de servidor para Internet.

J

- JAVA** Lenguaje de programación desarrollado por Sun Microsystems que puede ser ejecutado en cualquier sistema operativo.
- JPG** (*Join Photograph Expert Group*). Unión de Grupo de Expertos Fotográfico. Formato gráfico con compresión

L

- LAN** *Red De Area Local*. Generalmente se considera que son las redes cuyo ámbito está restringido a un edificio o a unidades físicas similares.
- LENGUAJE** Conjunto de normas que permiten escribir un programa y que éste sea

entendido por el ordenador y pueda ser trasladado a ordenadores similares para su funcionamiento en otros sistemas

M

MAILTO El protocolo de Internet que se utiliza para enviar correo electrónico.

MÉTODO En programación orientada a objetos, método es el procesamiento que realiza un objeto.

N

NCSA (*National Center for Supercomputing Applications*).

Centro Nacional de Aplicaciones de Supercomputación.

NETSCAPE NAVIGATOR Es el programa navegador más utilizado actualmente en Internet. Creado por la compañía Netscape Corporation.

O

ODBC *Open Data Base Connection (Conexión abierta a base de datos)*. Es una forma de conexión a veces de datos, independientemente del lenguaje o programa que estemos utilizando.

P

- PKI** *Public Key Infrastructure*. La infraestructura de clave pública es la que hace posible la distribución y el almacenamiento de claves criptográficas que permiten la certificación electrónica de forma segura.
- PGP** Programa conocido por estas *siglas (Pretty Good Privacy)* diseñado para asegurar la privacidad del correo electrónico
- PORTAL WEB** Sitio de Internet o Web site en el que se ofrecen una serie de servicios al usuario. Entre los servicios con los que suele contar figuran un buscador, servicio de noticias, e-mail gratuito, chat, comunidades virtuales, etc.
- PROCESADOR** Es el microchip encargado de ejecutar las instrucciones y procesar los datos que son necesarios para todas las funciones del computador.
- PROCESO** Operación o conjunto combinado de operaciones con datos, o bien una secuencia de acontecimientos definida única y delimitada, que obedece a una intención operacional en condiciones predeterminadas. También se denomina proceso a una función que se está ejecutando.
- PROTOCOLO** Lista de comandos a la que responde de manera estándar un servidor.
- PROXI** Servidor que sirve en las organizaciones como caché o como

cortafuegos (firewall).

P.U.C.E.S.A. Pontificia Universidad Católica del Ecuador Sede Ambato.

R

RAS *Remote Access Server*. Servidor de Acceso Remoto.

REGISTRO Es una pequeña unidad de almacenamiento destinada a contener cierto tipo de datos.

RED Grupo de computadoras y otros dispositivos periféricos conectados entre sí que pueden comunicarse y transmitir datos entre ellos.

S

SERVIDOR Aplicación que se encarga de procesar la petición que recibe del cliente. Una vez procesada la solicitud, se envía al cliente, quién la procesa a fin de mostrarla en un formato compresible para el usuario.

SERVLET Aplicación sin interfaz gráfica que se ejecuta en un servidor de Internet, procesando información HTML previamente recogida por un navegador.

SET Es la abreviatura de *Secure Electronic Transaction* (Transacciones electrónicas seguras). Protocolo que sirve para autenticar compras digitales en la red mediante el uso de firmas digitales de todas las partes implicadas en

la transacción.

SISTEMA OPERATIVO Conjunto de programas fundamentales sin los cuales no sería posible hacer funcionar el ordenador con los programas de aplicación que se desee utilizar.

SQL (*Structured Query Language*). Es un estándar en el lenguaje de acceso a bases de datos.

SITIO WEB Se refiere a una localización dada en Internet con una dirección (URL) específica. Puede constar de una sola página personal o de innumerables archivos que identifican a alguna institución o entidad

SSL (*Secure Socket Layer*). Protocolo de autenticación de usuario desarrollado por Netscape para la realización de transacciones de Comercio Electrónico.

T

TABLA Una o más filas de celdas de una página que se utilizan para organizar el diseño de una página Web o para ordenar datos sistemáticamente.

TAG Rótulo, etiqueta, identificador.

TCP/IP *Transmission Control Protocol / Internet Protocol*. Protocolos para la transmisión en Internet a través de un conjunto de reglas estandarizadas que permite a ordenadores de distintas redes

comunicarse entre sí.

TIEMPO REAL Se dice que un ordenador trabaja en tiempo real cuando realiza una transacción que le ha sido ordenada desde un terminal en ese mismo momento, sin espera alguna.

TRANSACCIÓN Operación que modifica el estado de una base de datos, sin que los datos en sí mismos pierdan consistencia alguna.

U

URL (*Universal Resource Locator*). Localizador Universal de Recursos. Sistema unificado de identificación de recursos en la red.

V

VRML (*Virtual Reality Modeling Lenguaje*). Lenguaje de Modelación de Realidad Virtual no-propietario y multiplataforma para el diseño de servidores Web en tres dimensiones (3D).

W

WAN Red de Area Amplia. Cualquier red pública es de este tipo. Su característica definitoria es que no tiene límites en cuanto a su amplitud.

WEB PAGE Es un archivo de computación escrito en lenguaje HTML.

WEB DINÁMICA Páginas Web que contienen, además de texto y gráficos,

archivos de sonido, de vídeo, animaciones o elementos interactivos.

WINDOWS Es el nombre del popular entorno, software creado por Microsoft. Su novedad es el uso de diferentes pantallas que se superponen, denominadas ventanas, para mostrar distintos tipos de información.

WINDOWS NT (*Windows New Technology*) Nueva tecnología de Windows. Sistema operativo avanzado de 32 bits para redes, de Microsoft, que ejecuta aplicaciones DOS y Windows.

WWW (*World Wide Web*). Sistema de información con mecanismos de hipertexto creado por investigadores del CERN.

WYSIWYG *What you see is what you get*, es decir, lo que se ve es lo que se obtiene.

X

X.25 Interfaz estándar para conexión de terminales de datos a redes públicas. Es un protocolo de empaquetamiento conmutado.

BIBLIOGRAFÍA

TEXTOS

- [1] SHELDON Tom, (1994). Enciclopedia de Redes. Editorial Osborne - McGraw-Hill, España.
- [2] TANENBAUM A, (1990), Redes de Computadoras. Primera Edición.
- [3] BHLENDORF Brian & CHANDLER David , (1996), Microsoft Internet.Information Server Running a Perfect Web sites with apache , Corporation Qua. Indianapolis Indiana. 46290 USA.
- [4] BERKELEY SOFTWARE DESIGN, INC, (February 1997), BSDI Interner Server Versión 3.0. California University.
- [5] Comercio Electrónico ya está en América Latina COMPUTERWORLD del 12-5 de Junio 2000 “Periódico de los Profesionales de las Tecnologías de Información”.

REFERENCIAS WEB

WEBS OFICIALES

- **ASP:** . <http://msdn.microsoft.com/workshop/server/asp/ASPOver.asp>
- **SQL SERVER:** <http://support.microsoft.com/support/sql/70faq.asp>
- **ULTRADEV:** . <http://www.macromedia.com/support/ultradev/>

OTRAS:

- [6] <http://www.aui.es/biblio/libros/mi99/13patrocinio.htm>
(Formas de patrocinio y soluciones publicitarias aplicables a los portales)
- [7] <http://www.extra-net.net/articulos/en990621.htm>
(El valor está en las ideas).
- [8] <http://www.aui.es/biblio/libros/mi99/3portales.htm>
(De Portales a Plazas; Presente y Futuro de los Portales en Internet)
- [9] <http://www.techweb.com/se/directlink.cgi?IWK19990125S0043>
(New Tools Integrate Personal Interests)
- [10] <http://www.aui.es/biblio/libros/mi2000/Zabalegui.htm>
(Los Contenidos y el Comercio Electrónico)
- [11] <http://www.estrelladigital.es/ciberestrella/secciones/saber/saber5.htm>
(Los motores de búsqueda en la gestión de información de las empresas)
- [12] http://www.aui.es/biblio/libros/mi99/16futuro_busqueda.htm
(El futuro de la búsqueda de información en Internet)
- [13] <http://www.techweb.com/encyclopedia/>
(Definición del concepto "corporate portal" de la TechEncyclopedia)
- [14] <http://archive.infoworld.com/cgi-in/displayStory.pl?features/990517portal.htm>
(Portal patrol. Corporate portals help early users control data deluge)
- [15] <http://www.techweb.com/encyclopedia/>
(Definición del concepto "vertical portal" de la TechEncyclopedia)

