UNIVERSIDAD DON BOSCO

"DISEÑO DE UN SISTEMA PARA LA ADMINISTRACIÓN Y MANTENIMIENTO DE LA LIBRERÍA VIRTUAL DON BOSCO"

TRABAJO DE GRADUACIÓN

PREPARADO PARA LA FACULTAD DE INGENIERIA

PARA OPTAR AL GRADO DE

INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

PRESENTADO POR:

MARLON ERNESTO LAZO TURCIOS

SOFIA ISABEL FORNOS BELLOSO

ABRIL DE 2001

CIUDADELA DON BOSCO

SAN SALVADOR, EL SALVADOR C.A.

UNIVERSIDAD DON BOSCO

RECTOR

ING. FEDERICO HUGUET RIVERA

SECRETARIO GENERAL

PBRO. PEDRO JOSE GARCIA CASTRO

DECANO DE LA FACUTAD DE INGENIERIA

ING. CARLOS GUILLERMO BRAN

ASESORA DEL TRABAJO DE GRADUACION

LIC. INGRID ROXANA DE BRAN

JURADO EVALUADOR

ING. CARLOS GUILLERMO BRAN

LIC. FIDIAS ALFARO

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA

ESCUELA DE COMPUTACION

JURADO EVALUADOR DEL TRABAJO DE GRADUACIÓN:

"DISEÑO DE UN SISTEMA PARA LA ADMINISTRACIÓN Y MANTENIMIENTO DE LA LIBRERÍA VIRTUAL DON BOSCO"

_____	_____
LIC. FIDIAS ALFARO	ING. CARLOS G. BRAN
JURADO	JURADO

_____

LIC. INGRID ROXANA DE BRAN

ASESOR

AGRADECIMIENTOS

A Dios todo poderoso y a Jesucristo mi salvador, por permitirme culminar esta meta tan valiosa en mi vida.

A mi queridísima madre, María Inés, por todo su amor y su apoyo incondicional en el momento que fuera. A la familia Fornos-Belloso, por su mano amiga que estuvo siempre en el transcurso de nuestra carrera de estudiante; gracias don Mauricio.

A mis amigos, Juan y Frank, por estar siempre en las buenas y en las malas conmigo, y a todos mis amigos, gracias por hacerme sentir su hermano.

A mi compañera de tesis, Sofía.

Y dedico este esfuerzo a mi angelito que alumbrará toda mi vida.

Marlon Lazo

DEDICATORIA

A Dios y a la Virgen María, por haberme permitido lograr esta meta.

A mi familia. A mis padres, Mauricio e Idalia, por tanto amor y apoyo en cada momento de mi vida. A mi hermanita, Miriam, por ayudarme y acompañarme siempre. A mis angelitos, mis abuelitos que me han cuidado y siempre están conmigo: Chepita, Sofía y Rafael. A mi tía madrina, Ana Cristina, por llevarme siempre en sus oraciones.

A todos mis amigos, gracias por tanto cariño.

A mi compañero de tesis, Marlon.

Sofía Fornos

CONTENIDO

ANEXOS

INTRODUCCIÓN

Estamos inmersos en un mundo que cada día cambia. Pero estos cambios se están produciendo cada vez con una mayor aceleración en el campo de la informática y el mundo de los negocios no es ajeno a ello; es más, es uno de los primeros sectores que debe aprovechar las oportunidades que ofrecen estos avances.

El comercio moderno se caracteriza por un incremento de la capacidad de los proveedores, de la competitividad global en todo el planeta y de las, cada vez más exigentes, expectativas de los consumidores. Por ello, el comercio mundial está cambiando tanto en su organización como en su forma de actuar. Los límites en los negocios están desapareciendo con la nueva llegada del "Comercio Electrónico".

El Comercio Electrónico es un medio de hacer posible y soportar tales cambios a escala global. Permite a las empresas promoverse en casi cualquier parte del mundo, haciendo más eficientes así sus ventas, ser más flexibles en sus operaciones internas y dar mejor respuesta a las necesidades y expectativas de sus clientes. En definitiva, les permite situarse como proveedores y como clientes, en un mercado global. Con todo esto, se tiene una expectativa muy grande de la utilización del "Comercio Electrónico" en El Salvador, se considera que a corto plazo no solo las empresas podrán utilizar este medio de hacer negocios sino que, cada uno de cinco hogares podrán de alguna manera utilizar este servicio que Internet brinda.

La Universidad Don Bosco y sus alumnos no son ajenos a este tema y se trata por medio de este proyecto diseñar la "Librería Virtual Don Bosco", ya que se sabe, que los costos de mantenimiento y administración en comparación con una librería convencional son muy bajos y de esta manera habría una mayor rentabilidad.

En el capítulo uno se realiza el planteamiento del problema, el cual pretende delimitar el proyecto.

En el capítulo dos se presentan los conceptos más importantes para la comprensión del comercio electrónico, así como todos sus componentes y elementos relacionados con este.

Para el capítulo tres se presenta la investigación realizada para determinar si es acertada la realización de este proyecto, así como también el análisis hecho para determinar componentes, elementos y herramientas a utilizar.

En el capítulo cuatro se describen los pasos para el desarrollo del sistema, que comprende el diseño, configuración e integración de componentes.

Para el capítulo cinco se plantean las conclusiones así como las recomendaciones para logara un mejor resultado en la implantación del sistema.

También se incluyen: Ley de Comercio Electrónico, la cual es una propuesta para regular su funcionamiento; Glosario, que contiene definiciones de términos técnicos; Manuales de referencia del sitio, para facilitar a los usuarios la operación del sistema.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES

Las empresas que utilizan el comercio electrónico como herramienta de negocios, comenzaron hace más de dos décadas con la introducción del EDI (Intercambio Electrónico de Datos) entre firmas comerciales (envío y recibo de pedidos, información de reparto y pago, etc.). Incluso el comercio electrónico orientado al consumidor tiene también una larga historia: cada vez que se utiliza un cajero automático o se presenta una tarjeta de crédito, se está efectuando una transacción electrónica. El EDI, sin embargo, opera en un sistema cerrado; es un medio de comunicación más conveniente, estrictamente entre las partes involucradas.

La World Wide Web (WWW), la parte cliente-servidor de Internet, ha abierto una nueva era combinando el carácter abierto de Internet con una interfaz de usuario sencilla y fácil de usar.

Los procesos del Comercio Electrónico actual, están basados en los ordenadores personales debido al origen de Internet, una red de ordenadores. *La primera etapa* de la expansión del Comercio Electrónico reside en la base instalada de usuarios de ordenador (más usuarios "conectados"). *La segunda etapa* vendrá cuando más gente tenga acceso a los ordenadores (vía precios más bajos de los ordenadores o a través de dispositivos más baratos). *La tercera*, y más importante, expansión se predice que vendrá de aquellos con un acceso a la red global a través de un medio distinto del ordenador: a través de TV de radiodifusión, TV por cable, redes telefónicas y nuevas aplicaciones. Un uso más amplio de estos medios de acceso baratos representa la fase de "llevar los ordenadores del centro de trabajo a la sala de estar de casa".

Sin embargo, el precio de estos dispositivos, la facilidad de uso o el modo de acceder a la red son menos importantes que la forma en que utilizaremos estos

dispositivos. Convertir el ordenador en un dispositivo tan conveniente como la TV es una meta actual.

1.2 JUSTIFICACIÓN

Gracias a que Internet es un canal de comunicación más rápido, confiable, bajo en costo y ampliamente accesible, los negocios de todos los tamaños pueden aprovechar los beneficios a través del desarrollo de una exitosa estrategia de Comercio Electrónico. Las compañías que integren las soluciones de comercio más apropiadas para las demandas de la era digital obtendrán ventajas competitivas.

Con transacciones y comunicaciones digitales se pueden ofrecer mejores servicios y soporte. De hecho, las ventas en línea se están volviendo una parte muy importante de muchas empresas, el número de empresas a nivel mundial en ofrecer productos de esta forma incrementa rápidamente, obteniendo buenos resultados, pero se observa que en El Salvador todavía no es muy común.

Las transacciones en línea tienden a incrementar el autoservicio, y a brindar un acceso más rápido y mayor a la vasta información en el Web que da a los consumidores más control y poder. Además el costo de mantenimiento un comercio virtual es mucho menor que el costo que implica el de una sala de ventas convencional.

Este proyecto realizará para fomentar el uso del Comercio Electrónico y además permitirá que los alumnos y personal de la Universidad Don Bosco puedan realizar compra de libros a través de Internet, sin necesidad de tener tarjeta de crédito.

Tomando en cuenta que los libros son actualmente el producto más vendido a través de Internet, es muy apropiado realizar una aplicación de esta índole para

crear un nuevo concepto de negocio y fomentar el uso de Internet para construir relaciones más fuertes con los clientes.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

El proyecto a realizar pretende proporcionar una alternativa más de comercio, utilizando para ello la vía electrónica, haciendo énfasis en las ventajas que proporciona como: medio de publicidad, de bajo costo, de fácil mantenimiento; para que sea más utilizado en nuestro medio, ya que actualmente ha sido usado muy poco para el mercadeo de productos.

De esta forma, dicho proyecto proporcionará a la Universidad Don Bosco una forma de promover el Comercio Electrónico a través de la venta de libros en el web, creando para esto la "Librería Virtual Don Bosco", que contará con un completo sistema de Comercio Virtual en Internet que se maneje de forma fácil, que su implementación y mantenimiento sea económico y que ofrezca seguridad en las transacciones.

1.3.2 OBJETIVOS ESPECÍFICOS

- Diseñar para la Universidad Don Bosco un sistema para la administración y mantenimiento de la Librería Virtual, que ofrezca un servicio más a sus alumnos, personal y a todas las personas que tengan acceso a Internet.

.

- Impulsar el uso de Internet no sólo para comunicarnos, sino como una nueva forma de hacer negocios en nuestro medio.

- Diseñar un sitio web con criterios de marketing y publicidad, que sea fácil de usar y que el cliente pueda hallar de forma rápida lo que necesita, en cuanto a libros se refiere.

- Crear un sistema que contenga la estructura de la base de datos que contará con toda la información de los libros a ofrecer.

- Simular la verificación en las transacciones realizadas por los clientes en procesadores en línea de tarjetas de crédito.

1.4 DEFINICIÓN DEL TEMA

El proyecto a realizar denominado “Diseño de un Sistema para la Administración y Mantenimiento de Librería Virtual Don Bosco”, pretende ofrecer una alternativa de solución a la falta de una librería en la universidad, ya que en la actualidad no se cuenta con una, pues la que existía (en las instalaciones de la Ciudadela Don Bosco) fue cerrada.

Una librería virtual universitaria, sería la primera de su tipo en El Salvador, ésta por su naturaleza, ofrecería ventajas con respecto a la anterior, pues implica menos gastos de mantenimiento y administración, no es necesario que el cliente se encuentre físicamente en las instalaciones de la librería. Cubriendo no solo la demanda de los estudiantes de esta universidad si no que facilitaría la compra a alumnos de otras universidades y a toda persona que los necesite.

El resultado esperado es un sitio web, con todas las herramientas que permitan manejar las transacciones realizadas para la venta de libros a través de Internet, cuando se accese a la página se pueden buscar los libros de acuerdo a diferentes criterios, presentando una descripción breve del contenido de los libros, para asegurarse que es el libro buscado; brindaría seguridad para la base de datos y para las transacciones de los clientes; contará con una interfaz de administración; los clientes podrán realizar las compras utilizando las formas de pago siguientes: a) utilizando tarjeta de crédito y b) con el uso de un PIN (exclusivo para alumnos y personal de la universidad).

1.5 ALCANCES Y LIMITACIONES

1.5.1 ALCANCES

- Por el hecho de que la librería virtual estará en Internet se dará servicio a todo lugar donde se tenga acceso a ella y siempre que el cliente pueda hacer efectivo el pago por medio de cualquiera de las formas establecidas, lo cual permite cubrir un segmento de mercado bastante grande.

- Las formas de pago que se utilizarán serán: a) en línea en la librería virtual por medio de una tarjeta de crédito internacional que esté asociada al proyecto, b) para los alumnos y personal de la universidad por medio de un PIN (contraseña) asociado con su carnet o número de empleado. Las cuales se detallan a continuación:

  Para tarjeta de crédito:

  - Se accesa al sitio web y se seleccionan los libros a comprar.

  - Se introduce la información pertinente (como nombre, dirección, información de la tarjeta de crédito y toda la información requerida para realizar el proceso de venta), que se envía a través de un servidor seguro (secure server)

  - Una vez completada la orden por el consumidor, hace click en el botón de Pagar y en ese momento se inicia el proceso de pago.

  - Se verifica que la tarjeta no esté vencida y que tenga saldo disponible.

  - Después de la verificación se realiza la compra-venta.

Con el uso de un PIN:

- Se accesa al sitio web y se seleccionan los libros a comprar.

- Se introduce la información pertinente (como nombre, dirección, PIN y toda la información requerida para realizar el proceso de venta), que se envía a través de un servidor seguro (secure server)

- Una vez completada la orden por el estudiante o empleado, hace click en el botón de Pagar y en ese momento se inicia el proceso de pago.

- Se verifica que el PIN esté activo.

- Después de la verificación se realiza la compra-venta.

- Luego se le enviará el libro al estudiante.

- Para hacer efectivos los pagos que se realicen con tarjeta de crédito se podrán utilizar las principales tarjetas de crédito internacionales asociadas a VISA, por ser la única en El Salvador que ofrece verificación digital de transacciones.

- Se dará servicio a los alumnos, docentes y personal administrativo de la universidad, sin que éstos posean una tarjeta de crédito, por medio de un PIN o contraseña que se asociará con su número de carnet ó número de empleado, luego efectuarán el pago de sus compras de acuerdo a la políticas que la universidad establezca.

- El sistema será diseñado exclusivamente para la venta de libros, permitiéndole al administrador crear nuevas áreas de libros, las cuales servirán para efectuar mejor las búsquedas en la base de datos.

- La administración de la base de datos se podrá hacer de forma remota, es decir, que se podrá acceder a ella por medio del web, donde sólo la cuenta del administrador podrá realizar el mantenimiento necesario, para que se encuentre actualizada.

1.5.2 LIMITACIONES

- El proyecto se diseñará para que trabaje bajo la plataforma Linux, por lo que la base de datos, el Web Server y la interfaz para manipular dicho sistema estarán basados en este Sistema Operativo.

- Se permitirán transacciones para la tarjeta establecida, y que esta sea del tipo Internacional (o la que permita acceder la verificación de datos en línea), dicha verificación digital será simulada en su proceso original, para que su implantación pueda ser casi inmediata, porque los parámetros transmitidos son exactamente los que se utilizan en las transacciones electrónicas.

- El modo de envío de libros se hará exclusivamente por medio de una empresa de correo internacional (DHL o TNT).

- Al momento que una persona haga una búsqueda de un libro y este no se encuentre en la base de datos, se ofrecerá al cliente la opción de llenar un formulario con los datos del libro solicitado y posteriormente avisarle por medio de correo electrónico cuando el libro se encuentre a disposición.

2. MARCO TEORICO

2.1 Definición de *"Comercio Electrónico" (e-comerce).*

Se puede definir el Comercio Electrónico (o e-comerce en inglés) como todo aquel conjunto de transacciones que se llevan a cabo a través de computadoras y sistemas de telecomunicaciones.

El comercio electrónico es un intercambio telemático de información entre empresas o entre empresas y consumidores que da lugar a una relación comercial. Esta conexión se manifiesta por la entrega en línea de bienes intangibles como datos, documentos, imágenes, música, vídeos, servicios, entre otros, o en un pedido electrónico de bienes tangibles.

El comercio electrónico es un vehículo a través del cual se pueden obtener: mayor eficiencia en operaciones comerciales, reducciones en costos y una mejor atención al cliente. De éste, se pueden diferenciar dos tipos: *el que se realiza entre empresas* (socios comerciales) *y el que se realiza entre una empresa y el consumidor.* De este último tipo encontramos infinidad de servicios en el Internet, a través de los cuales es posible adquirir desde un arreglo floral hasta un automóvil.

2.2 El comercio electrónico en Internet.

La evolución de Internet ha demostrado como los usos potenciales de la red pueden permanecer a la espera de una oportunidad. Así, se pasó de una red militar a una académica donde las distancias se debilitaron, y las relaciones interpersonales ya no requieren de contacto físico. Lo mejor de todo, es que el

salto a una nueva etapa no significa automáticamente la muerte de la anterior, pero sí la necesidad de reestructurar la forma como se venían haciendo las cosas.

El cambio más reciente lo constituye el comercio electrónico, o la repentina necesidad de transformar todo sitio Web en una vitrina. Y la clave está en que la transición hacia el comercio electrónico más que una moda, constituye una forma de competir ventajosamente en el ambiente de negocios actual.

El comercio electrónico permite comprar virtualmente cualquier producto o servicio en cualquier lugar del mundo con sólo apretar un botón. Un ordenador conectado a Internet se convierte en la mayor galería comercial. Nunca comprar fue tan fácil ni tan inmediato. Pero también nunca fue tan inteligente.

La motivación de compra se sustenta sobre mucha información (precios, características de productos, demos, etc.) y en la experiencia de la compra. Desde que las empresas se volcaron en la Red se han realizado transacciones de *compra-venta*, pero hasta ahora, no ha sido una práctica demasiado frecuente, ni en lo que se refiere a la oferta ni a la demanda. Sin embargo, la situación está cambiando muy rápidamente.

El primer paso de muchas empresas ha sido establecer su presencia en Internet. Tener un sitio y darse a conocer. Un segundo paso ha sido empezar a utilizar las posibilidades de Internet en el ámbito de los procesos internos de las empresas. Son las tan nombradas *Intranets,* y luego el comercio electrónico. Cuando la compra-venta de productos y servicios se realiza entre empresas (business to business o e-business) el modelo se llama *Extranet*. Estas establecen relaciones electrónicas de diverso tipo -no sólo comerciales-, entre proveedores y fabricantes o entre fabricantes y clientes. Son la versión Internet del EDI (Electronic Data Interchange) que se ha utilizado con tecnología muy específica, en los sectores industriales más avanzados.

En cambio, cuando el comercio electrónico se realiza al usuario final, al consumidor propiamente dicho, se le llama *business to consumer o e-commerce*, y

aunque es el que ahora tiene mayor éxito, todo parece indicar que el comercio entre empresas será muy superior.

2.3 América Latina y El Salvador.

Las transacciones comerciales a través de la red de redes Internet podrían multiplicarse en los próximos años en América Latina, una de las zonas del planeta en que el comercio electrónico presenta mayores posibilidades de expansión.

Un informe del Banco Interamericano de Desarrollo (BID) indica que en el 2002 las transacciones vía Internet en América Latina podrían llegar a los 327 millones de dólares, 40 veces más que el año pasado.

Más de 100 millones de personas tienen actualmente acceso a Internet en todo el planeta, previéndose que en el 2005 la cifra se multiplique al menos por tres. En América Latina no existe todavía un hábito de compra a distancia como el que se puede verificar en Estados Unidos y Europa occidental.[i]

Las empresas latinoamericanas que operan en el sector de servicios deberían encontrar en la red de redes un vector de crecimiento natural, pero deben vencer algunas falsas creencias y modificar ciertas prácticas. Entre las falsas creencias se subraya el supuesto alto costo en tecnología que supondría la presencia de las empresas en Internet.

En comercio electrónico el 70 por ciento de la inversión reside en la promoción del sitio propio y sólo el 30 por ciento restante en la concepción de un buen soporte tecnológico. Incluir la empresa en uno de los buscadores existentes en Internet es una forma fácil y económica de hacerse conocer.

La atención permanente del sitio electrónico y el cumplimiento de lo prometido, como si se tratara de un local comercial tradicional, es otra de las claves para el éxito de una transacción electrónica

En El Salvador se tienen los sitios web de almacenes como Simán, Kismet, Regalos UPS, entidades como el Centro Nacional de Registros (CNR), SERTRACEN, además algunas Universidades ya cuentan con su presencia en Internet tales como: Universidad Don Bosco, Universidad Centroamericana José Simeón Cañas, Universidad Francisco Gavidia, Universidad Tecnológica y otras.

En el caso del CNR se puede encontrar disponible toda la información de las propiedades registradas en el país, y no se tiene que acudir físicamente a hacer grandes colas para consultar sobre el estado de los bienes que se poseen.

Si se quiere comprar en el extranjero también se puede hacer; lo único que se debe tener es una tarjeta de crédito internacional para que den el aval de la compra.

El tipo de comercio electrónico que mayor crecimiento y difusión ha tenido es el que se realiza entre dos empresas. Este proceso es conocido como "business to business" (B2B), y en el país ya se aplica, por ejemplo, en el proyecto EDI (Electronic Data Interchange), implementado por la Dirección Estratégica de Comercio Electrónico (DIESCO) de la Cámara de Comercio e Industria de El Salvador.

Por ejemplo, DIESCO, a través del proyecto EDI, maneja un conjunto de redes privadas a través del Teledespacho, herramienta computacional que agiliza y simplifica los trámites de importación aduanal. Teledespacho funciona eficazmente con diferentes tipos de empresas usuarias, en donde están involucrados importadores, exportadores con su tramitador autorizado y los agentes aduanales.

Se unen además al proyecto los consolidadores de carga transportista, quienes se comunican a través de la red VAN (red de valores agregados) con las aduanas del país. Ambas redes tienen finalidad mercantil y se comunican mediante sistemas y redes, sin que exista contacto físico directo entre quien oferta un bien o servicio y quien lo demanda. Además cubre acciones preparatorias, como publicidad y mercadeo.

El tema del comercio electrónico es delicado, ya que existe una serie de temas legales relacionados. Un ejemplo de ello son las compañías de discos, que pueden tener problemas con el derecho de propiedad intelectual, ya que es difícil controlar las obras en Internet.

El problema no sólo es de propiedad intelectual; existen otras cosas más, como la formación del consentimiento, protección de la privacidad, firma digital, entidades certificadoras y valor probatorio del documento electrónico, entre otras. Además tiene que existir una regulación de las marcas registradas, pagos de derechos aduanales e impuestos, y lo básico, la sanción de la responsabilidad civil y penal.

Debe existir un marco de seguridad jurídica que garantice la certeza de las inversiones y además los proceso de encriptado mediante el uso de tarjetas y mecanismos de pago usados para el comercio electrónico.

En cuanto a la formación del consentimiento en el ciberespacio, se da la tradicional oferta más aceptación que trae consigo un contrato, pero surgen cuestionamientos como ¿se forma el consentimiento mediante impulsos electrónicos?, ¿Cuándo y dónde? Y ¿cuál es la ley aplicable al contrato?

Pero no solo eso queda en el espacio. Existen más elementos como la protección a la privacidad (la intimidad de la información). Así como existe un

"Habeas Corpus", en algunas legislaciones también existe un "Habeas Data", que regula el derecho a la información personal.

Un aspecto fundamental para que se dé el comercio electrónico, son las firmas y certificados digitales. La firma digital es un código similar al de las tarjetas de débito y crédito, a la que se le da una especie de PIN (número de identificación personal) para hacer la transacción.

En lo que respecta a las instancias certificadoras, son las que tendrían la facultad de revisar, supervisar y auditar todas las firmas digitales con el fin de asegurar que sean auténticas. El Concejo Nacional de Ciencia y Tecnología (CONACYT) o el CNR pueden ser idóneas, pero no necesariamente las únicas.

Antes de esto tiene que existir un trabajo multidisciplinario donde estén los ministerio de Economía y de Hacienda, la Superintendencia del Sistema Financiero (SSF), bancos, emisores de tarjetas, comerciantes, transportistas y empresas de correo, Cámara de Comercio y otras.

Una vez establecido el marco general, las entidades de certificación podrían velar por el proceso, como alguien que tiene la facultad de auditar el sistema de seguridad electrónica de los cibercomerciantes, así como la SSF auditaría los esquemas de seguridad electrónica de bancos y emisoras de las tarjetas de crédito.

Es conveniente que una institución vinculada al Estado se encargue no sólo de encriptar, sino de certificar el uso de las firmas digitales. Nadie descarta que El Salvador se encuentre vulnerable a ataques de “hackers” (piratas de internet), ya que carecemos de leyes y sanciones que regulen este tipo de actos. El Salvador poco a poco deberá definir su marco legal para el comercio y las transacciones electrónicas.[ii]

2.4 Desconfianza Vrs. Seguridad.

La barrera más importante es, la falta de confianza, ésta desconfianza hacia las nuevas tecnologías se articula en torno a tres temores fundamentales:

La privacidad que los usuarios finales sienten amenazada en la medida en que desconocen hasta qué punto los datos personales que suministran a un servidor de comercio electrónico serán tratados de forma confidencial.

La autenticación que inquieta a los usuarios, quienes dudan de si la persona con la que se comunican es verdaderamente quien dice ser.

La seguridad global que preocupa a los usuarios, pues temen que la tecnología no sea suficientemente robusta para protegerles frente a ataques y apropiaciones indebidas de información confidencial, especialmente en lo que respecta a los medios de pago. Es interesante el hecho de que de todo el proceso de compra, lo que más sigue preocupando es el pago, es decir, el momento en el que el comprador se enfrenta a la ventana donde ha introducido su número de tarjeta de crédito y duda a la hora de pulsar el botón de "Enviar".

Estos temores, tienen su fundamento real y su solución no resulta trivial.

En el primer caso, la tecnología, y en concreto la criptografía, ofrecen las herramientas necesarias para la protección de la información almacenada en las bases de datos corporativas, información como listas de clientes, sus datos personales y de pago, listas de pedidos, etc. Existen muchas técnicas de control de acceso que hábilmente implantadas garantizan el acceso a la información confidencial exclusivamente a aquellos usuarios autorizados para ello. Por lo tanto, aunque la criptografía provee de medios aptos, depende en última instancia del comerciante el nivel de compromiso que adopte respecto a la seguridad de los datos que conserva en sus ficheros y su política de control de acceso. Así pues, éste es un temor bien presente y sin fácil respuesta. La tecnología nada tiene que decir si un comerciante decide vender su

información a terceros. La delgada línea que protege la privacidad del usuario está constituida en este caso por la integridad moral del comerciante. En estas circunstancias, es mejor asegurarse con quién se comercia.

En el segundo caso, la solución inmediata que ofrece la criptografía viene de la mano de los certificados digitales. La tecnología de certificación está suficientemente apta como para autenticar adecuadamente a las partes involucradas en una transacción. La más comúnmente utilizada es SSL y a pesar de la tan llamada limitación criptográfica fuera de Norteamérica de claves débiles de 40 bits, lo cierto es que a la hora de autenticar a las partes, principalmente al servidor, SSL funciona satisfactoriamente. Otro asunto es si asegura o no la confidencialidad, cuestión más que dudosa, si se tiene en cuenta que una clave de 40 bits se rompe en cuestión de horas, con lo que los datos por ella protegidos quedan al descubierto rápidamente. Otras tecnologías emergentes, como SET, ofrecen mucha mayor confianza en este campo y, de paso, dan solución al primer problema de la privacidad. SET permite autenticar a las partes involucradas en la transacción de manera completamente segura, sin restricciones criptográficas debidas a absurdas leyes de exportación. Su mecanismo de firma dual garantiza además que el comerciante no conocerá los datos de pago (número de tarjeta de crédito), eliminando así la posibilidad de fraude por su parte. SET garantiza así que el comerciante cobra por la venta y que el comprador no es estafado por el comerciante ni por hackers.

En cuanto al tercer temor, nuevamente la criptografía moderna y los productos de seguridad proporcionan las soluciones a los problemas.

Por lo que se nota las verdaderas barreras al comercio electrónico no son tanto tecnológicas si no que son humanas. Esto prueba, que el eslabón más débil de la cadena es de índole personal, no tecnológico.

El comercio electrónico es tan seguro como las líneas de comercio que normalmente usamos, en las cuales existe la posibilidad de ser sujeto de todo tipo

de engaño o estafa, situación que pudiera presentarse con mayor frecuencia en el comercio electrónico por tratarse de una actividad nueva para muchos de los compradores.

Existen otras alternativas de pago, para comercio electrónico, como el "cibercash" (dinero electrónico), estas alternativas ofrecen mayores restricciones de seguridad para evitar un fraude.

Uno de los principales retos para hacer del comercio electrónico una línea de comercio estable, radica en eliminar la asociación que se tiene de "documento" con "papel" y pensar en medios magnéticos, de ésta manera será más fácil la comprensión de esta nueva actividad, de la cual, ya sea como compradores u oferente de algún producto, se puede obtener grandes beneficios.

Si no se pueden realizar transacciones económicas seguras, de nada sirve el comercio electrónico. Esta es una de las barreras que más preocupa al consumidor final. De todas maneras, es mucho más inseguro pagar con una tarjeta de crédito en un restaurante que en Internet y curiosamente hasta ahora nadie lo ha tomado en cuenta.

Desde el punto de vista del usuario existen diversas soluciones para realizar un pago seguro, pero siempre dependen de las opciones que le ofrezca el vendedor. Todo sistema de pago tiene una parte en el navegador cliente y otra parte en el servidor web, que deben entenderse. Si el vendedor le ofrece al comprador diversos sistemas éste podrá escoger, de otro modo no. Desde el punto de vista del comerciante, existen diversos aspectos de seguridad que exceden el mismo pago. El primer aspecto es el de la disponibilidad de los datos. Para que sean accesibles todo el año, a todas horas, se necesitan sistemas redundantes basados en clustering o mirroring (discos con idéntica información escrita en ellos al mismo tiempo). El segundo aspecto, es el de la seguridad del sistema, que se establece mediante un programa de filtrado de paquetes de datos llamado cortafuegos. Finalmente, a nivel de pago se necesita un servidor seguro que permita una comunicación confidencial, es decir, que nadie ajeno a esta

pueda entender o descifrar, y autenticada, o sea, que estemos seguros de la identidad tanto del emisor como del receptor. El nivel de seguridad de los agentes que intervienen en una comunicación con transacción económica viene dada por el tamaño de las claves utilizadas.

Se emplean algoritmos de clave pública como el RSA, y el MD5 para autenticación. Por ejemplo, en el protocolo SET, el cliente tiene una clave de 512 bits, el vendedor de 768 bits y las entidades financieras de 1024 bits. Para ver el nivel de seguridad de estas claves basta un ejemplo: se tardó casi un año y la concurrencia de cientos potentes ordenadores, en romper un mensaje encriptado con la clave RSA-126. El protocolo SSL (Secure Sockets Layer) versión 3, es el más utilizado hoy en día y permite crear una relación confidencial y autenticada. Su único inconveniente es que si el pago se realiza mediante una tarjeta de crédito, el número de esta y la fecha de caducidad son conocidos por el vendedor. Si éste nos ofrece confianza no tendremos mayor problema, pero de otro modo podemos temer que realice transacciones electrónicas, usurpando la titularidad de nuestra tarjeta.

En cambio, el protocolo SET (Secure Electronic Transaction) auspiciado por VISA, MasterCard y las mayores empresas de informática, sirve para autenticar tarjetas de pago sin que el número de la tarjeta sea conocido por el vendedor. Tan sólo el usuario y la entidad financiera lo conocen. El sistema SET es el más seguro que existe, ya que está pensado especialmente para el comercio electrónico, y aunque tiene otras muchas ventajas, su gran problema es que está poco implantado.

2.5 CONCEPTOS DE TECNOLOGÍA WEB UTILIZADA.

2.5.1 TECNOLOGIA CGI

2.5.1.1 Definición

Las siglas CGI, correspondientes a la expresión inglesa *"Common Gateway Interface"*, referencia una especificación técnica que posibilita una mayor interacción entre clientes y servidores WWW. CGI es el método por el cual un servidor Web puede obtener datos desde (o enviar datos a) bases de datos, documentos y otros programas, y presentar esos datos a usuarios vía Web. Más sencillo, CGI es programar para el Web. Un CGI puede ser escrito en cualquier lenguaje, y de todos esos Perl es el más popular.

CGI es un estándar, en términos simples es sólo un conjunto de variables usadas comúnmente con las convenciones usadas para accesarlas. Las variables proporcionadas por la convención CGI son usadas para intercambiar información entre el servidor http y el programa cliente.

Además CGI proporciona un medio para retornar salidas al browser. Toda salida es enviada a stdout (la salida estándar) por un programa CGI que aparece en el navegador web, proporcionando la cabecera correcta de tipo MIME que es enviado al programa CGI.

Las principales posibilidades de CGI se cifran en la posibilidad de generar documentos HTML de forma dinámica, es decir, enviar al cliente un documento previamente inexistente; el documento puede consistir en una página HTML, una imagen, texto plano, etc. pudiendo incluir información procesada por el ordenador servidor como resultado de un cálculo o de la consulta a una base de datos.

Otra importante ventaja de la especificación CGI, es que no exige grandes esfuerzos de programación, ya que los aspectos técnicos más complejos relativos a la comunicación entre sistemas serán gestionadas por el propio servidor HTTPd.

Para que esto sea posible, únicamente se tienen que agrupar los programas CGI en un directorio que dependa directamente del directorio correspondiente al software HTTPd. Se acepta la convención de crear este directorio con el nombre "cgi-bin" o "bin" se puede utilizar como depósito de los ficheros CGI cualquier otro directorio, siempre que en la configuración del servidor HTTPd se especifique mediante la cláusula ScriptAlias, pudiendo declarar tantos directorios depositarios de programas CGI como consideremos necesario.

La ejecución de una aplicación CGI consta de tres fases:

1 Llamada del cliente WWW al servidor, solicitándole la ejecución del programa.

2 Ejecución del programa CGI con los parámetros especificados (opcionalmente) por el cliente.

3 Generación del documento-resultado que será direccionado al ordenador cliente.

La forma más común de pasar argumentos al programa CGI será mediante un formulario diseñado en páginas HTML. Un formulario HTML cuenta con una serie de casillas de diálogo, cuadros de texto, etc. que se asocian a distintas variables de distinto tipo (textuales, numéricas...). Además, en la definición del formulario se especifica tanto el CGI que deberá ejecutarse, como la forma en que se van a pasar los parámetros (en el caso de que los haya).

En el momento en que se envíe el formulario al servidor (mediante la pulsación del botón asociado al proceso SUBMIT), el cliente solicitará al servidor la ejecución del programa CGI asociado, con los valores de variable que hayamos consignado en cada una de las casillas y cuadros de diálogo.

Un programa CGI enviará un documento-resultado al cliente que solicitó su ejecución. La salida estará formada por un encabezamiento y por la información que se mostrará en el visualizador cliente. Entre el encabezamiento y el

documento se dejará una línea en blanco que permita saber cuando termina uno y comienza el otro.

2.5.1.2 Funcionamiento

Los elementos requeridos para accesar una base de datos desde web se muestran en la Figura 2.5.1. El término interfaz se refiere al software de base de datos provisto, el término gateway se refiere al software para la conexión entre web y la base de datos.

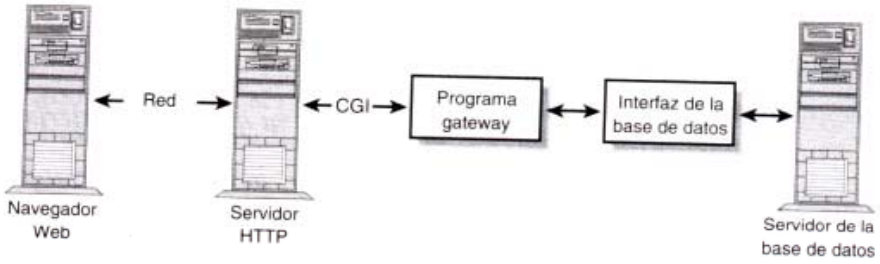


Figura 2.5.1

Cuando se usa un navegador web para accesar una base de datos, hay varios componentes que intervienen para transferir la consulta del usuario a la base de datos y devolver los resultados al navegador. La acción se desarrolla de la siguiente manera:

1. El usuario llama un programa gateway que utiliza CGI, generalmente haciendo clic en un hipervínculo, u oprimiendo un botón en el navegador web.
2. El navegador reúne toda la información escrita por el usuario para enviarla al programa CGI.

3. El navegador contacta al servidor HTTP en la máquina donde reside el programa CGI, pidiéndole que localice a este último, y le transfiere la información.
4. El servidor HTTP corrobora si la máquina solicitante tiene autorización de acceso al programa CGI.
5. Si el usuario tiene acceso, el servidor HTTP localiza el programa gateway y transfiere a éste la información del navegador Web. La figura 2.5.2 muestra los pasos del 1 al 5.

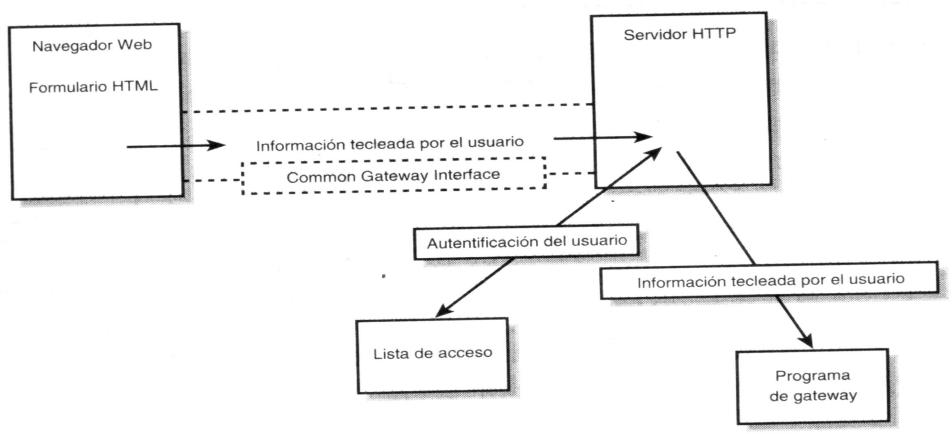


Figura 2.5.2

6. Se ejecuta el programa gateway.
7. El proceso gateway convierte la información recibida a un formato que la base de datos sea capaz de entender.
8. El gateway usa el módulo de la base de datos para transferir la consulta a la interfaz de la base.
9. La interfaz de la base de datos analiza la sintaxis de la consulta para asegurar que sea precisa.
10. Si la interfaz encuentra un error de sintaxis en la consulta, se envía un mensaje de error al programa gateway.

11. El mensaje de error se envía al servidor HTTP, el cual lo transfiere al navegador web para que este los despliegue al usuario. El proceso se detiene aquí. Los pasos 6 al 11 se muestran en la Figura 2.5.3.

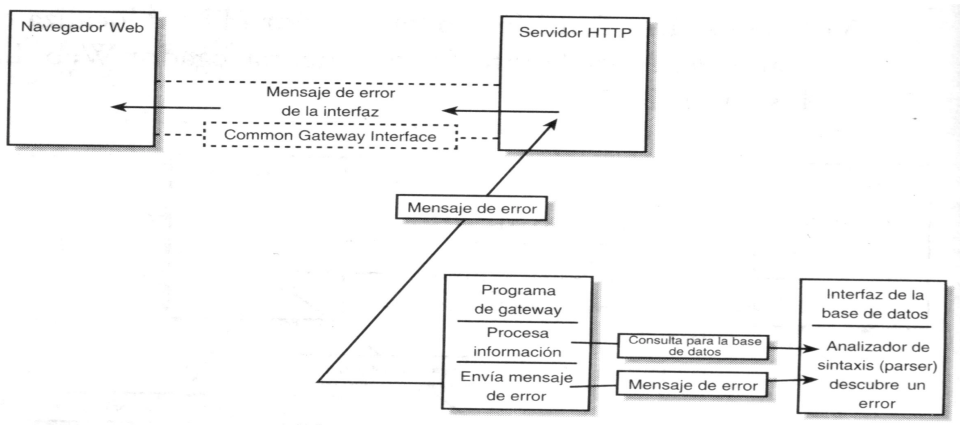


Figura 2.5.3

12. Si no hay error, la interfaz envía la consulta a la base de datos.
13. La base de datos atiende la consulta y devuelve los resultados al programa gateway a través de la interfaz.
14. El programa gateway formatea los resultados y los manda al servidor, por medio del CGI, para su envío al navegador Web.
15. El navegador web despliega los resultados. Los pasos 12 al 15 se muestran en la figura 2.5.4.

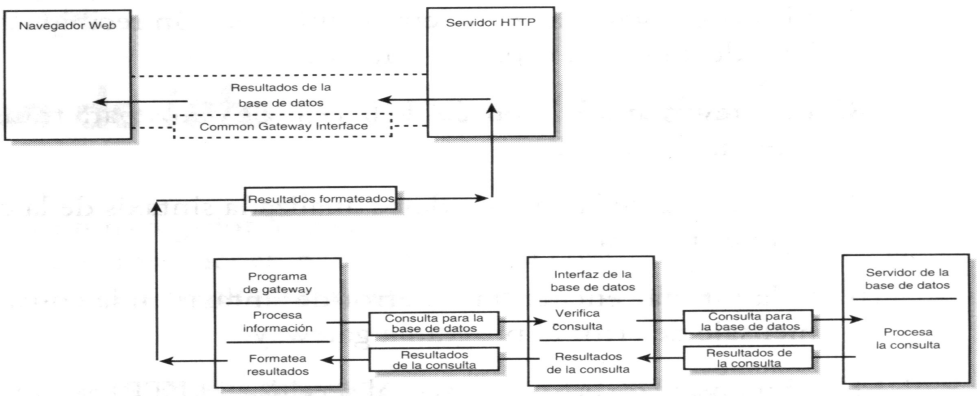


Figura 2.5.4

2.5.2 Sistema operativo

Linux es un sistema operativo muy parecido a UNIX, pero a diferencia de este es gratis, cualquier persona lo puede usar sin tener que pagarle a nadie ni tener que obtener ninguna licencia. El sistema es independiente, no contiene ningún código fuente de ninguna compañía privada. Linux corre en casi cualquier computadora: Intel, Digital/Compaq Alphas, PowerPC (Macintosh, BeBox, etc.), Sun Sparc & Sun Ultra, Amiga, Corel NetWinder, y también en la 3Com Palm Pilot.