- [16] <http://www.techweb.com/se/directlink.cgi?INW19990125S0012>
(Vertical Industry Portals)
- [17] <http://www.its.inmar-inc.com/wp/InmarWebportals.htm>
(Web Portals)
- [18] <http://www.ogilvyinteractive.es/portales/resumen.htm>
(Resultados de una encuesta sobre portales)
- [19] http://www.aui.es/biblio/libros/mi99/25comercio_electrónico.htm
(El Comercio Electrónico en España)
- [20] www.interware.com.mx/secciones/intranet/iweintranet04.html (Intranet)
- [21] http://www.geocities.com/ahh_miedo/intranets.html (Intranet)
- [22] www.redestb.es/inode/quees.htm
- [23] <http://www.redestb.es/inode/quees.htm>
- [24] <http://www.upv.es/snl/snl.htm>
- [25] <http://www.selfhtml.com.ar/tbac.htm>
- [26] http://translator.go.com/cb/trans_entry
- [27] http://www.abity.com/flash_index.html
- [28] <http://elrinconcito.com/dicciona/dicciona.htm>
- [29] <http://www.arrakis.es/~aikido/interdic/enlaces.htm>
- [30] <http://www.geocities.com/Athens/2693/glosario.html> (Glosario)
- [31] <http://adforce.imgis.com/?adiframe> (Glosario de Términos)
- [32] <http://www.eitig.com/lomasweb/cursillo/CSS.htm>
- [33] <http://www.w3.org/pub/WWW/Protocols/> (Bases de la Web I)

- [34] <http://www.marketingycomercio.com/servicios/informacion.htm>
(El Comercio Electrónico no es solo Internet)
- [35] <http://www.greco.dit.upm.es/~enrique/ce/sec1/part11.html>
(Comercio Electrónico: Marco General)
- [36] <http://www.maestrosdelweb.com/editorial/software/comercio2.asp>
(Comercio Electrónico)
- [37] <http://www.enredos.freesell.org/enre2-06/enre2-06.html> (Comercio Electrónico)
- [38] <http://www.ceocant.es/noticias/> (Qué es el Comercio Electrónico)
- [39] <http://www.corpece.com>
(Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de datos)
- [40] <http://www.wmaestro.com/webmaestro/docs/cap21.html> (20. Applets de Java)
- [41] <http://www.maestrosdelweb.com/ver.asp?cgi> (Introducción al CGI)
- [42] <http://www.maestrosdelweb.com/ver.asp?php> (Introducción al PHP)
- [43] <http://www.maestrosdelweb.com/ver.asp?asp> (Introducción al ASP)
- [44] <http://www.islagrande.cu/colombusnet/Drtaco/asp/Articulos/Articulos.html>
(Asp)
- [45] <http://www.asptutor.com/asp/vart.asp/?id=19> (Cookies)
- [46] <http://www.uady.mx/sitios/teleinfo/web.html> (Tipos de Interacción)
- [47] <http://www.lsi.us.es/docencia/asignaturas/dihm/html/cap2.html> (Páginas Web)
- [48] <http://www.marketingycomercio.com/numero12/12art1.htm> (Firma digital)
- [49] <http://www.publicaciones.derecho.org/redi/>
(Hacia la seguridad en el Comercio Electrónico)

[50] <http://latam/technet/articulos/windows2k/pkintro/>

(Introducción a la infraestructura de claves públicas de Windows 2000)

[51] http://webserver/pue.udlap.mx/~tesis/zuniga_va/c7.html (Medios de Pago)

[52] <http://globalaudit.com> (¿Qué es la Mensajería electrónica en Internet?)

PAQUETES INSTALADORES DE ASP PARA M\$ WINDOWS

- [DreamWeaver UltraDev 4.0](#)
- [Drumbeat 2000](#)
- [Visual Interdev de Microsoft.](#)

HOSTING GRATUITO CON ASP Y MSQL

- [http://www.microsoft.com/data/download.htm.](http://www.microsoft.com/data/download.htm)

BIBLIOTECA PERSONAL DE LOS AUTORES:

- Marjorie Cadena: Elaboración de los *Capítulos I-II-VI (Derechos Reservados)*
- Mónica Manobanda: Elaboración de los *Capítulos III-IV-V (Derechos Reservados)*








ANEXOS

ANEXO A

RED E INFORMACIÓN DE LA P.U.C.E.S.A.

SERVICIOS ADMINISTRATIVOS

Dentro de los servicios brindados por el área administrativa tenemos:

<p>. Crédito Educativo</p> 	<p>. Bibliotecas</p> 
<p>. Centro de Arbitraje y Mediación</p> 	<p>. Seguro de Accidentes</p> 
<p>. Becas Universitarias o Exoneraciones de pago</p> 	<p>. Servicio Comunitario</p> 
<p>. Servicio de Internet y laboratorio</p> 	

SERVICIOS ACADÉMICOS

<p style="text-align: center;">LENGUAS Y LINGÜÍSTICA</p> <ul style="list-style-type: none">· Licenciado en Lingüística Aplicada a la enseñanza del Idioma Inglés· Certificado de Aptitud y Peritaje <p>Es un programa en que el participante luego de ocho semestres de estudio, está preparado para dominar el idioma inglés.</p> 	<p style="text-align: center;">SISTEMAS</p> <ul style="list-style-type: none">· Analista de Sistem@s y Computación· Ingeniero de Sistem@s y Computación <p>Es un profesional capaz de llevar a cabo un plan de implementación informática, diseñar y planificar un sistema computarizado.</p> 
<p style="text-align: center;">DISEÑO INDUSTRIAL</p> <ul style="list-style-type: none">· Tecnólogo en Diseño de Objetos y Control de Procesos de Fabricación <p>Diseño Industrial forma diseñadores capacitados para determinar, diseñar, especificar y fabricar los objetos o los sistemas de producción.</p> 	<p style="text-align: center;">FORMACIÓN DUAL EN GERENCIA PYMES</p> <ul style="list-style-type: none">· Tecnólogo en Administración de Pequeñas y Medianas Empresas <p>Formación Dual significa aprendizaje en dos lugares distintos. En la Universidad se complementa y profundiza la formación obtenida en la pequeña o mediana empresa, mediante instrucción técnica, teórica, persiguiendo la</p> 
<p style="text-align: center;">TEOLOGÍA PARA LAICOS</p> <ul style="list-style-type: none">· Diploma de Estudios Teológicos <p>ESTELA pretende dar una visión de conjunto y sistemática de la Teología Católica. Capacitar en trabajos apostólicos y enseñanza media de la Religión.</p> 	<p style="text-align: center;">OPTOMETRÍA</p> <ul style="list-style-type: none">· Tecnólogo Médico en Optometría <p>El Optometrista es un profesional capacitado para detectar, prevenir y corregir los defectos visuales y reconocer las alteraciones oculares que requieren tratamiento oftalmológico.</p> 

RED INFORMATICA.

A continuación se realiza una descripción de la red informática de la P.U.C.E.S.A.

ACADEMICO	IP: 204.225.202.15 MASK : 205.225.225.224 PROXY: 64.46.84.161 NetBeui IPX
------------------	--

COMPAQ	IP: 10.10.10.21 . 10 .10.10. 29 MASK : 266.255.255.0 PROXY: 10.10.10.3.80 NetBeui IPX
---------------	--

IBM	IP: 10.10.10.11 . 10 .10.10. 20 MASK : 255..255.255.0 PROXY: 10.10.10.3.80 NetBeui IPX
------------	---

MAC DISEÑO	IP: 204.225.202.10 MASK : 255..255.255.224 OATEWAY: 204.225.202.1
-------------------	---

PYMES	IP: 204.225.202.14 MASK : 255..255.255.224 PROXY: 204.225.202.5 8080 NetBeui IPX
--------------	---

PROYECTOS SISTEMAS	IP: 204.225.202.9 MASK : 255..255.255.224 PROXY: 204.225.202.5 8080 NetBeui IPX
-------------------------------	--

FINANCIERO 1	IP: 204.225.202.13 MASK : 255..255.255.224 PROXY: 204.225.202.5 8080 NetBeui IPX
---------------------	---

SECRETARIA	IP: 204.225.202.11 MASK : 255..255.255.224 PROXY: 204.225.202.5 8080 NetBeui IPX
-------------------	---

ADMINISTRACIÓN	IP: 204.225.202.12 MASK : 255..255.255.224 PROXY: 204.225.202.5 8080 NetBeui IPX
-----------------------	---

SWITCH	IP: 10.10.10.250 MASK : 255..255.255.0 PROXY: 204.225.202.5 8080 NetBeui IPX
---------------	---

PRT	IP: 204.225.202.1 MASK : 255..255.255.224
------------	--

ACCESS SERVER	IP: 204.225.202.4 MASK : 255..255.255.224
----------------------	--

RAS	IP: 204.225.202.4 MASK : 255..255.255.224 PROXY: 204.225.202.5 8080
------------	---

SUN SERVER	IP: 10.10.10..2 MASK : 255..255.255.0 IP: 204.225.202.7 MASK : 255..255.255.224
-------------------	--

LINUX SERVER	IP: 10.10.10..5 MASK : 255..255.255.0 IP: 204.225.202.5 MASK : 255..255.255.224
---------------------	--

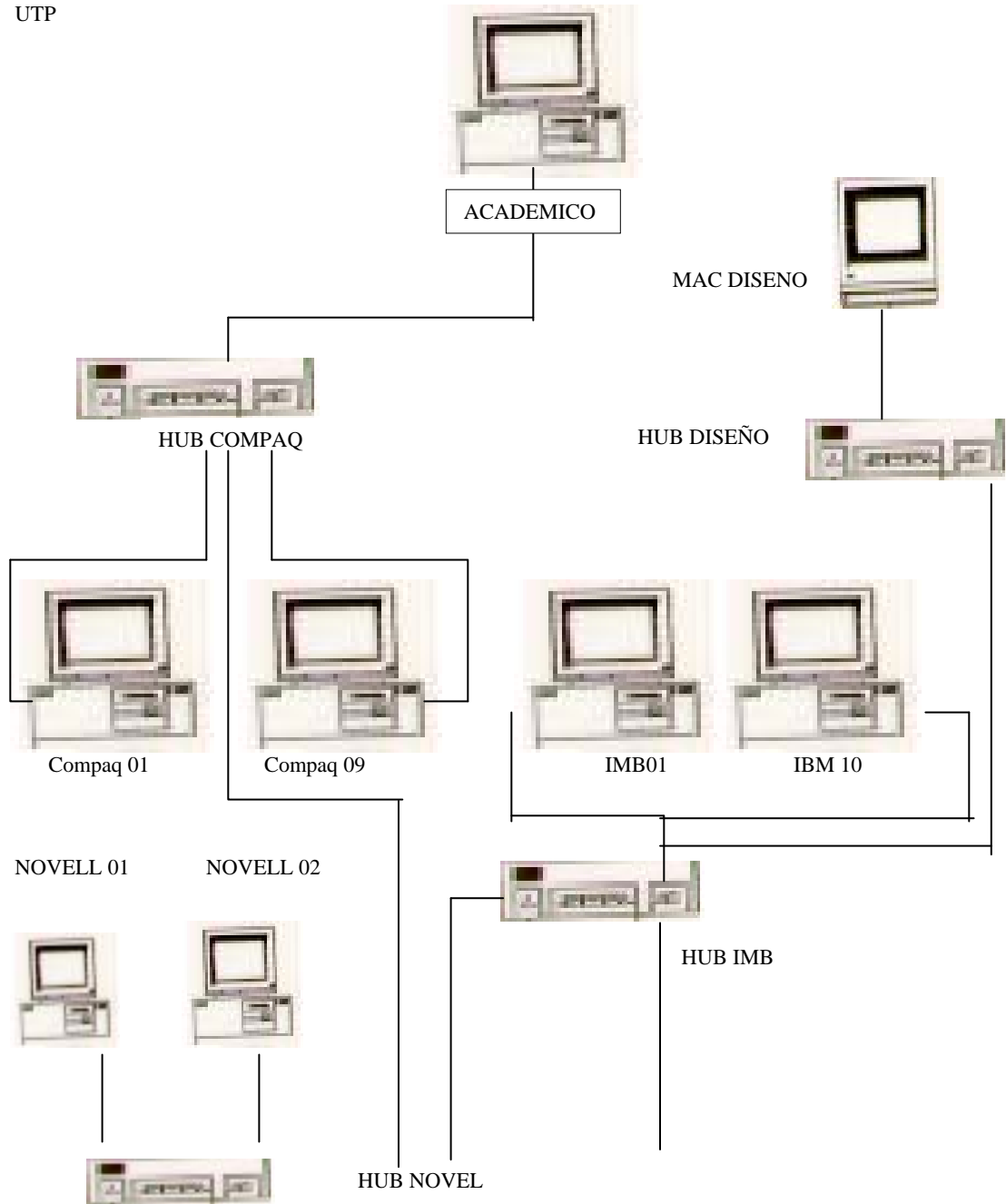
NT SERVER	IP: 10.10.10..3 MASK : 255..255.255.0 IP: 204.225.202..3 MASK : 255..255.255.224
------------------	---

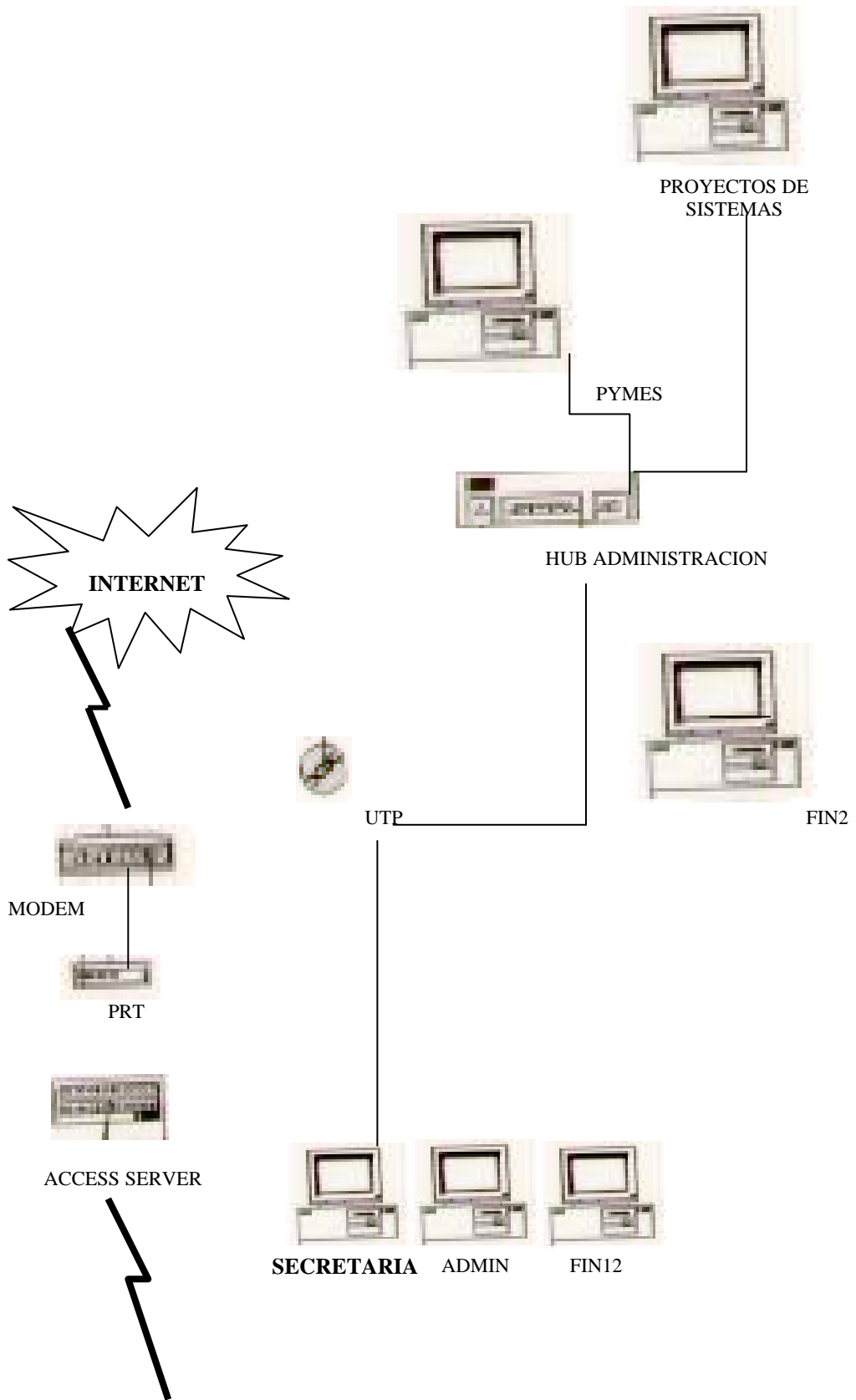


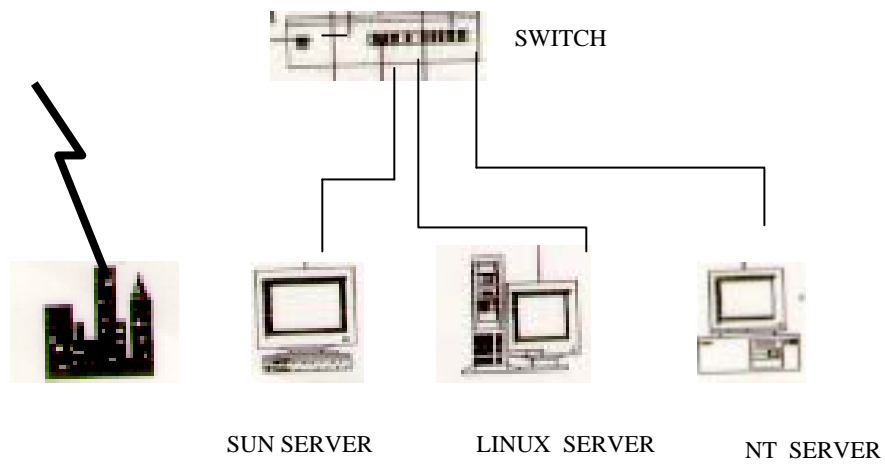
STAR NETWORK



UTP







ANEXO B

GESTIÓN DE TABLAS DE IMPUESTOS (CIBERTRIBUTACIÓN)

A continuación le mostraremos el **Proyecto de Ley de Comercio Electrónico, Firmas electrónicas y Mensaje de datos**, elaborado por la *Corporación Ecuatoriana De Comercio Electrónico* (C.O.R.P.E.C.E)

1. Título Preliminar

Art 1.- Ambito de Aplicación:

Esta Ley regula la eficacia y valor jurídico de los documentos electrónicos, el uso de la firma electrónica, la prestación de servicios de certificación, el manejo de bases de datos y la protección a los usuarios del comercio electrónico. Las disposiciones contenidas en esta Ley se complementarán y se regirán por los principios generales establecidos en la Constitución y las Leyes.