Ventajas de Linux

- Su distribución es gratuita.
- Es un sistema operativo estable y robusto como para que aplicaciones prestigiosas como Communicator (Netscape), Oracle (Oracle) y Wordperfect (Corel) corran sin ningún problema.
- Cumple con estándares POSIX.
- La parte gráfica XFree, la puede cambiar fácilmente, existen en el mercado distintas interfaces como KDE, GNOME, ENLIGHTENMENT, AFTERSTEP, etc.
- Posee millones de utilidades para programar y para la red.
- Existen varias distribuciones con característica especiales, como: Red Hat, Debian, Slackware, Suse.
- La posibilidad que el sistema operativo no responda es casi remota.
- Existen Suites como Microsoft Office (Koffice, Staroffice)
- Perfecto como servidor de Internet (Web, FTP, Telnet, etc.).
- Este sistema operativo se puede instalar en equipos desde 80386.
- Interoperabilidad

- Filesystem - ext2, fat, vfat, minix, hpfs, ntfs, fat32, hfs, bsdm
- Network Filesystems - NFS, SMB/CIFS, ncpfs, cryptographics NFS
- Network File Serving - NFS, SMB/CIFS, Appletalk, Netware, HTTP
- Binary Compatibility - SCO, Solaris, SunOS, Digital Unix

- Multi-Booting - LILO, loadlin, MILO, SILO, etc.
  - Soporte para múltiples plataformas
  - Fue hecho con la ayuda de todo el mundo.
  - Networking
- Routing
- IP Masquerading
- Firewalling

Las principales razones para que alguien use Linux incluirían el hecho de que este sistema está equipado internamente con un completo soporte para trabajo en red, lo que proporciona acceso total a Internet. Más generalmente, los usuarios son atraídos por el completo entorno de desarrollo incluido. También, a diferencia de la mayoría de los Entornos Gráficos de Usuario (GUI) modernos, la parte gráfica de Linux (XWindow) está claramente separada del entorno subyacente, y hay un completo grupo de programas modernos tales como navegadores web, bases de datos y software de fax que trabajan directamente en el entorno no-gráfico. Esto proporciona la forma de proveer caminos alternativos en el acceso a la funcionalidad del sistema.

Prácticamente no hay nada comercial disponible específicamente para Linux. Hay una notable cantidad de software de libre distribución que puede ser útil para la adaptación.

Linux tiene la gran ventaja sobre Windows de tener la mayoría de su software orientado a línea de comandos. Esto está cambiando y casi todo se encuentra disponible con una apariencia gráfica. Sin embargo, debido a que en sus orígenes fue un sistema operativo de programadores, todavía se escriben

programas orientados a línea de comandos, que cubren casi todas las nuevas áreas de interés.

Costo del NOS (Sistema Operativo de Red)

A la hora de iniciar un proyecto, el factor económico juega una pieza clave en la decisión a tomar, y la selección de un NOS no es la excepción. El costo varía entre cada NOS, partiendo desde precios bastante altos, hasta sistemas de distribución gratuita. El pagar más por un NOS no significa que éste vaya a resultar más productivo para la organización que uno de bajo costo, por lo que se debe buscar aquél que cumpla con las expectativas de la empresa, tratando, claro, que el desembolso sea siempre el menor posible. Enseguida se presenta información reciente sobre los costos de varios NOS analizados en este trabajo.

Linux es gratis ó cuesta $ 49.95 USD (CD-ROM). Sin restricción de licencias.[iii]

Requerimientos de Hardware

Cada sistema operativo de red tiene diferentes requerimientos de hardware para funcionar correctamente, si éstos no son satisfechos, el sistema puede no operar o trabajar en un nivel muy por debajo del esperado, ocasionando serios problemas en la red. Es conveniente entonces, conocer los requerimientos de cada NOS para ver si el equipo actual los satisface o si es necesario invertir en nuevo hardware.

- Procesador Intel 386 y posteriores, SPARC, Alpha, PowerPC, etc.
- Mínimo 4 MB de memoria.
- De 150 a 500 MB en disco duro.

2.5.3 Herramienta de Desarrollo (Programación).

Perl es un lenguaje interpretado que tiene varias utilidades, pero está principalmente orientado a la búsqueda, extracción y formateado de ficheros de tipo texto. También es muy usado para manejo y gestión de procesos (estado de procesos, conteo y extracción de parámetros característicos, etc).

Es una combinación de las características de los lenguajes más usados por los programadores de sistemas, como son los shell del sistema operativo UNIX, los utilidad (que incluye un lenguaje interpretado propio) awk para formateo y tratamiento de texto e incluso características de Pascal, aunque su potencia se basa en la similitud con las mejores características del lenguaje estructurado C. En general cualquier utilidad que se necesite realizar en sh, awk, o sed, se puede implementar de una manera mas potente y sencilla mediante el lenguaje Perl

Algunas de las ventajas del uso del lenguaje Perl son las siguientes:

1 Construcción de pequeños programas que pueden ser usados como filtros para obtener información de ficheros, realizar búsquedas.

2 Se puede utilizar en varios entornos, como puede ser Windows 95, OS/2, ..., sin realizar cambios de código, siendo únicamente necesario la introducción del interprete Perl correspondiente a cada sistema operativo.

3 También es uno de los lenguajes mas utilizados en la programación de CGI scripts, que son guiones o scripts que utilizan el Interface CGI (Common Gateway Interface), para intercambio de información entre aplicaciones externas y servicios de información. Como ejemplo de ello tenemos los programas de búsqueda usados por el browser Netscape.

4 El mantenimiento y depuración de un programa en Perl es mucho más sencillo que la de cualquier programa en C.

Perl rápidamente se ha convertido en el lenguaje más popular para escribir CGI. También es un buen lenguaje para sistemas con tareas administrativas. Un lenguaje práctico (fácil de usar, eficiente y completo).

2.5.4 Servidor de datos

La base de datos elegida es Mysql, es un motor de peso ligero para base de datos que aplica un subconjunto del estándar ANSI SQL. Dado que mSQL solo aplica un subconjunto de los comandos SQL disponibles, requiere muy pocos recursos de computo y es sencillo de configurar y usar. Las características que ofrece y los tipos de datos que admite son limitados, pero satisfacen la mayor parte de requerimientos de una aplicación. Cumple las siguientes características:

- Tiene diferentes tipos de columnas como: enteros con y sin signo de 1, 2, 3, 4 y 8 bytes de largo, float, double, char, varchar, text, blob, date, time, datetime, timestamp, year, set y enum.
- Joins muy rápidos utilizando un solo barrido multi-join optimizado .
- Soporte completo para operadores y funciones en las partes SELECT y WHERE de las consultas.
- Las funciones SQL son implementadas a través de una librería de clase optimizada y muy rápida.
- Soporte completo para cláusulas SQL: GROUP BY y ORDER BY. Soporte para funciones de grupo: COUNT(), AVG(), STD(), SUM(), MAX(), MIN(), COUNT(DISTINCT).
- Se pueden mezclar tablas desde diferentes bases de datos en la misma consulta.
- Un sistema de passwords y privilegios el cual es muy flexible y seguro y el cual permite verificación. Los passwords son seguros ya que todo el tráfico de passwords cuando se conecta a un servidor es encriptado.

2.5.5 Interfaz

HTML es un lenguaje de etiquetas que en español significa Lenguaje de Marcado de Hiper Texto (Hyper Text Markup Language), HTML no es un lenguaje de programación, es solamente como su nombre lo dice “Lenguaje de Marcado”, las etiquetas sirven para “encerrar” o delimitar el texto (o un gráfico) y definen como aparecerá en un navegador como Netscape, Internet Explorer o Mosaic, entre otros. Las etiquetas también describen dónde se dispondrán las cosas (ubicación).

HTML es un lenguaje muy primitivo, si se quieren hacer cosas muy atractivas se tiene que usar mucha imaginación para aprovechar al máximo las etiquetas disponibles. Los documentos de HTML (ó páginas web) se pueden crear en cualquier editor de texto que tenga la capacidad de guardar los archivos como “solo texto” (ó formato ASCII) por ej.: WordPad, Word 97, NotePad, Edit de MS-DOS, vi de Unix, etc. pero ahora hay aplicaciones o “herramientas de desarrollo” que facilitan el trabajo de escribir el código e incluso nos libran de aprendernos las etiquetas y cada uno de sus atributos, por ej.: FrontPage, Netscape Composer, HomeSite, etc. incluso un documento de Word puede guardarse como un documento HTML.

Estructura de una página WEB

Las etiquetas básicas de HTML especifican el tamaño, color y posición del texto. Para añadir formato al texto están las etiquetas negrita (<B></B>), cursiva (<I></I>), centrado (<CENTER></CENTER>), etc.

- ✓ Un documento HTML está formado por elementos. Cada elemento consta de una marca de comienzo, un bloque de texto y una marca de fin.
  <COMIENZO> bloque de texto </FIN>
  Por ejemplo,
  <H1>Encabezamiento de nivel 1</H1>

- ✓ También existen elementos vacíos, que no afectan a bloques de texto y, por tanto, no contienen marca de fin:
  <MARCA>
  Por ejemplo, el siguiente elemento produce una ruptura de línea
  línea 1
 línea 2

- ✓ Muchos elementos tienen atributos que definen propiedades del elemento:
  <COMIENZO ATRIBUTO=VALOR> bloque de texto </FIN>
  Por ejemplo,
  <H1 ALIGN=CENTER>Encabezamiento de nivel 1 centrado</H1>

- ✓ Comentarios
  Los comentarios se escriben en HTML de la siguiente forma:
  <!-- Esto es un comentario -- >

- ✓ Comienzo y final del documento
  <HTML>
  <HEAD>
  ... Encabezamiento del documento
  </HEAD>
  <BODY>
  ... Cuerpo del documento
  </BODY>
  </HTML>

2.5.6 Servidor web

Apache es uno de los mejores servidores de Web utilizados en la red Internet desde hace mucho tiempo, únicamente le hace competencia un servidor de

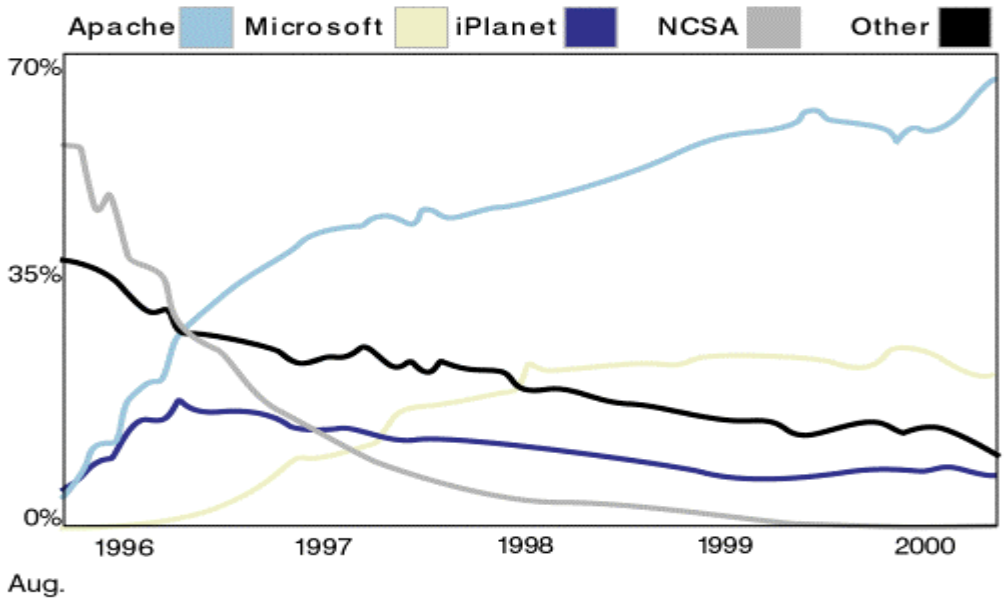
Microsoft, el IIS. Por lo que éste servidor es uno de los mejores del software libre, y que usan mucho los usuarios de LINUX.

Es un servidor de web flexible, rápido y eficiente, continuamente actualizado y adaptado a los nuevos protocolos (HTTP 1.1)

- Implementa los últimos protocolos, aunque se base en el HTTP / 1.1
- Puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo y con la API de programación de módulos.
- Incentiva la realimentación de los usuarios, obteniendo nuevas ideas, informes de fallos y parches para solución de los mismos.

La versión actual del apache es la 1.2.4 (1.3 ya está en beta). En la nueva versión se incluyen características como el soporte para windows NT y windows 95, así como la inclusión de cuatro dígitos en las fechas para evitar los problemas del año 2000.

Estadística publicada por IBM muestran al servidor web Apache como el más utilizado en la actualidad:



2.5.7 Seguridad

Cuando se transmiten datos mediante HTTP se establece una comunicación entre un cliente y un servidor. Para realizar transacciones seguras el protocolo más utilizado hoy día es SSL (Secure Sockets Layer) que impone la certificación del servidor, conociéndose como servidor seguro. Este protocolo encripta los datos transferidos mediante la versión segura de http, llamada HTTPS. Si se quiere comprar en una tienda on-line, en el momento en que piden los datos de la tarjeta de crédito se entra en su servidor seguro, el navegador avisa y se ve que se entra en una URL del tipo https://..., indicando que es una conexión segura.

En el navegador se pueden comprobar los datos de la tienda viendo los datos del certificado electrónico, se comprueba que CA lo ha emitido y datos de la tienda.

[i] Dirección del BID.

[ii] El Diario de Hoy, Domingo 12 de marzo de 2000. página 6-7.

[iii] Sitio de Distribución SUSE
http://www.suse.com.de/

3. INVESTIGACIÓN Y ANÁLISIS

3.1 LIBRERÍA DON BOSCO

La librería Don Bosco (actualmente cerrada) estuvo ubicada en las instalaciones de la Ciudadela Don Bosco, en su mayoría los libros a la venta eran los que se utilizaban en las materias impartidas en la diferentes carreras de la universidad, para otras carreras la oferta era mínima. Se contaba con variedad de títulos solamente al inicio de ciclo, ya que entonces es que los libros nuevos ingresaban, luego la existencia en libros disminuía.

La mayoría de clientes eran alumnos de la Universidad Don Bosco, entre los factores que influían en esto, están, la ubicación geográfica de la Ciudadela Don Bosco no es la más adecuada para atraer más compradores , la poca variedad de libros ofrecidos, además no se le hacía ninguna forma de publicidad, tampoco descuentos u otros atractivos.

Debido a las pocas ventas, el costo operativo se excedía, lo que impidió el sostenimiento y crecimiento del negocio.

3.2 LIBRERIAS EN INTERNET

Las principales compañías editoriales y librerías de Estados Unidos han iniciado una desenfrenada carrera a través de Internet para conseguir más clientes en un mercado que mueve al año 28.000 millones de dólares.

El espectacular crecimiento de la empresa "Amazon.com", que se autodefine como "la librería más grande de la Tierra", con una oferta de 2,5 millones de títulos, ha obligado a otras grandes cadenas como "Barnes & Noble" y "Simon & Schuster" a seguir sus pasos en la venta pionera de libros "on-line".

Desde su nacimiento en julio de 1995, "Amazon.com" ha registrado constantes aumentos en ventas y número de clientes que al 31 de diciembre de 1999 superaban el millón y medio.

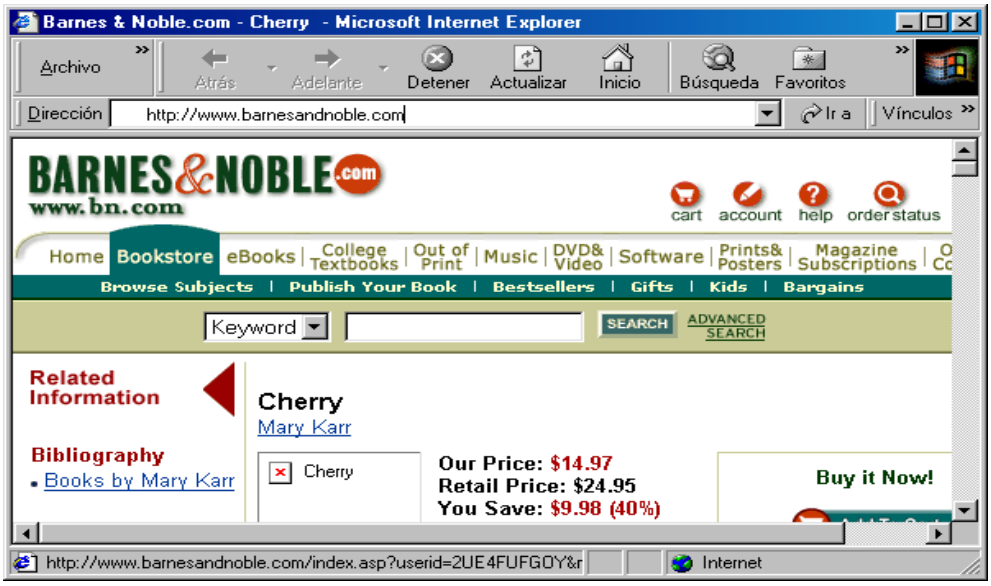
Según la empresa, en el cuarto trimestre de 1997 se alcanzó el nivel de ventas netas de 66 millones de dólares, un 74 % superior al del tercer trimestre y un 680 por ciento por encima del registrado durante el mismo período de 1996.

En 1997, las ventas de esta compañía, que afirma contar con más de 1,5 millones de clientes, ascendieron a 147,8 millones de dólares, un 838 % de crecimiento.

El éxito de esta fórmula interactiva de vender y comprar libros se basa en el cómodo y rápido acceso del comprador a los títulos publicados, el envío a domicilio en un plazo no superior a dos o tres días y la oferta de hasta un 40 % de descuento sobre el precio normal en la calle.

Superadas las cautelas iniciales sobre el rápido desarrollo de "Amazon.com", la primera cadena de venta de libros del mundo "Barnes & Noble" abrió su tienda en Internet en 1999 con el aval de 483 librerías convencionales repartidas por todo el país, su experiencia en el campo editorial y su solidez financiera.

"Barnes & Noble" firmó además un acuerdo con la compañía editora de "The New York Times" para ser el proveedor exclusivo de la página electrónica que dedica este prestigioso diario a los libros.

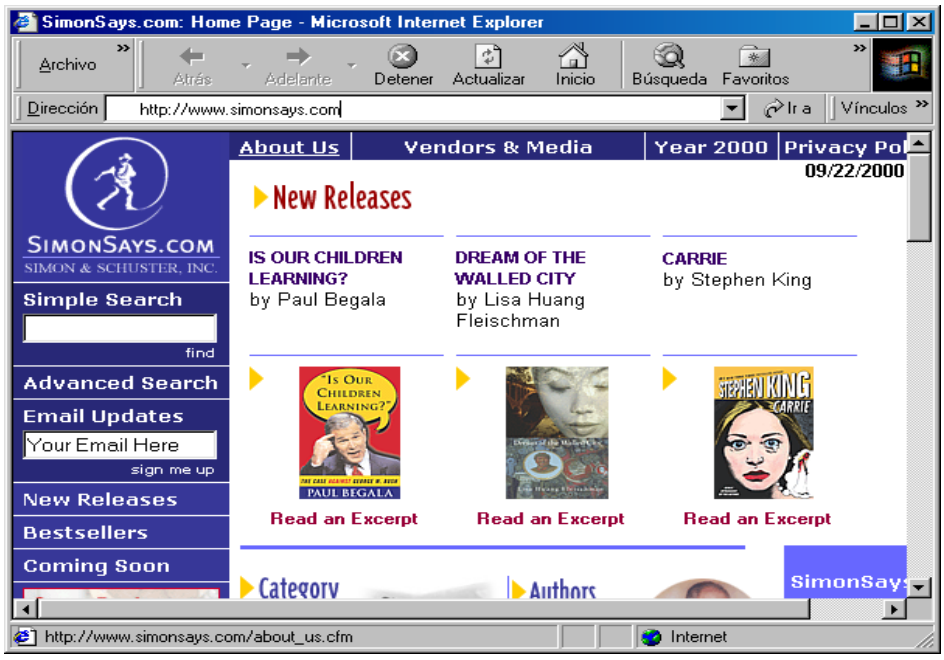


Una de sus características es que ofrece entre un 20 y un 30 % de descuento a sus clientes "on-line" por considerar que con esta forma de venta se ahorra importantes gastos de infraestructura, mercadeo y laborales.

"Barnes & Noble" informó de que su página en Internet había generado más de 8,2 millones de dólares de ventas en el último trimestre de 1999, y casi 15 millones de dólares durante su primer año de funcionamiento.

Sin embargo, estas cifras son todavía ridículas si las comparamos con la facturación total de la compañía que en 1997 se acercaron a los 2.800 millones de dólares, 400 millones más que lo registrado durante el año anterior de 1996.

"Simon & Schuster", otra de las principales compañías editoriales de este país especializada en libros educativos, ha creado también una "supertienda" en Internet y también la empresa "Borders", la segunda cadena nacional más importante.



Todas confían en que este nuevo sistema de ventas ayude a recuperar un mercado que en el último año registró un descenso de entre un 5 y un 7% en Estados Unidos.

El acceso a potenciales clientes en otros países, contar con valiosa información sobre las preferencias de los compradores y mantener viejos títulos al alcance del público en general son argumentos suficientes para probar fortuna en esta nueva aventura, argumentan algunos de los editores y librerías.

Los resultados que se alcancen en este mercado virtual a finales de 2000, que representan ahora unos 150 millones de dólares, indicarán la fuerza de los verdaderos competidores y la fidelidad de los lectores que, en definitiva, serán los grandes ganadores de esta nueva carrera por el negocio de venta de libros por la red. [i]

3.3 LIBRERIAS CONVENCIONALES VRS. LIBRERIAS VIRTUALES

Se analizó de una forma comparativa los aspectos principales para el funcionamiento de los dos tipos de librería y que es importante considerar al momento de decidir si es factible una librería virtual

Amazon.com es la compañía que ha establecido las tendencias porque ofrece grandes descuentos, posee un buen inventario, tiene un servicio de notificación, permite hacer compras con un solo clic y tiene un sentido de comunidad.

Caracterís-tica	**Librería convencional**	**Librería virtual Don Bosco**	**Conclusión**

Gastos de admón.	Incluye: renta de local, sueldo de empleados, papelería, pago de impuestos y servicios.	Incluye: sueldo de administrador, espacio en Internet, renta de local (bodega), comisión de entidad financiera.	Los gastos de administración son mayores en una librería convencional
Gastos de instalación	Acondicionamiento de local, legalización.	Certificado virtual, suscripciones, autorizaciones.	Para este caso los gastos disminuyen en la librería virtual ya que se ahorraría el costo de membresía y espacio en Internet.
Mobiliario y equipo	Estantes, vitrinas, caja registradora, calculadoras, sillas, escritorios, depósitos de paquetes.	Estantes, escritorio, sillas, computadora.	La UDB ya cuenta con equipo de cómputo necesario para la librería virtual, y además, para ésta el mobiliario a utilizar es menos.

Facilidad de acceso	Por la ubicación geográfica de la universidad, las compras son hechas en gran mayoría por estudiantes de la universidad.	Se facilita ya que puede accesar desde cualquier lugar, todos los días y a cualquier hora.	Es más accesible la librería virtual, ya que no hay restricciones de lugar ni de hora, lo que aumenta el número de clientes.
Preferencia del cliente	El cliente analiza mejor su compra, ya que conoce el producto que va a adquirir.	Puede tener aceptación entre los aficionados a Internet	La tendencia de los clientes se encamina hacia la compra por Internet, por lo que cada vez esta metodología de ventas está tomando más auge.
Administra-ción	Gestión de pedidos, control de inventarios, atención personal a clientes, procesos de facturación, orden e imagen del local.	Gestión de pedidos y envíos, control de stocks, verificación de datos de alumnos, impresión de reportes y búsquedas de pedidos en Internet.	En los comercios virtuales se orienta más el autoservicio, por lo que no es necesario personal para la atención del cliente, sólo para la administración del comercio en sí.

Publicidad	Se tendría que invertir en medios de publicidad para darse a conocer.	También se tienen que invertir en medios de publicidad para dar a conocer el sitio.	En ambos se utilizan los medios de publicidad. Para la librería virtual el medio de publicidad (Internet) sirve además como punto de ventas.
Hábitos de compra	Las personas lo consideran más confiable.	En nuestro medio la adquisición de bienes por medio de Internet no está muy difundido.	El incremento de comercio virtuales, aumentaría más la confiabilidad de los clientes.
Gastos de distribución y ventas.	No existen gastos de distribución solamente el empaque.	El valor se incrementa por el empaque y el costo de envío el cual varía según el lugar de donde se solicita.	Los clientes cuando hacen compras por Internet, son conocedores del valor agregado del producto.
Gastos por mantenimiento de inventario	Se tienen que comprar cierta cantidad de ejemplares para tener a disposición de clientes, por lo que se pueden deteriorar o volverse obsoletos.	No es necesario tener ejemplares en existencia para poder realizar ventas.	El mantener libros en existencia implica costos mayores.

Opciones de compra	Las alternativas de compra para el cliente son las que están en existencia.	Se cuenta con gran variedad de ejemplares aunque éstos no estén realmente en existencia.	Con el hecho de tener en la base una mayor cantidad de ejemplares, se puede alcanzar un mayor segmento de mercado.
Segmento de mercado.	Estudiantes y personal docente de las Universidades del área metropolitana.	Además de la anterior, profesionales, estudiantes y otros usuarios de la red.	El segmento de mercado para la venta en Internet es mucho mayor.
Precio de venta.	El precio de venta es fijo.	El precio del producto depende del lugar de origen y el tipo de envío que elija el cliente.	El valor que el cliente paga por el producto en su lugar de origen, siempre sufre un recargo por envío.
Activos Intangibles.	No tiene activos intangibles.	Incluye el desarrollo del sistema y licencias de software.	En este caso no sería un gasto ya que la UDB contaría con dicho sistema.

Caso comparativo

Barnes & Noble versus Amazon.Com. El caso de una cadena de librerías versus una librería en línea .

El negocio de librerías estaba claramente dominado por las cadenas de librerías. En cualquier centro comercial del pueblo más pequeño de los Estados

Unidos hay una tienda de Barnes & Noble, de Waldenbook o de alguna otra cadena. Amazon.Com apareció en Internet y produjo un impacto enorme con servicios en línea y precios inferiores basados en inventarios prácticamente nulos. Barnes & Noble acusó el golpe y aprendió la tecnología. Sin embargo, sus enormes inventarios y espacios de exhibición le producían costos enormes.[ii]

3.4 REQUERIMIENTOS BÁSICOS DEL SISTEMA

La mayoría de las librerías en Internet poseen procedimientos comunes tales como:

- Un registro de clientes para un mejor control de estos.
- Búsqueda de libros de acuerdo a diferentes criterios así como por título, por autor, si es una novedad etc.
- Ayuda acerca del manejo del sitio.
- Escoger los libros a comprar y guardarlos en una bolsa o carrito de compras virtual, pudiendo después modificar lo elegido.
- El pago se realiza por medio de tarjetas de crédito y es en este momento cuando se recolecta la información necesario para hacer llegar el libro a su destino.

Además de esto, se supone que debe haber una manera de administrar el sitio virtual, la forma más fácil de realizar esta tarea es por medio de un sistema que realice la tarea de mantenimiento de la base de datos tales como: adición, modificación, eliminación, consulta, reportes etc.

3.5 CONDICIONES NECESARIAS PARA EL FUNCIONAMIENTO DE LA LIBRERÍA EN INTERNET.

Aspectos técnicos del Hospedaje en Internet.

Se necesita tomar dos decisiones de gran importancia para tener presencia en Internet.

1. Primero, se deberá seleccionar y tramitar su propio nombre de dominio (www.suempresa.com) para este caso se sugiere: www.libudb.edu.sv
2. Segundo, se deberá seleccionar una empresa proveedora de hospedaje para las páginas web u hospedarla en los propios servidores de la Universidad Don Bosco. De estos dos aspectos técnicos depende en gran medida el éxito comercial de la librería.

Certificado Digital.

Los negocios que aceptan transacciones vía Internet pueden alcanzar una gran competitividad a nivel mundial a muy bajo costo. Los clientes enviaran información a través del web de números de tarjetas de crédito, datos financieros, o historial médico, *sólo si estos viajan seguros*.

VeriSign, Inc., es un proveedor de servicios de Comercio Electrónico y comunicaciones, ofrece un bajo costo, y provee una solución segura orientada a los negocios en el Web. Inmediatamente después de instalar el VeriSign Server Id, se puede establecer una comunicación segura con cualquier cliente usando el Netscape o Microsoft como navegador personal.

Credenciales en Internet por medio de Verisign Server ID

Un Server ID, también conocido como un Certificado Digital, es el equivalente electrónico de una licencia de negocios. El Server ID es también llamado “Certification Authority” (CA) o simplemente Certificado Digital.

Asegurando las transacciones en línea sin necesidad de hardware

Verisign Server Ids trabaja en conjunto con tecnología Secure Sockets Layer (SSL), el cual es en la industria el protocolo estándar de seguridad para las comunicaciones basadas en el Web.

Después de instalar el Verisign Server ID, el servidor automáticamente activa el SSL, creando un canal seguro entre el servidor y el cliente que está en el browser. El sitio puede comunicarse seguramente con cualquier cliente que use el Netscape Navigator, Microsoft Internet Explorer, ó los más populares programas para enviar emails. El SSL inmediatamente comienza a proveer los componentes de seguridad para las transacciones en línea:

- *Autenticación:* Los clientes pueden verificar que el Web Site le pertenece a quién dice ser y no a un impostor.
- *Mensajes Privados:* SSL encripta toda información enviada entre el Web Server y los clientes, tales como números de tarjeta y otros datos personales usando una llave de sesión única.
- *Integridad en los mensajes:* Cuando un mensaje es enviado, cada computadora genera un código basado en el contenido del mensaje. Si un simple carácter del mensaje es alterado en el envío, la computadora que recibe generará una alerta de que el mensaje que recibió no es legítimo.

Tipos de Secure Server IDs

40-bit SSL Secure Server IDs.

Esta versión es utilizada por más del 50% de usuarios de Internet. 40-bit SSL es fuerte para las Intranets y para los Web Sites con un volumen bajo de usuarios. Esta ha sido denominada la versión-doméstica. 128-bit SSL encriptación nunca ha sido quebrado: según los Laboratorios RSA, se tomarían un trillón de años en desencriptarlo utilizando la tecnología de hoy en día.

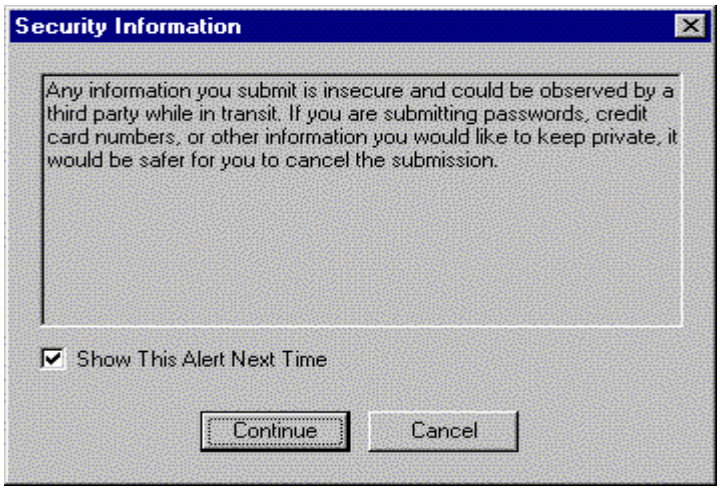
128-bit Global Server IDs.

La encriptación de 128-bit SSL Global Server IDs hace de los sitios el lugar ideal para el intercambio de información tal como: información personal, números

de tarjeta de crédito, con los clientes. Verisign es el único proveedor autorizado por el departamento del Los Estados Unidos en vender el 128-bit SSL IDs en Los Estados Unidos.

¿Cómo saber que un sitio es seguro?

Netscape Navigator y Microsoft Internet Explorer tienen desarrollados sus propios mecanismos de seguridad para prevenir al usuario cuando este intenta enviar información, si el canal es inseguro (un sitio sin Server ID o CA), el navegador muestra un mensaje de precaución, en donde se advierte al cliente que el canal es inseguro y si desea continuar de todas formas, para esto se le muestra la siguiente pantalla:



Los visitantes o clientes pueden asegurarse de que están en un sitio seguro siguiendo las siguientes pistas:

- La dirección (URL) en el navegador aparece “https” en el comienzo, en lugar de http.
- En los navegadores Netscape Communicator e Internet Explorer aparece en la esquina inferior izquierda un icono de un candado, si el candado está abierto significa que no existe ningún tipo de encriptación, si el candado está cerrado significa que existe seguridad ya sea de 40-bit o 128-bit.

Para saber que tipo de encriptación se está utilizando solo basta ubicar el puntero del ratón encima del candado y este mostrará el tipo de encriptación utilizado.[iii]

Afiliación a una entidad financiera.

En El Salvador las dos entidades financieras de tarjetas de crédito con mayor mercado son: MasterCard representadas por Credomatic de El Salvador y VISA representadas por Aval Card S.A. Actualmente, solo Aval Card ofrece el servicio de verificación de tarjeta en línea en nuestro país.

Para las ventas por Internet utilizando tarjeta de crédito es necesario que el negocio esté afiliado a una entidad financiera que brinde el servicio de verificación en línea. Para esto es necesario llenar un Contrato de Afiliación y Addendum de Contrato de Afiliación, además de presentar cierta documentación adicional que es común para ambas y que se define de la siguiente manera:

Documentos requeridos para una persona jurídica:
Fotocopia de:

- Escritura de constitución de la sociedad y su respectivo registro.
- Acta de nombramiento del Representante legal.
- Cédula del representante legal.
- NIT del representante legal.
- NIT de la empresa.
- Tarjeta del registro fiscal.
- Factura de Comprobante de Crédito Fiscal.

Documentos requeridos para una persona natural:

Fotocopia de:

- Cédula del propietario.
- NIT del propietario.
- Tarjeta de Registro Fiscal.
- Documento de Autorización de Vigilancia para la Práctica Profesional (Solo profesionales).
- Matrícula de Comerciante individual.
- Factura de Comprobante de Crédito Fiscal.

[i] Diario del Navegante, Internet Informática y nuevos medios
http://w3.el-mundo.es/navegante/diario/index.html

[ii] www.iesa.edu.ve/catedrati/gerencidigital/casos/index.html

[iii] Esta información se obtuvo del sito oficial de Verign http://www.verisign.com/

4. DESARROLLO DEL SISTEMA

4.1 Descripción de los Procesos del Sistema

Registro de Usuarios

Los clientes pueden registrarse al entrar al sitio web si lo desean, aunque no es necesario, si no hasta la hora de realizar compras, ya que al indicar que desea comprar si no está registrado lo deberá hacer. Después que ya se ha registrado y accese al sitio nuevamente puede entrar con su login y password, el registro se realiza solamente una vez. Inmediatamente el usuario queda habilitado para realizar compras.

Búsqueda en Catálogo.

Se proporciona a los clientes la posibilidad de revisar todos los ejemplares que se encuentra a disposición por medio de un listado o catálogo de libros. El cliente selecciona los que desea comprar agregándolos a la canasta de compras.

Búsqueda por categorías.

Se ofrece la opción de buscar libros de acuerdo a diferentes categorías (título, autor, área, ISBN), lo que facilita en gran manera saber si los ejemplares se encuentran a disposición. Pudiendo el cliente seleccionar los que desee comprar agregándolos a la canasta de compras.

Compra

Para cualquiera de las tres formas de pago, es necesario que los clientes proporcionen cierta información necesaria para la compra y entrega del libro; y existe información específica para cada una de las tres formas de pago, la cual se solicitará en formularios diferentes.

Revisar canasta de compras.

Por medio de esta opción se ofrece la posibilidad a los clientes de revisar los artículos que han seleccionado para su compra posterior; pudiendo quitarlos de la lista, cambiar las cantidades de éstos, etc.

4.2 ESQUEMAS DE PROCESOS Y ENTIDADES RELACIONADAS EN LAS VENTAS

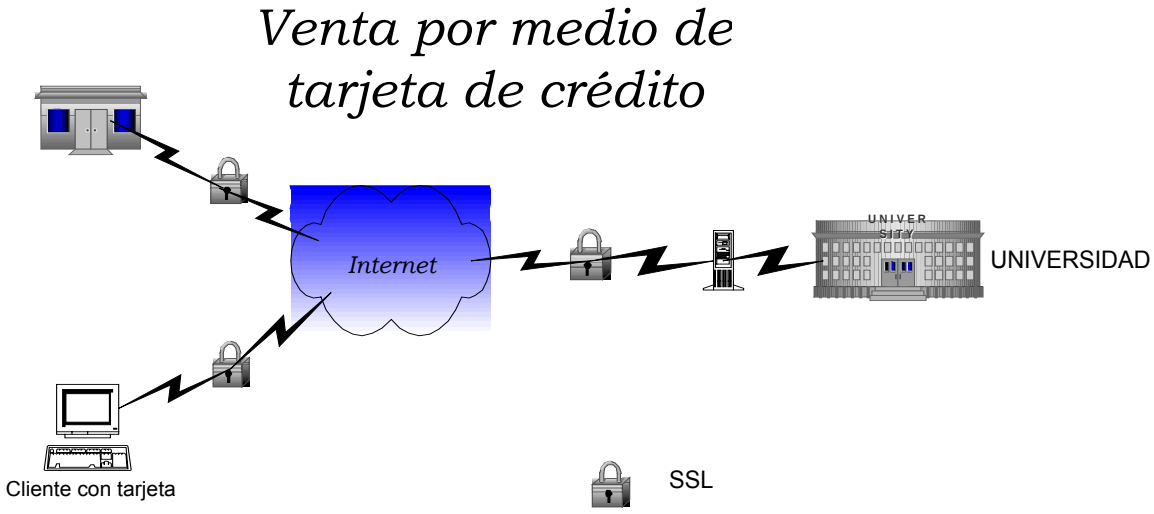


Figura 4.2.1

En la figura 4.2.1 se muestra la forma en que la entidad financiera, el cliente y el comercio, todos tendrán que enviar sus datos por medio del protocolo SSL, el cual será transparente a la hora de la transacción.

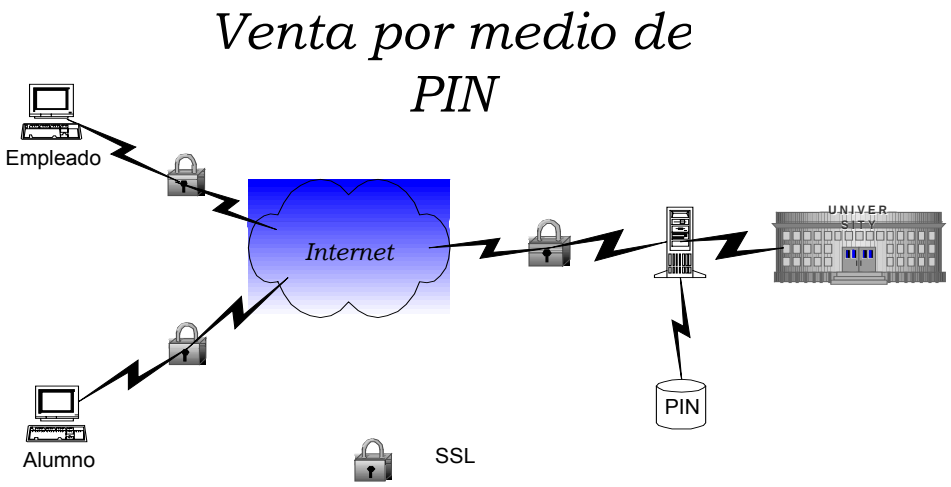


Figura 4.2.2

En la figura 4.2.2 además de utilizar el protocolo SSL para el transporte de datos, se valida al usuario en una base de datos proporcionada por la Universidad Don Bosco.

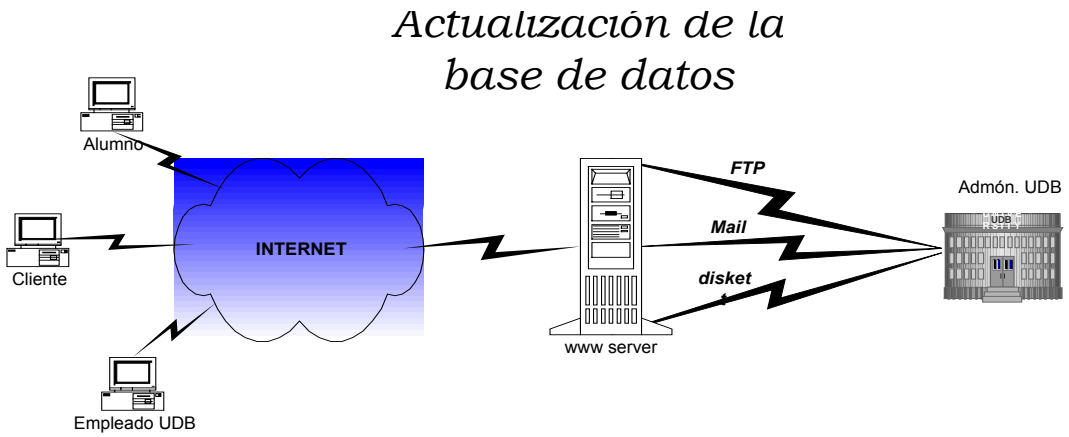


Figura 4.2.3

En la figura 4.2.3, se muestra las diferentes formas en que la Universidad Don Bosco puede actualizar la base de datos del PIN, ya sea esta por medio magnético o vía FTP.