Art. 2.- Glosario de Términos:

- **Mensajes de Datos:** Toda aquella información generada por medios electrónicos, digitales o similares que puede ser almacenada o intercambiada por cualquier medio. Podrán ser mensajes de datos sin que esta enumeración

limite su definición los siguientes: Documentos Electrónicos, Correo electrónico, páginas web, telegrama, telex, fax, facsímile e Intercambio electrónico de datos.

- **Documento Electrónico:** Documento en formato electrónico con información electrónica o digital que se genera o almacena por cualquier medio.
- **Comercio Electrónico:** Toda transacción civil, comercial o financiera, contractual o no, que se efectúe a través del intercambio de mensajes de datos o medios similares.
- **Firma Electrónica:** Dato en formato electrónico asignado a un documento electrónico o mensaje de datos por el autor del mismo, su representante o mecanismo autorizado por él y que permitirá certificar su autenticidad e integridad a través de procedimientos técnicos de comprobación.
- **Intercambio Electrónico de Datos:** Intercambio normalizado de datos entre dos o más sistemas.
- **Mecanismo de emisión:** Instrumento físico o lógico utilizado por el signatario de un documento para crear mensajes de datos o una firma electrónica. **Mecanismo de comprobación:** Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o un documento creado con una firma electrónica.
- **Certificado electrónico de Identidad:** Documento electrónico que vincula a un mecanismo de comprobación con una persona natural o jurídica y confirma su identidad.

- **Proveedor del servicio de certificación:** Persona natural o jurídica que está legalmente en capacidad de emitir certificados de identidad y proporcionar servicios relacionados con comercio y firma electrónica y para lo cual debe cumplir con los requisitos determinados en esta Ley y sus Reglamentos, deberá disponer de las herramientas físicas y lógicas necesarias y acordes al tipo de servicio a prestar.
- **Emisor:** Persona natural o jurídica que firma y origina un mensaje de datos. Se entenderá como emisor aun cuando no genere el mensaje por sí mismo o lo haga a través de terceros o de mecanismos automatizados de cualquier tipo siempre y cuando éstos se encuentren debidamente autorizados.
- **Destinatario:** Persona natural o jurídica a quien va destinado el mensaje de datos. Se entenderá como Destinatario aun cuando no reciba el mensaje por sí mismo o lo haga a través de terceros o de mecanismos automatizados de cualquier tipo siempre y cuando éstos se encuentren debidamente autorizados.
- **Signatario:** Se entenderá la persona que consigna, o en cuyo nombre se consigne una firma electrónica.
- **Suscriptor:** Será el Destinatario que hubiere aceptado las condiciones de un contrato preestablecido siguiendo las instrucciones contenidas en un mensaje de datos.
- **Fedatario Público Electrónico:** Serán los Notarios que de acuerdo con la Leyes que regulan su actividad, cumplan los requisitos señalados en ésta ley para certificar firmas electrónicas.

- **Sistema de información:** Se entenderá como sistema de información, a todo sistema utilizado para enviar, recibir, procesar o archivar de cualquier forma mensajes de datos.
- **Criptografía:** Es la codificación de mensajes de datos ilegibles y que mediante un uso de algoritmos matemáticos o señales autorizadas puede ser devuelto a su forma original o legible.
- **Usuario:** Toda persona que utilice sistemas de información o comunicación electrónica. Este podrá estar suscrito o no a un Proveedor de Servicios de Certificación y en base al uso de un certificado o al manejo de claves o códigos entregados por el emisor, podrá acceder a la información intercambiada.
- **Quiebra técnica:** Es la incapacidad temporal o permanente del proveedor de servicios de certificación que impida garantizar el cumplimiento de los requisitos establecidos para la firma electrónica.

Título i

Capítulo i: Principios Generales

Art. 3.- Efectos de la Ley.- Se reconoce la fuerza jurídica y la validez de los mensajes de datos, cualquiera sea su forma, así como la información que estos contengan. Los mensajes de datos, su información y contenido tendrán igual valor jurídico que los documentos públicos y privados y su eficacia y valoración se someterán al cumplimiento de lo establecido en esta Ley.

Art. 4.- Interpretación.- La interpretación de esta Ley se someterá a los métodos de interpretación del Código Civil y demás leyes concordantes. La interpretación de aquellos casos no determinados en esta Ley se basarán en el uso normalmente conocido de los términos relacionados con el Comercio Electrónico o en su aplicación técnica de uso general, en las Normas, Acuerdos y Tratados Internacionales que sobre la materia se hubieren celebrado.

Art. 5.- Propiedad Intelectual.- Toda la información relacionada con los mensajes de datos o transmisión de datos por cualquier forma o medio, sea esta dentro o fuera del Comercio Electrónico, estará sometida a las Leyes, Reglamentos y Acuerdos Internacionales relativos a la Propiedad Intelectual.

Art. 6.- Confidencialidad.- El principio de la confidencialidad regirá para los mensajes de datos, cualquiera sea su forma medio o intención. Toda violación a este principio será sancionado conforme a lo dispuesto en el Código Penal, Ley de Propiedad Intelectual y demás leyes que rijan la materia.

Art. 7.- Información escrita.- Cuando las Leyes requieran que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.

Art. 8 .- Información original.- Cuando la Ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con un

mensaje de datos, si siendo requerido conforme a la Ley, existe garantía fidedigna de que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma. Se considera que un mensaje de datos permanece íntegro si se mantiene completo e inalterable, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Art. 9.- Conservación de los mensajes de datos.- Cuando la Ley requiera que ciertos documentos, registros, o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las siguientes condiciones:

- a) Que la información que contengan sea accesible para su ulterior consulta;
- b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada o recibida; y
- c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

La obligación de conservar ciertos documentos, registros o informaciones no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje. Toda persona podrá recurrir a los servicios de un tercero para observar o verificar los requisitos señalados en éste artículo.

Art. 10.- Obligatoriedad de Firma.- Cuando la Ley exija la firma de una persona, ese requisito quedará satisfecho en un mensaje de datos, si se utiliza un método seguro y fiable para identificar al titular de esa firma electrónica de acuerdo a lo establecido en esta Ley.

Art. 11. - Protección de datos.- Para la elaboración de bases de datos obtenidas en la transmisión de mensajes de datos, se requerirá de la autorización expresa y afirmativa del usuario, el mismo que podrá seleccionar la información a compartirse con terceros.

Las bases de datos obtenidas como resultado del intercambio de mensajes de datos, serán protegidas de acuerdo con los derechos de propiedad intelectual vigentes, su uso y disposición estarán sometidos a la autorización expresa de su titular.

Los datos obtenidos con el consentimiento y voluntad de una persona responderán a los principios de privacidad e intimidad garantizados por la Constitución de la República y podrán ser utilizados o transferidos únicamente con su autorización u orden de autoridad competente. Toda persona tiene derecho al libre acceso a los datos públicos o privados que contengan información relacionada con su persona, para lo cual ejercerá su derecho al habeas data consagrado en la Constitución vigente o en las leyes que regulen la institución.

Capítulo ii: Firmas Electrónicas

Art. 12.- Efectos de la firma electrónica: La firma electrónica, tendrá igual validez y se le reconocerá los mismos efectos jurídicos que a una firma manuscrita. Deberá reunir los requisitos determinados en esta Ley, guardar concordancia con el cuerpo de Leyes ecuatoriano y cumplir con las reglamentaciones que para el efecto se dictare.

Art. 13.- Requisitos de la firma electrónica: Para tener validez, la firma electrónica reunirá como mínimo los siguientes requisitos:

- a) Ser individual, única o vinculada exclusivamente a su titular, y capaz de ser mantenida bajo el estricto control de la persona a quien pertenece y usa.
- b) Disponer de las seguridades necesarias que garanticen su integridad.
- c) Ser verificable inequívocamente mediante mecanismos técnicos de comprobación, establecidos por la Ley, los Reglamentos o el acuerdo de las partes.

Cualquier requisito adicional a los aquí señalados, deberá constar expresamente determinado en la Ley.

Art. 14.- La firma electrónica en un mensaje de datos: Debe ser parte integrante del mensaje de datos, enviarse en un mismo acto y ser inalterable, de tal forma que si

se cambia el documento o la firma, ésta se invalide. Cumplidos los requisitos de seguridad e inalterabilidad, se presumirá la integridad del mensaje de datos.