5.3 Descripción de tablas y Diagrama Entidad Relación (E-R)

Descripción de tablas

Tabla Area

Campo	Tipo	Null	Key	Default	Descripción
idarea	int(11)		PRI	0	Identificador de Area
nombrearea	char(50)	YES		NULL	Nombre de Area

Tabla Autor

Campo	Tipo	Null	Key	Default	Descripción
idautor	int(11)		PRI	0	Identificador de autor
nombres	char(50)	YES		NULL	Nombres del autor
apellidos	char(50)	YES		NULL	Apellidos del autor
nombreautor	char(100)	YES		NULL	Nombre completo del autor

Tabla detallefactura

Campo	Tipo	Null	Key	Default	Descripción
idfactura	int(11)		PRI	0	Identificador de factura
idlibro	int(11)		PRI	0	Identificador de libro
cantidad	int(11)	YES		NULL	Cantidad
precio	float(10,2)	YES		NULL	Precio
login	char(10)		PRI		Login
ip	char(15)		PRI		Dirección IP
fechatran	date	YES		NULL	Fecha transacción

Tabla Editorial

Campo	Tipo	Null	Key	Default	Descripción
ideditorial	int(11)		PRI	0	Identificador de editorial
editorial	char(50)	YES		NULL	Editorial

Tabla Factura

Campo	Tipo	Null	Key	Default	Descripción
idfactura	int(11)		PRI	0	Identificador de factura
login	char(10)	YES		NULL	Login
idformapago	int(11)	YES		NULL	Identificador de forma pago
descripcion	char(50)	YES		NULL	Descripción
pnombre	char(25)	YES		NULL	Primer Nombre
snombre	char(25)	YES		NULL	Segundo Nombre

papellido	char(25)	YES		NULL	Primer Apellido
sapellido	char(25)	YES		NULL	Segundo Apellido
apecasada	char(25)	YES		NULL	Apellido de Casada
codpostal	char(25)	YES		NULL	Código Postal
idpais	int(11)	YES		NULL	Identificador de país
estado	char(25)	YES		NULL	Estado
ciudad	char(25)	YES		NULL	Ciudad
direccion	char(50)	YES		NULL	Dirección
fechafactura	date	YES		NULL	Fecha de la factura
carnetidemp	int(11)	YES		NULL	Carnet o ID del empleado

Tabla FormaPago

Campo	Tipo	Null	Key	Default	Descripción
idformapago	int(11)		PRI	0	Identificador forma pago
formapago	char(50)	YES		NULL	Forma de pago

Tabla Libro

Campo	Tipo	Null	Key	Default	Descripción
idlibro	int(11)		PRI	0	Identificador de libro
idautor	int(11)			0	Identificador de autor
ideditorial	int(11)			0	Identificador de editorial
idarea	int(11)			0	Identificador de area
isbn	int(11)	YES		NULL	Número ISBN
titulo	char(100)	YES		NULL	Título del libro
descripcion	char(200)	YES		NULL	Descripción
image	char(60)	YES		NULL	Imagen
peso	float(10,2)	YES		NULL	Peso
preciocosto	float(10,2)	YES		NULL	Precio de costo
precioventa	float(10,2)	YES		NULL	Precio de venta
nivelmax	int(11)	YES		NULL	Nivel máximo
nivelmin	int(11)	YES		NULL	Nivel mínimo
existencia	int(11)	YES		NULL	Existencia
fecha	date	YES		NULL	Fecha de introducción

Tabla Login

Campo	Tipo	Null	Key	Default	Descripción
login	varchar(10)		PRI		Login
pnombre	varchar(25)				Primer nombre
papellido	varchar(25)				Primer apellido
email	varchar(25)	YES		NULL	Correo electrónico
fechaingreso	date	YES		NULL	Fecha de ingreso
ip	varchar(15)	YES		NULL	Dirección IP

idpais	int(11)	YES		NULL	Identificador de pais
ciudad	varchar(25)	YES		NULL	Ciudad
direccion	varchar(50)	YES		NULL	Dirección

Tabla Mails

Campo	Tipo	Null	Key	Default	Descripción
nombre	varchar(25)	YES		NULL	Nombre
mail	varchar(25)	YES		NULL	Correo electrónico
comentario	varchar(200)	YES		NULL	Comentario

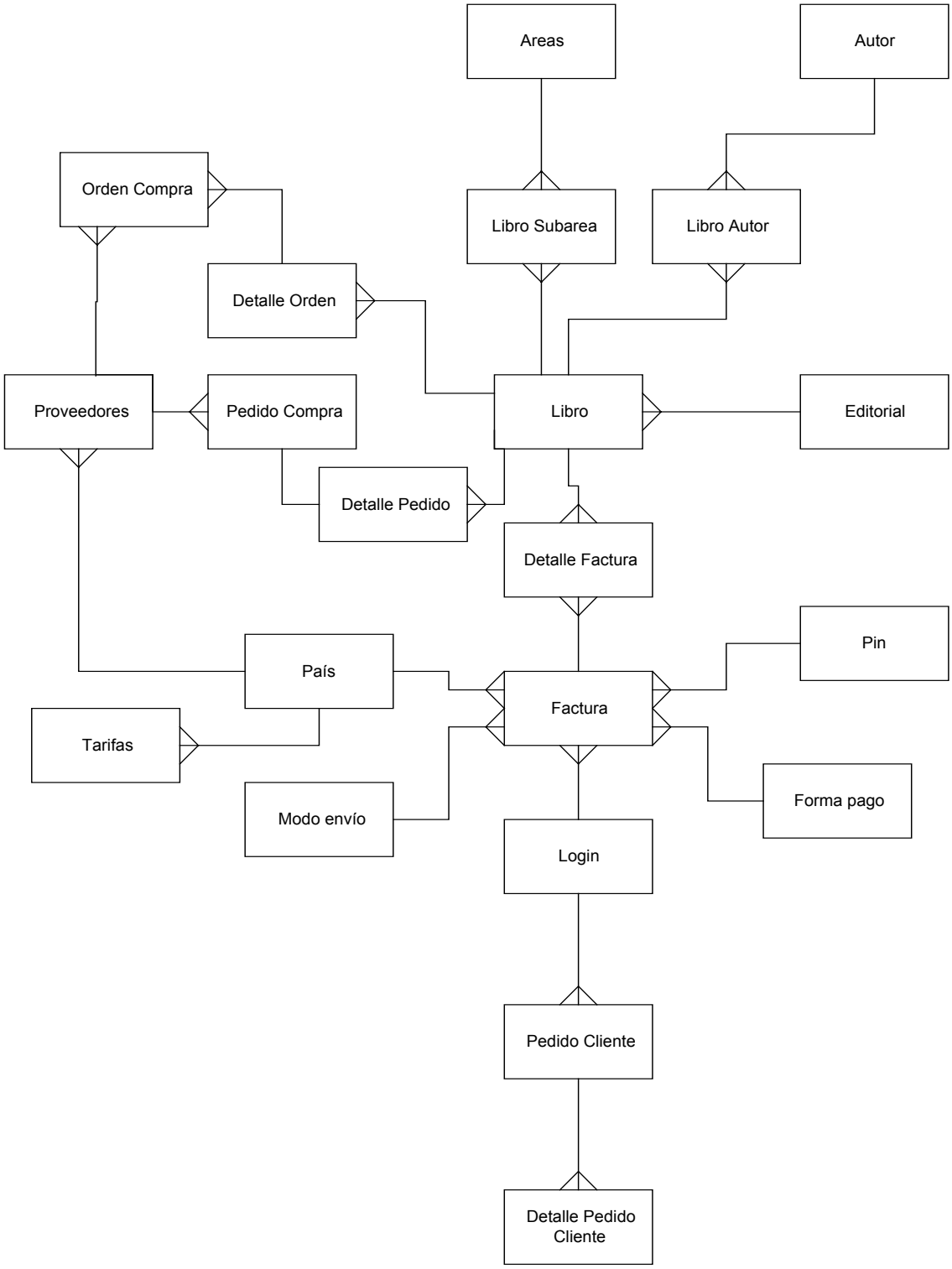
Tabla pais

Campo	Tipo	Null	Key	Default	Descripción
idpais	int(11)		PRI	0	Identificador de país
pais	char(50)	YES		NULL	Nombre de país

Tabla Proveedor

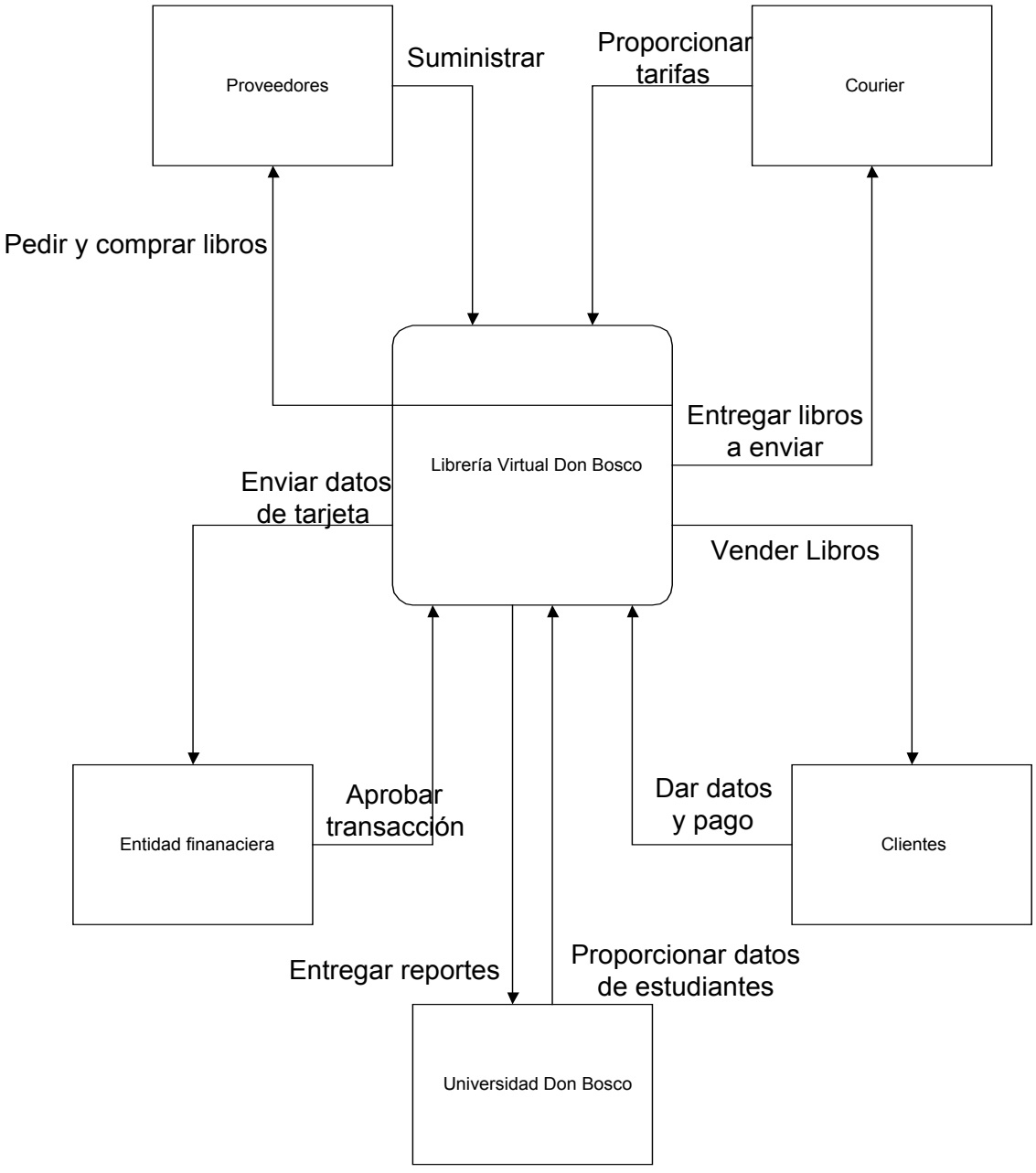
Campo	Tipo	Null	Key	Default	Descripción
idproveedor	int(11)		PRI	0	Identificador de proveedor
proveedor	char(50)	YES		NULL	Proveedor
contacto	char(50)	YES		NULL	Contacto
cargo	char(25)	YES		NULL	Cargo del contacto
idpais	int(11)	YES		NULL	Identificador de país
ciudad	char(50)	YES		NULL	Ciudad
direccion	char(50)	YES		NULL	Dirección
codpostal	char(25)	YES		NULL	Código Postal
telefono	char(15)	YES		NULL	Teléfono
fax	char(15)	YES		NULL	Fax
email	char(50)	YES		NULL	Correo electrónico

Diagrama Entidad Relación

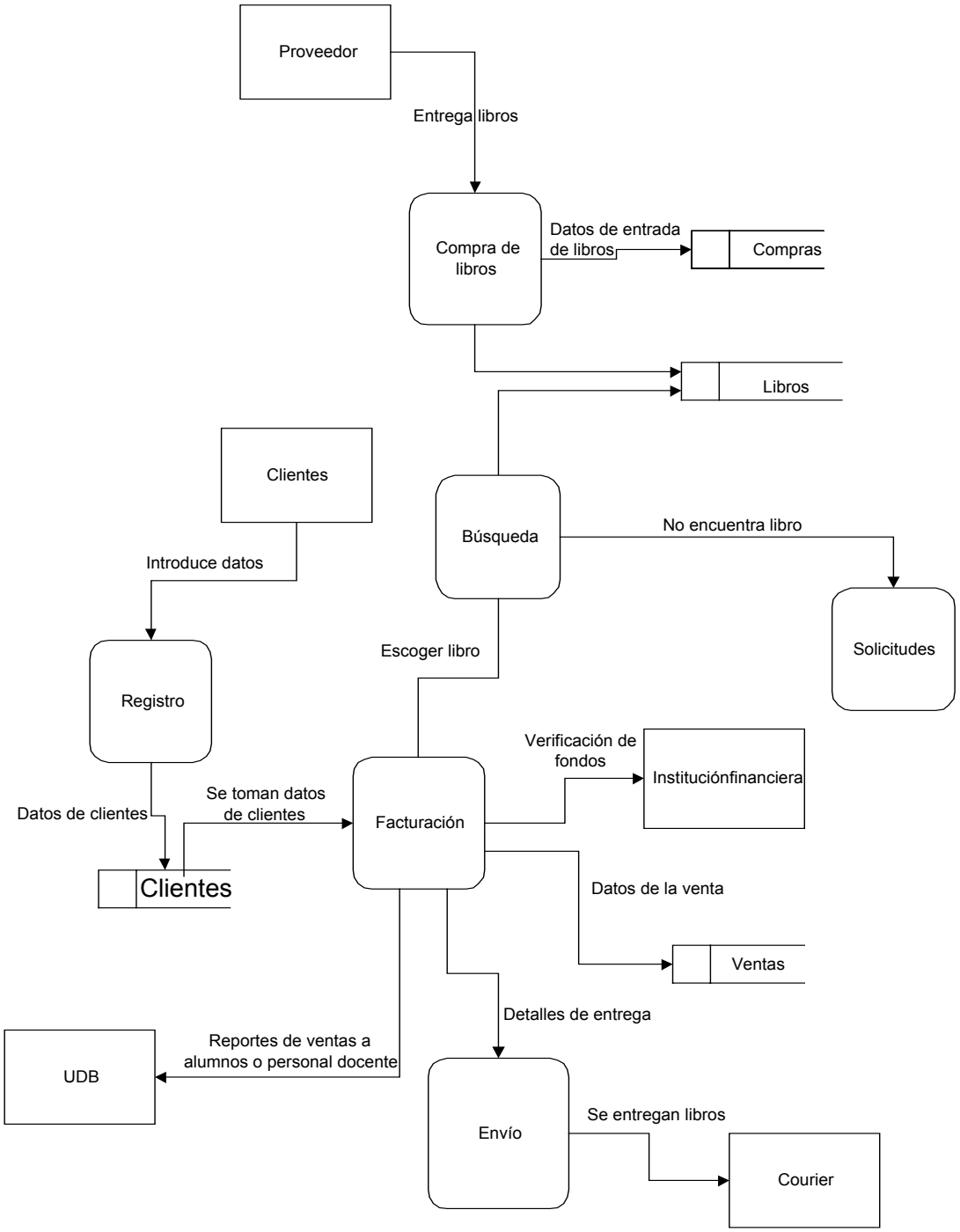


4.4 Diagramas de Flujos de Datos (DFD).

DFD Nivel 0

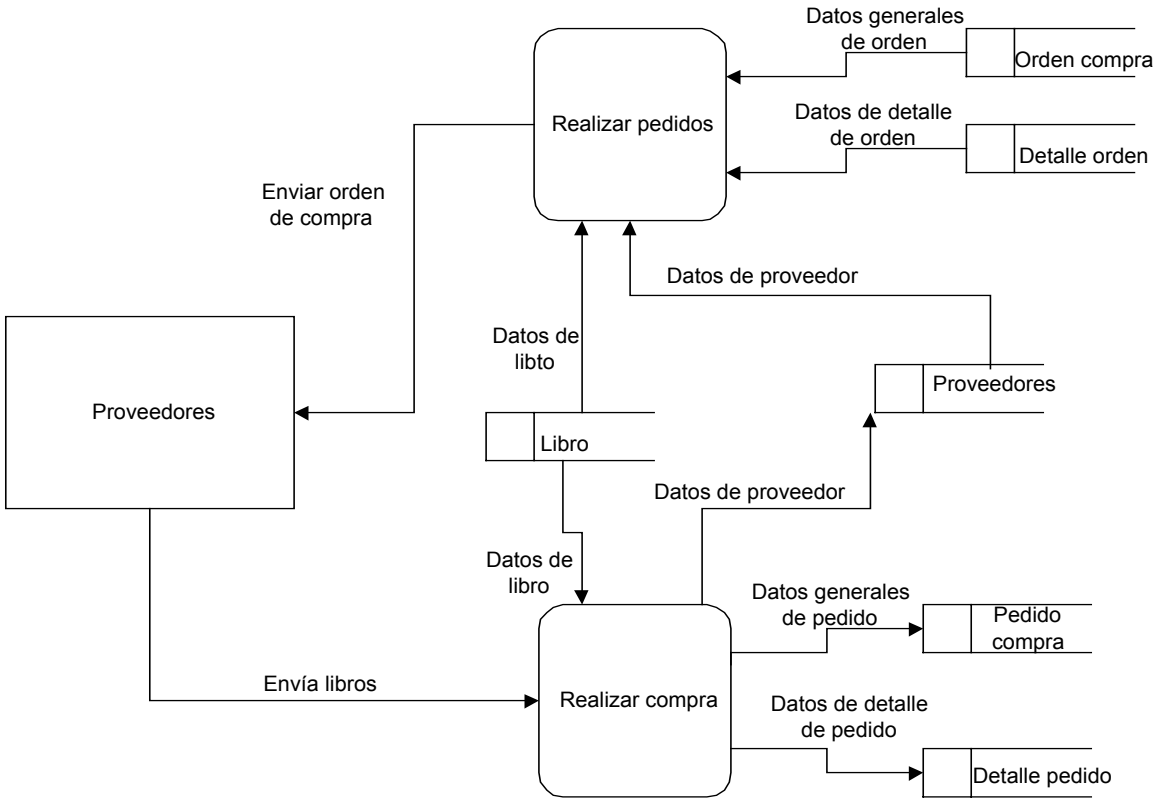


DFD Nivel 1

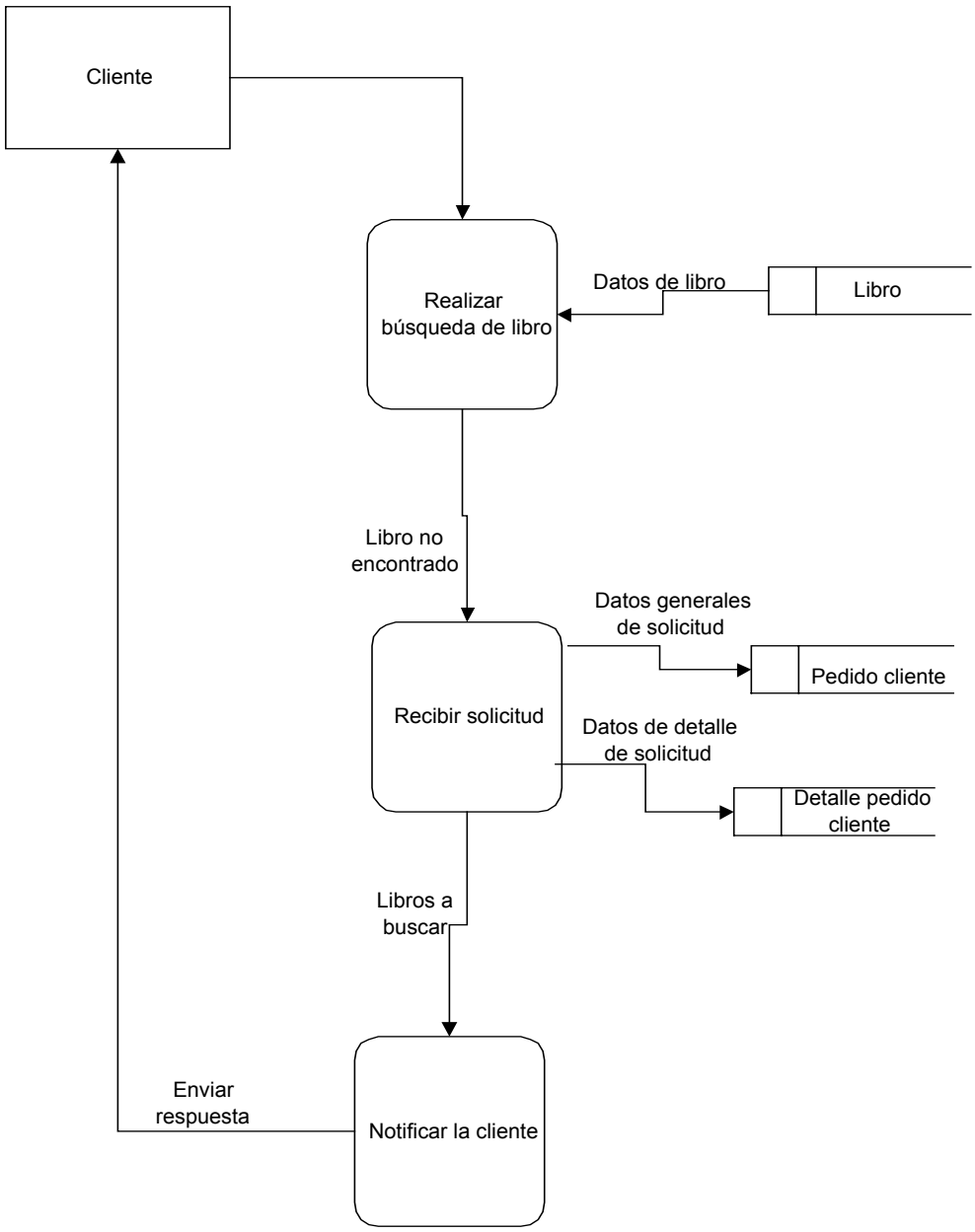

Proveedor
Entrega libros
Compra de libros
Datos de entrada de libros
Compras
Libros
Clientes
Búsqueda
No encuentra libro
Introduce datos
Solicitudes
Escoger libro
Registro
Verificación de fondos
Institucióñfinanciera
Se toman datos de clientes
Datos de clientes
Facturación
Clientes
Datos de la venta
Ventas
Detalles de entrega
Reportes de ventas a alumnos o personal docente
UDB
Envío
Se entregan libros
Courier

DFD Nivel 2

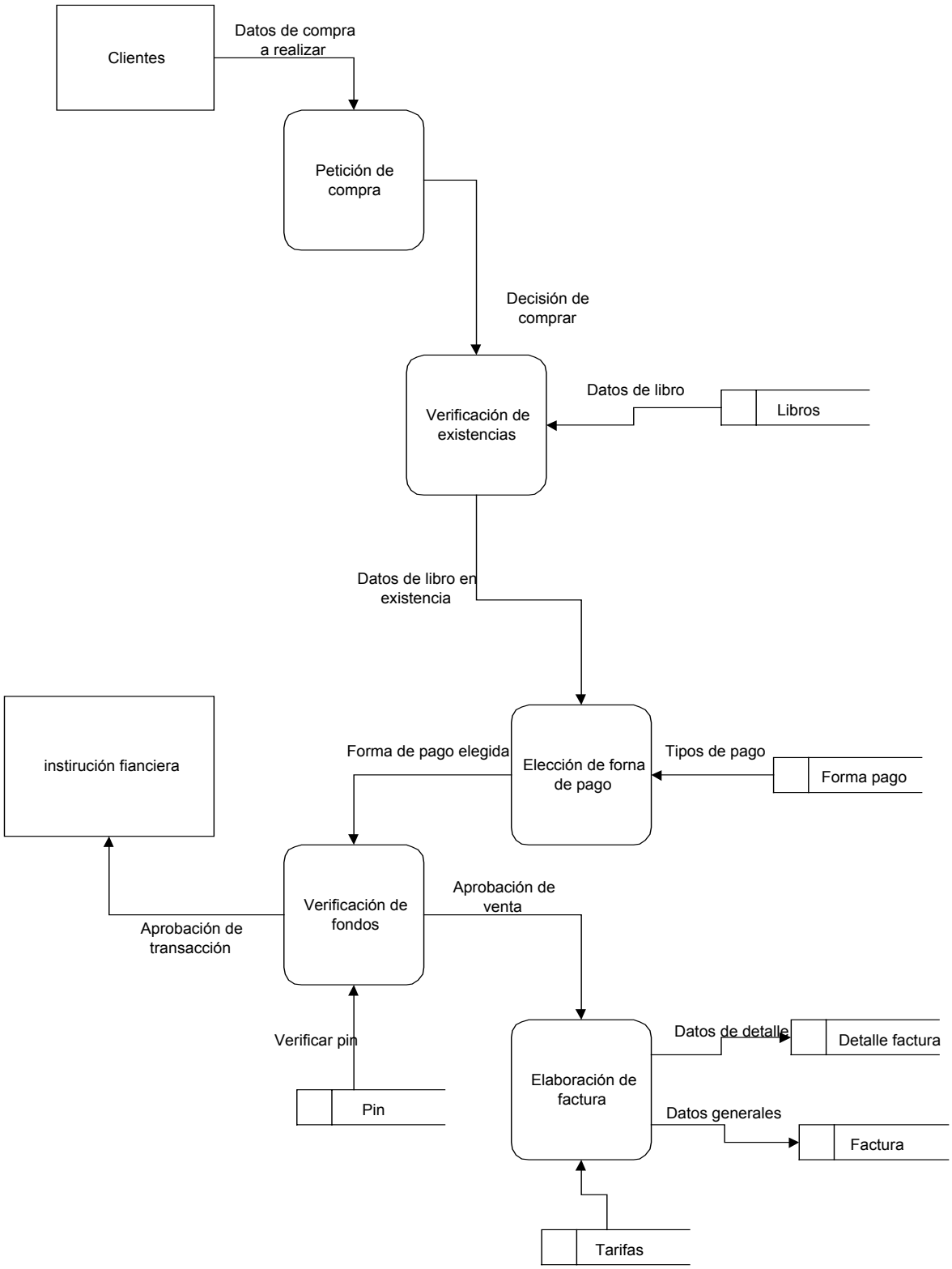
Compras



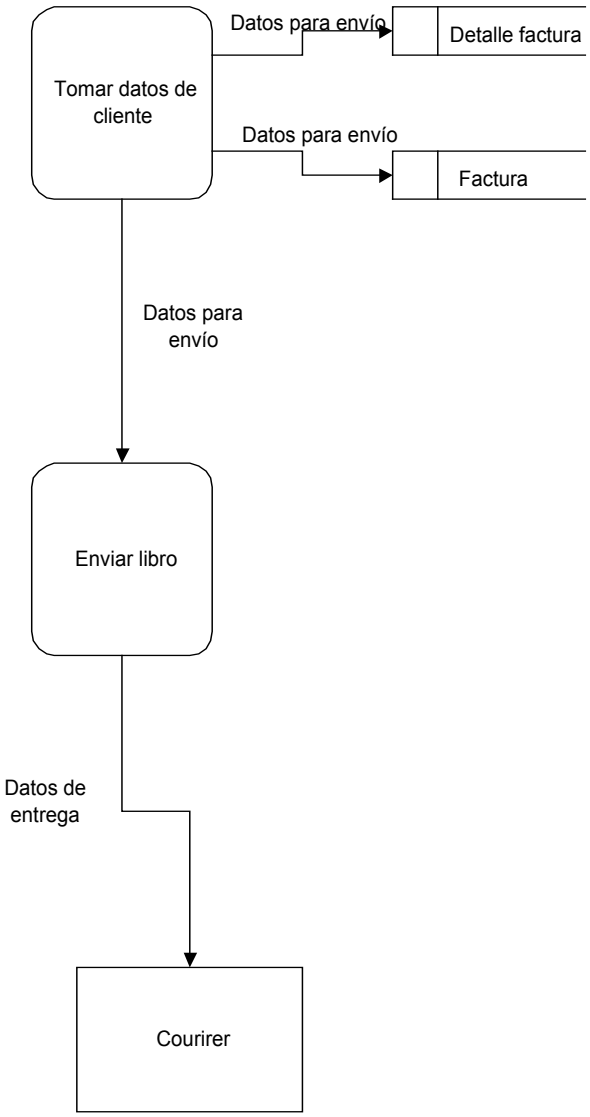
DFD Búsqueda



DFD Venta


Clientes
Datos de compra a realizar
Petición de compra
Decisión de comprar
Verificación de existencias
Datos de libro
Libros
Datos de libro en existencia
instirución fianciera
Forma de pago elegida
Elección de forna de pago
Tipos de pago
Forma pago
Verificación de fondos
Aprobación de venta
Aprobación de transacción
Verificar pin
Pin
Elaboración de factura
Datos de detalle
Detalle factura
Datos generales
Factura
Tarifas

DFD Envío


Tomar datos de cliente
Datos para envío
Detalle factura
Datos para envío
Factura
Datos para envío
Enviar libro
Datos de entrega
Courirer

Descripción de diagramas de flujo de nivel 2

DFD de Compras

Se realiza el pedido al proveedor, se obtienen los datos de este del almacén de proveedores, de Detalle Orden y Orden Compra se obtiene los datos del pedido, y de Libros la información de los libros a pedir. Luego se realiza la compra, en Pedido Compra y Detalle Pedido, se guardan los datos de la compra.

DFD Búsqueda

El cliente realiza la búsqueda de libros, de acuerdo al criterio que desea, en base a la información de la tabla de Libros. Si el libro no fue encontrado el cliente puede realizar una solicitud los datos se guardan en Pedido Cliente y Detalle Pedido Cliente, luego se notifica al cliente si el libro solicitado fue encontrado.

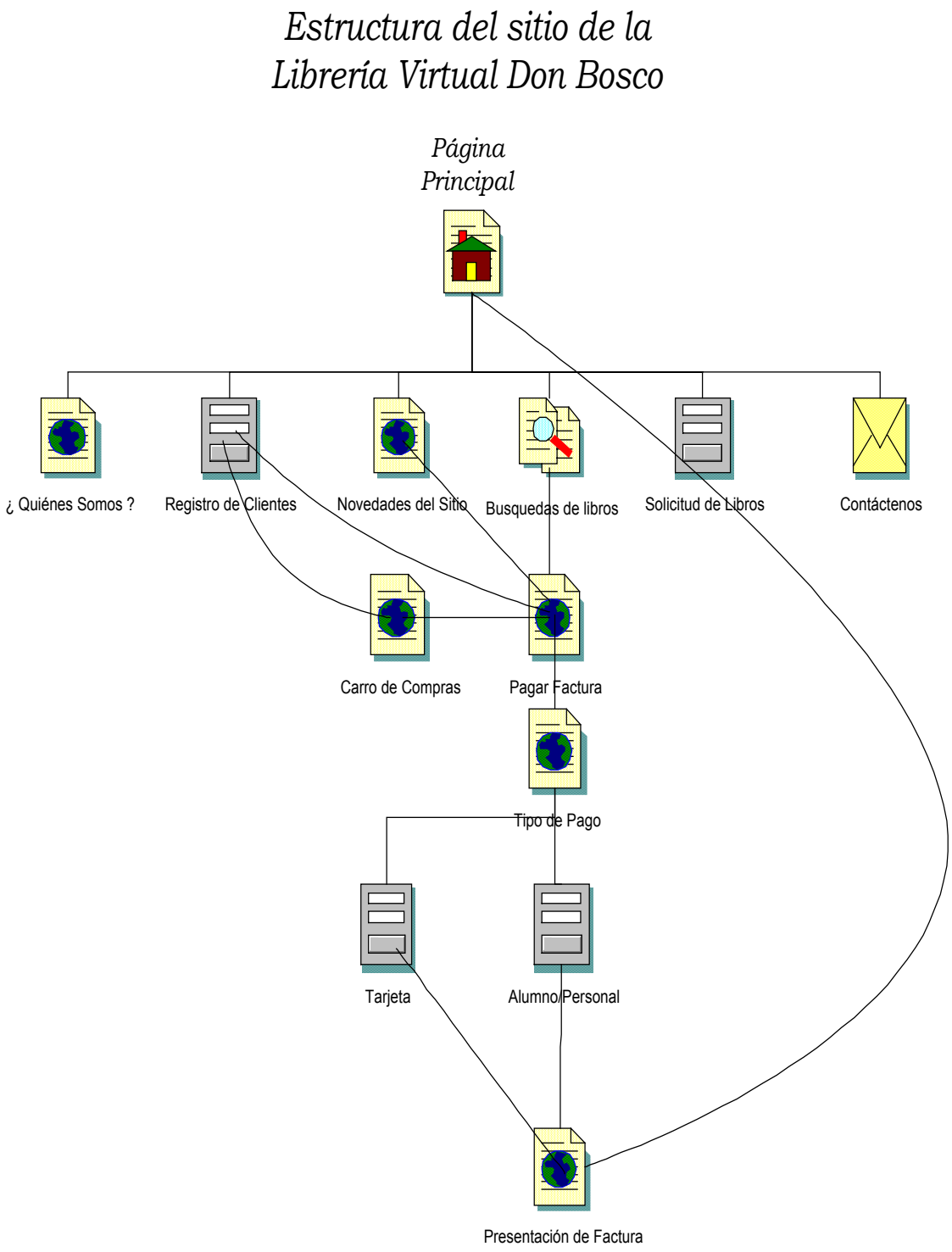
DFD Venta

El cliente indica que desea comprar, se realiza una verificación de existencias, luego el cliente debe escoger la forma de pago que utilizará, luego se realiza una verificación de los fondos del cliente, luego se elabora la factura, cuyos datos se guardan en Detalle Factura y Factura

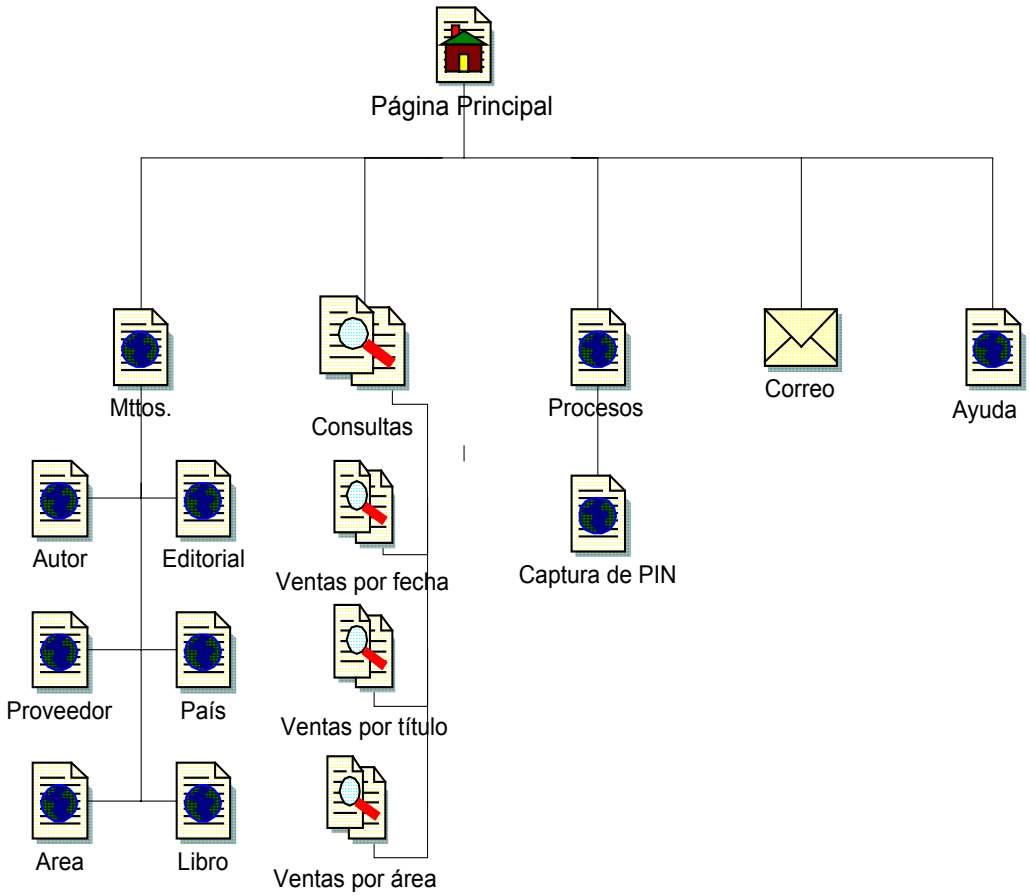
DFD Envío

Se toman los datos del cliente y se guardan en Detalle Factura y Factura, luego se envía el libro por medio del courier.

4.5 Diseño del sitio WEB.



Estructura del sitio de administración de la Librería Virtual Don Bosco



4.6 INTEGRACIÒN DE COMPONENTES

Este apartado pretende explicar de una manera sencilla los pasos que se siguieron para la integración de los componentes necesarios para la publicación de una base de datos en el web.

Ahora que se conoce acerca de WWW, de cómo funciona la tecnología CGI para acceder a una base de datos, crear una base de datos y elegir una interfaz apropiada; se llega a la interrogante de ¿qué se debe hacer para integrar todos esos elementos y posibilitar la publicación de la base de datos?.

Unix es el sistema operativo (SO) tradicional para Internet, y con la invención de clones Unix de dominio público, como Linux y FreeBSD, ha puesto el poder de Unix como un servidor de Web y base de datos, a la disposición de cualquiera que tenga una conexión con Internet.

Además, este capítulo se centra en mostrar cómo poner una base de datos en el Web del modo más económico posible, es decir, utilizando productos de freeware o shareware que satisfagan la mayor parte de las necesidades. También pretende dar una idea de los tipos de problemas y dificultades que pueden surgir cuando se utilizan productos que cuentan con poco o nulo soporte técnico.

En este caso se cubre los siguientes aspectos:

- Requerimientos técnicos.
- Configuración de software necesario.

Si se planea utilizar una costosa máquina Unix y una base de datos comercial se puede aplicar gran parte de este proyecto. Se podrán usar todos los productos utilizados en este caso en muchas versiones comerciales de Unix

(Linux), y los principios básicos de la conexión de una base de datos a Web son aplicables, independientemente del tipo de equipo y software que se use.

Un aspecto a considerar cuando se utiliza software de dominio público es el cambio constante de los números de versión. Dado que este tipo de software no está sujeto a rígidos estándares de prueba característicos del software comercial, literalmente, aparecen versiones nuevas con relativa rapidez. Esta es una buena manera de agregar nuevas características y de arreglar imperfecciones en las versiones anteriores, pero estar en la cúspide del avance tecnológico tiene su precio.

4.6.1 Requerimientos técnicos.

La computadora utilizada para el desarrollo de este proyecto es un Clon con procesador Celerón/333 mhz con 32 megabytes de memoria RAM. La Celerón/333 es relativamente lenta si la comparamos con las nuevas máquinas Pentium del mercado. Con un sistema operativo Linux, la Celerón opera sorprendentemente rápido y maneja con facilidad las cargas moderadas de procesamiento.

El sistema operativo Linux se instala en un disco duro de 8 GB. y puede arrancarse en formal dual con Window 98. Esto significa que la computadora puede arrancarse en forma dual con Windows 98 o Linux, dependiendo de que sistema operativo se seleccione al encender la computadora. Si se planea correr el servidor sólo una parte del tiempo, y utilizar otro sistema operativo para otras tareas, Linux puede coexistir con los sistemas operativos más populares. Sólo es de asegurarse de que se dispone de suficiente espacio en el disco para admitir varios sistemas y sus aplicaciones asociadas.

4.6.2 Configuración de módulos.

Para desarrollar este proyecto son necesarios varios paquetes de software. El software debe de instalarse y configurarse para que todas las piezas funcionen conjuntamente. El software requerido se enlista a continuación:

- Sistema operativo Linux
- Servidor de Web Apache+Mod_ssl+openssl
- Servidor de base de datos MySql
- Lenguaje Perl y Módulos DBI

 Instalación y configuración del Sistema operativo Linux

La mayoría de las distribuciones ofrecen la posibilidad de instalar o no XWindows, siendo posible, entonces y en caso de tener una PC poco potente, prescindir de todo lo relacionado con la GUI (esto excluirá el uso de aplicaciones como WordPerfect 8 o StarOffice 5.1). Este tipo de instalaciones se pueden hacer en discos duros pequeños (400 o menos MB). Para este proyecto se escogió instalar la distribución de SuSe Linux 6.3. Una distribución consiste en el Kernel, bibliotecas y programas.

Principales pasos a seguir a la hora de instalar Linux en un equipo:

- Es necesario hacer una lista completa y detallada de todos los dispositivos presentes en el equipo incluyendo marca, modelo y especificaciones (la cantidad de memoria de vídeo es imprescindible). Para esto, se debe consultar el manual del equipo.

- Obtener la distribución por medio de un sitio ftp, revistas etc. Para este caso se obtuvo por medio de la organización Linux de El Salvador. www.linux.org.sv

- Se escogió el método de instalación por medio de cdrom, luego se utilizó el espacio libre del disco duro ya que este puede coexistir con otro sistema operativo y se realizaron las dos particiones principales para linux: la / raiz y la swap.

- Se selecciona el tipo de instalación para servidor web, y luego se seleccionan los paquetes necesarios.

- Después de la instalación se configura lo siguiente:
  - ✓ Configurar ratón, teclado, tarjeta de red y módem.
  - ✓ Configurar el servidor Xfree86 (modo gráfico).
  - ✓ Configurar red (dirección ip, DNS) e impresor.
  - ✓ Configurar LILO, (para que cargue en modo dual windows 98 ó Linux)

- Luego se seleccionan los servicios que se desean que se inicien automáticamente, y por último se reinicia la computadora.

- Se inicia el modo gráfico con el comando startx.

Servidor de Web Apache+Mod-ssl+Openssl.

Apache es el programa servidor HTTP que se utiliza en este proyecto. Gracias a él se puede practicar la creación y publicación de documentos HTML de la misma forma que se hace en Internet con una estabilidad y eficacia ampliamente comprobada en la gran cantidad de servidores apache actualmente en uso. Además se instala y configura el mod_ssl el cual es una interface entre el Apache y el Openssl (librerías de encriptación de datos).

Mod_ssl es un módulo que se instala con el Apache server y sirve como interface con el OpenSSL. (www.modssl.org, ftp.modssl.org)

Pasos a seguir:

Debido a que mod_ssl es un paquete complejo, existen muchas maneras de instalarlo. Por tal motivo se detallan a continuación la manera de configurar el Apache+mod_ssl bajo linux.