Cuando se fijare la firma electrónica en un mensaje de datos, salvo prueba en contrario, se presumirá que éste conlleva el acuerdo de voluntad del Emisor y se someterá al cumplimiento de las obligaciones o contratos de acuerdo a lo determinado en la presente Ley y demás Leyes pertinentes.

Art. 15.- Obligaciones vinculadas a la firma electrónica: La firma electrónica, mientras el certificado no sea revocado, suspendido o cancelado vincula al titular o a su representado en sus obligaciones frente a terceros de buena fe.

Frente al tercero de buena fe no cesará la eficacia de la firma electrónica por muerte, incapacidad, liquidación, quiebra o cualquier otra causa restrictiva de la capacidad de la persona a quien se impute los efectos de la firma electrónica.

Art. 16.- Obligaciones del titular de la firma electrónica:

- a) Actuar con diligencia para evitar toda utilización no autorizada de su firma.
- b) Notificar al proveedor de servicios o a los interesados, por cualquier medio, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y pueda utilizarse para falsificar su firma electrónica.
- c) Asegurar la exactitud de sus declaraciones en todos sus actos.

- d) Cumplir con las obligaciones derivadas del uso ilegal de su firma si no ha obrado con la debida diligencia para impedir la utilización no autorizada de su firma y para evitar que el destinatario confíe en ella, salvo que el destinatario supiera o hubiera debido saber que la firma no era autorizada.

Art. 17.- Duración de la firma electrónica: Esta duración estará sujeta a la voluntad del titular de dicha firma, de acuerdo a lo que se estableciere en la Ley y sus reglamentos.

Art. 18.- Revocación de la firma electrónica: La revocación de la firma electrónica se producirá a solicitud del titular de la misma y el proveedor del servicio de certificación está obligado a proceder a la revocación inmediata y a su publicación de acuerdo con ésta Ley.

La revocación de la firma electrónica no exime a su titular de las obligaciones previamente contraídas.

Art. 19.- Cancelación y suspensión de la firma electrónica: El proveedor del servicio de certificación podrá suspender de modo temporal o cancelar el certificado de firma electrónica cuando:

- a) Sea solicitado por autoridad competente de acuerdo a la legislación vigente.
- b) Se compruebe que alguno de los datos del certificado es falso.

- c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación y el Usuario.
- d) El proveedor del servicio de certificación cese en sus actividades y los certificados vigentes ya emitidos por el mismo servicio de certificación no sean asumidos por otro servicio de certificación.
- e) El proveedor del servicio de certificación está en la obligación de publicar inmediatamente dicha cancelación, de acuerdo con el literal i) del artículo 25 de esta Ley.
- f) Se produzca una quiebra técnica del sistema de seguridad del proveedor del servicio de certificación que afecte a la integridad y confiabilidad del certificado.

En los casos de suspensión temporal, la misma podrá ser levantada una vez desvanecidas las causas que la originaron, en cuyo caso igualmente el proveedor del servicio de certificación está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Capítulo iii: Certificados De Firma Electrónica

Art. 20.- Funciones: Los certificados de firma electrónica buscarán dar mayor seguridad y confianza a los mensajes de datos y a las transacciones dentro del comercio electrónico, su uso y validez serán regulados por esta ley o por el acuerdo de las partes.

Art. 21 .- Requisitos de los Certificados de firma electrónica:

Los certificados deberán contener como mínimo los siguientes requisitos para considerarse válidos:

- a) Identificación del proveedor del certificado.
- b) Datos del domicilio legal del proveedor del certificado.
- c) Código de proveedor del certificado asignado por el respectivo órgano de control.
- d) Los atributos específicos del titular del certificado que permitan su ubicación e identificación, códigos, nombres, domicilio del titular y, adicionalmente, el número de la persona natural o jurídica asignado por el Registro de firmas electrónicas del órgano de control respectivo.
- e) El método de verificación de que el dispositivo de verificación de firma se corresponde con el dispositivo de creación de firma controlado por el titular del certificado
- f) El identificador del certificado, que deberá ser único, y;
- g) La firma electrónica del proveedor del servicio de certificación debidamente acreditado por el órgano de control respectivo.
- h) Cualquier limitación que contenga, sea de uso, responsabilidad o montos de transacciones del certificado en caso de tenerlas y de responsabilidad del proveedor de certificaciones.
- i) El procedimiento para comprobar la revocación o cancelación de un certificado.
- j) Las fechas de inicio y fin del periodo de validez del certificado.

Art. 22.- Requisitos adicionales: Cualquier requisito adicional a los aquí señalados, deberá constar expresamente determinado en la Ley.

Art. 23.- Tratados Internacionales: Aquellos Acuerdos internacionales, bilaterales, multilaterales o comunitarios suscritos por el Estado Ecuatoriano buscarán la unificación de normas para la validez y reconocimiento de los certificados entre los países miembros.

Capítulo iv: Proveedores De Servicios De Certificación

Art. 24.- Control: El control, supervisión, vigilancia y sanción de los Proveedores de Servicios de Certificación será ejercido por el Superintendente de Telecomunicaciones.

Art.- 25.- Proveedores de Servicios de Certificación: Toda persona puede contratar al Proveedor de Servicios de Certificación de firma electrónica que desee, el mismo que deberá estar debidamente acreditado ante el órgano de control respectivo. Los proveedores deberán cumplir los siguientes requisitos:

- a) Encontrarse legalmente constituidos.
- b) Justificar la confiabilidad y probidad necesarias para ofertar servicios de certificación.
- c) Ser entidades con independencia financiera.

- d) No haber sido condenados previamente en proceso judicial,
- e) Contar con un servicio de suspensión y revocación rápido y seguro.
- f) Mantener el personal técnico adecuado con conocimiento especializado en la materia y experiencia para el servicio a prestar
- g) Utilizar sistemas técnicamente confiables para los servicios a prestar tanto en el uso de software como de hardware.
- h) Mantener sistemas de resguardo y respaldo de la información relativa a los certificados.
- i) Mantener una publicación en internet u otros medios determinados en el contrato de suscripción, en la cual conste la información relativa a los procedimientos, reglamentos, prácticas aplicadas a los contratos celebrados con los Usuarios y los certificados suspendidos o cancelados.
- j) Estar inscritos y habilitados en el Registro de Servicios de Certificación del órgano de control respectivo.
- k) Verificar por los medios establecidos en la ley la identidad y capacidad de actuar de la persona natural o jurídica sobre la cual emiten un certificado.
- l) Utilizar herramientas de firma electrónica que estén protegidas contra la modificación de las mismas, de tal forma que no puedan realizar funciones distintas a aquéllas para las que han sido diseñadas. Deben utilizar productos de firma electrónica que bajo estándares internacionales garanticen la seguridad técnica y criptográfica de los procesos de certificación soportados por los productos.

- m) Adoptar medidas para evitar la falsificación de certificados, y, en el caso de que el Proveedor de Servicios de Certificación intervenga en la generación de claves criptográficas privadas, garantizar la seguridad y confidencialidad durante el proceso de generación de dichas claves.
- n) Mantener recursos financieros suficientes para actuar en conformidad con los requisitos establecidos en la presente ley, especialmente garantizar la responsabilidad por daños y perjuicios.
- o) Almacenar toda la información relevante relativa a un certificado por un periodo mínimo de 10 años, especialmente a efectos de prueba en procedimientos judiciales. El almacenamiento podrá ser realizado por medios electrónicos.
- p) No almacenar o copiar las claves criptográficas privadas de firma electrónica de la persona a la cual el proveedor del servicio de certificación ofrezca servicios de administración de las claves, a menos que la persona lo solicite expresamente
- q) Informar a los consumidores antes de iniciar una relación contractual, por escrito utilizando un lenguaje entendible y un medio duradero de comunicación, acerca de los términos precisos y condiciones para el uso del certificado, incluyendo cualquier limitación sobre responsabilidad, la existencia de una acreditación voluntaria y los procedimientos existentes para resolver cualquier conflicto.
- r) Mantener la confidencialidad de la información y protegerla frente a terceros.
- s) Transferir a un Notario para su archivo confidencial las claves, revocaciones y la documentación que las justifique, en caso de liquidación o cese de las actividades.
- t) Garantizar la integridad, disponibilidad y entrega de la información y documentos a su cargo a fin de que puedan ser usados como medio de prueba.