Prerrequisitos:

Para usa mod_ssl se necesitan los siguientes programas:

- Paquete: Apache
  Version: 1.3.x
  Descripción: The Apache Group HTTP Server
  Razón: The webserver base package on which all is based
  Homepage: http://www.apache.org/
  Distribución: ftp://ftp.apache.org/apache/dist/
  Tarball: apache_1.3.x.tar.gz
  Localidad: SF, USA
  Autor(es): The Apache Group <apache@apache.org>
  Tipo: MANDATORY

- Paquete: mod_ssl
  Version: 2.6.x
  Descripción: The Apache Interface to OpenSSL
  Razón: The interface module for Apache
  Homepage: http://www.modssl.org/
  Distribución: ftp://ftp.modssl.org/source/
  Tarball: mod_ssl-2.6.x-1.3.x.tar.gz
  Localidad: Zurich, Switzerland, Europe
  Autor(es): Ralf S. Engelschall <rse@engelschall.com>
  Tipo: MANDATORY

- Paquete: OpenSSL
  Version: 0.9.x
  Descripción: The Open Source Toolkit for SSL/TLS
  Razón: The library which implements SSL/TLS
  Homepage: http://www.openssl.org/
  Distribución: ftp://ftp.openssl.org/source/
  Tarball: openssl-0.9.x.tar.gz
  Localidad: Zurich, Switzerland, Europe
  Autor(es): The OpenSSL Project <openssl@openssl.org>
  Tipo: MANDATORY

o Paquete: GZip
Version: 1.2.4
Descripción: The compression utility
Razón: To unpack the above tarballs
Homepage: http://www.gnu.org/
Distribución: ftp://ftp.gnu.org/pub/gnu/
Tarball: gzip-1.2.4.tar.Z
Localidad: USA
Autor(es): Free Software Foundation (FSF)
Tipo: MANDATORY

o Paquete: Perl
Version: 5.004 or 5.005
Descripción: The Practical Extraction and Reporting Language
Razón: To configure OpenSSL and for APXS tool in Apache
Homepage: http://www.perl.com/
Distribución: http://www.perl.com/CPAN/src/
Tarball: perl5.00x.tar.gz
Localidad: USA
Autor(es): Larry Wall
Tipo: MANDATORY

Instalación:

1. Asegúrese de que Gzip y Perl están actualmente instalados y disponibles los comandos 'gzip' y 'perl'. Ya que son necesarios para desempaquetar y configurar OpenSSL. NO continúe si no están estos paquetes intalados.
2. Extraiga los paquetes requeridos:

   $ gzip -d -c apache_1.3.x.tar.gz | tar xvf -

   $ gzip -d -c mod_ssl-2.6.x-1.3.x.tar.gz | tar xvf -

   $ gzip -d -c openssl-0.9.x.tar.gz | tar xvf -

3. Configure y compile la librería OpenSSL.

   $ cd openssl-0.9.x

   $ sh config \

   $ make

```
$ make test

$ cd ..
```

4. Configurar y compilar mod-ssl+APACI.

```
$ cd mod_ssl-2.6.x-1.3.x

$ ./configure \

  --with-apache=../apache_1.3.x \

  --with-ssl=../openssl-0.9.x \

  --prefix=/usr/local/apache \

$ cd ..

$ cd apache_1.3.x

$ make

$ make certificate

$ make install

$ cd ..
```

5. Probando el Apache sin SSL.

```
$ /usr/local/apache/bin/apachectl start

$ netscape http://<local-host-name>/

$ /usr/local/apache/bin/apachectl stop
```

6. Probando el apache con SSL.

```
$ /usr/local/apache/bin/apachectl startssl

$ netscape http://<local-host-name><http-port>/

$ netscape https://<local-host-name><https-port>/

$ /usr/local/apache/bin/apachectl stop
```

en donde http-port = 80 y https-port = 443.

Una vez instalado el Apache se debe asegurar que el demonio (httpd) del servicio inicie automáticamente.

Hay que tener en cuenta que todos los documentos deberán estar en el directorio:

/usr/local/apache/htdocs#

Dentro de ese directorio se pueden dejar las distintas páginas web que se quieran tener por defecto, el documento que mostrará en primer lugar por defecto, debe llamarse index.html.

Además, existen otros directorios de suma importancia tales como:
/usr/local/apache/cgi-bin/

En este directorio es donde se almacenan todos los programas *.cgi que actúan como interfaz y la base de datos. Dentro de este directorio se pueden crear otros directorios para cada sistema que se tenga, para este proyecto se creo el directorio /cgi-udb que es el que contiene todos los scripts que utiliza dicho sistema.

/usr/local/apache//icons/

Este directorio se utiliza para almacenar todos los gráficos que el sitio web pueda llevar, así mismo como en el anterior se ha creado el directorio /icons-udb dentro de este un directorio específico para almacenar los gráficos del proyecto.

Control de acceso a recursos web

Para restringir el acceso a ciertos recursos podemos añadir lo siguiente en el archivo de configuración httpd.conf:

```
#
#Definición de directorios con permisos
#

<Directory /usr/local/apache/htdocs/admon>
   AuthType Basic
   AuthName admon
   AuthUserFile /var/mysql/users
   <Limit PUT GET>
      require valid-user
   </Limit>
</Directory>
```

De esa forma estaríamos limitando el acceso al directorio

/usr/local/apache/cgi-bin/cgi-adm/

Los siguientes apartados son:

· AuthType: Existen 2 tipos de autentificación implementados en la actualidad estos son:

· Basic

· Digest

· AuthName: Se refiere al nombre del recurso al que queremos acceder.

usuarios

· AuthUserFile: Archivo en el que estarán las parejas de usuario-passwd que podrán acceder al recurso.

/tesis/passwd/usrs-udb

La configuración anterior daría lugar a un dialogo como el siguiente, al intentar acceder a http://www.libudb.edu.sv/administracion/

Creación del archivo de usuarios y claves.

Con htpasswd -c creamos el archivo nuevo, el programa nos pide el *usuario* y el *password* que queremos para él.

Creando el archivo.

Así pues para crear un archivo nuevo llamado /tmp/users que contenga al usuario *jperez*, con la clave *juancito*, la sintaxis seria la siguiente:

```
htpasswd -c  -b /tmp/users pgonzalez pakito
Adding password for user pgonzalez
```

Agregando un usuario al archivo.

Para añadir un usuario nuevo al archivo anterior por ejemplo el usuario *david* con el *password* angelitos tendríamos:

```
htpasswd -b /tmp/users david angelitos
Adding password for user david
```

Actualizando el password de un usuario.

Para actualizar el *password* simplemente tenemos que añadir de nuevo el usuario

```
htpasswd -b /tmp/users david demonios
Updating password for user david
```

Servidor de base de datos MySql.

Con las nuevas versiones de Linux, los paquetes adicionales se instalan automáticamente en la instalación del sistema operativo.

Una vez instalada la base de datos, se asegura que el servicio *mysqld* se levante cada vez que se inicia el servidor, o sino esto se puede hacer manual con el comando mysql start (para iniciar el servicio) o mysql stop (para parar el inicio), pero lo más recomendable es que se levante el servicio automáticamente.

Luego, se crea la base de datos con el comando: CREATE DATABASE libudb e inmediatamente se le tienen que otorgar los permisos al administrador de la base de datos, esto se hace de la siguiente forma:

GRANT ALL PRIVILEGES ON *.* TO admin@"%";

Lo anterior significa que se le dan todos los privilegios al usuario "admin" en todas las bases de datos que existan en MySQL. Ademas se le tienen que dar permisos al usuario del apache "wwwrun" que es por medio del cual se accesa desde internet.

El directorio en donde se encuentra almacenados todos los archivos relacionados con la base de datos "libudb" es: /var/mysql/libudb

Después se crean las tablas de la siguiente forma:

```
CREATE TABLE area (
  idarea int(11) DEFAULT '0' NOT NULL auto_increment,
  nombrearea char(50),
  PRIMARY KEY (idarea)
);
```

Lenguaje Perl y Módulos DBI.

Este lenguaje es uno de los más utilizados en desarrollo de sitios dinámicos en Internet y trabajo muy en conjunto con los DBI.

Para que este paquete esté funcionando bien no se necesita mucho trabajo, basta con digitar el siguiente comando: perl -v, luego el despliega la información de su versión, si esto lo hace sin problemas, significa que está instalado y funcionando.

El directorio en donde se encuentra el binario (archivo ejecutable) es: /usr/bin/perl.

Como se menciona en la introducción, Perl no obliga a casi nada, así pues, lo que se plantea como estructura básica es mas bien una convención que un requisito del lenguaje, a diferencia de Pascal (por ejemplo) Perl no tiene una plantilla para sus programas y si se adoptan algunos protocolos es solo por comodidad.

Los programas de Perl, por lo regular, inician con la línea:

```
#!/usr/bin/perl
```

Esta línea, indica al Sistema Operativo que lo que sigue es un script de Perl, y que "Perl" (el programa con el cual debe ejecutarse) está en el directorio "/usr/bin", la secuencia "#!" es una secuencia que UNIX reconoce, no Perl.

Un método alterno, que funciona para otras plataformas, es: en lugar de colocar esa primera línea ejecutamos:

```
Perl nombre_del_script.pl
```

De modo que directamente se ejecuta el intérprete de Perl pasándole como primer parámetro el script a ejecutar (los demás parámetros se tomarán como parámetros al programa). Si se requiere deberá sustituirse "Perl" por la ruta completa del programa y el nombre que el programa tenga.

Un ejemplo sería el siguiente:

Programa Hola mundo:

```
#!/usr/bin/perl
print "Hola Mundo\n";
```

Este programa, se escribe en un archivo de texto común, (al que se recomienda ponerle extensión ".pl") y se cambian sus permisos para que pueda ser ejecutado (por lo regular con un "chmod o+x nombre_programa.pl" en sistemas UNIX), para ejecutarlo simplemente se invoca el nuevo script "nombre_programa.pl", hay que recordar que para el sistema particular en que se este trabajando es muy probable que deba modificarse "/usr/bin/" por otra ruta.

Así, la ejecución en un sistema UNIX podría verse como:

```
>perl Hola.pl
Hola Mundo
>
```

Los módulos DBI se utilizan con Perl para la conexión de la base de datos, para este proyecto se utilizo el DBI::Mysql, que es el módulo que se utiliza para accesar la base de datos MySQL.

Un típico programa utilizando DBI::mysql sería:

```
#!/usr/bin/perl

use CGI;
use DBI;

#$cgiparms = new CGI;

$dbh = DBI->connect("DBI:mysql:libudb","wwwrun",$password) || die "No se pudo";

$query = "select * from novedad";
$sth = $dbh->prepare($query);
$sth -> execute;
$num = $sth->rows;
```

5. CONCLUSIONES Y RECOMENDACIONES.

5.1 CONCLUSIONES

- Ya que Internet tiene un alcance mundial, el mercado que cubre un comercio virtual siempre es mayor que el de uno convencional.

- Un punto muy importante en las transacciones de comercio electrónico es la seguridad, ya que a veces esta puede llegar a ser una debilidad si no se utilizan las herramientas adecuadas.

- En la actualidad en El Salvador el comercio electrónico todavía no es una forma muy utilizada de realizar transacciones, como lo es en otros lugares.

- Las empresas tanto grandes como pequeñas están viendo en Internet un nuevo campo para realizar negocios, esto vendrá a revolucionar muchos aspectos de nuestra cultura.

- La publicidad en este tipo de negocios es un punto muy importante, ya que es por medio de ella que los comercios adquieren su mercado.

5.2 RECOMENDACIONES

- Al tratarse de un mercado tan grande como el que permite Internet, se deberá considerar ciertos aspectos, que permitan cubrir las necesidades de la diversidad de clientes a atender, como la variedad de títulos a ofrecer, la calidad del servicio.

- Se deberá prestar atención especial a la seguridad del sitio, utilizando debidamente las herramientas con que se dispone.

- Debe hacerse énfasis en el uso del "comercio electrónico" como un medio eficiente de realizar compras, utilizando medios como la publicidad para que la comunidad conozca la existencia y funcionamiento de este tipo de sitios.

- El mantenimiento adecuado del sitio y la actualización oportuna de nuevos títulos, ediciones etc. generará una buena imagen del mismo.

- El Ministerio de Economía a través del Registro de Comercio o de una ley reguladora como "El Código de Comercio", podrían establecer normas para el establecimiento de "Comercios Electrónicos", lo que vendrá a formalizar este tipo de negocios.

6. REFERENCIAS Y BIBLIOGRAFÍA

6.1 Referencias y Bibliografía.

- Sitio en Internet acerca del Comercio Electrónico. http://www.pagofacil.com/

- Sitio Web que ofrece información acerca de uno de los mayores servidores de páginas web utilizados en el mundo. http://www.apache.org/

- Sitio Web en donde se promueve el código abierto (open source) para su uso libre (no comercial). Hay un equipo de desarrolladores promoviendo el OpenSSL (módulo de encriptación que funciona con el Apache) para su desarrollo y uso gratis. http://www.openssl.org/

- Sitio Web que brinda información acerca del uso de las tarjetas de crédito en el comercio electrónico. http://www.visa.com/

- Sitio Web que brinda el servicio a las empresas que desean tener su negocio en Internet, el poder certificarse para que estas puedan trabajar de una forma segura en la red. http://www.verisign.com.

- Revista electrónica TiMagazine. Artículo: “SET, seguridad en la Red”. Por Martin. http://www.timagazien.net/

- El Diario de Hoy, Lunes 31 de Enero de 2000, Sección TecnoVida, Pág. 95.

- Creación de servidores de bases de datos para Internet con CGI; Rowe, Jeff; Prentice Hall Hispanoamericana S. A.; México; 1996.

- Diario del Navegante, Internet Informática y nuevos medios http://w3.el-mundo.es/navegante/diario/index.html

- www.iesa.edu.ve/catedrati/gerencidigital/casos/index.html

- Esta información se obtuvo del sito oficial de Verign http://www.verisign.com/
- Dirección del BID.
- El Diario de Hoy, Domingo 12 de marzo de 2000. página 6-7.
- Sitio de Distribución SUSE http://www.suse.com.de/

ANEXO A

El sistema se ha desarrollado tomando en cuenta las leyes internacionales del comercio electrónico, las cuales se describen a continuación.

Ley Modelo de la CNUDMI sobre Comercio Electrónico

CAPÍTULO I. DISPOSICIONES GENERALES

Articulo 1. **Ámbito de aplicación**

La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto de actividades comerciales.

Artículo 2. **Definiciones**

Para los fines de la presente Ley:

a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, óptimos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax;

b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;

d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no éste actuando a título de intermediario con respecto a él;

e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3**. Interpretación**

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. **Modificación mediante acuerdo**

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III podrán ser modificadas mediante acuerdo.

2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II.

CAPITULO II

APLICACIÓN DE LOS REQUISITOS JURÍDICOS A LOS MENSAJES DE DATOS.

Artículo 5. **Reconocimiento jurídico de los mensajes de datos**

No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

Artículo 6**. Escrito**

1) Cuando la ley requiera 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.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.

Artículo 7. **Firma**

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

Artículo 8. **Original**

1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

a) Si existe alguna garantía fidedigna de que se 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;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del inciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún

cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

Artículo 9. **Admisibilidad y fuerza probatoria de los mensajes de datos.**

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

a) Por la sola razón de que se trate de un mensaje de datos; o

b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 10. **Conservación de los mensajes de datos**

1) Cuando la ley requiera que ciertos documentos, registro o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su ulterior consulta; y

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, enviada 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.

2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.
3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos. a), b) y c) del párrafo 1).

CAPÍTULO III COMUNICACIÓN DE LOS MENSAJES DE DATOS

Artículo 11. **Formación y validez de los contratos**
1) En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por sola razón de haberse utilizado en su formación un mensaje de datos.

Artículo 12. **Reconocimientos por las partes de los mensajes de datos**
1) En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Artículo 13. **Atribución de los mensajes de datos**
1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.
2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:
a) Por alguna persona facultada para actuar en nombre del iniciado respecto de ese mensaje; o
b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:

a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o

b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

4) El párrafo 3) no se aplicará:

a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o

b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.

5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.

6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.

Artículo 14. **Acuse de recibo**

1) Los párrafos 2) a 4) del presente artículo serán aplicable cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o acuerde con el destinatario que se acuse recibo del mensaje de datos.

2) Cuando el iniciador no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

3) Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.

4) Cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:

a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y

b) De no recibirse acuse dentro del plazo fijado conforme al inciso a), podrá dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

5) Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.

6) Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

7) Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

Artículo 15**. Tiempo y lugar del envío y la recepción de un mensaje de datos**

1) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.

2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:

i) En el momento en que entre el mensaje de datos en el sistema de información designado; o

ii) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario.

3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4).

4) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo.

Para los fines del presente párrafo:

a) Si el iniciador o el destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación

subyacente o, de no haber una operación subyacente, su establecimiento principal;

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

ANEXO B

GLOSARIO DE TÉRMINOS INFORMÁTICOS.

Applet. Aplicación escrita en JAVA y compilada.

ARPANET. (Advanced Research Projects Agency Network). Red de la Agencia de Proyectos de Investigación Avanzada. Red militar Norteamericana a través de líneas telefónicas de la que posteriormente derivó Internet.

ASCII. American Standard Code for Information Interchange. Estándar Americano para Intercambio de Información. La tabla básica de caracteres ASCII esta compuesta por 128 caracteres incluyendo símbolos y caracteres de control. Existe una versión extendida de 256

Browser. Navegador. Término aplicado normalmente a los programas que permiten acceder al servicio WWW.

CGI (Common Gateway Interface). Interfaz de Acceso Común. Programas usados para hacer llamadas a rutinas o controlar otros programas o bases de datos desde una página Web. También pueden generar directamente HTML.

Cookie. Pequeño trozo de datos que entrega el programa servidor de HTTP al navegador WWW para que este lo guarde. Normalmente se trata de información sobre la conexión o los datos requeridos, de esta manera puede saber que hizo el usuario en la última visita.

Cracker. Individuo con amplios conocimientos informáticos que desprotege/piratea programas o produce daños en sistemas o redes.

DNS (Domain Name System). Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

Domain Dominio. Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda.

FAQ (Frecuent Asked Question). Preguntas Formuladas Frecuentemente. Las "faqs" de un sistema son archivos con las preguntas y respuestas más habituales sobre el mismo.

FTP. File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los potocolos de transferencia de ficheros mas usado en Internet.

Gateway. Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

GUI. Graphic User Interface. Interface Gráfico de Usuario.

Hacker. Experto en informática capaz de de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones

Homepage. Página principal o inicial de un sitio WEB.

Host. Anfitrión. Computador conectado a Internet. Computador en general.

HTML. Acrónimo de *Hypertext Markup Language,* lenguaje de marcas de hipertexto. En informática, formato estándar de documentos de texto que se utiliza desde 1989 en World Wide Web (WWW). Los documentos HTML contienen dos tipos de información: la que se muestra en pantalla y códigos (*tags* o etiquetas), transparentes al usuario, que indican cómo mostrar esa información. El lenguaje HTML es un subconjunto de SGML (acrónimo de *Standard Generalized Markup Language,* lenguaje estándar de marcado de documentos), que es un estándar de descripción de página independiente del dispositivo.

HTTP. HyperText Transfer Protocol. Protocolo de Transferencia de Hypertexto. Protocolo usado en WWW.

Internet. Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

INTERNIC. Entidad administrativa de Internet que se encarga de gestionar los nombres de dominio en EEUU.

Intranet. Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW. IP Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de Internet. También se refiere a las direcciones de red Internet.

Java. Lenguaje de programación orientado a objeto parecido al C++. Usado en WWW para la telecarga y telejecución de programas en el computador cliente. Desarrollado por Sun Microsystems.

Java Script. Programa escrito en el lenguaje script de Java que es interpretado por la aplicación cliente, normalmente un navegador (Browser).

JPEG. (Join Photograph Expert Group). Unión de Grupo de Expertos Fotográficos. Formato gráfico con pérdidas que consigue elevados ratios de compresión.

Linux. Versión Shareware del conocido sistema operativo Unix. Es un sistema multitarea multiusuario de 32 bits para PC.

Módem. Modulator/Demodulator. Modulador/Demodulador. Dispositivo que adapta las señales digitales para su transmisión a través de una línea analógica. Normalmente telefónica.

Nodo. Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red. Punto de interconexión a una RED.

Perl. Lenguaje para manipular textos, ficheros y procesos. Con estructura de script. Desarrollado por Larry Wall, es multiplataforma ya que funciona en Unix.

PING. (Packet Internet Groper). Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible. Envía paquetes de control para comprobar si el anfitrión está activo y los devuelve.

PPP. (Point to Point Protocol). Protocolo Punto a Punto. Un sucesor del SLIP. El PPP provee las conexiones sobre los circuitos síncronos o asíncronos, entre router y router, o entre host y la red. Protocolo Internet para establecer enlace entre dos puntos.

Proxy. Servidor Caché. El Proxy es un servidor que conectado normalmente al servidor de acceso a la WWW de un proveedor va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

Router. Dispositivo conectado a dos o mas redes que se encarga únicamente de tareas de comunicaciones

SMPT. Simple Mail Transfer Protocol. Protocolo de Transferencia Simple de Correo. Es el protocolo usado para transportar el correo a través de Internet.

Sniffer. Literalmente "Husmeador". Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente su uso es ilegal.

SSL. (Secure Sockets Layer). Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

TCP/IP. Transmission Control Protocol / Internet Protocol. Protocolo de Control de Transmisión / Protocolo Internet. Nombre común para una serie de protocolos desarrollados por DARPA en los Estados Unidos en los años 70, para dar soporte a la construcción de redes interconectadas a nivel mundial. TCP corresponde a la capa (layer) de transporte del modelo OSI y ofrece transmisión de datos. El IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal característica es comunicar sistemas diferentes. Fueron diseñados inicialmente para

ambiente Unix por Victor G. Cerf y Robert E. Kahn. El TCP / IP son básicamente dos de los mejores protocolos conocidos.

Telnet. Protocolo y aplicaciones que permiten conexión como terminal remota a una computadora anfitriona, en una localización remota.

Unix. Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas mas conocidos como MS-DOS están basadas en este sistema muy extendido para grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

URL. (Uniform Resource Locator). Localizador Uniforme de Recursos. Denominación que no solo representa una dirección de Internet sino que apunta aun recurso concreto dentro de esa dirección.

Web Site. Sitio en el World Wide Web. Conjunto de páginas Web que forman una unidad de presentación, como una revista o libro. Un sitio está formado por una colección de páginas Web. RELI - Revista en Línea puede considerarse un sitio web

www, web o w3. (World Wide Web). Telaraña mundial. Sistema de arquitectura cliente-servidor para distribución y obtención de información en Internet, basado en hipertexto e hipermedia. Fue creado en el Laboratorio de Física de Energía Nuclear del CERN, en Suiza, en 1991 y ha sido el elemento clave en el desarrollo y masificación del uso de Internet.

ANEXO C

MANUALES DE REFERENCIA DEL SITIO.

SITIO PRINCIPAL: http://www.libudb.edu.sv/

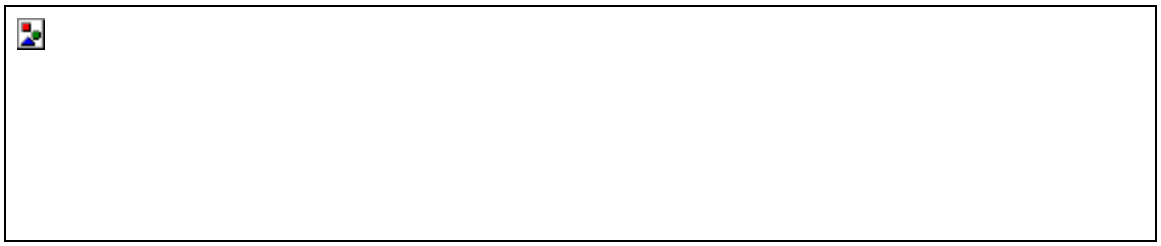
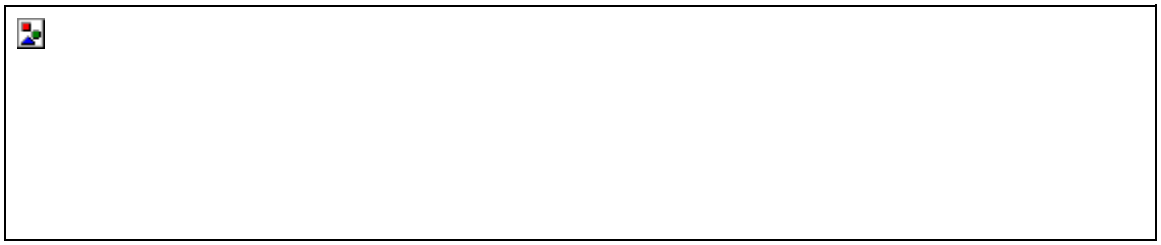


Tabla de Contenido

Siguiente Anterior Contenido

Hecho por ***Marlon Lazo***
melazo@yahoo.com
Versión 1.0
Universidad Don Bosco
Enero/2001



Siguiente Anterior Contenido

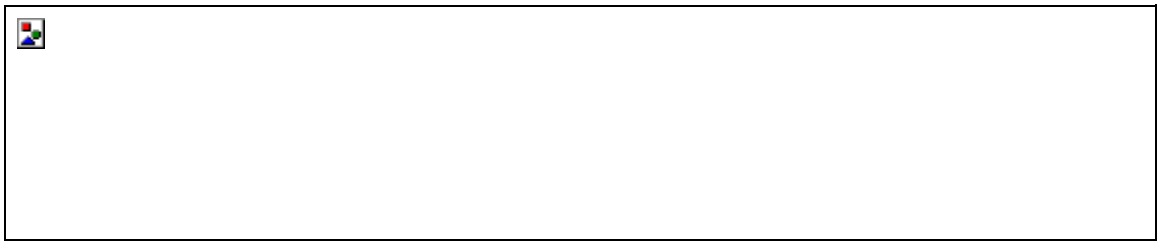
Introducción.-

Este manual se ha hecho con el propósito de que todos los cibernautas que entren a la página web de la Librería Virtual Don Bosco, tengan una guía de cómo navegar en el sitio, hacer búsquedas de libros, encontrar las novedades del mes y así mismo poder enviarnos todos sus comentarios.

Además, se incluye un apartado especial de **¿Cómo comprar?,** todos los pasos que se tienen que dar através de la compra con tarjeta de crédito o de PIN.

Siguiente Anterior Contenido

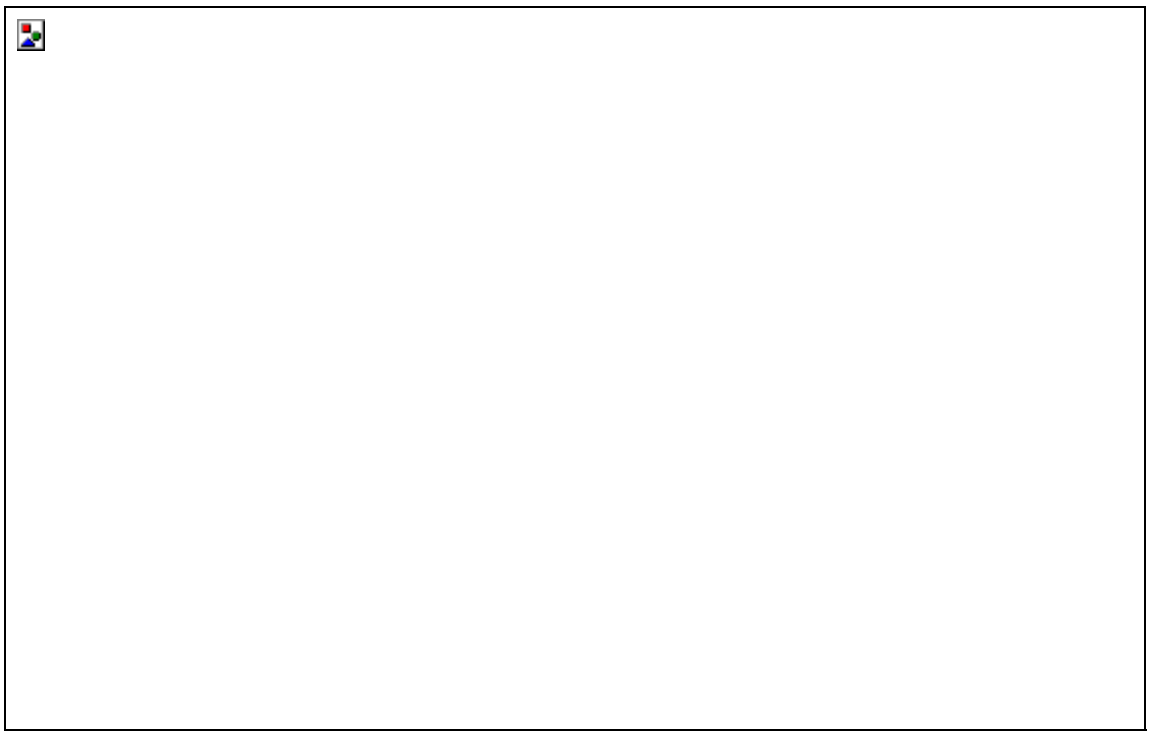
*Hecho por **Marlon Lazo***
melazo@yahoo.com
Versión 1.0 Universidad Don Bosco Enero/2001



Siguiente Anterior Contenido

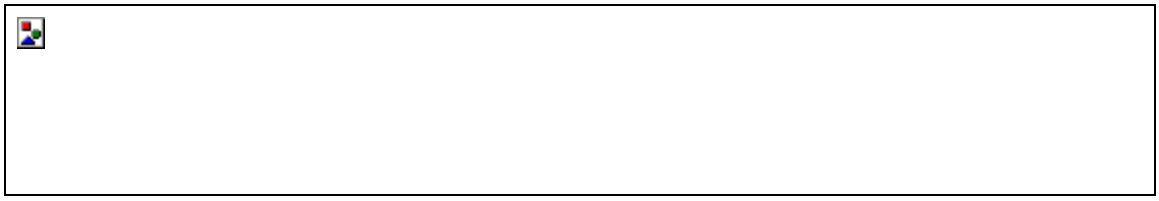
¿Quiénes Somos?

Esta página muestra el objetivo principal de "La Librería Virtual Don Bosco", cuál es su misión en la Internet.



Siguiente Anterior Contenido

Hecho por ***Marlon Lazo***
melazo@yahoo.com
Versión 1.0
Universidad Don Bosco
Enero/2001

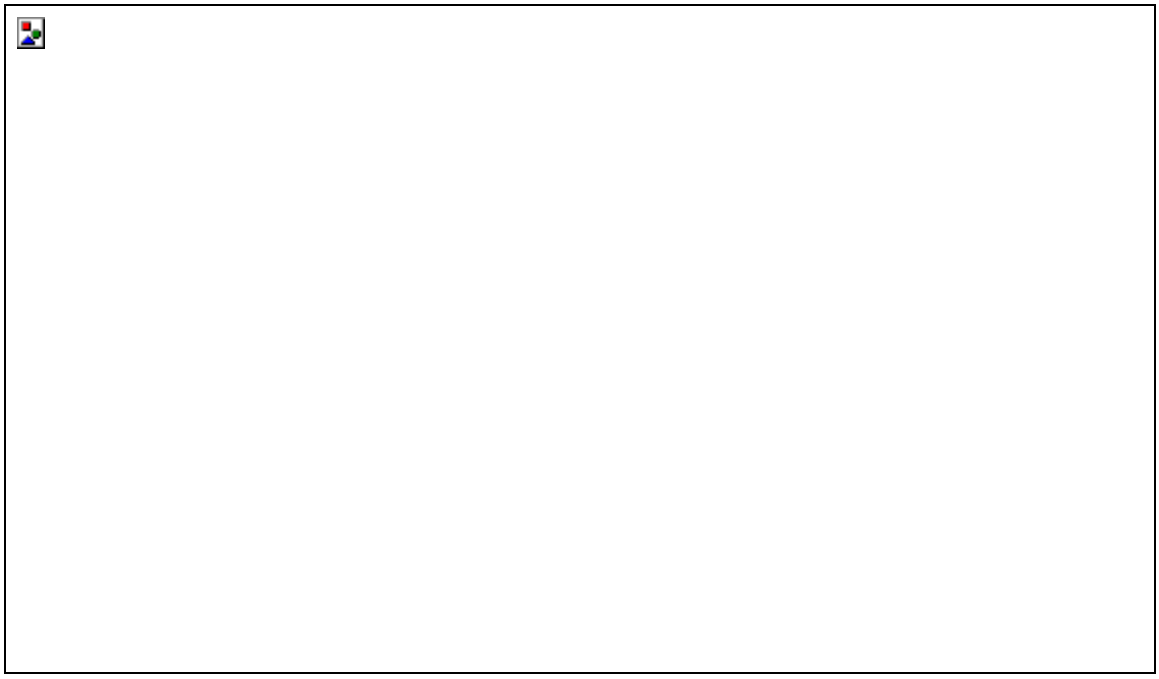


Siguiente Anterior Contenido

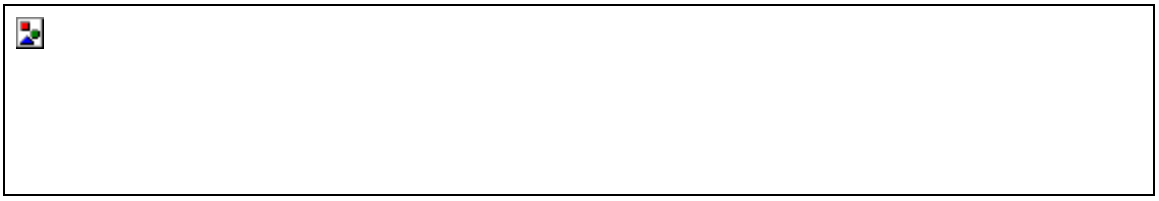
¿Cómo Registrarse?

Para poder comprar en el sitio es obligatorio crear su cuenta personal, esto se hace por razones de seguridad, además se puede llevar un mejor control de sus compras al momento de enviarlas.

Su login (nombre clave) debe ser mínimo de 4 y máximo de 10 caracteres, el cual servirá para identificarlo a lo largo de su compra. También tiene que introducir su correo electrónico, nombres ,apellidos y su dirección actual.



Siguiente Anterior Contenido

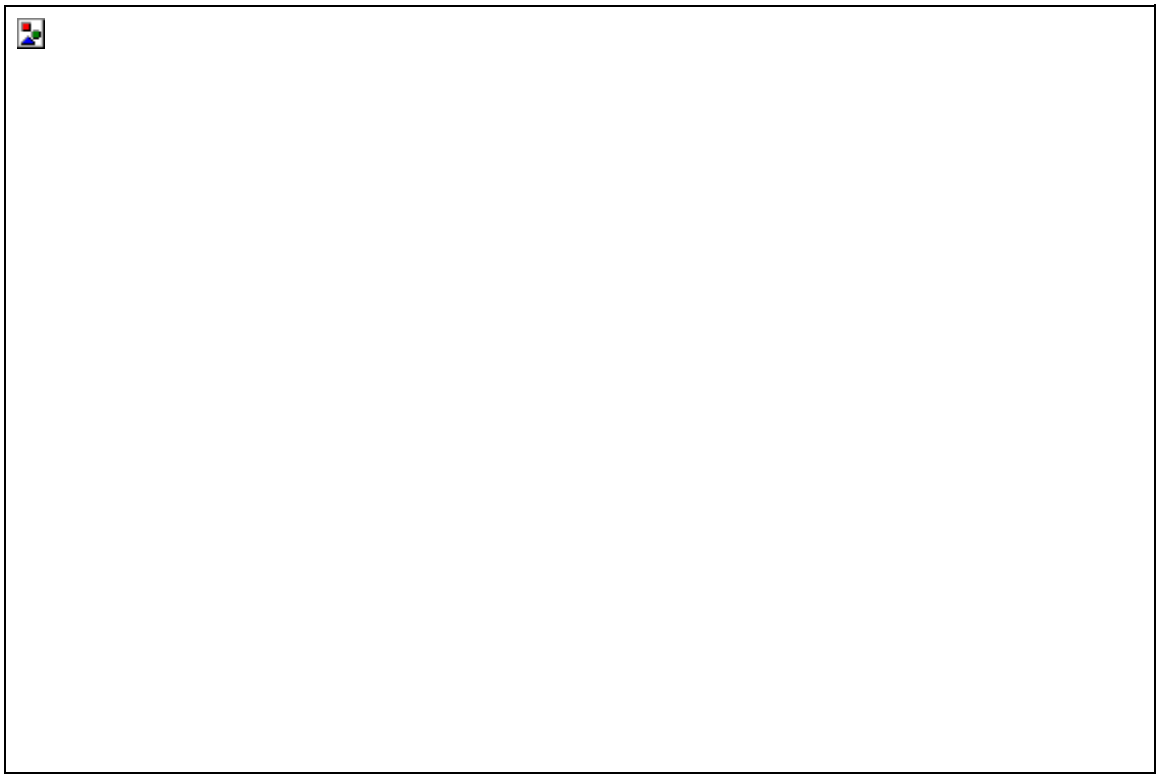


Siguiente Anterior Contenido

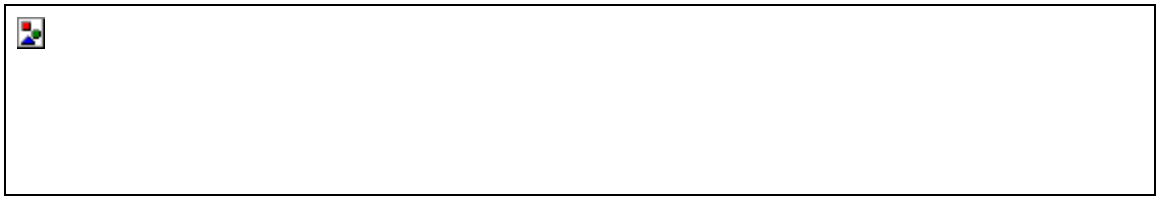
Novedades

En esta opción del sitio se muestran las novedades (en cuanto a libros) del mes, nuevos libros editados, nuevas ediciones de libros anteriores etc. Además esta opción le dá la oportunidad de agregar a su carrito de compras la cantidad de ejemplares que desea de ese libro.

También, se muestra la información principal del libro como: su autor, editorial, número ISBN, título y hasta un breve bosquejo del contenido del libro.



Siguiente Anterior Contenido

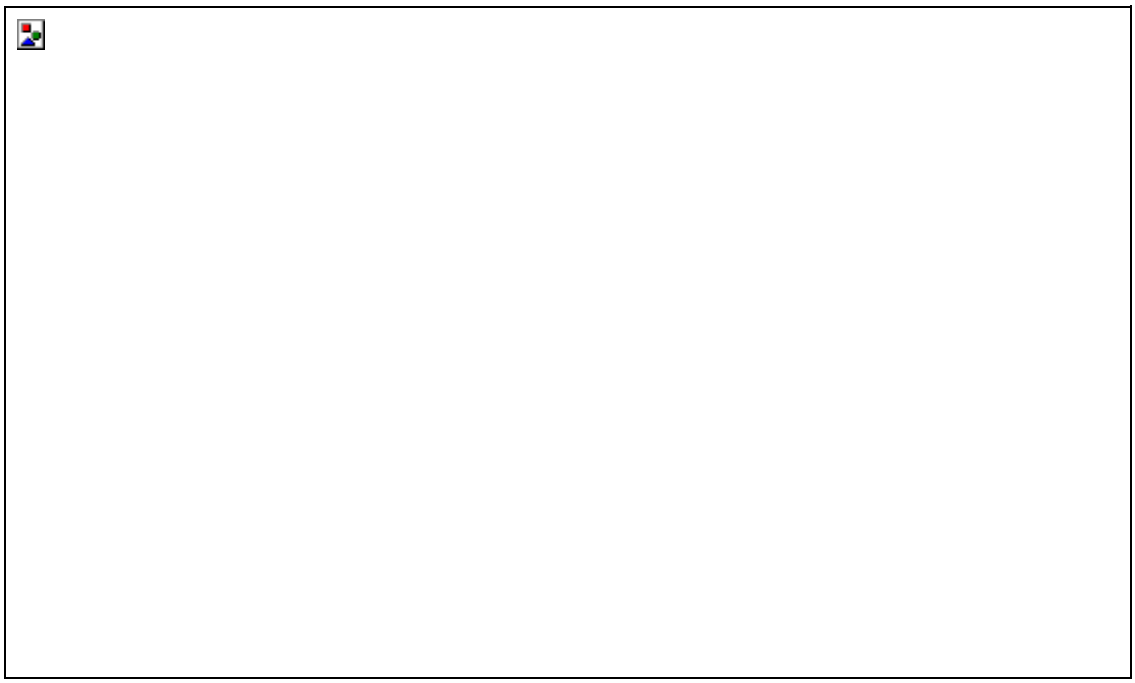


Siguiente Anterior Contenido

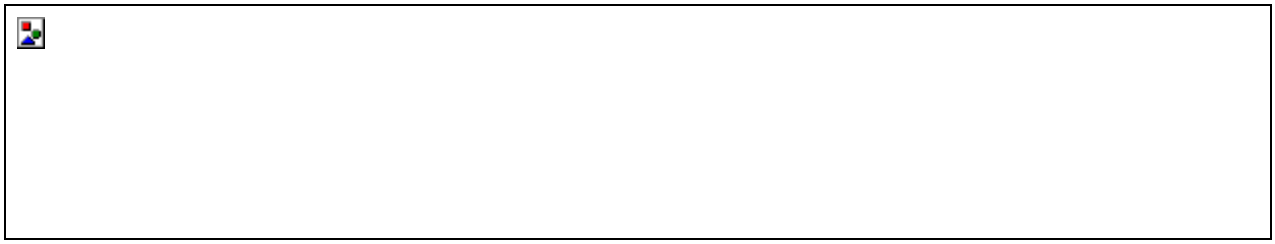
Busqueda de libros

En este pequeño formulario ud. podrá introducir un criterio de búsqueda, ya sea este por autor, título o una palabra clave que se identifique con lo que ud. está buscando, en el ejemplo se utiliza la búsqueda por palabra clave la cual busca en los campos de Autor, Título y descripción.

y el resultado es el siguiente:



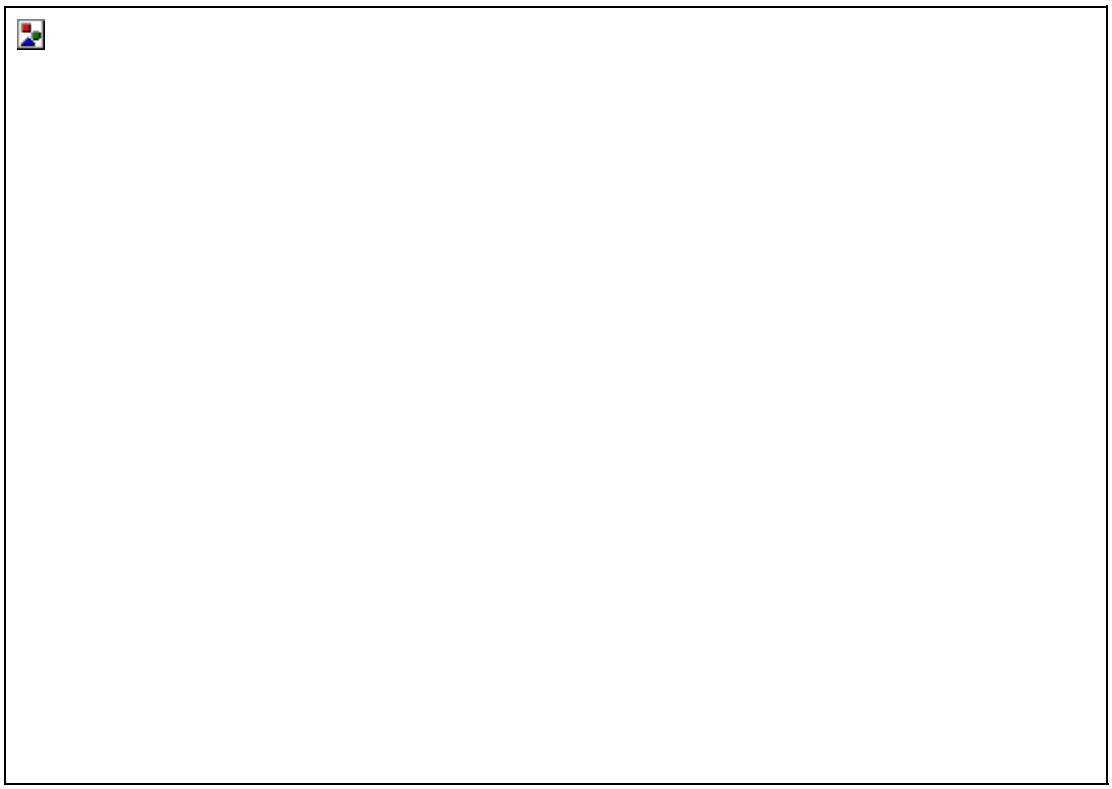
Siguiente Anterior Contenido



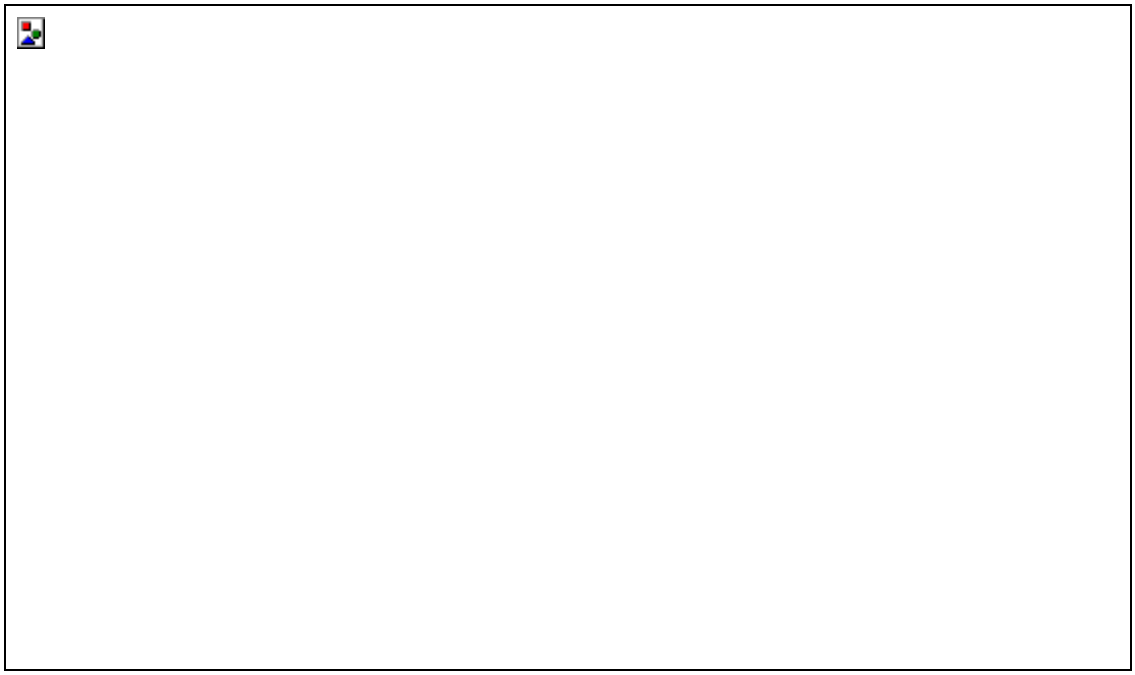
Siguiente Anterior Contenido

Catálogo

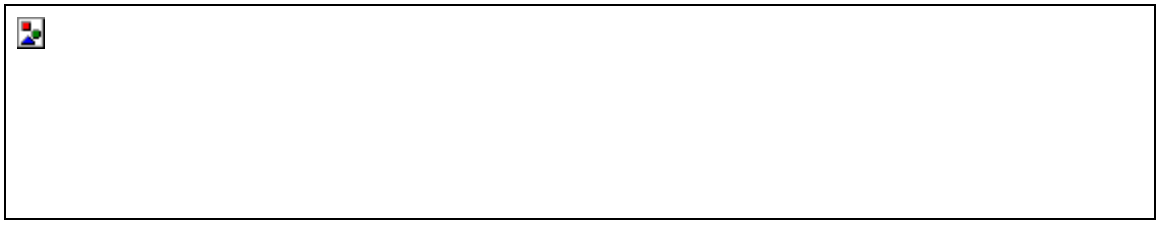
Esta opción permite tener una consulta de todos los libros por medio de un filtro que nosotros designemos, por ejemplo se escoje que se muestren todos lo libros que pertenezcan al area de computación.



Luego, el resultado será de todos los libros que pertenezcan a ese tipo, el cual se verá así.



Siguiente Anterior Contenido

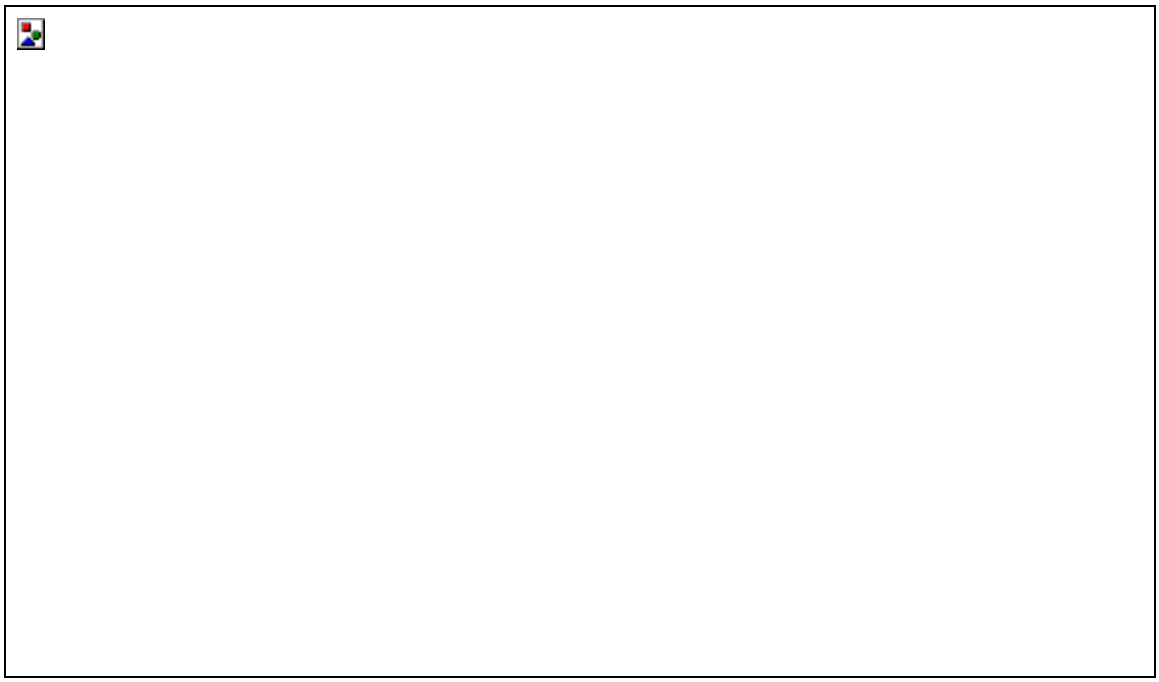


Siguiente Anterior Contenido

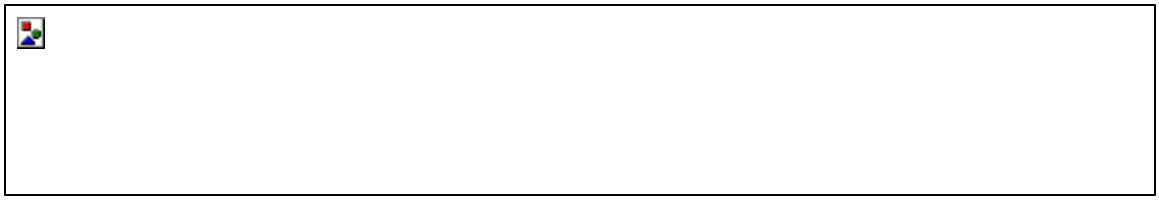
Comentarios

Este formulario recopila los comentarios que se tienen acerca del sitio, el cual se hace para ir recolentando información de que es lo que los clientes esperan de la "Librería Virtual Don Bosco".

Ejemplo:



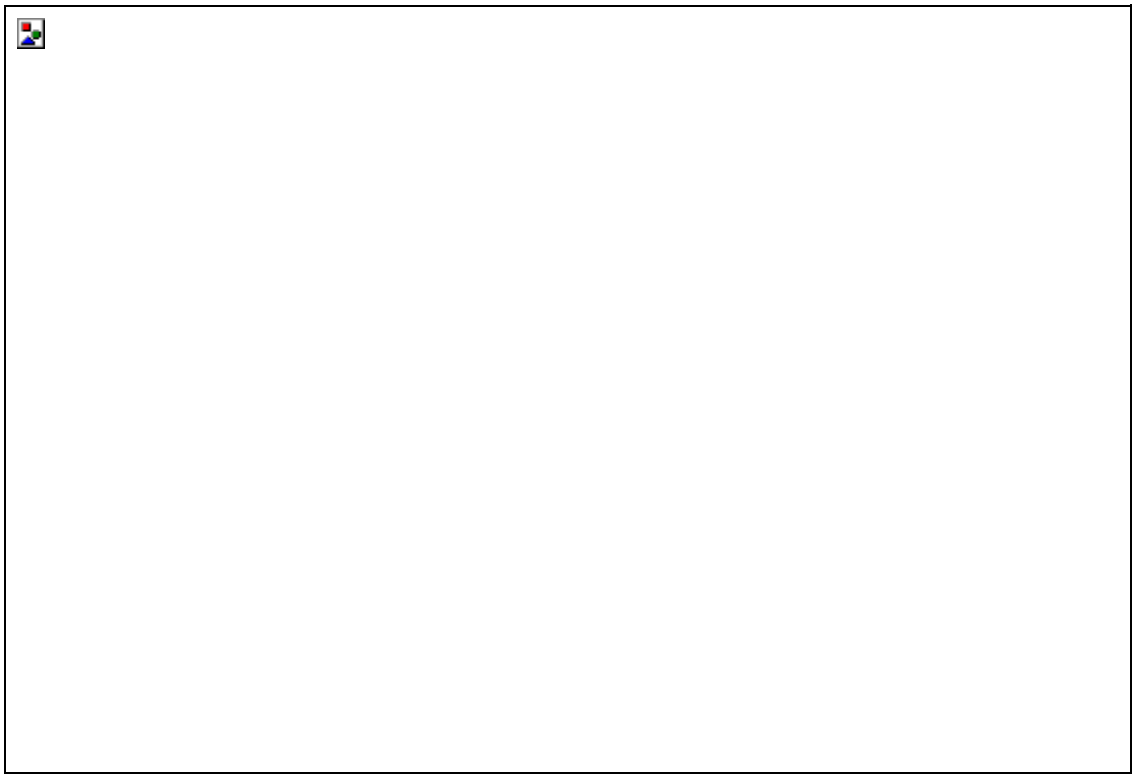
Siguiente Anterior Contenido



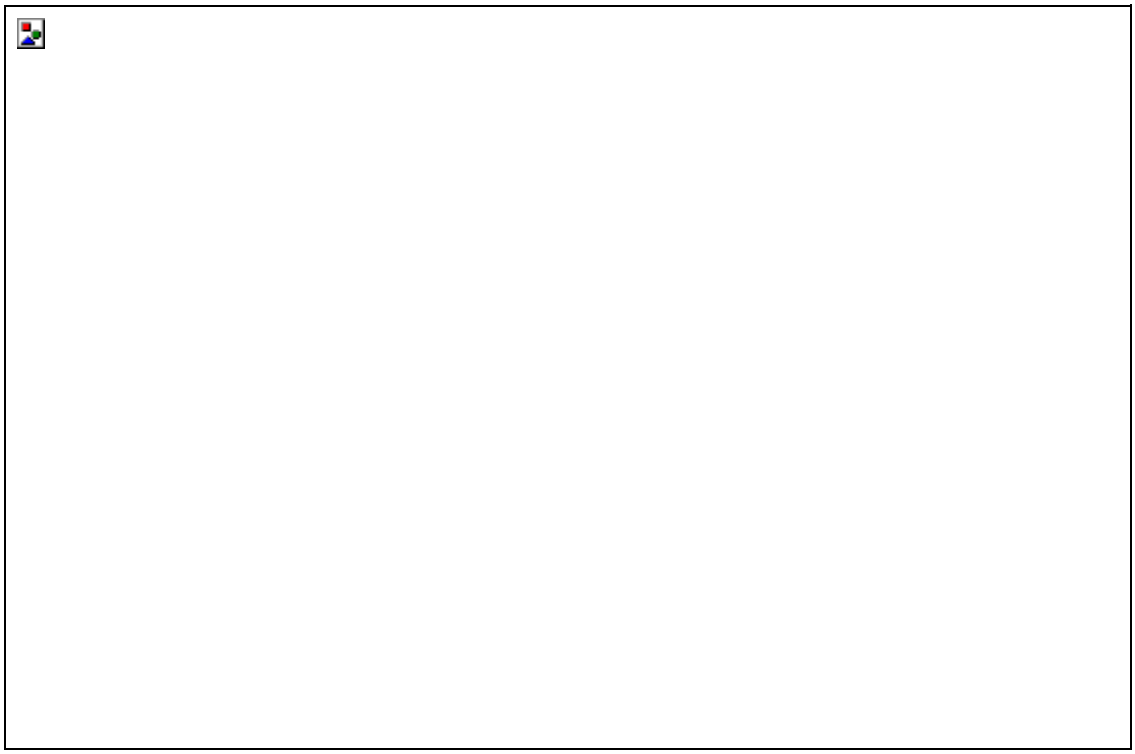
Siguiente Anterior Contenido

Carrito de Compras

En esta opción ud. puede visualizar todos lo items o libros que tiene en su canasta de compras. En el caso de que no haya seleccionado ninguno le aparecerá que está vacío.



Y si ud. anteriormente había seleccionado libros para su compra le aparecerá algo similar a esto:

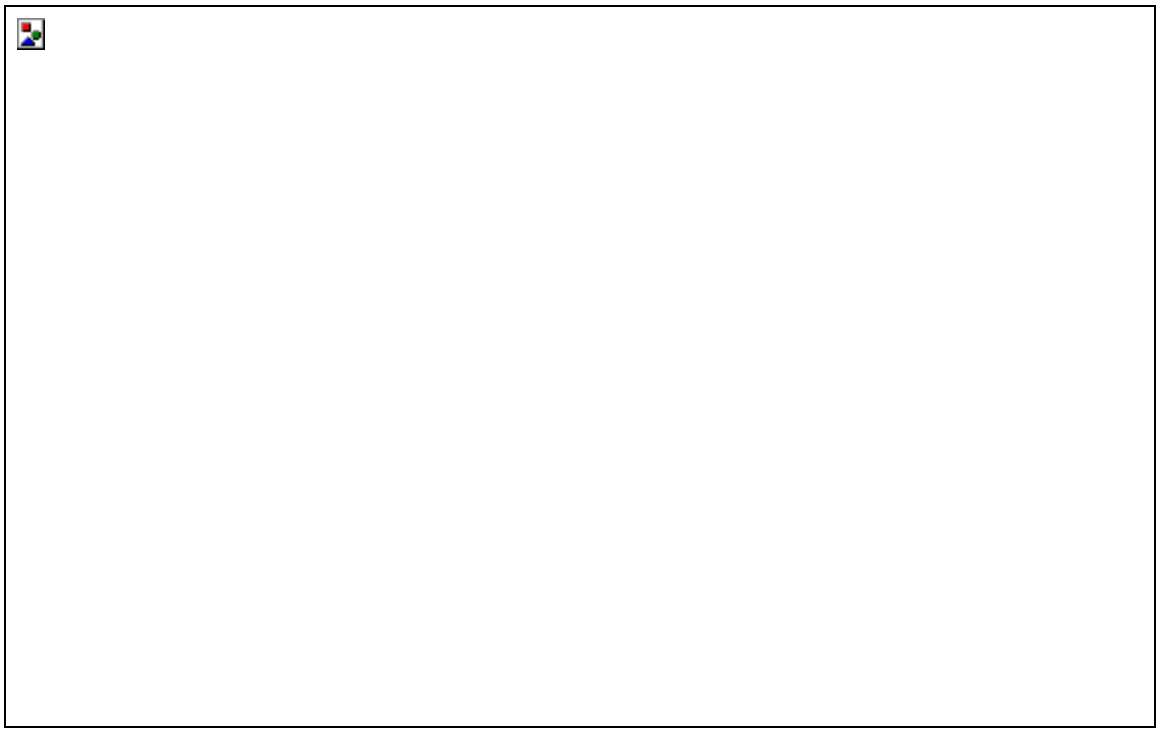


Siguiente Anterior Contenido

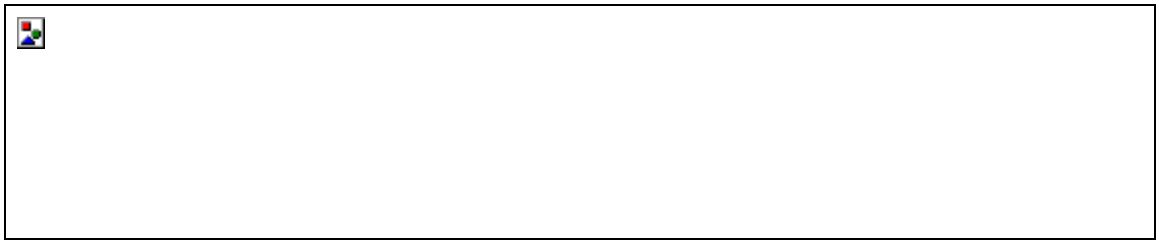
Siguiente Anterior Contenido

Información

Es una página de informción en donde se puede encontrar un link a este manual.



Siguiente Anterior Contenido



Siguiente Anterior Contenido

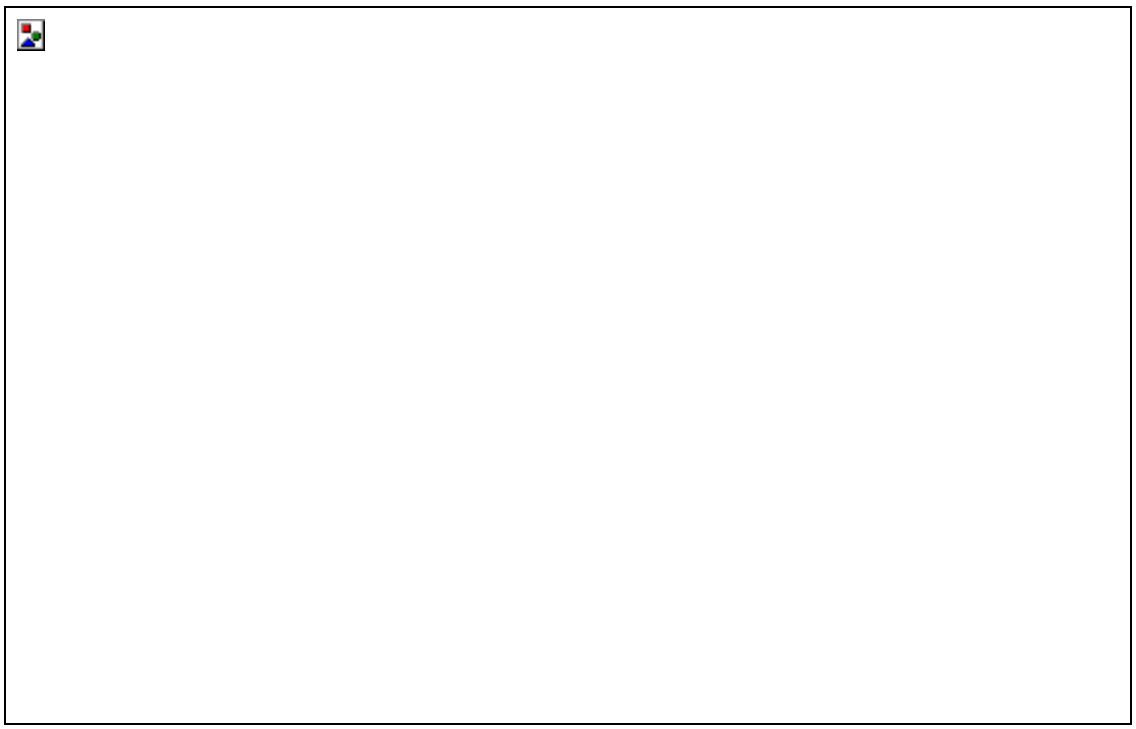
¿Cómo comprar?

Media vez ud. haya seleccionado todo lo que va a comprar, tiene dos opciones de como pagar lo que lleva:

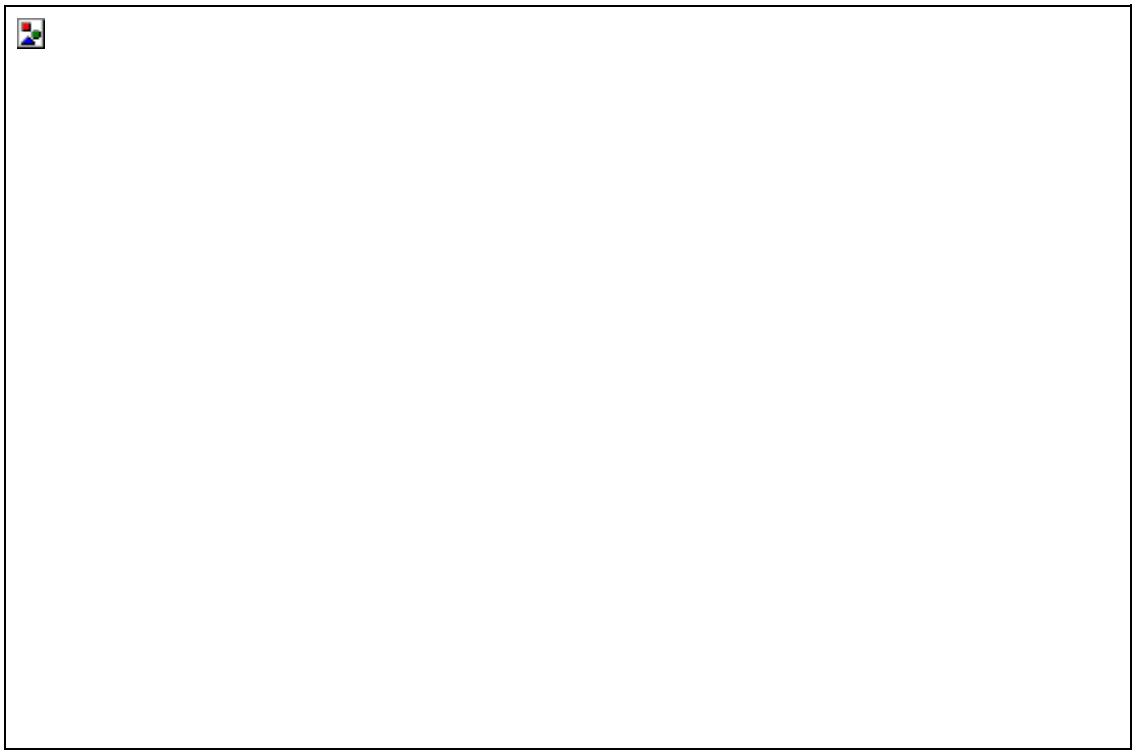
por medio de Tarjeta de Crédito

por medio de PIN

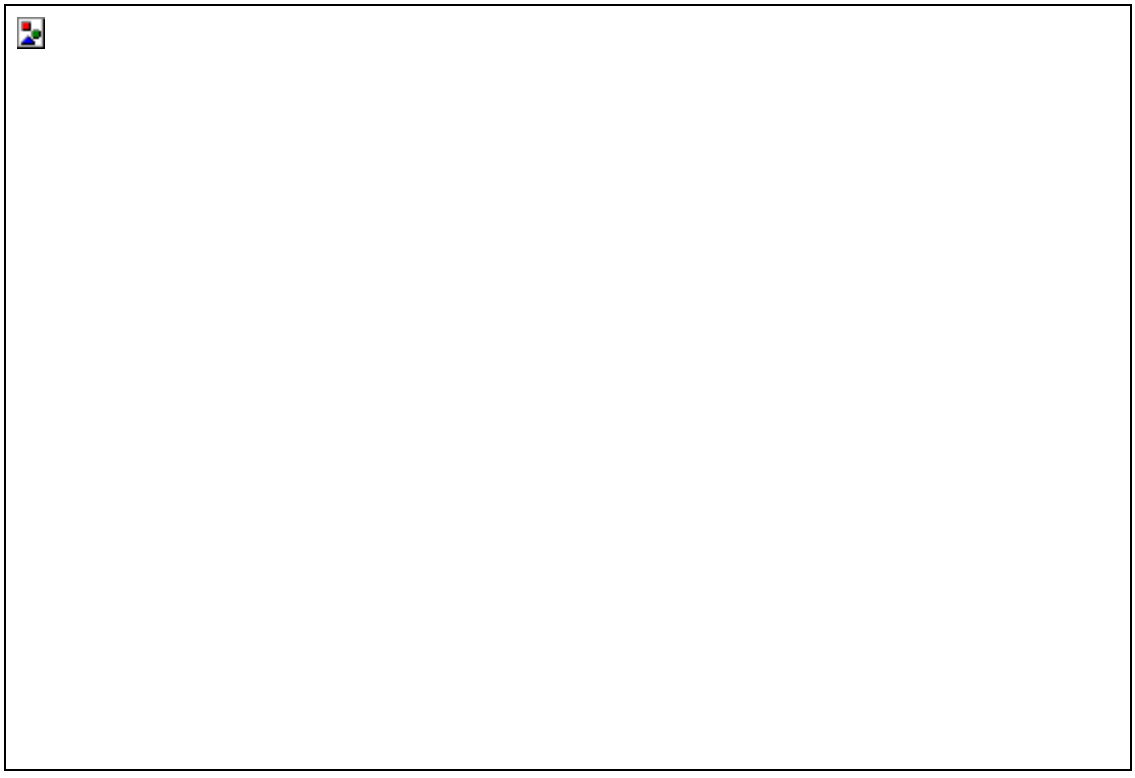
Lo primero que ud. visualiza es su carrito de compras:



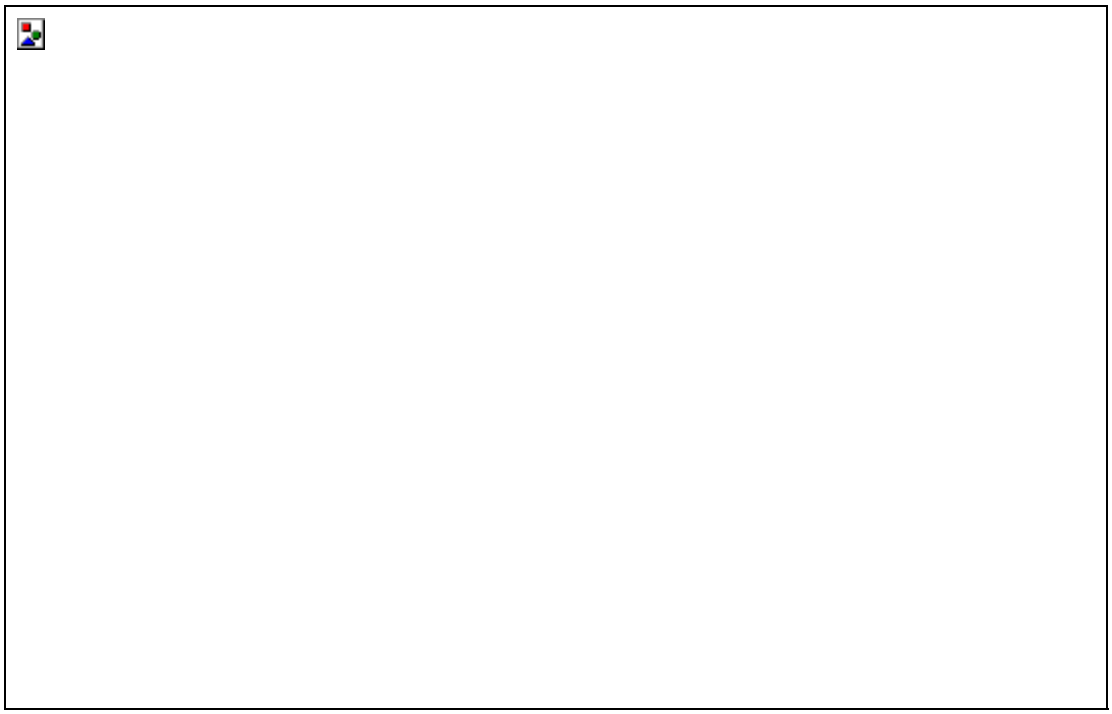
Tiene que llenar un formulario en donde se le pide la dirección a donde quiere que le dejen su pedido. Luego ud. decide si el pago lo hace por tarjeta o por PIN.



En el caso que decida pagar por medio de la tarjeta de crédito, se tiene que introducir el número de la tarjeta y su fecha de vencimiento para que pueda ser efectuada la transacción.

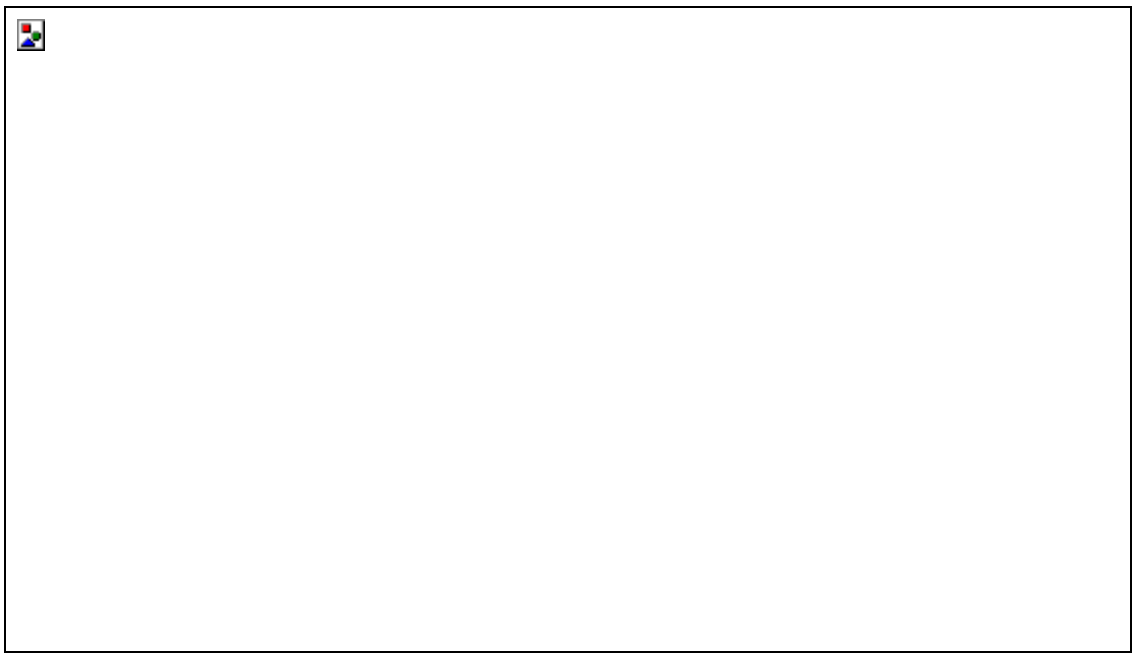


Si ud. es alumno o personal administrativo de la Universidad Don Bosco y decidió pagar por medio del PIN asignado por la Universidad, entonces sólo se llenará el número de Identificación (carnet o id del empleado) y el PIN asignado.

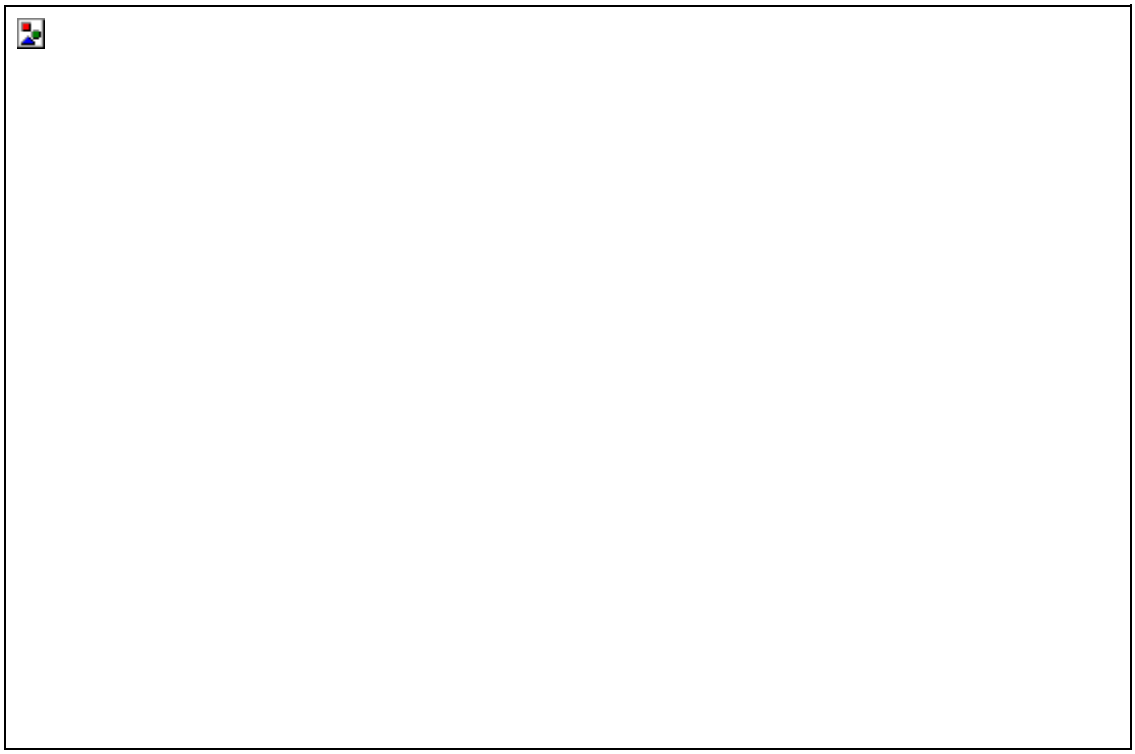


Después de esto sólo hay que esperar que la transacción haya sido aprobada....

si la trasacción fue aprobada aparecerá lo siguiente:



De lo contrario aparecerá lo siguiente:



Siguiente Anterior Contenido

SITIO DEL ADMINISTRADOR http://www.libudb.edu.sv/admon/

AYUDA DE SITIO DE ADMINISTRACION

- Introducción

- Mantenimientos

  Areas

  Autor

  Editoriales

  Formas de pago

  Libros

  Paises

  Proveedores

- Reporte de ventas

  Fecha

  Libro

  Area

- Consultas

  Niveles de existencia

  Temporales

Página Principal Siguiente

INTRODUCCION

El sitio de administración es de suma importancia para el funcionamiento de la Librería Virtual Don Bosco, por lo que es necesario saberlo utilizar bien.

La ayuda para todas las opciones, se describirán, de tal manera que sea fácil realizar todas las tareas a realizar.

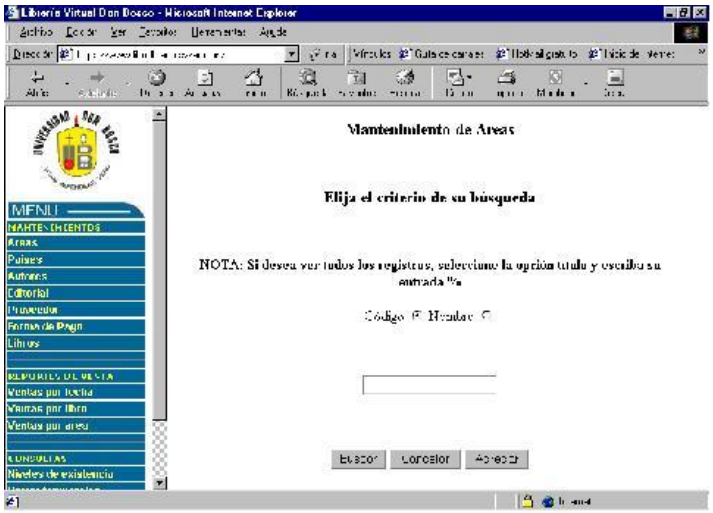
Se ha subdividido en una parte de Mantenimiento a las tablas de la base de datos que lo requieren, Reportes de Venta que son de suma importancia y otra parte para Consultas, sobre la información más importante que se necesita.

Página Principal Anterior Siguiente

AYUDA DE MANTENIMIENTO DE AREAS

Las áreas sirven para clasificar los libros en grupos, para facilitar las búsquedas a los usuarios y para llevar un mejor control de que tipo de libros son los más vendidos.

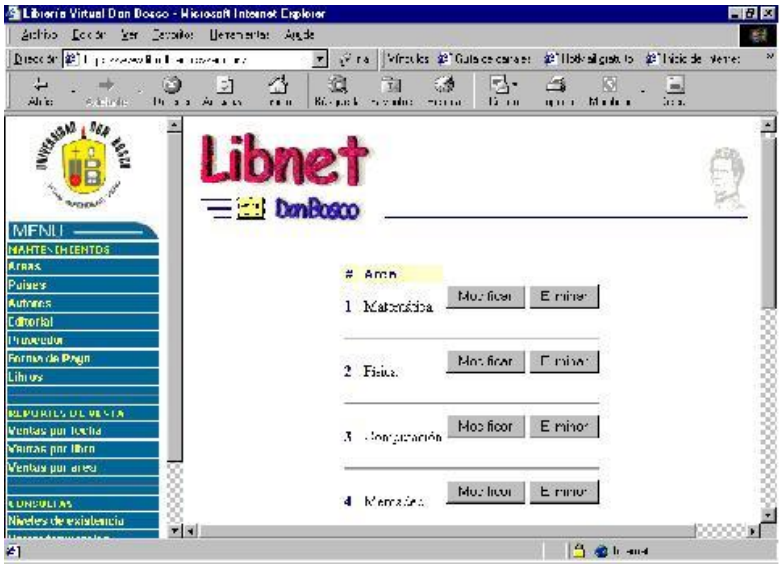
Al presionar la opción de área del grupo de Mantenimientos en el menú, aparece una página principal. Esta contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito.



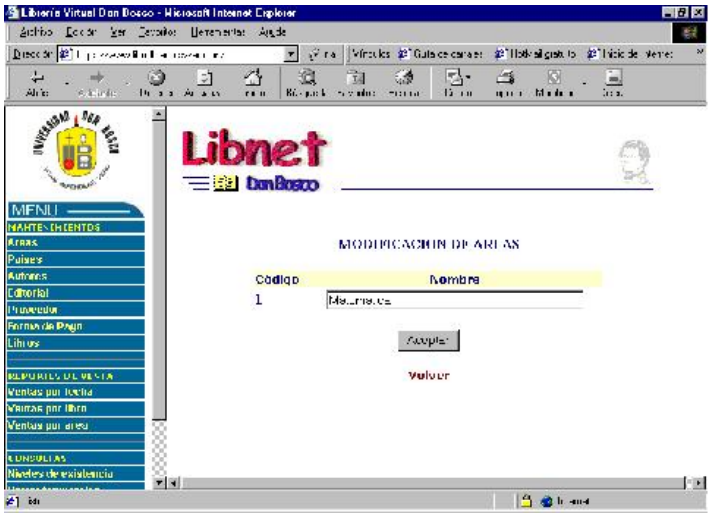
También existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del área que se desea y dar clic al botón de búsqueda, lo cual desplegará otra página con el o los registros seleccionados, si existen; si no se observará un página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.

En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje preguntando si se está seguro de eliminar el registro, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que el registro fue eliminado.

En la página de adición de áreas, deberá digitar únicamente el nombre del área y dar clic al botón de Agregar , lo cual desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.



En la página de modificación tendrá la opción de editar solamente el nombre del área al dar clic en la opción de Aceptar el registro es actualizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver.

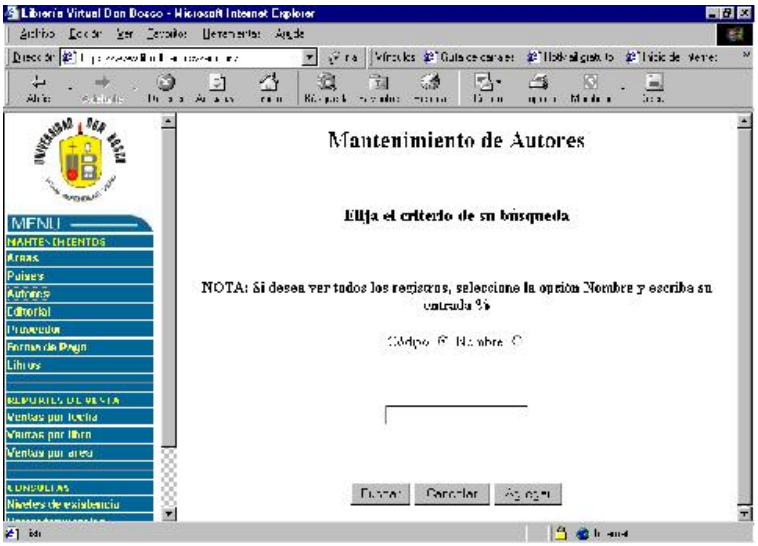


Página Principal Anterior Siguiente

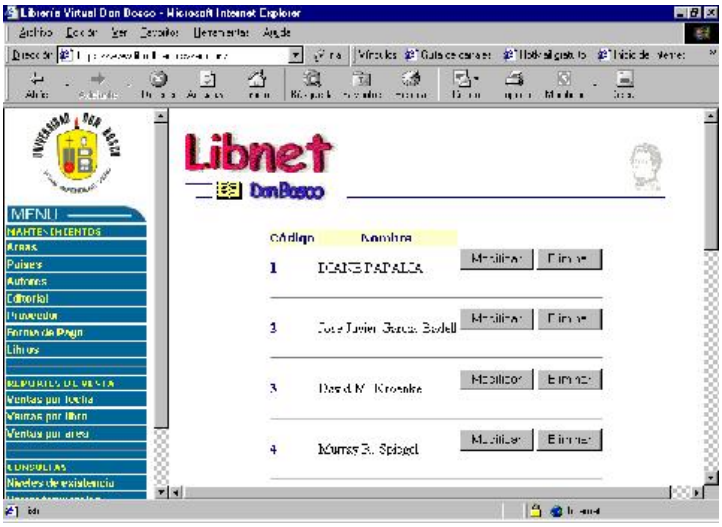
AYUDA DE MANTENIMIENTO DE AUTORES

Para tener información completa de los libros, se guardan datos de los autores como los nombres y apellidos, así se pueden realizar búsquedas de los libros utilizando como parámetro el nombre del autor.