Art. 26.- Responsabilidades de los proveedores de servicios de certificación:

El proveedor de servicio de certificación será responsable por:

- a) Adoptar las medidas necesarias para determinar la identidad del titular de la firma y la exactitud de sus certificaciones.
- b) La validez, vigencia y legalidad del certificado emitido.
- c) Certificar que la información contenida en el certificado era exacta en el momento en el que fue emitido, a no ser que el proveedor del servicio de certificación hubiera establecido otra cosa en el certificado,
- d) Asegurar que el titular del certificado tenía, en el momento de creación del mismo, el instrumento de generación de firma correspondiente al instrumento de verificación del mismo reseñado o identificado en el certificado, y
- e) Asegurar que en los casos en los que el proveedor del servicio de certificación generara los instrumentos de creación y comprobación de firma, ambos instrumentos funcionaran juntos de una forma complementaria.
- f) Mantener un listado de las firmas suspendidas, canceladas o revocadas.
- g) Almacenar y garantizar la seguridad de las claves criptográficas de firmas electrónicas que se le solicitara expresamente.
- h) La Correspondencia de funcionamiento entre la clave pública y privada de acuerdo con el certificado expedido.

- i) Proporcionar a los titulares de firmas un medio para dar aviso de que una firma electrónica tiene riesgo de uso indebido, en cuyo caso el titular deberá solicitar la suspensión de la firma electrónica.

Todo Proveedor de Servicios de Certificación será responsable del incumplimiento de sus obligaciones. En todos los casos, la responsabilidad del proveedor del servicio de certificación deberá constar claramente establecida tanto en el contrato con los usuarios como en el certificado de firma electrónica concedido y su omisión no será eximente de responsabilidad.

Art. 27.- Los Proveedores de Servicios de Certificación en el archivo, uso y manejo de datos obtenidos en función de su trabajo, garantizarán:

- a) Privacidad, protección y confidencialidad de la información y datos que manejen,
- b) Obtener información únicamente con el consentimiento y voluntad de la persona relacionada con dicha información.
- c) La no divulgación de la información obtenida por cualquier medio,
- d) La protección frente a terceros de la información y datos obtenidos, y
- e) Otros requisitos establecidos en las leyes y reglamentos que regulen la materia.

Los Proveedores de Servicios de Certificación bajo pena de cancelación de su calidad de tales, y otras consecuencias legales establecidas en la presente ley recopilarán datos personales o particulares únicamente de los propios sujetos o sus representantes

legalmente acreditados y sólo en la medida que sean necesarios para la emisión de un certificado. Los datos no pueden ser recopilados o procesados para fines distintos o distribuidos sin el consentimiento expreso del titular de los mismos. En caso de que una persona natural o jurídica recopilase información por medios fraudulentos, cedere bajo cualquier modalidad datos fuera de los casos permitidos por la Ley y en general vulnerase el derecho a la confidencialidad de los individuos o instituciones, se prohibirá su actividad y funcionamiento y se comunicará del efecto al Superintendente de Compañías para que proceda a su inmediata liquidación y será reprimido con multa de 500 a 2.500 UVCs y prisión de dos meses a dos años sin perjuicio de la acción de daños y perjuicios.

Título ii

Capítulo i: Contratos

Art. 28 .- Formación de un contrato electrónico: La elaboración, envío y aceptación de un contrato podrá ser efectuada mediante mensajes de datos.

Estos mensajes de datos gozarán de completa validez y fuerza jurídica, sea que se trate de una oferta, la aceptación de la misma o cualquier otra forma que genere obligaciones entre las partes.

Art. 29.- Contratos de adhesión: En contratos cuyas condiciones se encuentren preestablecidas, bastará que el suscriptor cumpla con las instrucciones de adhesión establecidas en el mensaje de datos para crear obligaciones entre emisor y suscriptor.

Art. 30.- Perfeccionamiento de los contratos electrónicos: Los contratos concluidos electrónicamente se entenderán perfeccionados cuando la declaración de voluntad del aceptante llegue a conocimiento del Oferente. Se entenderá como el lugar de perfeccionamiento del contrato el que acordaren las partes, en caso de no fijarlo, será el lugar de envío o recepción del mensaje de datos.

Art. 31.- Aceptación de un contrato electrónico: Si alguna de las partes solicitare que previa a la aceptación legal de un documento electrónico, se deba confirmar su recepción y conformidad, se entenderá que el documento electrónico no surtirá sus efectos legales mientras no se cumpla dicho requisito.

Art. 32.- Recepción y Aceptación: En caso de que cualquiera de las partes solicitare confirmación de recepción o aceptación de un documento electrónico, sin especificar el medio, se considerará haberse emitido dicha confirmación cuando:

- a) **Expresa.-** Se hubiere enviado un mensaje por cualquier medio electrónico haciendo referencia a dicho documento o su conformidad con el mismo.
- b) **Tácita.-** Se hubiere enviado un mensaje electrónico por cualquier medio, en el cual se entienda por el sentido del mismo, que se recibió dicho mensaje o su conformidad con el contenido.
- c) **La confirmación de la recepción de un mensaje, indicando que éste ha cumplido los requisitos técnicamente reconocidos o acordados, no implicará presunción de aceptación de su contenido.**

Art. 33.- Tiempo de validez: A Criterio del Emisor, el mensaje de datos enviado y condicionado a confirmación de recepción o aceptación, podrá tener un tiempo de validez durante el cual generará obligaciones para las partes.

En caso de no señalarse tiempo de validez, éste será de cinco días hábiles, luego de los cuales se deberá ratificar las condiciones establecidas y aceptadas por las partes para proceder a la ejecución del contrato.

Art. 34.- Procedencia e identidad de un mensaje datos: Se entenderá que un mensaje de datos proviene de quién lo envía y autorizará a quién lo recibe a actuar conforme al contenido de dicho documento, cuando de la verificación acordada entre las partes, exista concordancia entre la identificación del envío y la recepción del mensaje de datos, sea por si mismo, por interpuesta persona o por cualquier medio.

Art. 35.- Excepciones: Lo señalado en el artículo anterior se entiende que no surte efectos cuando:

- a) Se hubiere dado aviso que el mensaje de datos no provenía de quién lo suscribe electrónicamente. Este aviso se lo deberá hacer antes de que quién lo recibe actúe conforme a dicho mensaje. En caso contrario deberá justificar plenamente que el mensaje no se inició por orden suya o que el documento fue alterado.
- b) Si el Destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o si hubiera hecho caso omiso de su resultado.

Art. 36.- Envío y recepción de un mensaje de datos: Salvo pacto en contrario, se presumirán los siguientes:

1.- Tiempo:

- a) Se tendrá como expedido cuando entre en un sistema de información que no esté bajo control del Emisor, de quién éste autorizara o del medio programado para el efecto.
- b) Se considerará momento de recepción cuando ingrese al sistema de información señalado por el Destinatario. En caso enviarse a otro sistema de información o de no haber señalado un lugar preciso de recepción, el momento de recepción será cuando el Destinatario recupere el mensaje de datos en cualquier sistema de información.

2.- Lugar:

Se considerará como lugar de envío y recepción, el domicilio que conste en el certificado de firma electrónica del Emisor y del Destinatario. Si por errores en el certificado, no se pudiere establecer el domicilio, será el lugar de trabajo o donde desarrollen el giro principal de sus negocios o del negocio relacionado con el mensaje de datos.

Art. 37.- Duplicación del mensaje de datos: Cada mensaje de datos se presume diferente, de acuerdo al negocio entre las partes. En caso de duda el Destinatario deberá solicitar la confirmación del nuevo mensaje. Todo mensaje lleva implícita la obligación de verificar técnicamente la autenticidad del mismo.

Art. 38.- Modificación contractual: Las disposiciones señaladas en este Capítulo podrán ser modificadas por el acuerdo de las partes.

Capítulo ii: De Los Derechos Del Usuario De Consumo

Art. 39.- Protección al usuario: Se garantizan los derechos de los usuarios de servicios de certificación y de quienes actúen intercambiando mensajes de datos, o efectuando transacciones de cualquier tipo relacionadas con el acceso a Internet, Comercio Electrónico, otros medios de comunicación y Tecnologías de Información.

Art. 40.- Información: El Oferente en internet deberá informar al usuario, en forma objetiva, veraz y en detalle lo que se está adquiriendo, para que sirva y como utilizarlo.

Art. 41.- Contratos de consumo: Luego de celebrados estos contratos, el Usuario o adquirente tiene el derecho de desistir del contrato veinte y cuatro horas después de suscrito el mismo. Dentro de éste término el Usuario será responsable por los gastos que hubiere ocasionado al Oferente por ese contrato. En caso de no notificar dicho desistimiento dentro del término señalado el Usuario será responsable del pago o de los daños y perjuicios que le cause al Oferente.

Art. 42.- Privacidad: Como privacidad del usuario se entiende el derecho a la intimidad y el derecho a no recibir información o mensajes no solicitados. Para el

envío o recepción de mensajes o información directamente o mediante cadenas, el usuario deberá haber suscrito una autorización expresa al iniciador o emisor del mensaje de datos.

El usuario podrá solicitar en cualquier momento su exclusión de cadenas de mensajes o de bases de datos en las cuales conste inscrito. En caso de violarse el derecho a la privacidad, el usuario podrá iniciar las acciones que le concede la Ley y el iniciador o emisor del mensaje de datos será condenado al pago de la respectiva indemnización por daños y perjuicios.