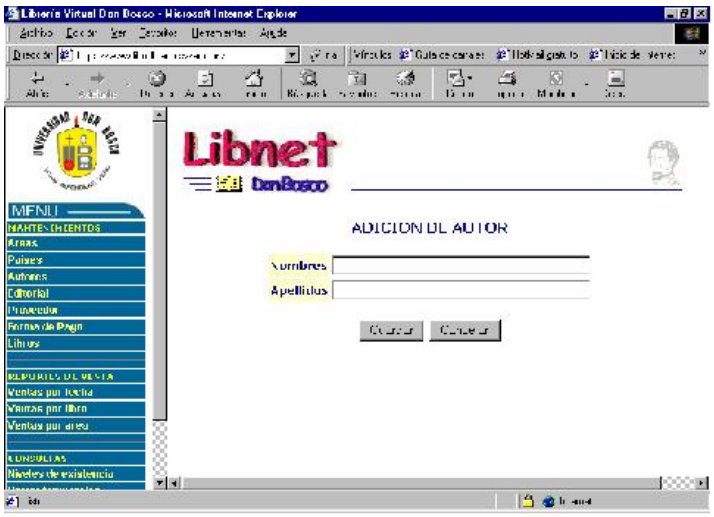
Al presionar la opción del mantenimiento de autor en el menú, aaprece una página principal, la cual contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito, también existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del autor que se desea y dar clic al botón de búsqueda, lo cual deplegará otra página con el o los registros seleccionados, si esxisten; si no se observará una página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.



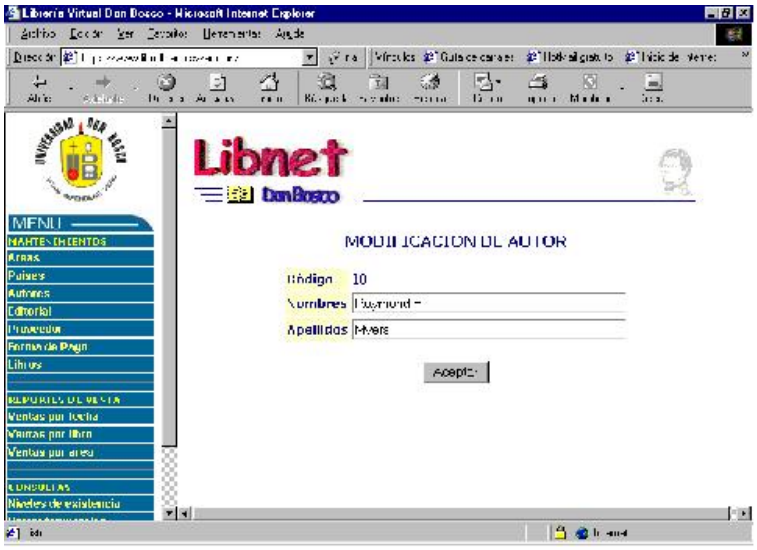
En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje preguntando si se está seguro de eliminar, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que la eliminación ha sido realizada.



En la página de adición de autores, deberá digitar el nombre(s) y el apellido(s) del autor y dar clic al botón de Agregar , lo cual desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.



En la página de modificación tendrá la opción de editar el nombre(s) y apellido(s) del autor al dar clic en la opción de Aceptar el registro es actulizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver a la página principal del mantenimiento.

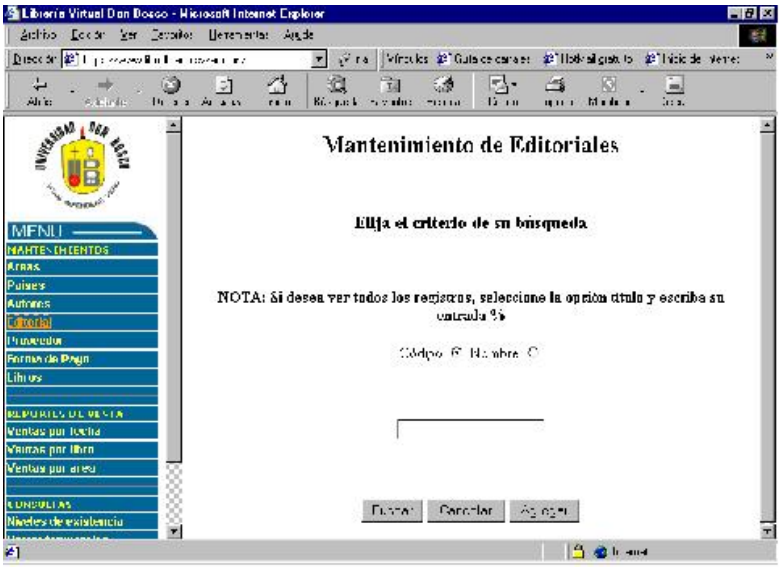


Página Principal Anterior Siguiente

AYUDA DE MANTENIMIENTO DE EDITORIALES

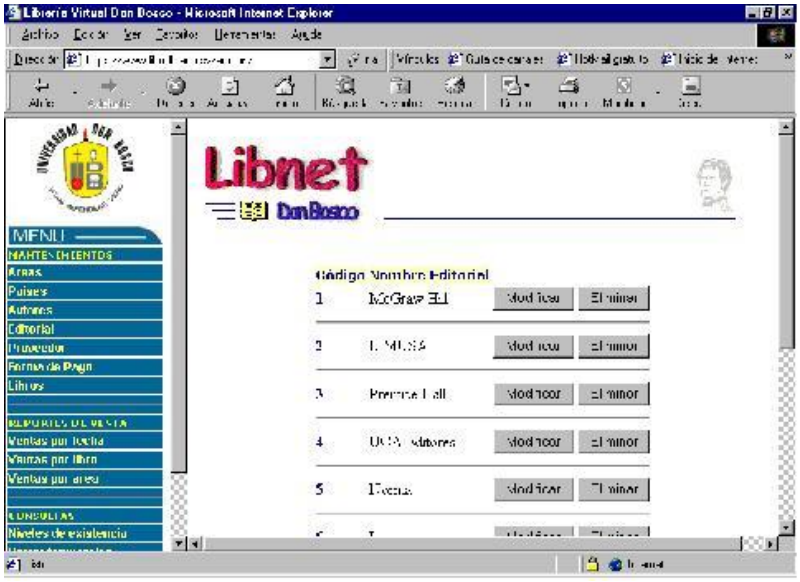
Para tener información completa de los libros, se guardan datos de las editoriales.

Al presionar la opción del mantenimiento de editorial en el menú, aparece una página principal, la cual contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito, también existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del editorial que se desea y dar clic al botón de búsqueda, lo cual desplegará otra página con el o los registros seleccionados, si existen; si no se observará una página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.

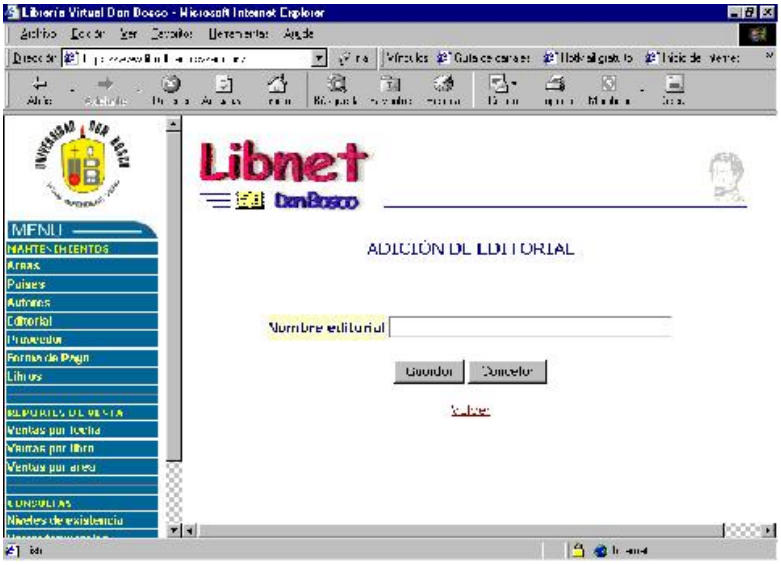


En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje

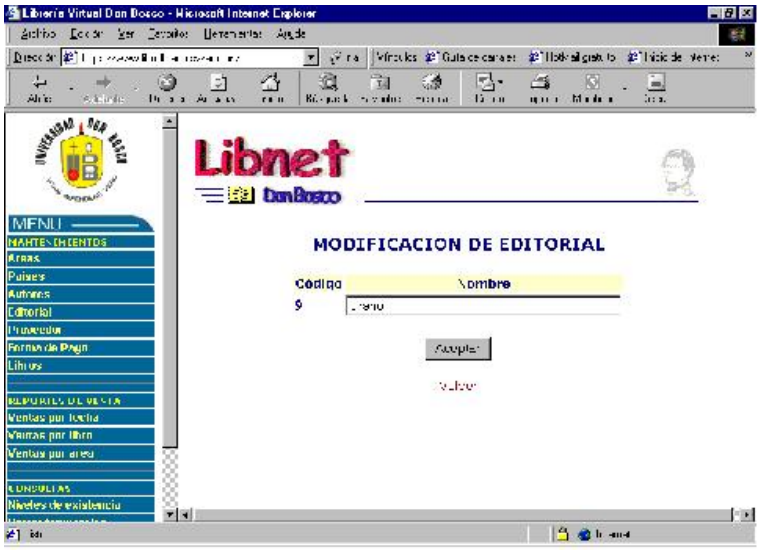
preguntando si se está seguro de eliminar, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que la eliminación ha sido realizada.



En la página de adición de editoriales, deberá digitar el nombre de la editorial y dar clic al botón de Agregar , lo cual desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.



En la página de modificación tendrá la opción de editar el nombre de la editorial, al dar clic en la opción de Aceptar el registro es actualizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver a la página principal del mantenimiento.

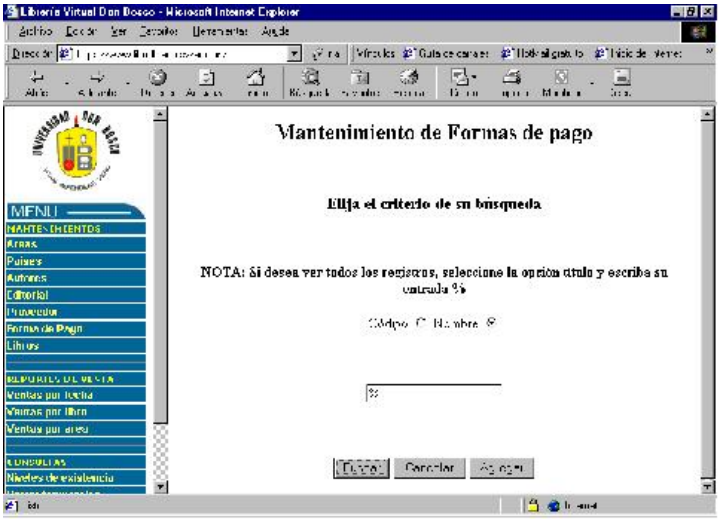


Página Principal Anterior Siguiente

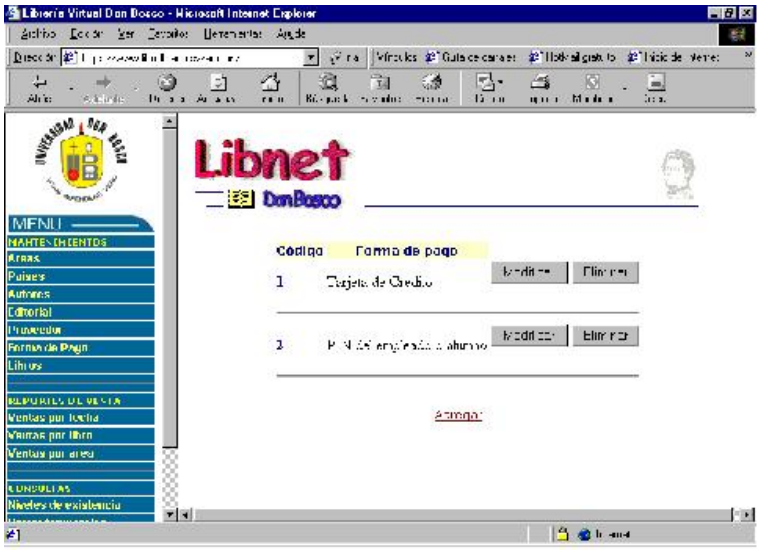
AYUDA DE MANTENIMIENTO DE FORMAS DE PAGO

Las formas de pago, indican el medio por el cual realizarán el pago por la compra los clientes, por ejemplo: si lo hará en efectivo o con tarjeta de crédito.

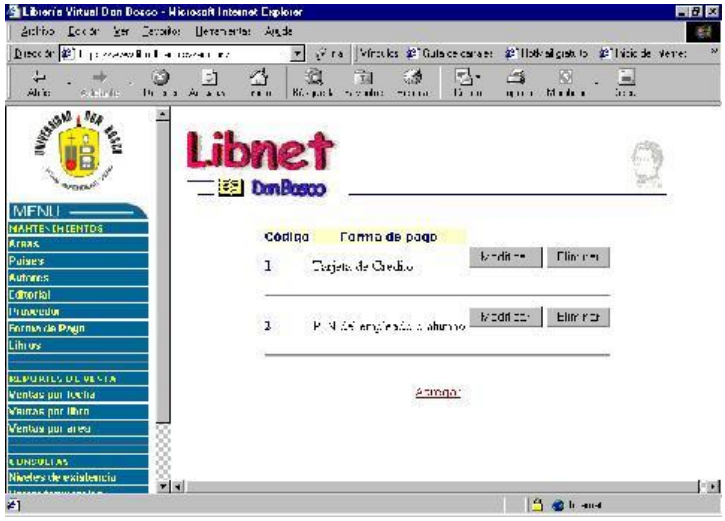
Al presionar la opción del mantenimiento de forma de pago en el menú, aparece una página principal, la cual contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito, también existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del forma de pago que se desea y dar clic al botón de búsqueda, lo cual desplegará otra página con el o los registros seleccionados, si existen; si no se observará una página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.



En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje preguntando si se está seguro de eliminar, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que la eliminación ha sido realizada.



En la página de adición de formas de pago, deberá digitar el nombre de la forma de pago y dar clic al botón de Agregar , lo cual desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.



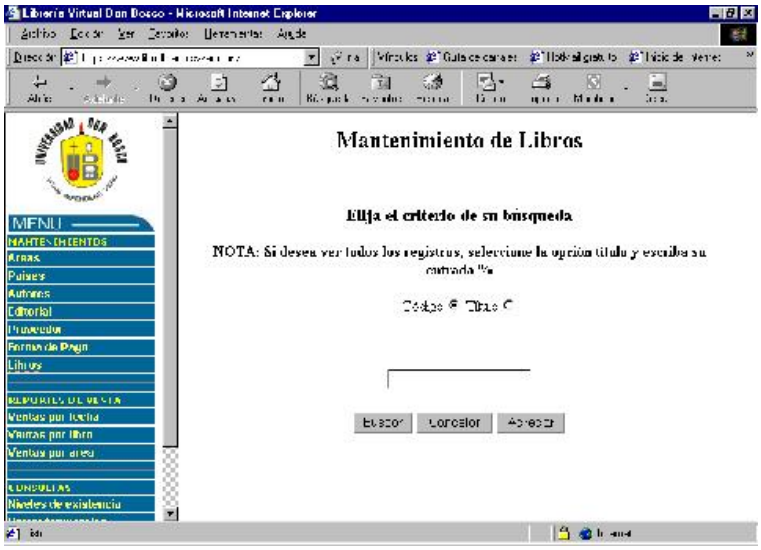
En la página de modificación tendrá la opción de editar el nombre de la forma de pago, al dar clic en la opción de Aceptar el registro es actulizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver a la página principal del mantenimiento.

Página Principal Anterior Siguiente

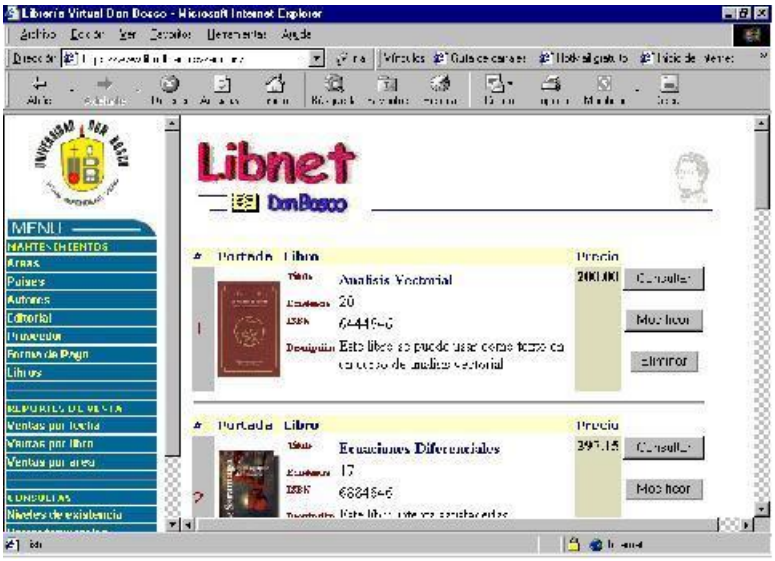
AYUDA DE MANTENIMIENTO DE LIBROS

Esta opción permitirá realizar cambios de varios datos indispensables acerca de los libros para que se pueda realizar la venta de éstos, llevar un control adecuado y mantener la información actualizada.

Al presionar la opción del mantenimiento de libro en el menú, aparece una página principal, la cual contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito, también existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del libro que se desea y dar clic al botón de búsqueda, lo cual desplegará otra página con el o los registros seleccionados, si existen; si no se observará una página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.



En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje preguntando si se está seguro de eliminar, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que la eliminación ha sido realizada.



En la página de adición de libros, deberá digitar el título, la descripción, el número de ISBN, el nombre del archivo de la imagen correspondiente al libro, el precio de compra, el precio de venta, el nivel mínimo que debe existir en inventario, el nivel máximo en existencia, así como elegir una opción de la lista desplegable que aparecerá para autor, área, editorial, luego que toda la información ha sido llenada correctamente, dar clic al botón de Agregar , si existen errores, se desplegará un mensales, si no se desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.

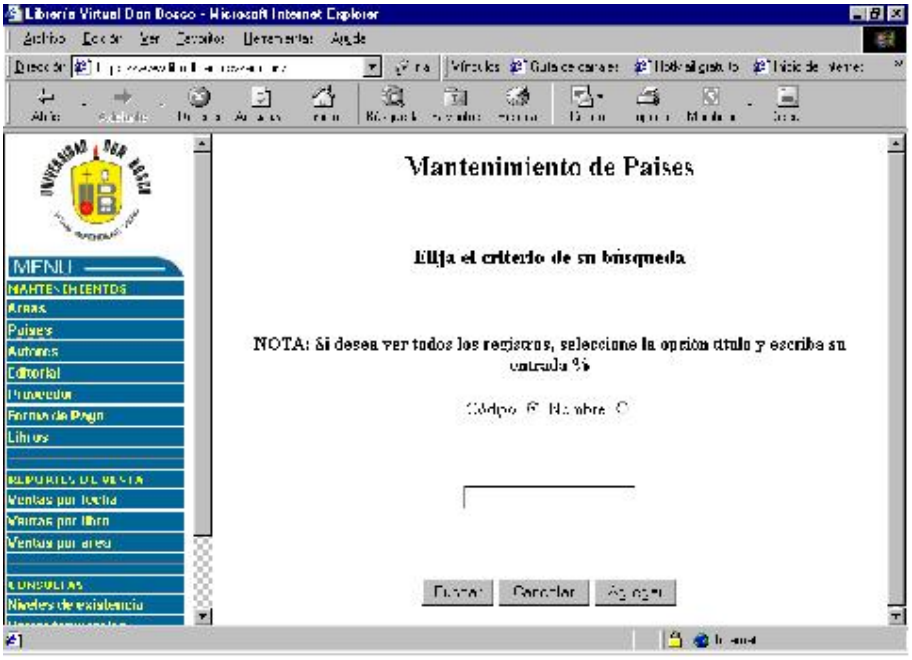
En la página de modificación tendrá la opción de editar los datos del libro seleccionado, como el título, descipción, nombre del archivo de la imagen, el número de ISBN, el nivel máximo y mínimo, el precio de costo y de venta, cambiar el autor, área o editorial; al dar clic en la opción de Aceptar el registro es actualizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver a la página principal del mantenimiento.

Página Principal Anterior Siguiente

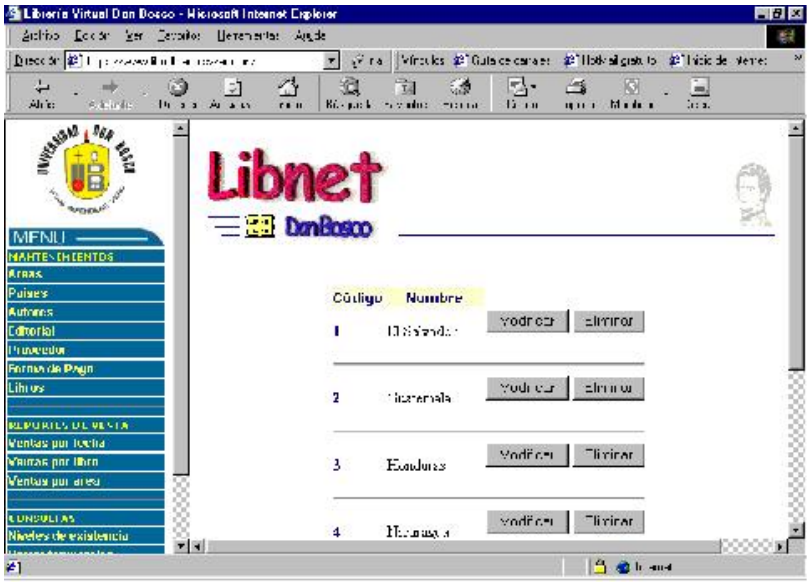
AYUDA DE MANTENIMIENTO DE PAISES

Al presionar la opción del mantenimiento de país en el menú, aparece una página principal, la cual contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito, también existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del país que se desea y dar clic al botón de búsqueda, lo cual desplegará otra página con

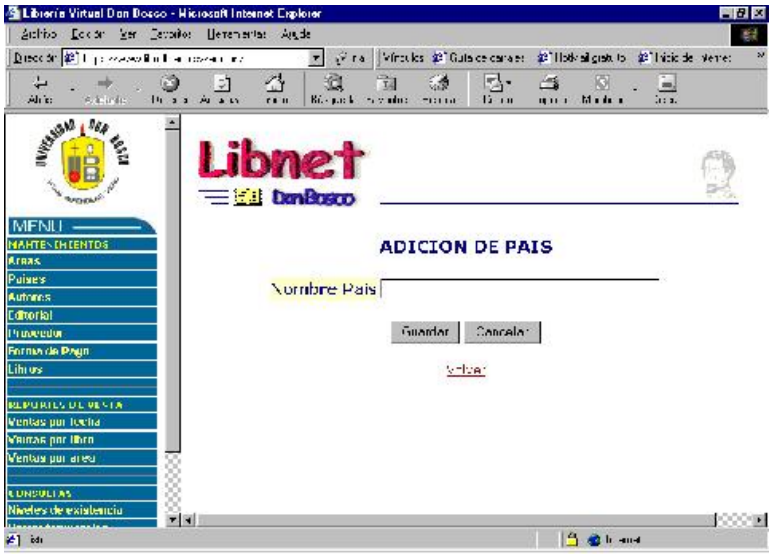
el o los registros seleccionados, si existen; si no se observará un página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.



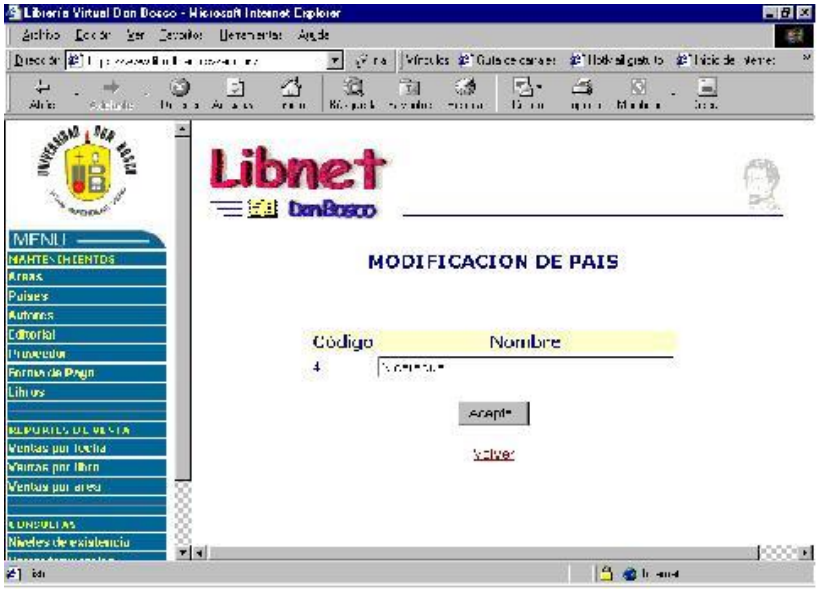
En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje preguntando si se está seguro de eliminar el registro, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que el registro fue eliminado.



En la página de adición de paises, deberá digitar únicamente el nombre del país y dar clic al botón de Agregar , lo cual desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.



En la página de modificación tendrá la opción de editar solamente el nombre del país al dar clic en la opción de Aceptar el registro es actualizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver.

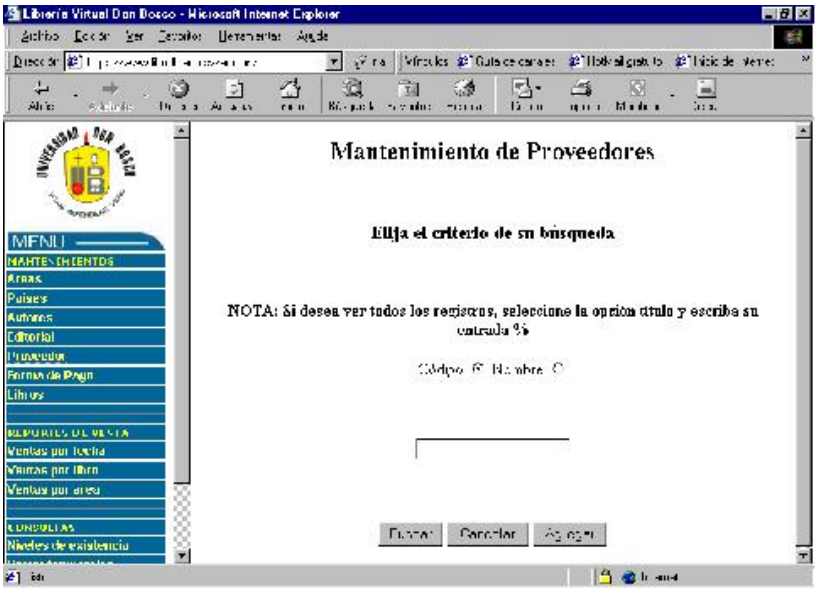


Página Principal Anterior Siguiente

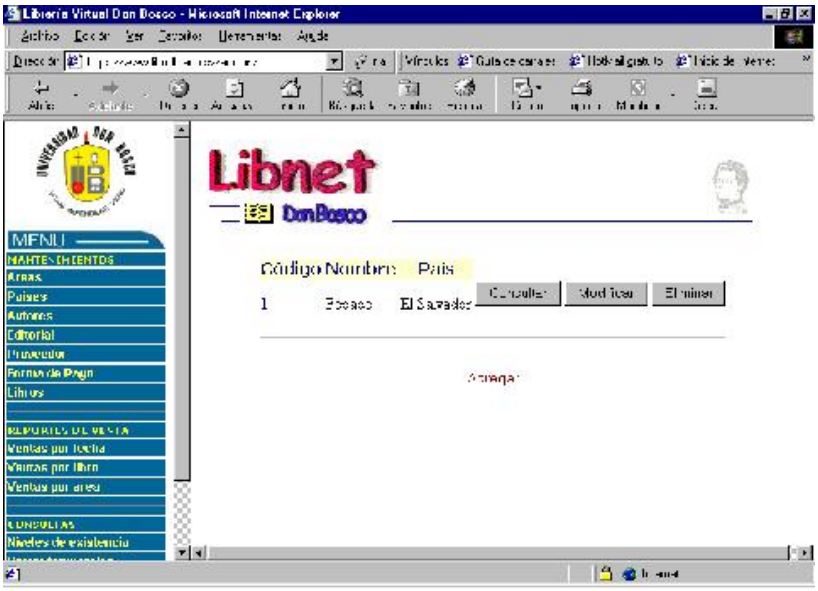
AYUDA DE MANTENIMIENTO DE PROVEEDORES

Acerca de los proveedores se guardan varios datos para facilitar el contacto constante que debe tenerse con ellos.

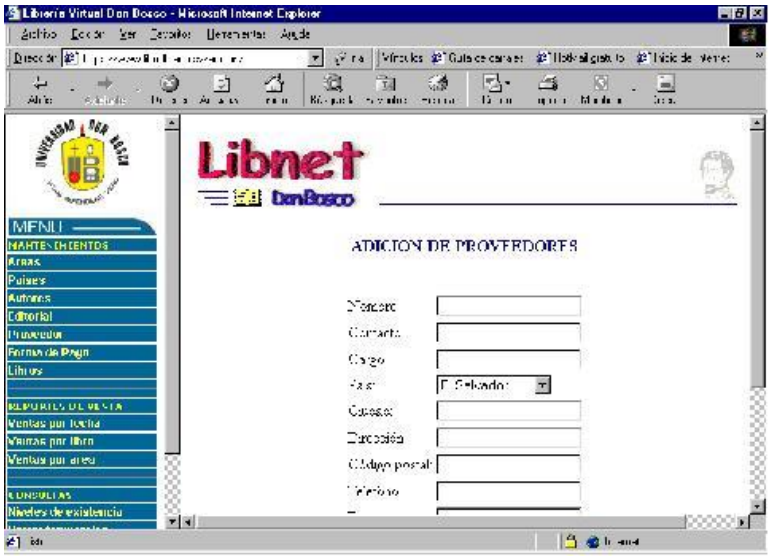
Al presionar la opción del mantenimiento de proveedor en el menú, aprece una página principal, la cual contiene una opción para agregar registros, la cual al dar clic en ésta nos mostrará una página para este propósito, también existen botones para elegir el criterio por el cual desea realizar la búsqueda del registro o registros, luego debe digitar el código o nombre del proveedor que se desea y dar clic al botón de búsqueda, lo cual deplegará otra página con el o los registros seleccionados, si esxisten; si no se observará una página que dirá que no existen registros con esos datos, con la opción de volver a la página anterior o agregar el registro.



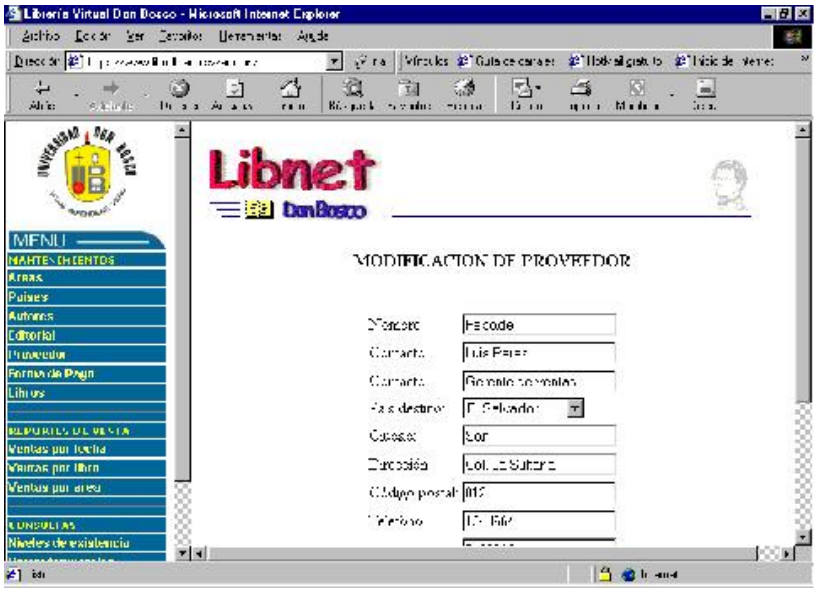
En la página de resultado que contendrá los registros encontrados, por cada registro tendrá opción de modificar o eliminar, además la opción de agregar. Para la opción de eliminar al dar clic en este botón, aprecerá un mensaje preguntando si se está seguro de eliminar, si se presiona el botón de cancelar no se elimina el registro, si se presiona el de aceptar, se despliega una página donde se confirma que la eliminación ha sido realizada.



En la página de adición de proveedores, deberá digitar el título, la descripción, el número de ISBN, el nombre del archivo de la imagen correspondiente al proveedor, el precio de compra, el precio de venta, el nivel mínimo que debe existir en inventario, el nivel máximo en existencia, así como elegir una opción de la lista desplegable que aparecerá para autor, área, editorial, luego que toda la información ha sido llenada correctamente, dar clic al botón de Agregar , si existen errores, se desplegará un mensales, si no se desplegará otra página confirmando que el registro ha sido agregado. También existe la opción de volver a la página anterior si no desea agregar registros.



En la página de modificación tendrá la opción de editar los datos del proveedor seleccionado, como el título, descipción, nombre del archivo de la imagen, el número de ISBN, el nivel máximo y mínimo, el precio de costo y de venta, cambiar el autor, área o editorial; al dar clic en la opción de Aceptar el registro es actualizado en la base de datos, lo cual desplegará otra página confirmando que la actualización se se ha llevado a cabo. Si no desea que la modificación se realice, tendrá la opción de volver a la página principal del mantenimiento.

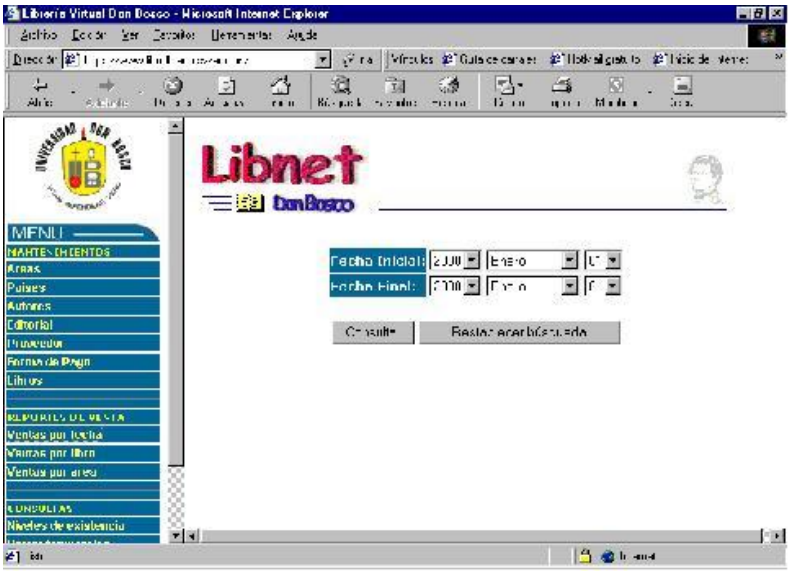


Página Principal Anterior Siguiente

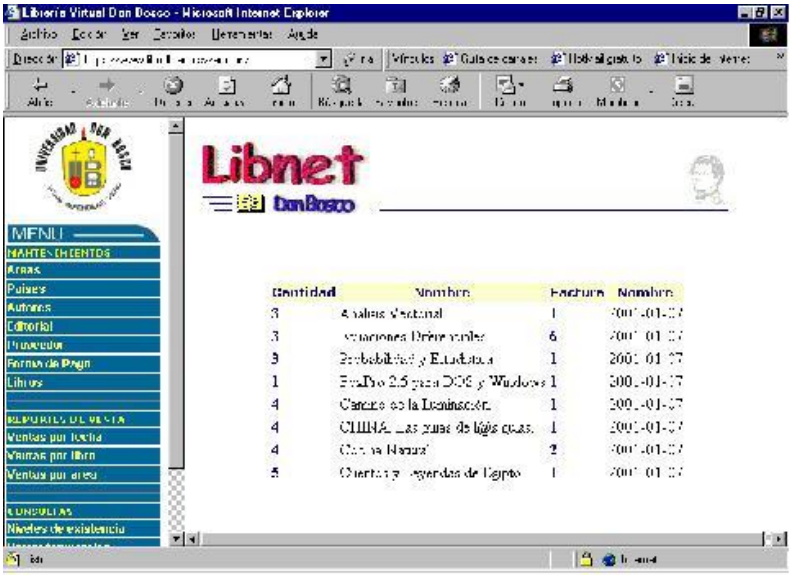
AYUDA DE REPORTE DE VENTAS POR FECHA

Esta opción permite mostrar las ventas que se han realizado para un período especificado.

Se deberá elegir una fecha inicial, y una fecha final,par amostrar las ventas que han sido realizado entre estas.



Luego se despliega la información respectiva.

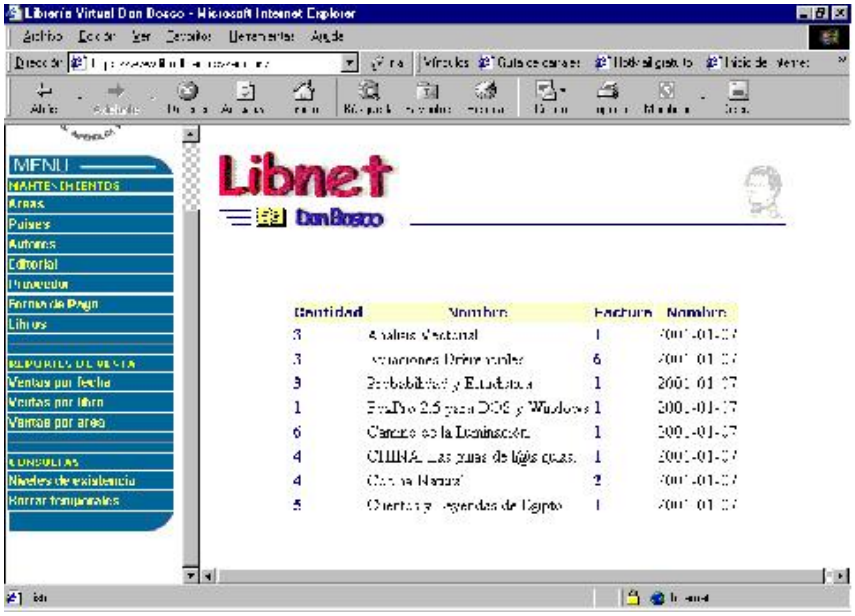


Página Principal Anterior Siguiente

AYUDA DE REPORTE DE VENTAS POR LIBRO

Esta opción permite mostrar las ventas que se han realizado para un libro especificado.

Se tendrá opción de elegir el código o el título del libro del cual desea consultar las ventas.

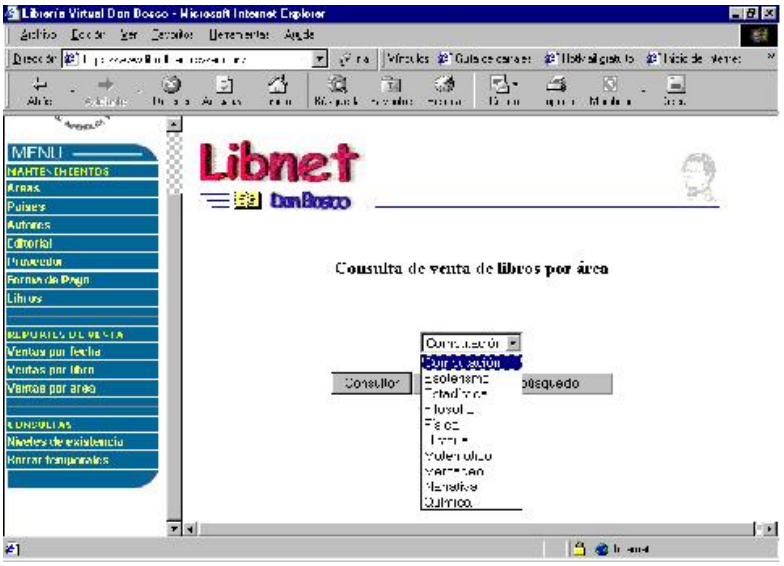


Luego se despliega la información respectiva.

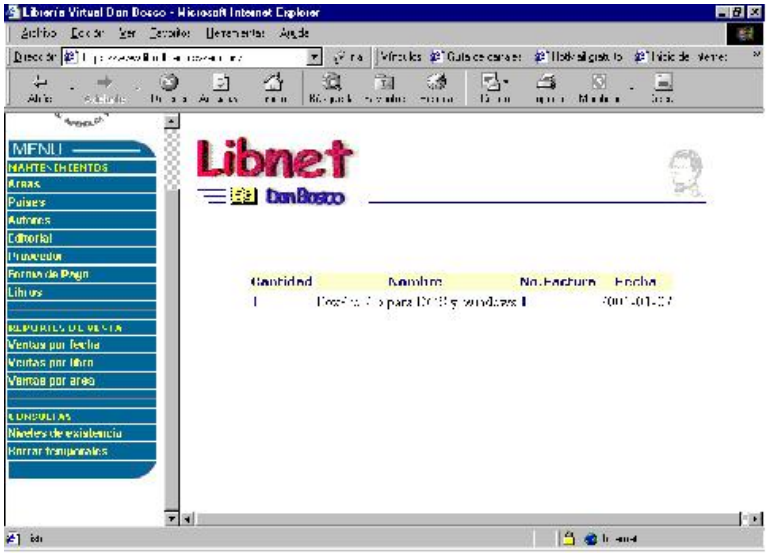
Página Principal Anterior Siguiente

AYUDA DE REPORTE DE VENTAS POR AREA

Esta opción permite mostrar las ventas que se han realizado por área de libros.



Se tendrá opción de selecionar el área a la que pertenencen lo libros de los cuales se desea consultar las ventas.

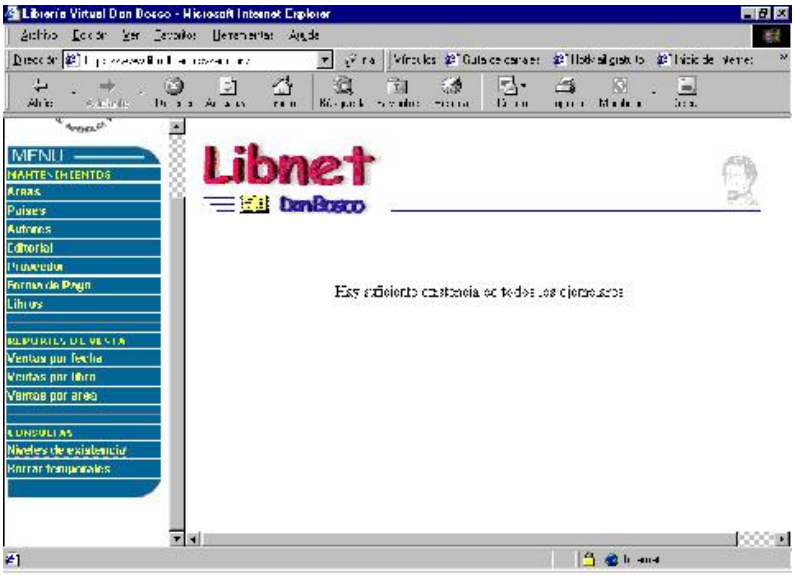


Luego se despliega la información respectiva.

Página Principal Anterior Siguiente

AYUDA DE CONSULTA DE NIVEL DE EXISTENCIA

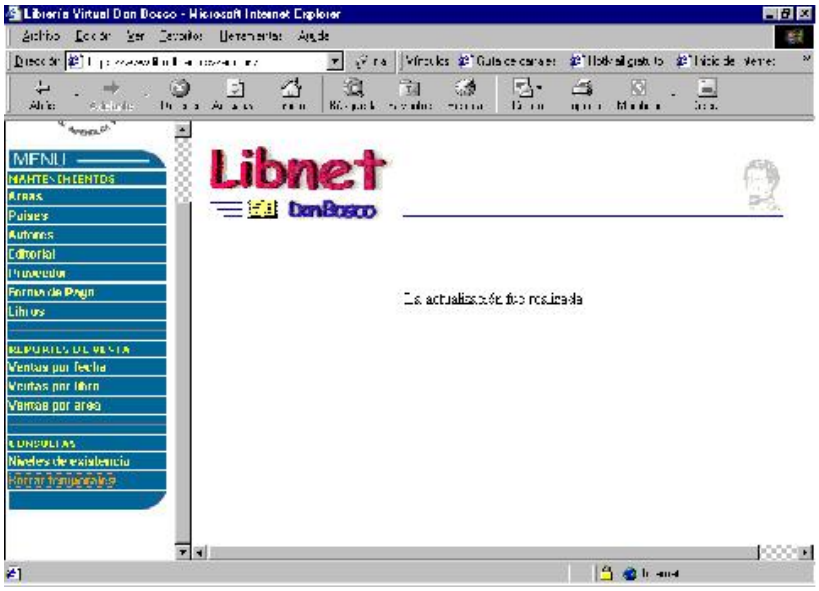
Esta opción permite mostrar los títulos para los cuales los niveles de existencia son próximos al nivel mínimo requerido.



Página Principal Anterior

AYUDA DE ACTUALIZACIÓN DE TEMPORALES

Permite llevar una adecuado control de datos que deben ser manejados de manera temporal para que las bases de datos no crezcan demasiado, con datos innecesarios.



ANEXO D

CRIPTOGRAFÍA

Introducción

La palabra criptografía proviene del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o descencriptar)

Desde sus inicios la criptografía llegó a ser una herramienta muy usada en el ambiente militar, por ejemplo en la segunda gran guerra tuvo un papel determinante, una de las máquinas de cifrado que tuvo gran popularidad se llamó **ENIGMA**. Al terminar la guerra las agencias de seguridad de las grandes potencias invirtieron muchos recursos para su investigación. La criptografía como la conocemos hoy, surgió con la invención de la computadora.

La criptografía actual se inicia en la segunda mitad de la década de los años 70. No es hasta la invención del sistema conocido como **DES** (**D**ata **E**ncryption **S**tandard) en 1976 que se da a conocer mas ampliamente, principalmente en el mundo industrial y comercial. Posteriormente con el sistema **RSA** (**R**ivest, **S**hamir, **A**dleman) en 1978, se abre el comienzo de la criptografía en un gran rango de aplicaciones: en transmisiones militares, en transacciones financieras, en comunicación de satélite, en redes de computadoras, en líneas telefónicas, en transmisiones de televisión etcétera.

La criptografía se divide en dos grandes ramas, la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica, **DES** pertenece al primer grupo y **RSA** al segundo.

Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo.

La privacidad, se refiere a que la información sólo pueda ser leída por personas autorizadas.
Ejemplos: en la comunicación por teléfono, que alguien intercepte la comunicación y escucha la conversación quiere decir que no existe privacidad. Si mandamos una carta y por alguna razón alguien rompe el sobre para leer la carta, ha violado la privacidad.
En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación. Por lo tanto al cifrar (esconder) la información cualquier intercepción no autorizada no podrá entender la información. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

La integridad, se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Ejemplos: cuando compramos un boleto de avión y están cambiados los datos del vuelo, puede afectar los planes del viajero. Una vez hecho un deposito en el banco, si no es capturada la cantidad correcta causará problemas. La integridad es muy importante en las transmisiones militares ya que un cambio de información puede causar graves problemas.
En internet las compra se puede hacer desde dos ciudades muy distantes, la información tiene necesariamente que viajar por una línea de transmisión de la cual no se tiene control, si no existe integridad podrían cambiarse por ejemplo el número de una tarjeta de crédito, los datos del pedido en fin información que causaría problemas a cualquier comercio y cliente.
La integridad también se puede solucionar con técnicas criptográficas particularmente con procesos simétricos o asimétricos.

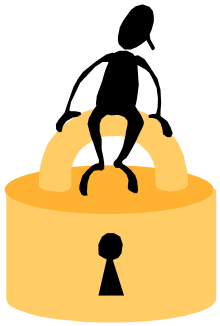
La autenticidad, se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

Ejemplo: cuando se quiere cobrar un cheque a nombre de alguien, quien lo cobra debe de someterse a un proceso de verificación de identidad para comprobar que en efecto es la persona quien dice ser, esto en general se lleva a cabo con una credencial que anteriormente fue certifica y acredita la identidad de la persona que la porta. La verificación se lleva a cabo comparando la persona con una foto o con la comparación de una firma convencional.

Por internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad, resolver este problema es por lo tanto muy importante para efectuar comunicación confiable.

Las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usan quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, de algún modo ésta reemplaza a la firma autógrafa que se usa comúnmente. Para autenticar mensajes se usa criptografía simétrica.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado.



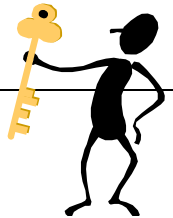
Información Segura **Persona Autorizada**

Cuando se diseña un sistema de seguridad, una gran cantidad de problemas puedes ser evitados si se puede comprobar autenticidad, garantizar privacidad, asegurar integridad y evitar el no-rechazo.

La criptografía simétrica y asimétrica conjuntamente con otras técnicas, como el buen manejo de las claves y la legislación adecuada resuelven satisfactoriamente los anteriormente problemas planteados, como lo veremos en los capítulos posteriores.

Criptografía Simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.



Este tipo de criptografía se conoce también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias, la criptografía simétrica de bloques (block cipher), la criptografía simétrica de lluvia (stream cipher) y la criptografia simétrica de resumen (hash functions). Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones.

La criptografía simétrica ha sido la más usada en toda la historia, ésta a podido ser implementada en diferente dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, **DES**.

DES es un sistema criptográfico, que toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, una clave de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usada como de paridad.

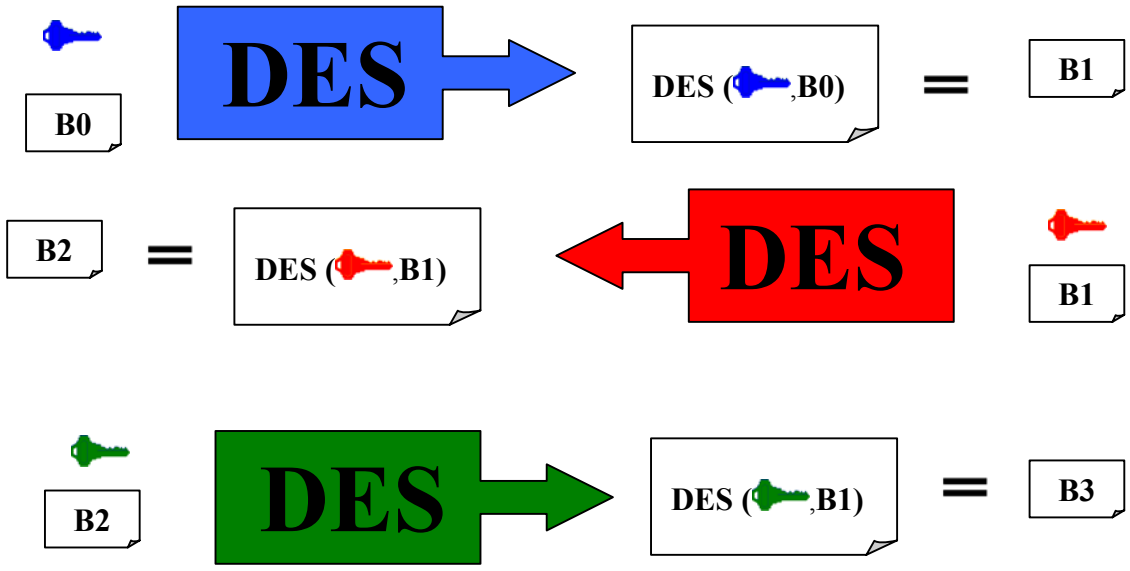
Dependiendo de la naturaleza de la aplicación DES tiene 4 modos de operación para poder implementarse: **ECB** (**E**lectronic **C**odebook **M**ode) para mensajes cortos, de menos de 64 bits, **CBC** (**C**ipher **B**lock **C**haining **M**ode) para mensajes largos, **CFB** (**C**ipher **B**lock **F**eedback) para cifrar bit por bit ó byte por byte y el **OFB** (**O**utput **F**eedback **M**ode) el mismo uso pero evitando propagación de error.

En la actualidad no se ha podido romper el sistema **DES** desde la perspectiva de poder deducir la clave simétrica a partir de la información interceptada, sin embargo con un método a fuerza bruta, es decir probando alrededor de 2^{56} posibles claves, se pudo romper **DES** en Enero de 1999. Lo anterior quiere decir que, es posible obtener la clave del sistema **DES** en un tiempo relativamente corto, por lo que lo hace inseguro para propósitos de alta seguridad. La opción que se ha tomado para poder suplantar a **DES** ha sido usar lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave, esto a tomado la forma de un nuevo sistema de cifrado que se conoce actualmente como **triple-DES** o **TDES**.

TDES El funcionamiento de **TDES** consiste en aplicar 3 veces **DES** de la siguiente manera: la primera vez se usa una clave **K1**(azul) junto con el bloque **B0**, de forma ordinaria **E** (de Encription), obteniendo el bloque **B1**. La segunda ves se toma a **B1** con la clave **K2** (roja), diferente a **K1** de forma inversa, llamada **D** (de Descencription) y la

tercera vez a **B2** con una clave **K3** (verde) diferente a **K1** y **K2**, de forma ordinaria **E** (de Encription), es decir, aplica de la interacción 1 a la 16 a **B0** con la clave **K1**, después aplica de la 16 a la 1, a **B1** con la clave **K2**, finalmente aplica una vez mas de la 1 a la 16 a **B2** usando la clave **K3**, obteniendo finalmente a **B3**. En cada una de estas tres veces aplica el modo de operación más adecuado.

El proceso del cifrado con **TDES** se puede apreciar en las siguientes figuras:



Este sistema **TDES** usa entonces una clave de 168 bits, aunque se ha podido mostrar que los ataques actualmente pueden romper a **TDES** con una complejidad de 2^{112}, es decir efectuar al menos 2^{112} operaciones para obtener la clave a fuerza bruta, además de la memoria requerida.

Se optó por TDES ya que es muy fácil Inter-operar con **DES** y proporciona seguridad a mediano plazo.

En los últimos 20 años se han diseñado una gran cantidad de sistemas criptográficos simétricos, entre algunos de ellos están: **RC-5**, **IDEA**, **FEAL**, **LOKI'91**, **DESX**, **Blowfish**, **CAST, GOST,** etcétera. Sin embargo no han tenido el alcance de **DES**, a pesar de que algunos de ellos tienen mejores propiedades.

Podemos afirmar que el estado actual de la criptografía simétrica es la búsqueda de un nuevo sistema que pueda reemplazar a **DES** en la mayor parte de aplicaciones. Es así como se ha optado por convocar a un concurso de sistemas criptográficos simétricos y que este decida quien será el nuevo estándar al menos para los próximos 20 años.

AES El **NIST** (**N**ational **I**nstitute of **S**tandards **T**echnology) convocó a un concurso para poder tener un sistema simétrico que sea seguro y pueda usarse al menos en los próximos 20 años como estándar. En la mitad del año de 1998 se aceptaron 15 candidatos, estos se han sometido a pruebas públicas y por parte del **NIST**. Actualmente se cuentan con 5 finalistas que son: **MARS**, **RC6**, **Rijndael**, **Serpent**, y **Twofish**, se espera que el candidato elegido se tenga a mediados del año 2000.

Las principales características que se pide a **AES** son que al menos sea tan seguro y rápido como **TDES**, es decir, que al menos evite los ataques conocidos. Además de que pueda ser implementado en una gran parte de aplicaciones. Una vez designado **AES** este podrá ser usado tanto como cifrador de bloques (block cipher), como cifrador de lluvia (stream cipher), como función resumen (hash function), y como generador de números seudoaleatorios.

Los cifradores de flujo o stream ciphers, son usados donde se cuente con un ancho de banda restringido (el número de bits que se transmiten a la vez), además de que se requiere independencia en los bloques transmitidos, entonces la mejor opción es cifrar bit por bit o byte por byte, este tipo de cifradores tiene la característica además de ser muy rápido. Los algoritmos más conocidos de este tipo están **RC-4**, **SEAL** y **WAKE.**

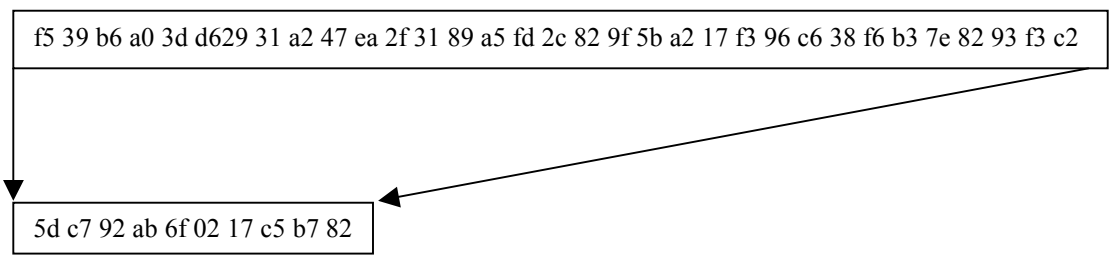
Entre los ataques más potentes a la criptografía simétrica están el criptoanálisis diferencial y lineal, sin embargo no han podido ser muy eficientes en la práctica por lo tanto, por el momento después de que un sistema criptografíco es publicado y se muestra inmune a estos dos tipos de ataques (y algunos otros más) la mayor preocupación es la longitud de las claves.

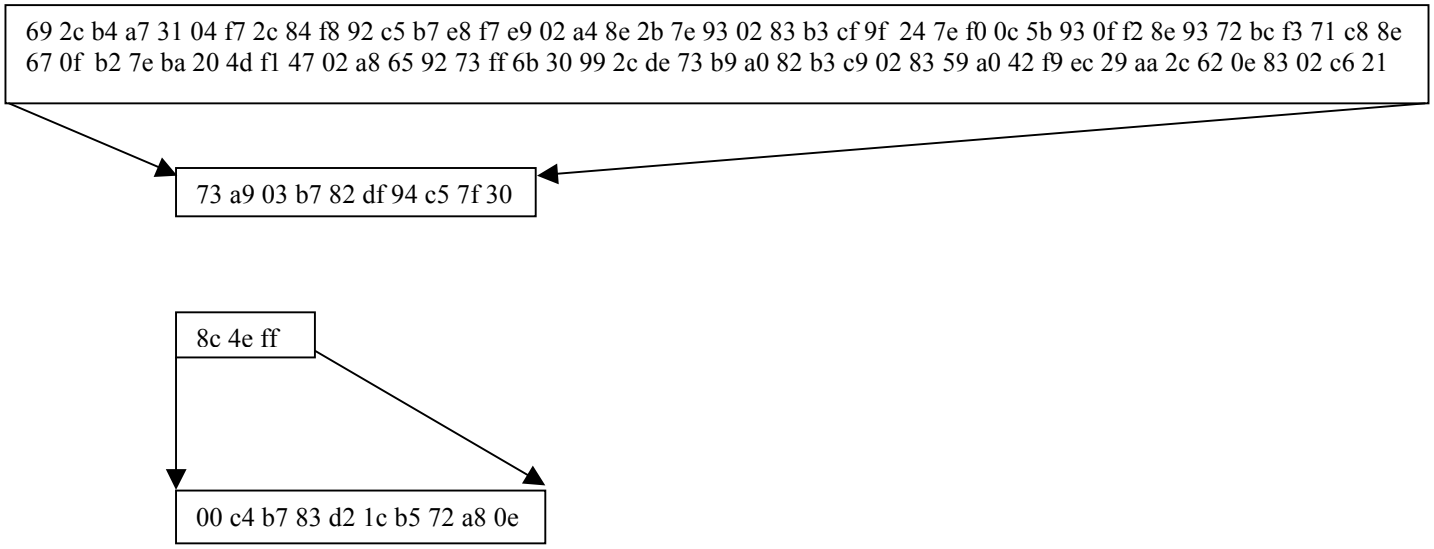
Funciones Hash

Una herramienta fundamental en la cripotografía, son las funciones hash, son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.

Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función hash les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital.

De forma gráfica la función hash efectúa lo siguiente:





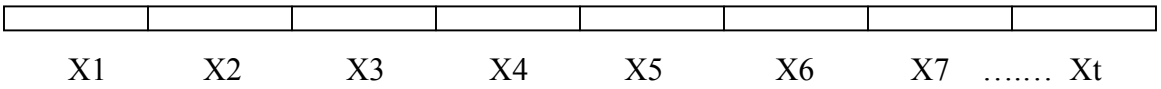
Esto es, un mensaje de longitud arbitraria lo transforma de forma "única" a un mensaje de longitud constante.

¿Cómo hace esto?

La idea general es la siguiente:

La función hash toma como entrada una cadena de longitud arbitraria, digamos 5259 bits, luego divide éste mensaje en pedazos iguales, digamos de 160bits, como en este caso y en general el mensaje original no será un múltiplo de 160, entonces para completar un número entero de pedazos de 160 bits al último se le agrega un relleno, digamos de puros ceros. En nuestro caso en 5259 caben 32 pedazos de 160 bits y sobran 139, entonces se agregaran 21 ceros más.

Entonces el mensaje toma la forma X = X1, X2, X3,…,Xt donde cada Xi tiene igual longitud (160bits por ejemplo).



Posteriormente se asocia un valor constante a un vector inicial IV y

H0=IV

Ahora se obtiene H1 que es el resultado de combinar H0 con X1 usando una función de compresión *f*

H1 = *f*(H0,X1)

Posteriormente se obtiene H2, combinando H1 y X2 con f

H2 = *f*(H1,X2)

Se hace lo mismo para obtener H3

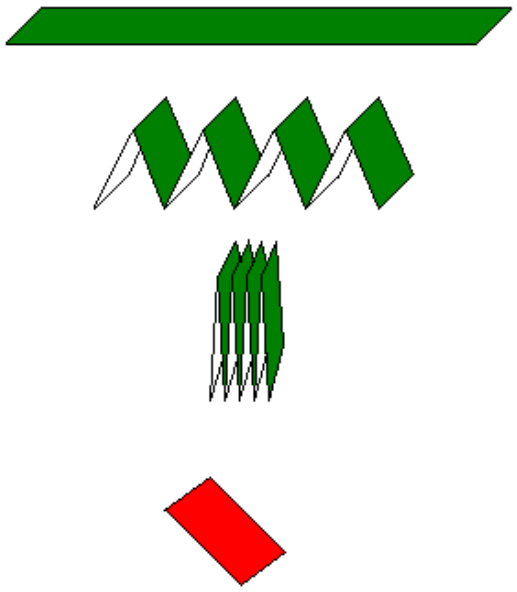
H3 = *f*(H2,X3)

Hasta llegar a Ht

Ht = *f*(Ht-1, Xt)

Entonces el valor hash será $h(M) = Ht$

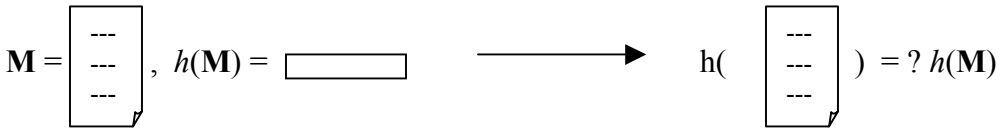
De alguna forma lo que se hace es tomar el mensaje partirlo en pedazos de longitud constante y combinar de alguna forma pedazo por pedazo hasta obtener un solo mensaje de longitud fija como muestra la figura siguiente:



Las funciones hash (o primitivas hash) pueden operar como: **MDC** (**M**odification **D**etection **C**odes) ó **MAC** (**M**assage **A**uthentication **C**odes).

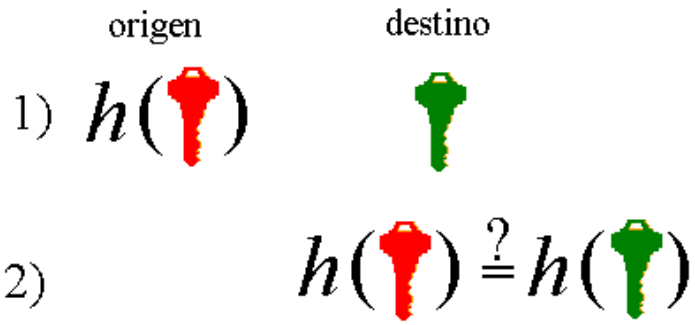
Los **MDC** sirven para resolver el problema de la integridad de la información, al mensaje se le aplica un **MDC** (una función hash) y se manda junto con el propio mensaje, al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes.

Es decir, se aplica un hash al mensaje **M** y se envía con el mensaje (**M**, *h*(**M**)), cuando se recibe se le aplica una vez más el hash (ya que **M** es público) obteniendo *h*'(**M**), si *h*(**M**)=*h*'(**M**), entonces se acepta que el mensaje se a transmitido sin alteración.



Los **MAC** sirven para autenticar el origen de los mensajes (junto con la integridad), un **MAC**. Es decir, se combina el mensaje **M** con una clave privada **K** y se les aplica un hash *h*(**M,K**), si al llegar a su destino *h*(**M, K**) se comprueba de integridad de la clave privada **K**, entonces se demuestra que el origen es solo el que tiene la misma clave **K**, probando así la autenticidad del origen del mensaje.

De forma simple se muestra en la siguiente figura el funcionamiento de un **MAC**.



Las propiedades que deben de tener las primitivas hash son:

1) **Resistencia a la preimagen**: significa que dada cualquier imagen, es cómputacionalmente imposible encontrar un mensaje *x* tal que *h*(*x*)=*y*. Otra forma como se conoce esta propiedad es que *h* sea de un solo sentido.
2) **Resistencia a una 2° preimagen**: significa que dado *x*, es cómputacionalmente imposible encontrar una *x*' tal que *h*(*x*)=*h*(*x*'). Otra forma de conocer esta propiedad es que h sea resistente a una colisión suave.
3) **Resistencia a colisión**: significa que es cómputacionalmente imposible encontrar dos diferentes mensajes *x*, *x*' tal que *h*(*x*)=*h*(*x*'). Esta propiedad también se conoce como resistencia a colisión fuerte.

Para ilustrar la necesidad de estas propiedades veamos los siguientes ejemplos:

Consideremos un esquema de firma digital con apéndice, entonces la firma se aplica a $h(x)$, en este caso h debe ser un **MDC** con resistencia a una 2° preimagen, ya que de lo contrario un atacante **C** que conozca la firma sobre $h(x)$, puede encontrar otro mensaje x' tal que $h(x) = h(x')$ y reclamar que la firma es del documento x'.

Si el atacante **C** puede hacer que el usuario firme un mensaje, entonces el atacante puede encontrar una colisión (x, x') (en lugar de lo más difícil que es encontrar una segunda preimagen de x) y hacer firmar al usuario a x diciendo que firmo x'. En este caso es necesaria la propiedad de resistencia a colisión.

Por último si (e,n) es la clave pública **RSA** de **A**, **C** puede elegir aleatoriamente un y y calcular $z = y^e \bmod n$, y reclamar que y es la firma de z, si **C** puede encontrar una preimagen x tal que $z = h(x)$, donde x es importante para **A**. Esto es evitable si h es resistente a preimagen.

Las funciones hash más conocidas son las siguientes: las que se crean a partir de un block cipher como **DES**, **MD5**, **SHA-1**, y **RIPEMD 160**.

Actualmente se ha podido encontrar debilidades en las funciones hash que tienen como salida una cadena de 128 bits, por lo que se ha recomendado usar salidas de 160bits. Así mismo se han encontrado ataques a **MD5** y **SHA-0** (antecesora de **SHA-1**), esto ha dado lugar que se dirija la atención sobre la función has **RIPEMD-160**.

El ataque más conocido (a fuerza bruta) a una función hash es conocido como "birthday attack" y se basa en la siguiente paradoja, si hay 23 personas en un local existe una probabilidad de al menos 1/2, de que existan dos personas con el mismo cumpleaños. Aunque parezca muy difícil esa posibilidad se puede mostrar que en general al recorre la raíz cuadrada del número de un conjunto de datos, se tiene la probabilidad de al menos ½ de encontrar dos iguales.

Al aplicar esto a una función hash, es necesario recorrer entonces la raíz cuadrada de 2^{160} mensajes para poder encontrar dos con el mismo hash, o sea encontrar una colisión. Por lo tanto una función hash son salida 2^{160} tiene una complejidad de 2^{80}, y una función de 128 bits de salida tiene una complejidad de 2^{64}, por lo que es recomendable usar actualmente salida de 160 bits.

Criptografía Asimétrica

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Hellman, proponen una forma

para hacer esto, sin embargo no fue hasta que el popular método de **R**ivest **S**hamir y **A**dleman **RSA** publicado en 1978, cuando toma forma la criptografía asimétrica, su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

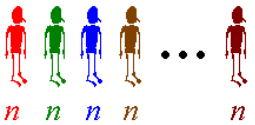
Actualmente la Criptografía asimétrica es muy usada, sus dos principales aplicaciones son el intercambio de claves privadas y la firma digital, una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica pertenecen a la teoría de números.

En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias según el problema matemático del cual basan su seguridad. La primera familias la que basa su seguridad en el **P**roblema de **F**actorización **E**ntera **PFE**, los sistemas que pertenecen a esta familia son, el sistema **RSA**, y el de **R**abin **W**illiams **RW**. La segunda familia es la que basa su seguridad en el **P**roblema del **L**ogaritmo **D**iscreto **PLD**, a esta familia pertenece el sistema de **D**iffie **H**ellman **DH** de intercambio de claves y el sistema **DSA** de firma digital. La tercera familia es la que basa su seguridad en el **P**roblema del **L**ogaritmo **D**iscreto **E**líptico **PLDE**, en este caso hay varios esquemas tanto de intercambio de claves como de firma digital que existen como el **DHE** (Diffie Hellman Elíptico), **DSAE**, (**N**yberg-**R**ueppel) **NRE**, (**M**enezes, **Q**u, **V**anstone) **MQV**, etcétera.

Aunque a las familias anteriores pertenecen los sistemas asimétricos más conocidos, existen otro tipo de sistemas que basan su seguridad en problemas diferentes como por ejemplo, en el Problema del Logaritmo Discreto Hiperelíptico, sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

RSA, en el caso de **RSA** el problema matemático es el de la factorización de un número entero *n* grande (1024 bits), este número entero se sabe es producto de dos números primos *p,q* de la misma longitud, entonces la clave pública es el número *n* y la privada es *p,q*. El razonamiento del funcionamiento de **RSA** es el siguiente:

a) a cada usuario se le asigna un número entero *n*, que funciona como su clave pública
b) solo el usuario respectivo conoce la factorización de *n* (o sea *p,q*), que mantiene en secreto y es la clave privada

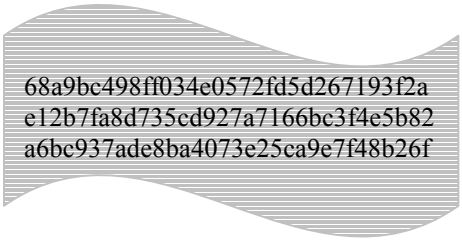


c) existe un directorio de claves públicas

d) si alguien quiere mandar un mensaje *m* a algún usuario entonces elige su clave pública *n* y con información adicional también pública puede mandar el mensaje cifrado **c**, que solo podrá descifrar el usuario correspondiente, el mensaje *m* convertido a número (codificación) se somete a la siguiente operación (donde *e* es constante y público)

$$c = m^e \bmod n$$

e) Entonces el mensaje *c* puede viajar sin problema por cualquier canal inseguro



f) cuando la información cifrada llega a su destino el receptor procede a descifrar el mensaje con la siguiente fórmula

$$m = c^d \bmod n$$

g) Se puede mostrar que estas formulas son inversas y por lo tanto dan el resultado deseado, (*n,e*) son la clave pública, la clave privada es la pareja (*p,q*) o equivalentemente el número *d*. La relación que existe entre *d* y *e* es que uno es el inverso multiplicativo del otro módulo $\lambda(n)$ donde $\lambda(n)$ es el mínimo común múltiplo de *p*-1 y *q*-1, o también puede usarse $\varphi(n)=(p-1)(q-1)$ esto significa que la clave privada o el la pareja *p,q* o es el número *d*.

En términos muy generales es así como funciona el sistema **RSA**. Sin embargo en la realidad existen dos formas que son las más comunes, estas formas depende de la

aplicación y se llaman el esquema de firma y el esquema de cifrado, cada una de estas dos diferentes aplicaciones consiste en una serie de pasos que a continuación se describen

Esquema de cifrado

Uso: este esquema se usa principalmente en cifrar claves de sistemas simétricos (claves de 128 bits aprox.)

1) Se toma el mensaje **M** (por ejemplo una clave simétrica de 128 bits), como en la practica actual es recomendable usar arreglos de longitud de 1024 bits, los complementa esos 128 bits con una serie de técnicas para obtener un arreglo de 1024 bits, después se aplica un proceso de codificación para que la computadora entienda al mensaje como un número entero *m*.

2) Se le aplica la formula de cifrado de **RSA** al entero *m*
3) Se envía el número entero *c*
4) Al recibir este número se aplica la formula de descifrado al entero *c* para obtener el entero *m*
5) Se decodifica m para obtener el mensaje **M**

Ejemplo simple

Generación de parámetros

1) $p = 3$, $q = 5$ (se eligen don números primos como clave privada)
2) $n = 15$ (se calcula el producto, es la clave pública)
3) $\varphi(n)=(3-1)(5-1)=8$
4) Sea $e=3$, entonces $d=3$, ya que $e*d = 3*3 =9 \bmod 8 =1$ (como este caso solo es para mostrar el funcionamiento no importa que *d* sea igual a *e*, sin embargo en la práctica *e* es pequeño y *d* es muy grande)
5) Si el mensaje es $m=2$

Proceso de cifrado

6) El mensaje cifrado es $c= m^e \bmod n$, es decir, $c=2^3 \bmod 15$, o sea $c=8$

Proceso de descifrado

7) Para descifrar el mensaje $m=8^3 \bmod 15$, es decir, $m=512 \bmod 15$, asi $m=2$ (ya que $512/15=2 \bmod 15 = m$)

Por lo tanto es correcto el funcionamiento.

Esquema de Firma Digital

Existen dos tipos de esquemas sobre firma digital, el que se denomina esquema de firma digital con apéndice y el esquema de firma digital con mensaje recuperable. También cualquier esquema de firma cuenta con dos partes la primera parte se denomina proceso de firma (similar al cifrado) y la segunda parte proceso de verificación de la firma (similar al descifrado). Otros esquemas de firna digital se encuentran en.

El esquema más usado y conocido es el esquema de firma con apéndice y consiste en los siguientes puntos:

Proceso de Firma

1) El mensaje a firmar es M, se le aplica una función hash que reduce su longitud de forma única a un mensaje H(M*)* de longitud de 128 o 160 bits, lo que permite ver cualquier mensaje de cualquier longitud como una cadena de caracteres de longitud constante.

2) H(M) se somete también a un proceso de codificación, por lo tanto se obtiene un número h(M), al que se le aplica la formula con la potencia d, equivalentemente con la clave privada del firmante para obtener

$$s = h(M)^d \bmod n$$

3) Se envía entonces el mensaje firmado *s*

Proceso de Verificación

1) El que recibe *s*, se supone conoce el mensaje M, aplica la función de verificación que depende de la clave pública de quien se dice propietario del mensaje

$$h' = s^e \bmod n$$

2) Ahora se aplica la función hash al mensaje M y si *h(*M*)=h'* entonces acepta la firma

En un esquema con mensaje recuperable no es necesario saber el mensaje, después de que la firma es aceptada el mensaje puede recuperarse a partir de la firma.

Ejemplo simple:

Tomemos los mismos parámetros del ejemplo en el esquema de cifrado, p=3, q=5, m=2, φ=8, e=3, d=3

Proceso de Firma

1) La firma del documento m es: $s = m^d \bmod n = 2^3 \bmod 15 = 8$
2) El mensaje firmado es entonces $(m,s) = (2,8)$

Proceso de verificación

3) Aplicando la función de verificación $s^e \bmod n = 8^3 \bmod 15 = 2$
4) Como 2 (el obtenido de la anterior fórmula) = 2 (el mensaje enviado)
5) Entonces la firma es válida

Aspectos Importantes

1) La longitud de las claves

Existe una gran discusión, sobre este aspecto pero sin duda en la actualidad se acepta que es recomendable usar claves de longitud 768 para actividades personales,1024 bits para corporaciones y 2048 para actividades de alto riesgo. La longitud de las claves tiene que ver con la seguridad del sistema si el número n pudiese ser factorizado entonces sin mucha dificultad puede calcular a d a partir de e, p, y q por lo tanto descifrar cualquier mensaje. El último récord conocido sobre factorización de números enteros producto de dos primos de la misma longitud es de 155 (512 bits) dígitos alcanzado en Jul de 1999.

2) La aleatoriedad de las claves

La generación de las claves **RSA** es muy importante, muchos ataques son evitados si las claves son elegidas de forma aleatoria, esto incrementara la seguridad del sistema.

3) método de codificación

El método que actualmente es usado para aplicaciones en el esquema de cifrado es el **OAEP**, este resiste a los ataques que actualmente se conocen y el estándar más conocido sobre **RSA** es el **PKCS**#1 v.2 de la RSA Data Security.
En el caso de Esquemas de firma digital el método de codificación recomendable es **PSS** que esta descrito en **PKCS**#1 v 2.1

4) Elección de parámetros

La elección adecuada de los parámetros que se usan aumenta la seguridad del sistema así como su fácil y rápida implementación. Como elegir a $e=65537 = (01\ 00\ 01)_{16}$, para poder efectuar la operación exponente eficientemente. Además de elegir d la clave privada de longitud grande para evitar el ataque de Wiener. Los números primos p,q además de ser generados aleatoriamente deben de tener la misma longitud y no estar cerca.

CCE otro tipo de criptografía de clave pública es el que usa curvas elípticas definidas en un campo finito. La diferencia que existe entre este sistema y **RSA** es el problema del cual basan su seguridad, mientras **RSA** razona de la siguiente manera: te doy el número 15 y te reta a encontrar los factores primos. El problema del cual están basados los sistemas que usan curvas elípticas que denotaremos como **CCE** es el problema del logaritmo discreto elíptico, en este caso su razonamiento con números sería algo como: te doy el número 15 y el 3 y te reta a encontrar cuantas veces tienes que sumar el mismo 3 para obtener 15.

En lo que sigue nos dedicaremos a explicar un poco mas lo más importante de los **CCE**

1) Entenderemos como una curva elíptica a una ecuación de la forma siguiente:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Donde las constantes *a,b,c,d* y e pertenecen a cierto conjunto llamado campo **F,** que para propósitos de la criptografía o es un campo primo ($\mathbf{Z_p}$) o un campo de característica 2, o sea donde los elementos son n-adas de ceros y unos ($\mathbf{F_2^n}$)

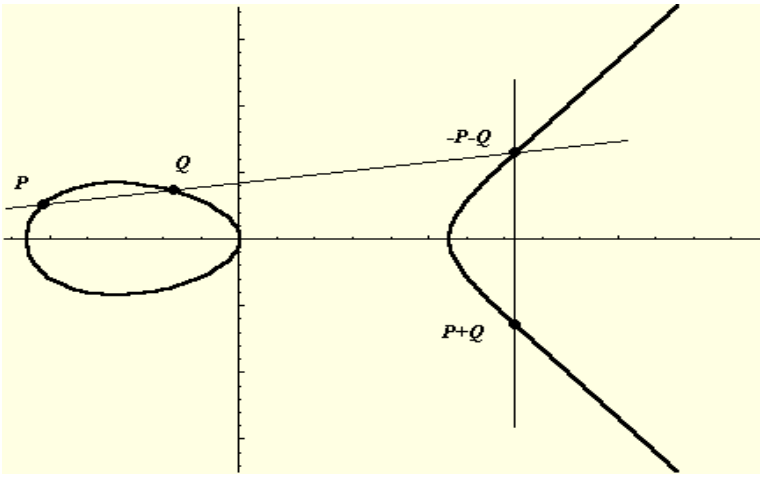
2) A un punto que satisface la ecuación anterior se le llama punto racional. Si el campo es finito, entonces el conjunto de puntos (*x,y*) que satisfacen la ecuación es finito y es llamado conjunto de puntos racionales de la curva ***E*** sobre el campo **F**. Al conjunto de puntos racionales lo podemos representar como

$$E : O, P_1, P_2, P_3, \ldots, P_n$$

E representa la ecuación y ***O*** es un punto que no tiene coordenadas y hace el papel de cero (llamado punto al infinito) ya que en este conjunto los puntos puede sumarse y tiene las mismas propiedades que la suma de los números enteros, es decir lo que se conoce como un grupo abeliano.

Ejemplo: veamos una curva elíptica simple, si la ecuación es $y^2=x^3+4x+3$ y el campo $\mathbf{Z}_5$, es decir el conjunto {0,1,2,3,4}, entonces las parejas que satisfacen la ecuación son {(2,2), (2,3}, por lo tanto la curva elíptica es ***E***: {***O***, (2,2), (2.3)}. En este caso ***E*** tiene 3 puntos racionales.

3) La suma de estos puntos tiene una explicación geométrica muy simple, si la gráfica representa a todos los puntos que satisfacen la ecuación de la curva elíptica, y queremos sumar a *P* y *Q*, trazamos una línea recta que pase por *P* y *Q*, la ecuación de la curva es de grado 3 y la línea de grado 1, entonces existen siempre tres soluciones, en este caso la tercera solución esta dibujada como el punto *-P-Q*, enseguida se procede a dibujar una línea recta paralela al eje Y que pase por *-P-Q*, esta línea vertical también intercepta tres veces a la recta, todas las líneas verticales interceptan al punto especial llamado infinito y que geométricamente esta en el horizonte del plano, el tercer punto es por definición *P+Q*, como se muestra en la figura



4) No es difícil obtener fórmulas para calcular las coordenadas del punto $P+Q$ a partir de las coordenadas del punto P y del punto Q. Por ejemplo si el campo de definición de la curva es un campo primo $\mathbf{Z_p}$, entonces las fórmulas de suma son las siguientes

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q \end{cases}$$

5) La anterior forma de sumar puntos de una curva elíptica es un poco extraña sin embargo, es esta extrañeza lo que permita que sea un poco más difícil romper los **CCE**. En el área de las matemáticas conocida como teoría de grupos se sabe que estos grupos son muy simples llamados grupo abelianos finitos lo que permite también que los **CCE** sean fácil de implementar, llamaremos al número de puntos racionales de la curva como el orden de la curva. En nuestro ejemplo $P_0=\boldsymbol{O}$, $P_1=(2,2)$, $P_2=(2,3)$, donde $2P_1=P_2$.

6) Los **CCE** basan su seguridad en el Problema del Logaritmo Discreto Elíptico (**PLDE**), esto quiere decir que dados P,Q puntos de la curva hay que encontrar un número entero x tal que $xP = Q$ ($xP = P+P+\ldots+P$, x veces). Obsérvese que a diferencia del **PFE** (Problema de Factorización Entera) el **PLDE** no maneja completamente números, lo que hace más complicado su solución.