Art. 43.- Prohibición de oferta: Una vez rechazado una oferta electrónica por parte del Destinatario del mensaje, el Oferente no podrá seguir enviando mensajes si hay oposición para recibirlos. En caso de incumplimiento, el Oferente será condenado a cumplir con una indemnización por daños y perjuicios de acuerdo a lo determinado por la autoridad competente.

Capítulo iii: Documentos Públicos

Artículo.- 44 .- Documentos públicos electrónicos.-

- a) Los documentos escritos que se transformen en documentos electrónicos en presencia de un Notario se considerarán copias electrónicas auténticas. Lo mismo sucederá a la inversa.

- a) La afirmación hecha por un Notario o autoridad competente acerca de que la firma electrónica ha sido puesta o reconocida en presencia del mismo por su titular será considerada una legitimación de la firma electrónica, la misma que deberá cumplir con los requisitos técnicos y legales establecidos
- b) Cuando una declaración de voluntad sea transmitida telemáticamente por un Notario o autoridad competente, la actuación de éste acreditará la realización de la comunicación del hecho, su lugar y fecha.
- c) Los Fedatarios Públicos deberán cumplir los mismos requisitos que los Proveedores de Servicios de Certificación para dar fe sobre mensajes de datos.
- d) Los documentos electrónicos expedidos por Notario o autoridad competente y firmados electrónicamente por ellos tienen los mismos efectos jurídicos que los documentos escritos de su misma clase.

Artículo.- 45.- Delegación de firmas: La delegación de firmas electrónicas se registrará de acuerdo a lo dispuesto en los siguientes literales:

- a) La solicitud de una firma electrónica ante los proveedores acreditados de servicios de certificación no podrá realizarse a través de representante voluntario.
- b) La solicitud de una firma electrónica ante los proveedores acreditados de servicios de certificación, para usarla en nombre de otra persona por el apoderado, tendrá que ser realizada por el poderdante y el apoderado.
- c) Para la delegación de firmas se cumplirá con los demás requisitos exigidos por la Ley.

Título iii

Capítulo i

Art. 46.- Jurisdicción: Las partes libremente pueden acordar los términos y condiciones bajo los cuales establecen relaciones electrónicas.

En caso de no acordar el lugar de resolución de controversias, se aplicarán las normas señaladas en la Sección Segunda del Título Primero, del libro Primero del Código de Procedimiento Civil. Para la identificación de la procedencia de un mensaje se utilizarán los medios tecnológicos disponibles y se aplicarán las normas señaladas en esta Ley y en las Leyes relacionadas con el proceso judicial.

Art. 47.- Notificaciones: En las controversias derivadas de la aplicación de esta Ley, también se deberá citar y notificar al demandado a su dirección de correo electrónico, con todas las providencias que se dictaren en el transcurso de la litis.

Capítulo ii

Art. 48.- Medio de prueba: El mensaje de datos, cualquiera sea su procedencia o generación, será considerado medio de prueba con todos los efectos legales que tienen los principios probatorios determinados en las Leyes que regulan la materia.

Art. 49.- Presunción: Existe presunción legal sobre un documento electrónico presentado como prueba, siempre y cuando la firma electrónica hubiere sido

certificada por un Proveedor de Servicios de Certificación que cumpla con los requisitos señalados en la Ley. En este caso se presumirá que:

- a) Los datos no han sido alterados desde su firma.
- b) La firma electrónica pertenece al suscribiente.
- c) Fue añadida al documento con la intención de manifestar su voluntad.

En caso de que alguna de las partes niegue la validez del contrato deberá justificar conforme a la Ley que el contrato electrónico adolece de uno o varios vicios que lo invalidan. Entre otros pueden ser:

- a) Que el procedimiento de seguridad, incluyendo los medios, utilizados para verificar la firma no pueden ser reconocidos técnicamente como seguros.
- b) Insuficiencia del procedimiento empleado.
- c) Adulteración técnica.
- d) Los demás establecidos en la Ley.

Artículo.- 50.- Pruebas: Para la validez de la prueba se deberán respetar los principios procesales consagrados en la Constitución y en la Ley. Las partes deberán seguir las siguientes normas para el uso de la prueba.

- a) Siempre que se presente un documento firmado electrónicamente ante un Juzgado o Tribunal se deberá presentar junto al soporte informático la transcripción en

papel del documento electrónico, así como los elementos necesarios para su lectura en claro y la verificación de la firma.

- b) Cuando la parte que se oponga a un documento firmado electrónicamente no reconozca su firma, la parte que haya presentado el documento deberá designar al proveedor del servicio de certificación en el que se encuentre el certificado, y solicitar del Juzgado que reclame dicho certificado y los documentos en los que se basó la solicitud del firmante.
- c) La información obtenida por medios electrónicos o por certificaciones de los proveedores o autoridades competentes, formarán parte del expediente al que se incorporen.
- d) El telegrama, telex, fax, facsímile en un documento escrito, deberá guardar su integridad, haber sido conservado conforme a lo prescrito en esta ley, cumplir los requisitos que les fueran aplicables y ser presentados cuando así lo solicite la Autoridad Competente.

Art. 51.- Valoración de la prueba: La prueba será analizada bajo los principios determinados en la Ley y de acuerdo con la seguridad y fiabilidad con la cual se la verificó, envió, archivó y recibió. Estos parámetros no son excluyentes y se ajustarán en base a la técnica y la tecnología. Para la valoración de las pruebas, el Juez, Arbitro o Mediador competente que juzgue el caso deberá designar los peritos que considere necesarios para el análisis, perfecto conocimiento técnico e interpretación de las pruebas presentadas.

Art. 52.- Infracciones: Para el juzgamiento de las infracciones cometidas en el Comercio Electrónico, regirán las normas del Código Penal, la Ley de Propiedad Intelectual y demás leyes pertinentes.

La violación a la confidencialidad será sancionado en base a lo dispuesto por el capítulo V, del título II, del libro Segundo del Código Penal y a las normas de la Ley de Propiedad Intelectual. Cualquier alteración o falsificación de un mensaje de datos, será sancionado de acuerdo a lo dispuesto en el Capítulo III, del Título IV, del Libro Segundo del Código Penal.

Art. 53.- Artículo Final: Esta ley entrará en vigencia a partir de su publicación en el Registro Oficial.

ANEXO C

DATOS INFORMATIVOS DEL ENCUESTADO

ESCUELA :

NOMBRE :

CARGO :

FECHA :

1. Le interesaría que los servicios que le ofrece la Escuela se promocionen y se comercialicen en el Portal?

- a.** Alto Interés
- b.** Medio Interes
- c.** Bajo Interes
- d.** No hay Interes

2. Qué tipo de servicios desearía que se promocióne y se comercialicen en el Portal?

- a.** Proyectos desarrollados por los alumnos
- b.** Servicios que ofrece la carrera
- c.** Promoción de la carrera

d. Otros. _____

3. Le gustaría que la reservación de los servicios se desarrolle a través del Portal?

a. Si

b. No

4. En su criterio la información de los servicios que ofrece la Escuela cada que tiempo se actualiza?

a. Bimestral

b. Trimestral

c. Semestral

d. Otros _____

5. Qué tipo computacional nos ofrece la Escuela para el desarrollo del Proyecto?

a. Completo (Computador, Modem, Acceso a Internet)

b. Incompleto

c. Ninguno

6. En su forma de ver la Escuela se considera preparada para enfrentar los procesos del negocio a través del Comercio Electrónico?