7) La creación de un protocolo con criptografía de curvas elípticas requiere fundamentalmente una alta seguridad y una buena implementación, para el primer punto se requiere que la elección de la curva sea adecuada, principalmente que sea no-

supersingular y que el orden del grupo de puntos racionales tenga un factor primo de al menos 163 bits, además de que este orden no divida al orden de un número adecuado de extensiones del campo finito, para que no pueda ser sumergido en él, si el campo es $\mathbf{Z_P}$, se pide que la curva no sea anómala o sea que no tenga p puntos racionales. Todo esto con el fin de evitar los ataques conocidos.
Para el caso de la implementación hay que contar con buenos programas que realicen la aritmética del campo finito, además de buenos algoritmos que sumen puntos racionales, tanto en el caso de $\mathbf{Z_p}$ como $\mathbf{F_2^n}$, en este último se toma una base polinomial que tenga el mínimo de términos por ejemplo un trinomio para generar los elementos del campo finito esto si la implementación es en software, y se toma una base normal si es en hardware. Además de contemplar que las operaciones de puntos racionales pueden hacerse en el espacio proyectivo, esto elimina el hacer divisiones, ahorrando tiempo.

8) Lo anterior se ve reflejado en las ventajas que ofrecen los **CCE** en comparación con **RSA**, la principal es la longitud de la clave secreta. Se puede mostrar que mientras en **RSA** se tiene que usar una clave de 1024 para ofrecer una considerable seguridad, los **CCE** solo usan 163 bits para ofrecer la misma seguridad, así también las claves **RSA** de 2048 son equivalentes en seguridad a 210 de **CCE**. Esto se debe a que para resolver el **PLDE** el único algoritmo conocido toma tiempo de ejecución totalmente exponencial, mientras que el algoritmo que resuelve **PFE** incluso también el **PLD** en $\mathbf{Z_p}$ toman un tiempo subexponencial.

9) Otra buena noticia sobre **CCE** es que los elementos de los puntos racionales pueden ser elementos de un campo finito de característica 2, es decir pueden ser arreglos de ceros y unos de longitud finita (01001101110010010111), en este caso es posible construir una aritmética que optimice la rapidez y construir un circuito especial para esa aritmética, a esto se le conoce como Base Normal Optima.

10) Lo anterior permite con mucho que los **CCE** sean idóneos para ser implementados en donde el poder de cómputo y el espacio del circuito sea reducido, donde sea requerida una alta velocidad de procesamiento o grandes volúmenes de transacciones, donde el espacio de almacenamiento, la memoria o el ancho de banda sea limitado. Lo que permite su uso en Smart Cards, Teléfonos celulares, Fax, Organizadores de Palma, PCs, etcétera.

11) En la actualidad existen varios estándares que permiten el uso adecuado y óptimo de los **CCE**, entre los cuales se encuentran: **IEEE P1363** (Institute of Electrical and Electronics Engineers), el **ANSI X9.62**, **ANSI X9.63**, **ANSI TG-17**, **ANSI X12** (American National Standards Institute), **UN/EDIFACT**, **ISO/IEC 14888**, **ISO/IEC 9796-4**, **ISO/IEC 14946** (International Standards Organization), **ATM** Forum (Asynchronous Transport Mode), **WAP** (Wireless Application Protocol). En comercio electrónico: **FSTC** (Financial Services Technology Consortion), **OTP 0.9** (Open Trading Protocol), **SET** (Secure Electronic Transactions). En internet **IETF** (The Internet Engineering Task Force), **IPSec** (Internet Protocol Security Protocol)

12) Los **CCE** son el mejor candidato para reemplazar a las aplicaciones que tienen implementado **RSA**, estas definen también esquemas de firma digital, Intercambio de claves simétricas y otros. Los **CCE** se pueden estudiar en.

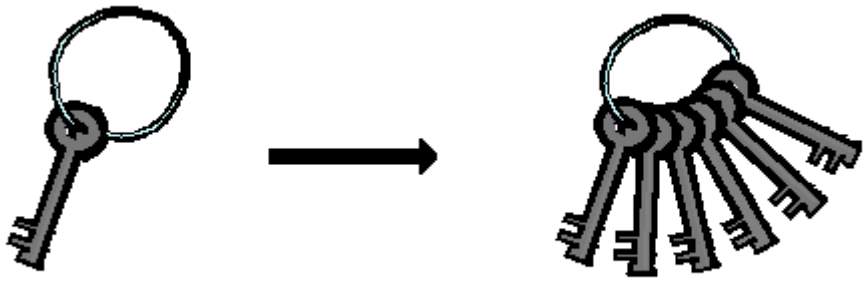
3) Otras Herramientas criptográficas

En esta sección me dedicare principalmente a enumerar otro tipo de herramientas o técnicas que son usadas en criptografía, cada una de ellas tiene una gran aplicación y tienen un propósito muy especifico dentro del ámbito de la criptografía, sin embargo su descripción completa no es el propósito para un lector novato así que solo se mencionarán, para un mayor estudio puede consultarse la bibliografía.

A) Compartición de Secretos

La compartición de secretos, como su nombre lo dice es una técnica criptográfica que se dedica a partir un secreto, que puede ser una clave secreta, en la responsabilidad de varias personas y que solo con el número mínimo de personas se podrá reconstruir el secreto compartido. Por ejemplo si el secreto es el número 100 y este debe ser compartido por tres personas A1, A2 y A3 una forma de poder hacerlo es generar un número aleatorio menor a 100, digamos el 33 posteriormente se genera otro número aleatorio menor a 100-33, digamos el 27, y finalmente la tercera parte será *100-(27+33)=46*. Así el secreto 100 esta compartido por A1(33), A2(27) y A3(46), cada quién con su parte correspondiente. Como ninguno de ellos sabe las otras partes, solo los tres juntos podrán reconstruir el mensaje sumando sus partes. Claro esta este es solo un ejemplo para explicar el concepto.

La comparición de secretos puede ser usada para compartir digamos la combinación de una caja fuerte, la clave de lanzamiento de algún proyectil, la clave secreta de una autoridad certificadora, la clave de activación de algún dispositivo de alto riesgo, etc.,



Uno de los mejores métodos de comparición de secretos y mas conocido es el esquema (*n,k*) límite de Shamir. Este método consiste en partir una clave *K* en *n* partes, y se tiene como mínimo (límite) el número *k* de partes para reconstruir la clave, es decir cualquiera *k* de los *n* custodios pueden reconstruir la clave *K*, pero ningún subgrupo de *k*-1 custodios podrá hacerlo.

Un ejemplo simple de esquema de Shamir se basa en lo siguiente:

1) Se define el número de custodios *t*, digamos *t*=2
2) Se generan aleatoriamente los coeficientes necesarios para construir un polinomio de *t*-1 grado, en nuestro caso

$$f(x) = 2 + 3x$$

donde el coeficiente es aleatorio y 2 el secreto a compartir

3) Las partes serán $f(1)=2+3*1=5$ y $f(2)=2+3*2=8$

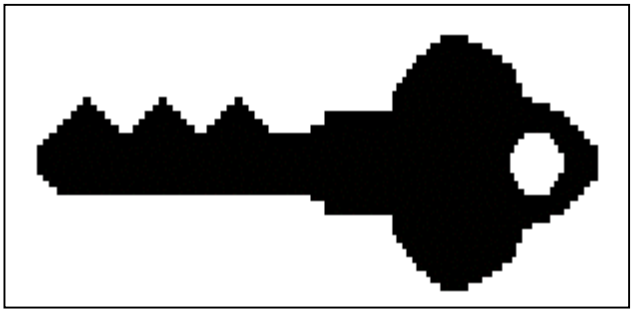
El método para recuperar el secreto *s*, es reconstruir el polinomio $f(x)$ a partir de las partes cualquiera, esto se hace por medio de la interpolación de Lagrange.
En nuestro caso el secreto se puede reconstruir de la siguiente formula:

$$s = c_1 y_1 + c_2 y_2$$

donde y_1 y_2 son las partes (5 y el 8) y $c_1=2$, $c_2= -1$. El secreto es entonces 2(5)-(8)=2.

B) Criptografía Visual

Una idea ingeniosa de usar un método de comparición de secretos con un esquemas límite (*n,k*) es la criptografía visual, esto consiste en lo siguiente: una imagen es partida en *n* partes, y si se sobreponen al menos *k* de estas partes se puede reconstruir la imagen.
Veamos en ejemplo de un esquema (2,2), esto trabaja considerando que si la imagen es de banco y negro, entonces la imagen podrá ser un conjunto de cuadros completamente negros y completamente negros, por ejemplo la siguiente imagen



Ahora cada cuadro de la imagen podrá ser considerado como blanco o negro, equivalentemente con valores 0 y 1. Para partir esta imagen en dos partes n=2 y considerando el límite con k=2, se procede como sigue:

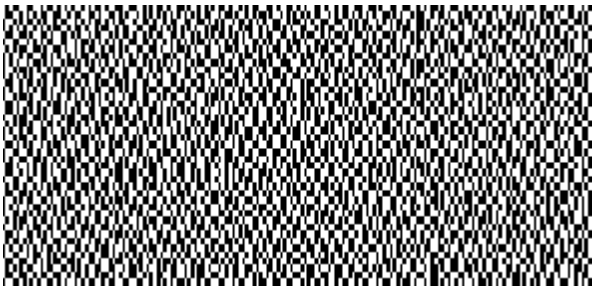
Cada cuadro que es completamente negro podrá ser partido en dos partes de la siguiente forma:

Y un cuadro completamente blando podrá ser partido en dos de la forma siguiente:

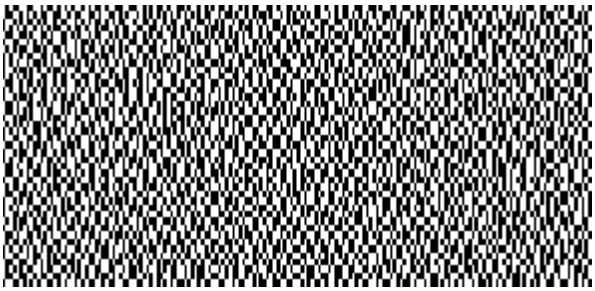
Que significa suma módulo 2, es decir 1+0=1, 0+1=1, 0+0=0 pero también 1+1=0, de este modo se pueden tomar cualquiera de las dos particiones de los cuadros de color blanco.

Para formar las dos partes de la figura en un acetato se elige aleatoriamente una de las combinaciones anteriores según se parta un cuadro blanco o uno negro

En el caso de nuestra figura una ves elegidas las partes, la figura partida en un esquema limite (2,2) queda así:



Parte 1



Parte 2

De esta forma se tiene partida la figura en dos partes y se recuperara solo sobreponiendo una sobre la otra.
Al sobreponer las dos partes se recupera la figura, de la siguiente forma:

En el caso general se parte los cuadros blancos y negros en *n* pedazos y hasta no tener *k* pedazos negros el cuadro reconstruido será siendo blanco, a partir de k pedazos negros hasta *n* el cuadro reconstruido será negro. En nuestro caso, un cuadro con solo la mitad negra será considerado blanco, es necesario que tenga dos mitades negras para que el cuadro reconstruido se considere negro, que es el caso del esquema (2,2).

C) Dinero Electrónico

Una aplicación más, que puede ser realidad gracias a la criptografía de clave pública es conocida como dinero electrónico, en términos sencillos el dinero electrónico es otra representación de lo que conocemos como dinero o valor, por ejemplo tenemos dinero en billetes emitidos por algún país, podemos tener cheques pagaderos en un banco, bonos, pagares pagaderos en algún plazo, en fin. El dinero electrónico es físicamente un número que se genera aleatoriamente, se le asigna un valor, se cifra y firma y se envía al banco, ahí el banco valida el número y certifica el valor, y lo regresa al usuario firmado por el banco, entonces el usuario puede efectuar alguna transacción con ese billete electrónico.

= f5 6a 80 b2....03

Las principales propiedades del dinero electrónico son las siguientes:

1) **Independencia**: la seguridad del dinero digital no debe depender de la el lugar físico donde se encuentre, por ejemplo en el disco duro de una PC

2) **Seguridad**: el dinero digital (el número) no debe de ser usado en dos diferentes transacciones

3) **Privacidad**: el dinero electrónico debe de proteger la privacidad de su usuario, de esta forma cuando se haga una transacción debe de poder cambiarse el número a otro usuario sin que el banco sepa que dueños tuvo antes.

4) **Pagos fuera de línea**: el dinero electrónico no debe de depender de la conexión de la red, así un usuario puede transferir dinero electrónico que tenga en una "smart card" a una computadora, el dinero digital debe ser independiente al medio de transporte que use.

5) **Transferibilidad**: el dinero electrónico debe de ser transferible, cuando un usuario transfiere dinero electrónico a otro usuario debe de borrarse la identidad del primero.

6) **Divisibilidad**: el dinero electrónico debe de poder dividirse en valores fraccionarios según sea el uso que se da, por ejemplo en valor de 100, 50 y 25

La serie de pasos que puede seguir una transacción que se realiza con dinero electrónico en un escenario simple es la siguiente:

Supóngase que el usuario **A** quiere mandar un cheque a **B**, usando ahora dinero electrónico.

1) **A** genera un número aleatorio grande N de digamos 100 dígitos y le da un valor digamos 1000 pesos
2) **A** cifra este número junto a su valor con su clave secreta asimétrica.
3) **A** firma este número y lo transmite a su banco.
4) El banco de **A** usa, la clave pública de **A** para descifrar el número y verificar la firma, así recibe la orden y sabe que es de **A**. El banco borra la firma de **A** del documento electrónico.
5) El banco revisa que **A** tenga en sus cuentas la cantidad pedida 1000 pesos y la debita de alguna de sus cuentas.
6) El banco firma el número que mando **A**, con el valor asignado de 1000 pesos
7) El banco regresa el número que ya es dinero a, **A**
8) **A** envía este dinero a **B**
9) **B** verifica la firma del banco de **A**, que esta en N
10) **B** envía N a su banco
11) EL banco de **B** re-verifica la firma del banco de **A** en N
12) El banco de **B** verifica que N no este en la lista de números "ya usados"
13) El banco de **B** acredita la cantidad de 1000 pesos a la cuenta de **B**
14) El banco de **B** pone a N en la lista de números "ya usados"
15) Finalmente el banco de **B** envía un recibo firmado donde establece que tiene 1000 pesos más en su cuenta

En el mundo comercial existen varias empresas privadas que proveen el servicio de dinero electrónico en diferentes modalidades entre ellas están: CheckFree, CyberCash, DigiCash, First Virtual, Open Market, NetBill y Netscape.

En http://www.ecashtechnologies.com/ pueden encontrarse algunos ejemplos interactivos de cómo trabaja el dinero electrónico en la práctica

Certificados digitales

Los certificados digitales, tienen una similitud con las licencias de conducir, las primeras permiten viajar por las carreteras, los certificados digitales permiten navegar por la red Internet, la principal característica es que da identidad al usuario y puede navegar con seguridad. De igual forma que la sola licencia de conducir o un pasaporte sirve para dar identidad a quien la porta en ciertos casos, el certificado digital da identidad a una clave pública y se comporta como una persona en el espacio cibernético.

El nacimiento del certificado digital fue a raíz de resolver el problema de administrar las claves públicas y que la identidad del dueño no pueda ser falsificada. La idea es que una tercera entidad intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado. Esto fue inicialmente planteado por Kohnfelder del MIT en su tesis de licenciatura.

Las tres partes más importantes de un certificado digital son:

1) Una clave pública
2) La identidad del implicado: nombre y datos generales,
3) La firma privada de una tercera entidad llamada autoridad certificadora que todos reconocen como tal y que válida la asociación de la clave pública en cuestión con el tipo que dice ser.

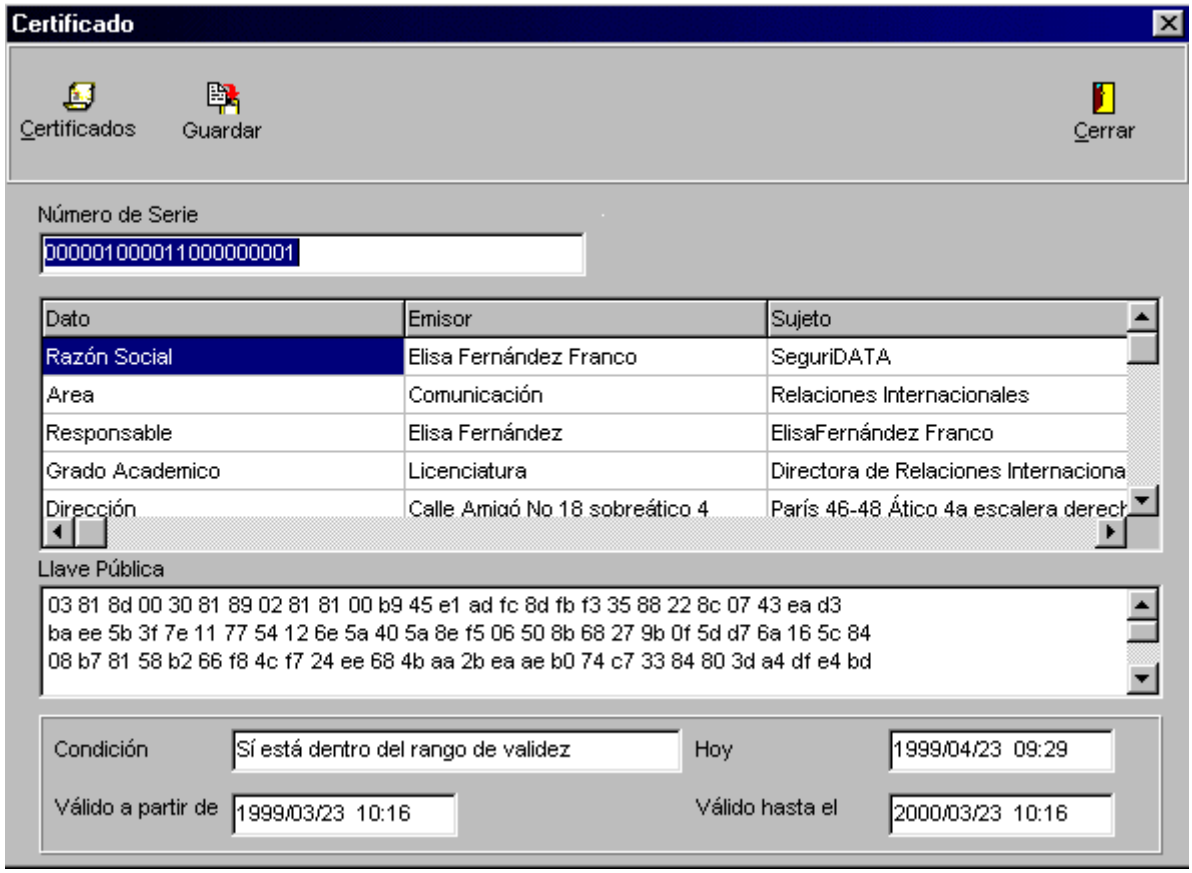
En la actualidad casi todas las aplicaciones de comercio electrónico y transacciones seguras requieren un certificado digital, se ha propagado tanto su uso que se tiene ya un formato estándar de certificado digital, este es conocido como X509 v. 3.

Algunos de los datos más importantes de este formato son los siguientes:

Versión: 1,2 o 3
Número de Serie: 0000000000000000
Emisor del Certificado: VeriMex
Identificador del Algoritmo usado en la firma: RSA, DSA o CE
Periodo de Validez: De Enero 2000 a Dic 2000
Sujeto: Jesús Angel
Información de la clave pública del sujeto: la clave, longitud, y demás parámetros
Algunos datos opcionales, extensiones que permite la v3
Firma de la Autoridad Certificadora

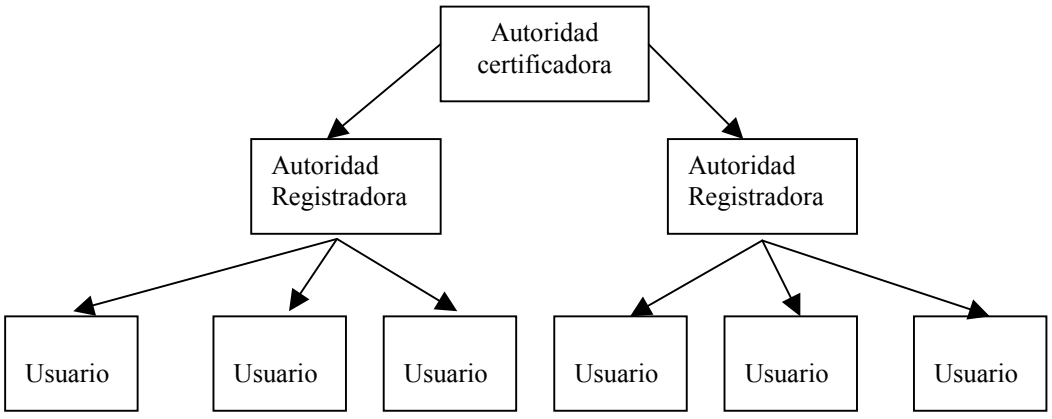
Un certificado digital entonces se reduce a un archivo de uno o dos k de tamaño, que autentica a un usuario de la red.

En una aplicación un certificado digital se puede ver como la siguiente pantalla:



Infraestructura de claves públicas

Teniendo ya un certificado digital que es generado con la ayuda de un algoritmo de clave pública ahora el problema es como administración todos estos, la estructura más básica es la siguiente:



El papel de la Autoridad certificadora (**AC**) es de firmar los certificados digitales de los usuarios, generar los certificados, mantener el status correcto de los certificados, esto cumple el siguiente ciclo:

1) La generación del certificado se hace primero por una solicitud de un usuario, el usuario genera sus claves pública y privada y manda junto con los requerimientos de la solicitud su clave pública para que esta sea certificada por la **AC**.
2) Una vez que la **AR** (es la **AC** regional) verifica la autenticidad del usuario, la **AC** vía la **AR** firma el certificado digital y es mandado al usuario
3) El status del usuario puede estar en: activo, inactivo o revocado. Si es activo el usuario puede hacer uso del certificado digital durante todo su periodo válido
4) Cuando termina el período de activación del certificado el usuario puede solicitar su renovación.

Entre las operaciones que pudiera realizar una **AC** están:

Generar certificados
Revocar certificados
Suspender certificados
Renovar certificados
Mantener un respaldo de certificados…..

Entre las que pudiera realizar una **AR** están:

Recibir las solicitudes de certificación
Proceso de la autenticación de usuarios
Generar las claves
Respaldo de las claves
Proceso de Recobrar las claves
Reportar las revocaciones….

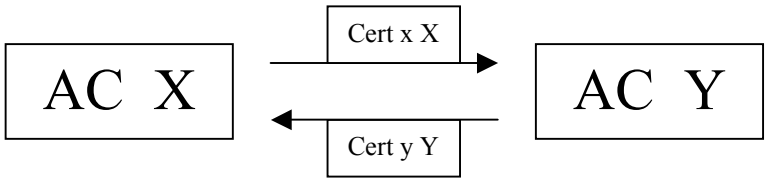
Y las actividades de los usuarios:

Solicitar el certificado
Solicitar la revocación del certificado
Solicitar la renovación del certificado….

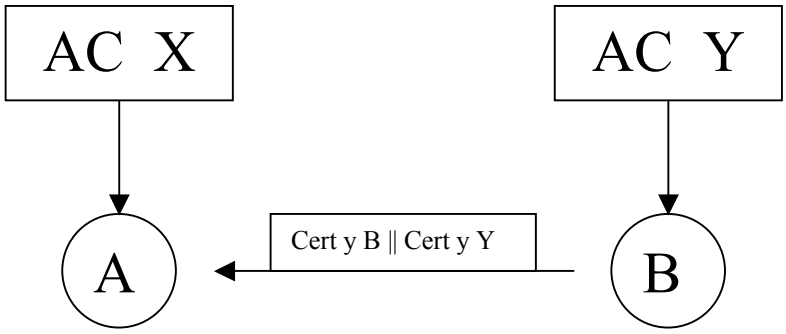
Una vez que algún usuario tiene un certificado digital este puede usarlo para poder navegar por la red con nombre y apellido en forma de bits, esto permite entrar al mundo del comercio electrónico, al mundo de las finanzas electrónicas y en general a la vida cibernética con personalidad certificada. El usuario dueño de un certificado digital tiene la potencialidad de poder autentificarse con cualquier otra entidad usuaria, también puede intercambiar información de forma confidencial y estar seguro de que esta es integra, así estar seguro que contactos vía el certificado digital no serán rechazados. Los primeros usuarios de certificados digitales fueron los servidores, actualmente son quienes más los usan, sin embargo también se ha incrementado el número de personas que los usan.

Si suponemos que algún tipo de aplicación funciona ya con certificados digitales, esta tendrá una **AC** y las correspondientes **AR**, sin embargo es común que haya mas autoridades certificadoras y que sus usuarios puedan interoperar con sus respectivos certificados, a esto se le conoce como certificación cruzada y opera de la siguiente forma:

1) Las diferentes **AC** pueden estar certificadas enviándose una a otra sus respectivos certificados que ellas mismas generan



2) Entonces la **AC X** tendrá el certificado de la **AC Y** y viceversa, podiendo generar un certificado para **Y** que genera **X** y otro para **X** que genera **Y**
3) Ahora como un usuario **A** de la **AC X** puede comunicarse con un usuario **B** de la **AC Y**



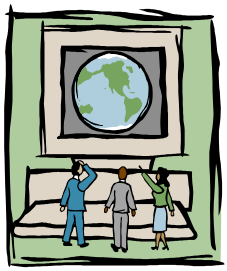
4) El usuario **B** envía a **A** el certificado de **B** que genera **Y** (**Cert y B**) junto con el certificado de **Y** que el mismo se genera (**Cert y Y**)
5) Ahora **A** puede validar a **B** (**Cert y B**) usando el certificado de **Y** que genera **X**

En la práctica se ha demostrado que el estatus de un certificado cambia con gran frecuencia, entonces la cantidad de certificados digitales revocados crece considerablemente, el problema esta en que cada vez que se piensa realizar una comunicación y es necesario validar un certificado se debe de comprobar que este no esta revocado. La solución que se ha venido usando es la de crear una lista de certificados revocados **LCR** y así verificar que el certificado no esta en esa lista, para poder iniciar la comunicación. El manejo de las listas de certificados revocados ha llegado a tener un gran costo que sin embargo aún no se ha reemplazar por otra técnica a pesar que se han propuesto ya salidas al problema.

Las operaciones de la administración de los certificados digitales puede cambiar de acuerdo a las leyes particulares de cada país o entidad.

Comercio electrónico

Hoy en día, gran parte de la actividad comercial ha podido transformarse gracias a redes de conexión por computadoras como Internet, esta transformación facilita hacer transacciones en cualquier momento, de cualquier lugar del mundo. Todo lo que esta alrededor de esta nueva forma de hacer negocios es lo que se ha llamado comercio electrónico, sin duda la gran variedad de actividades que giraban alrededor del quehacer comercial se ha tenido que juntar con las nuevas técnicas cibernéticas. Así hoy tanto un comerciante, un banquero, un abogado o una matemático puede hablar de comercio electrónico enfocándose a la parte que le corresponde.



Existen diferentes niveles de hacer comercio electrónico, y su clasificación aún esta por formarse, sin embargo, la parte más visible es la que cualquier usuario en una computadora

personal puede ver, esto es hacer comercio electrónico se convierte a comprar o vender usando una conexión por Internet en lugar de ir a la tienda. La forma de hacer esto es muy similar a lo que tradicionalmente se hace, por ejemplo: en la tienda uno entra al establecimiento, de forma electrónica se prende la computadora y una ves conectado a Internet entra a la página del negocio, enseguida un comprador revisa los productos que posiblemente compre y los coloca en una carrito, de la misma forma en la computadora se navega por la página del negocio y con el browser se revisa los productos que éste vende, al escoger éstos se colocan en un carrito virtual, que no es nada mas que un archivo del usuario. Una vez elegido bien los productos de compra se pasa a la caja, donde se elige un sistema de pago y se facturan los productos al comprador. De forma similar en la computadora se pueden borrar productos que no se quieren comprar o añadir nuevos, una ves elegidos éstos se procede a una parte de la pagina que toma los datos y solicita el método de pago, generalmente se lleva a cabo con tarjeta de crédito.

En la parte tradicional de comprar al pagar en la caja termina el proceso, en la parte por computadora aún tiene que esperarse que sean enviados los productos. A pesar de esto las ventajas que ofrece el comercio electrónico son magníficas, ya que es posible comprar en un relativo corto tiempo una gran cantidad de productos sin necesidad de moverse de lugar, es decir al mismo tiempo se puede comprar una computadora, un libro, un regalo, una pizza, hacer una transacción bancaria etc., de la forma tradicional se llevaría al menos un día completo y eso si los negocios esta en la misma ciudad, si no, el ahorro de tiempo que representa comprar por Internet es incalculable.

Al efectuar una operación comercial por Internet se presentan nuevos problemas, por ejemplo cómo saber que la tienda virtual existe verdaderamente, una vez hecho el pedido cómo saber que no se cambia la información, cuando se envía el número de tarjeta de crédito cómo saber si este permanecerá privado, en fin, para el comerciante también se presentan problemas similares, cómo saber que el cliente es honesto y no envía información falsa, etc. Todos estos problemas pueden ser resueltos de manera satisfactoria si se implementan protocolos de comunicación segura usando criptografía. En la siguiente sección nos dedicamos a describir como es que estos protocolos resuelven los problemas planteados.

Protocolos de seguridad

Un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo especifico y que usan esquemas de seguridad criptográfica.
El ejemplo más común es **SSL** (**S**ecure **S**ockets **L**ayer) (que vemos integrado en el Browser de Netscape y hace su aparición cuando el candado de la barra de herramientas se cierra y también sí la dirección de Internet cambia de http a https, otro ejemplo es **PGP** que es un protocolo libre ampliamente usado de intercambio de correo electrónico seguro, uno más es el conocido y muy publicitado **SET** que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito, **IPsec** que proporciona seguridad en la conexión de Internet a un nivel más bajo.
Estos y cualquier protocolo de seguridad procura resolver algunos de los problemas de la seguridad como la integridad, la confidencialidad, la autenticación y el no rechazo, mediante sus diferentes características
Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

Enseguida vemos un escenario donde puede ocurrir algo de esto:

Por ejemplo sobre la seguridad por Internet se deben de considerar las siguientes tres partes: seguridad en el browser (Netscape o Explorer), la seguridad en el Web server (el servidor al cual nos conectamos) y la seguridad de la conexión.

Un ejemplo de protocolo es **SET**, objetivo efectuar transacciones seguras con tarjeta de crédito, usa certificados digitales, criptografía de clave pública y criptografía clave privada.

SSL Es el protocolo de comunicación segura más conocido y usado actualmente, **SSL** actúa en la capa de comunicación y es como un túnel que protege a toda la información enviada y recibida. **SSL** es usado en gran cantidad de aplicaciones que requieren proteger la comunicación.

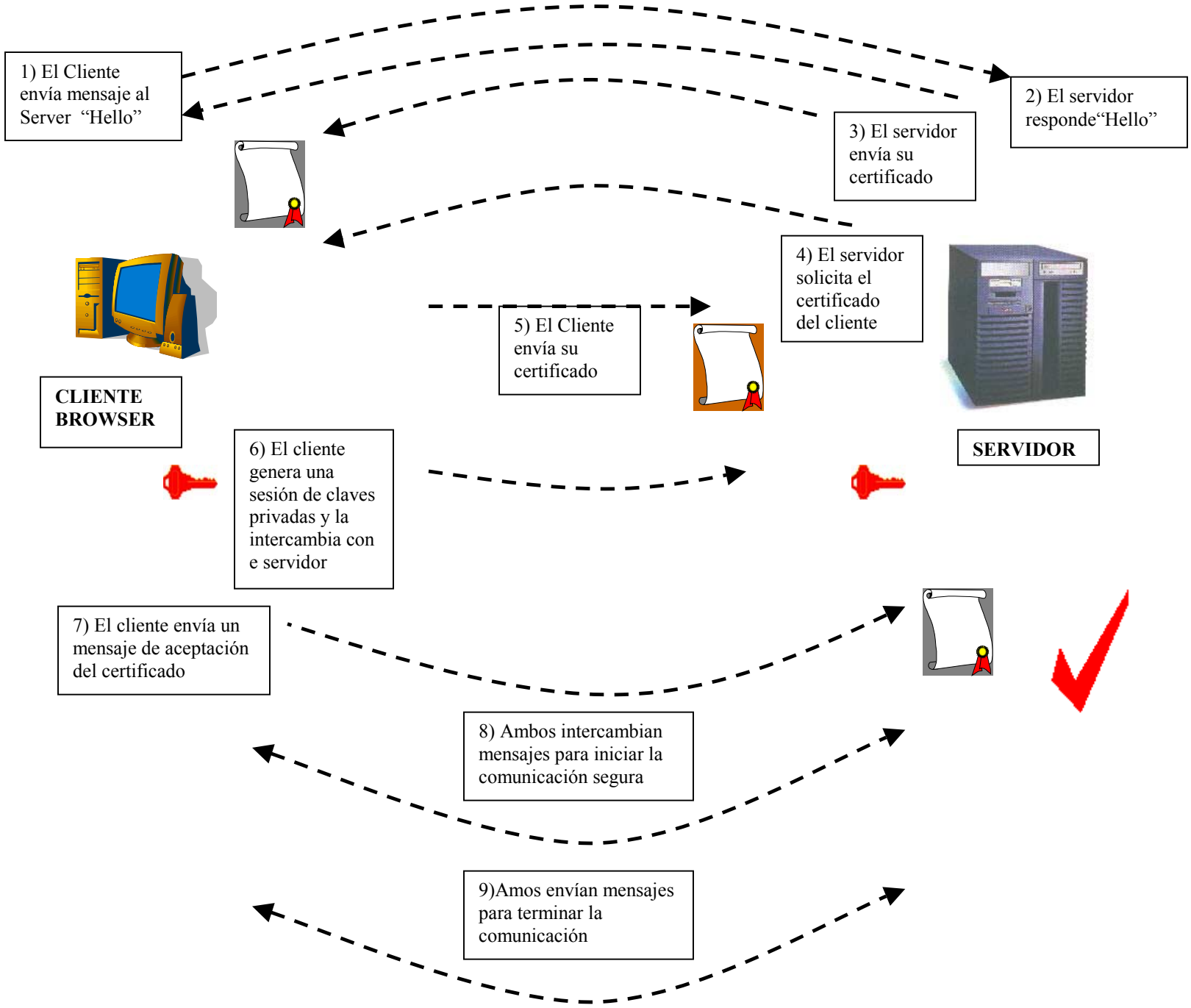
Con **SSL** se pueden usar diferentes algoritmos para las diferentes aplicaciones, por ejemplo usa **DES**, **TDES**, **RC2**, **RC4**, **MD5**, **SHA-1**, **DH** y **RSA**, cuando una comunicación esta bajo **SSL** la información que es cifrada es:

El URL del documento requerido
El contenido del documento requerido
El contenido de cualquier forma requerida
Los “cookies” enviados del browser al servidor
Los “cookies” enviados del servidor al browser
El contenido de las cabeceras de los http

El procedimiento que se lleva acabo para establecer una comunicación segura con **SSL** es el siguiente:

1) EL cliente (browser) envía un mensaje de saludo al Server “ClientHello”
2) El servidor responde con un mensaje “ServerHello”
3) El servidor envía su certificado
4) El servidor solicita el certificado del cliente
5) El cliente envía su certificado: si es válido continua la comunicación si no para o sigue la comunicación sin certificado del cliente
6) El cliente envía un mensaje “ClientKeyExchange” solicitando un intercambio de claves simétricas si es el caso
7) El cliente envía un mensaje “CertificateVerify” si se ha verificado el certificado del servidor, en caso de que el cliente este en estado de autenticado
8) Ambos cliente y servidor envían un mensaje “ChangeCipherSpec” que significa el comienzo de la comunicación segura.
9) Al término de la comunicación ambos envían el mensaje “finished” con lo que termina la comunicación segura, este mensaje consiste en un intercambio del hash de toda la conversación, de manera que ambos están seguros que los mensajes fueron recibidos intactos (íntegros).

La versión más actual de **SSL** es la v3, existen otro protocolo parecido a **SSL** solo que es desarrollado por **IETF** que se denomina **TLS** (**T**ransport **L**ayer **S**ecurity Protocol) y difiere en que usa un conjunto un poco más amplio de algoritmos criptográficos. Por otra parte existe también **SSL** plus, un protocolo que extiende las capacidades de **SSL** y tiene por mayor característica que es interoperable con **RSA**, **DSA/DH** y **CE** (**C**riptografía **E**líptica).



El protocolo SSL

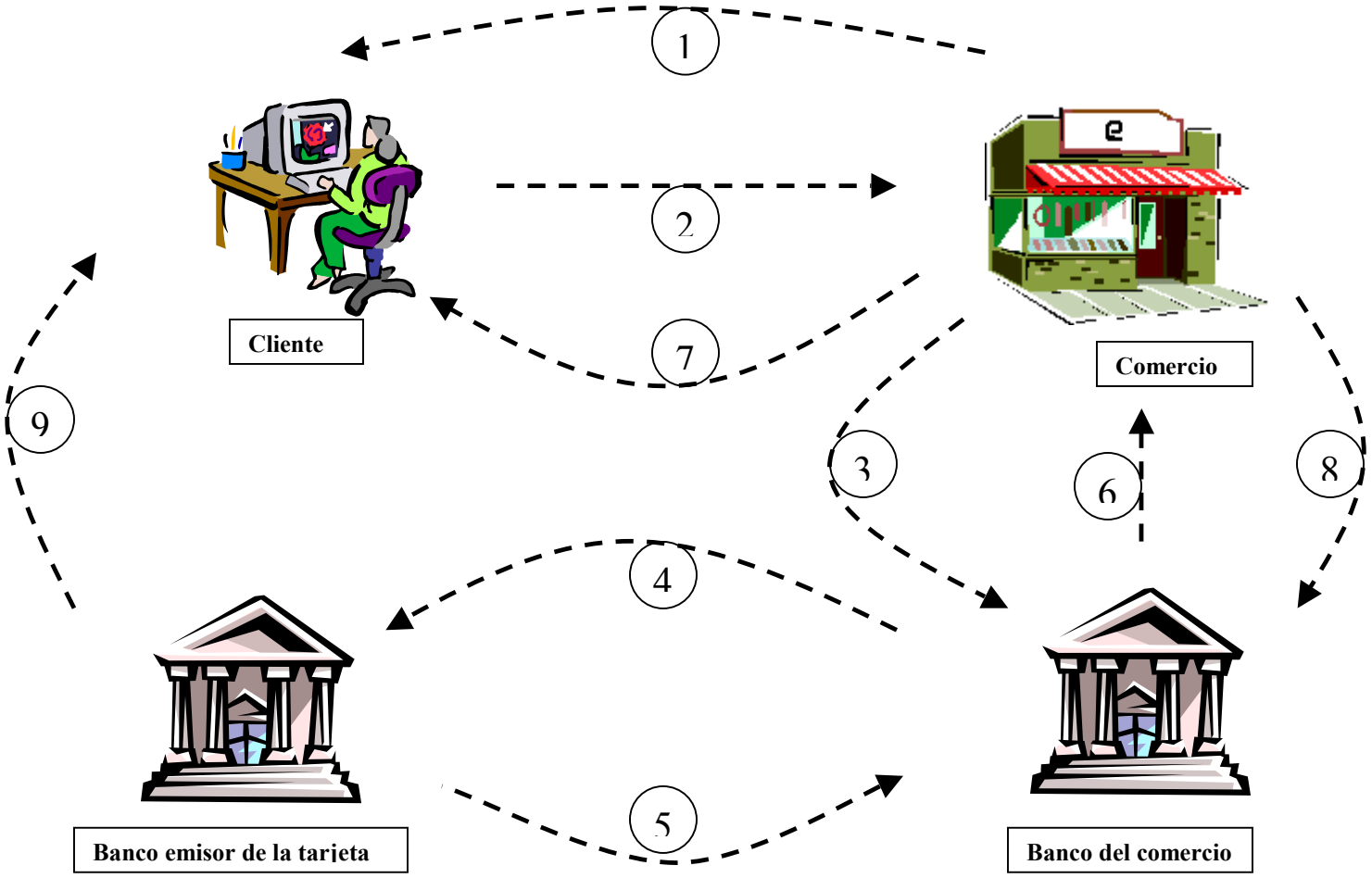
SET este protocolo esta especialmente diseñado para asegurar las transacciones por Internet que se pagan con tarjeta de crédito. Esto es debido a que una gran cantidad de transacciones de compra por Internet son efectuadas con tarjeta de crédito, por otro lado **SSL** deja descubierto alguna información sensible cuando se usa para lo mismo. La principal característica de **SET**, es que cubre estos huecos en la seguridad que deja **SSL**.

Por ejemplo con **SSL** solo protege el número de tarjeta cuando se envía del cliente al comerciante, sin embargo no hace nada para la validación del número de tarjeta, para chequear sí el cliente esta autorizado a usar ese número de tarjeta, para ver la autorización de la transacción del banco del comerciante etc., Además que el comerciante puede fácilmente guardar el número de tarjeta del cliente. En fin todas estas debilidades son cubiertas por **SET**, éste permite dar seguridad tanto al cliente, al comerciante como al banco emisor de la tarjeta y al banco del comerciante.

El proceso de **SET** es mas o menos el siguiente:

1) **El cliente inicializa la compra**: consiste en que el cliente usa el browser para seleccionar los productos a comprar y llena la forma de orden correspondiente. **SET** comienza cuando el cliente hace clic en "pagar" y se envía un mensaje de iniciar **SET**.
2) **El cliente usando SET envía la orden y la información de pago al comerciante**: el software **SET** del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.
3) **El comerciante pasa la información de pago al banco**: el software **SET** del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.
4) **El banco verifica la validez del requerimiento**: el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.
5) **El emisor de la tarjeta autoriza la transacción**: el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.
6) **El banco del comerciante autoriza la transacción**: una ves recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.

7) **El servidor del comerciante complementa la transacción**: el servidor del comerciante da a conocer que la transacción que la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.
8) **El comerciante captura la transacción**: en la fase final de SET el comerciante envía un mensaje de "captura" a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.
9) **El generador de la tarjeta envía el aviso de crédito al cliente**: el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.



SET requiere un certificado digital en cada paso de autenticación y usa dos pares de claves, una para el cifrado del sobre digital y otra para la firma, (**SSL** solo usa un par de claves), actualmente **SET** usa la función hash **SHA-1**, **DES** y **RSA** de 1024 bits, estos

parámetros fueron tomados para ser compatible con los certificados existentes, aunque el piloto de **SET** usó el sistema asimétrico de cifrado con curvas elípticas y se piensa que soporte también curvas elípticas en la próxima versión de **SET**.