- a.** Activo
- b.** Poco activo
- c.** No activo

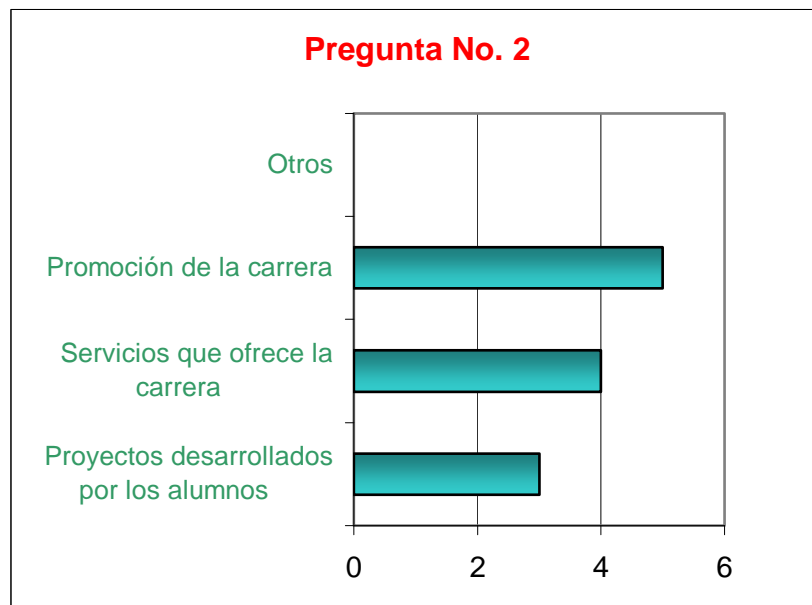
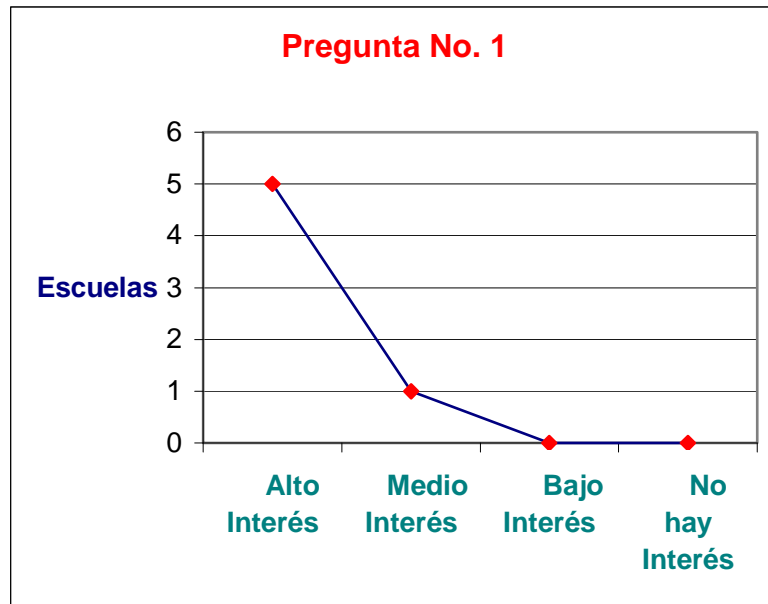
7. Que haría usted para adaptar los servicios de la Escuela a través del Comercio Electrónico en el Sitio Web?

- a.** Integrar a los docentes y alumnado para asociarse en el emergente mercado del Comercio Electrónico.
- b.** Seleccionar los mejores servicios que ofrece la Escuela
- c.** Concentrar a los alumnos a través del nivel académico y la ingeniosidad, comercialicen los servicios.

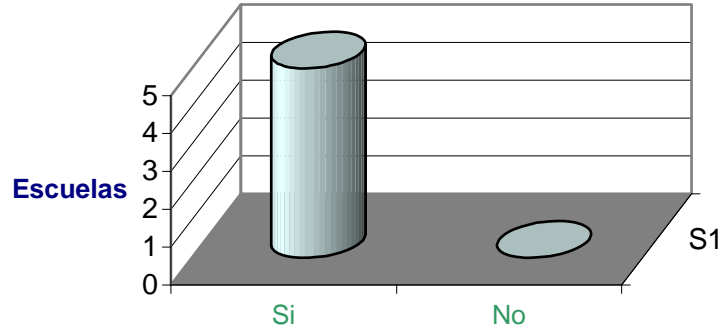
8. Cree usted que a través de este proyecto los servicios que brinda la Escuela tenga una audiencia empresarial activa?

- a.** Si
- b.** No

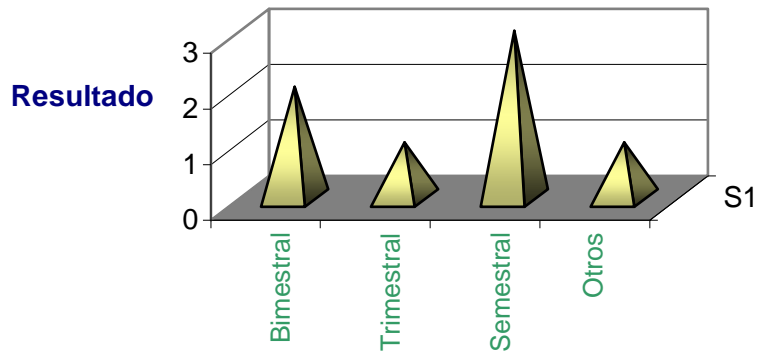
A continuación se muestra los resultados obtenidos a través de la encuesta

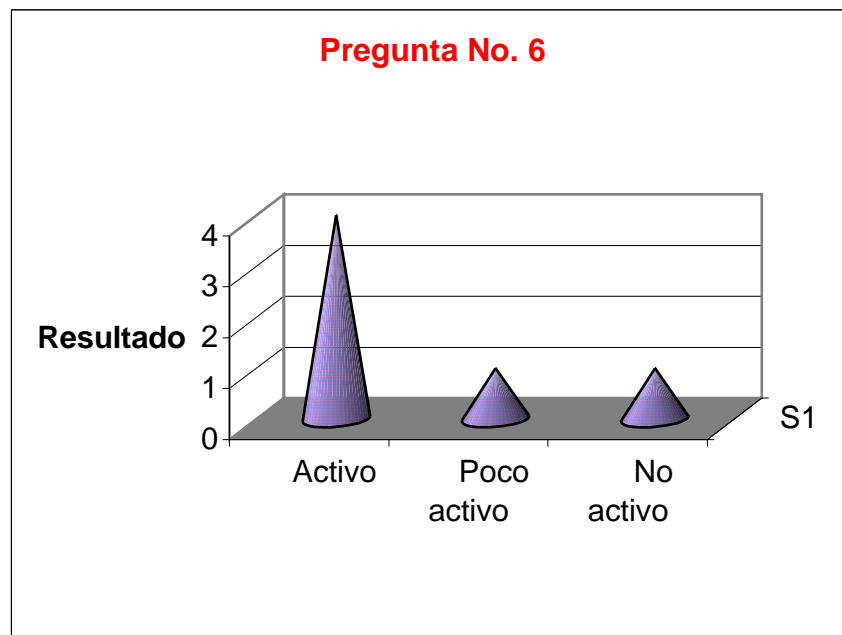
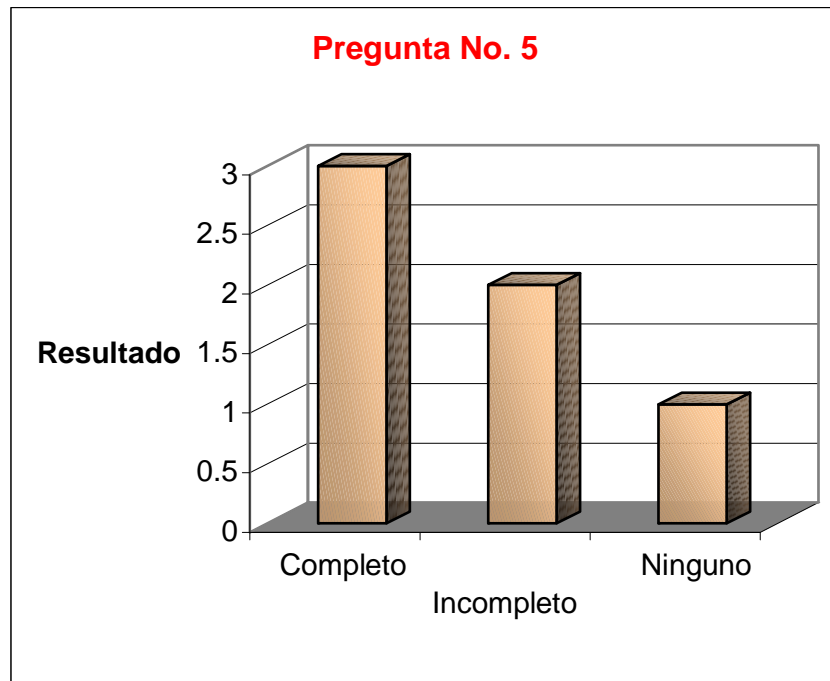


Pregunta No. 3

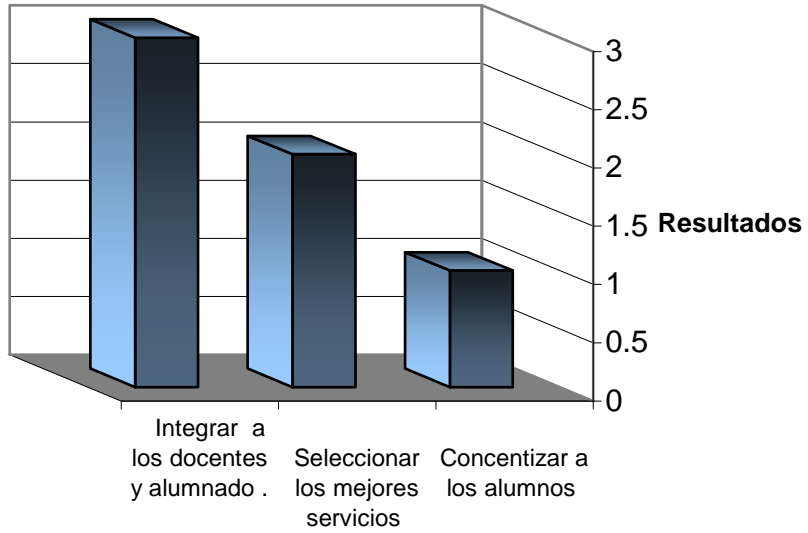


Pregunta No.4





Pregunta No. 7



Pregunta No. 8

