# DISEÑO DE UN CENTRO COMERCIAL VIRTUAL EN INTERNET PARA SOPORTAR SERVICIOS DE COMERCIO ELECTRÓNICO EN EL PORTAL TAMPU

## ANEXO I AL PROYECTO DE GRADO

## FUNDAMENTO TEORICO Y ARQUITECTURA DE INTERNET


**Jairo Iván Sánchez M.**

**Director:**
**Ing. Diego Mauricio López**

**UNIVERSIDAD DEL CAUCA.**
**FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES.**
**POPAYÁN**
**2002**

# INDICE DE CONTENIDO

# 1. FUNDAMENTO TEÓRICO.

Para lograr un mejor y mayor entendimiento de este proyecto, es necesario cubrir brevemente algunos temas y elementos relacionados con las tecnologías y el enfoque del área a la que pertenece.

## 1.1 BASES DE DATOS.

Una Base de Datos es, esencialmente, un conjunto de datos ordenados en filas y columnas que se cargan y se ven en un programa de Planilla de Cálculos. Cada dato esta compuesto por un grupo de informaciones llamadas **campos**; entonces podemos decir que una base de datos es un banco de informaciones ordenadas en filas y columnas.

*¿Por qué utilizar un Sistema de Base de Datos?*

- Un sistema de Base de Datos ofrece a la organización un control centralizado de su información.
- Esto contrasta con un enfoque de archivos donde cada aplicación tiene sus propios datos (archivos), de modo que los datos están dispersos y difíciles de controlar.

## 1.2 SERVIDORES.

Básicamente, un servidor es un dispositivo que provee uno o más servicios para varios clientes a través de una red.

Hay multitud de tipos de Servidores. Algunos de los más importantes para Internet son:

- Servidor de aplicaciones WEB.
  Por medio de los servidores de aplicaciones Web, es posible consolidar la funcionalidad de toda clase de aplicaciones en una nueva interfaz de usuario, es decir, la *World Wide Web.*

  Los servidores en cuestión eliminan la necesidad de que los clientes conecten directamente todos los sistemas cruciales en los servicios de *back-end*, dado que para eso hace falta que todos los empleados tengan conocimientos extra sobre cada aplicación. Con un servidor de aplicaciones web, las aplicaciones del *back-end* son accesibles mediante un navegador

- Servidor de avisos:
  Responsable de la administración de avisos tipo *Banner* de varios sitios Web. Estos servidores ofrecen estadísticas acerca de las visitas y de los movimientos de los clientes, además de funcionalidades tales como rotación de banners, de manera tal que el cliente no vea dos veces el mismo aviso cuando vuelve a visitar una de las páginas web del sitio.

- Servidor Proxy:
  Un servidor proxy recupera documentos solicitados de un servidor, y los traslada a un cliente. La ventaja de emplear este tipo de servidor es que generalmente almacena documentos. Es mucho mas rápido recuperar documentos de un servidor proxy que de un servidor web, especialmente si los documentos ya han sido solicitados por otro usuario.

- Servidor DNS :
  Es un ordenador que traduce nombres de ordenadores en direcciones IP.

En Internet todos los ordenadores son referenciados por el protocolo IP por un grupo de cuatro números. Si todos los ordenadores fuesen referenciados de esa manera, y debido a la inmensa cantidad de Servidores que hay, sería fácil confundirnos de número e irnos a uno indeseado. Pues bien, si nosotros pudiéramos escribir el nombre del sitio donde queremos ir, sería más sencillo. De eso se trata. Nosotros escribimos un nombre, y el DNS traduce ese nombre en número y nos devuelve el número de dónde debemos ir.

El servidor DNS es tan importante que se tiende a duplicar, es decir, si nosotros accedemos a un Servidor DNS "caído", deberemos contemplar la posibilidad de acceder a otro.

Igualmente, existen diversos servidores con características y funcionalidades determinadas por un servicio tales como servidores FTP, servidores de correo, servidores de noticias, servidores IRC, etc.

No hay razón por la cual un ordenador sólo pueda tener un Servicio en marcha. Podemos encontrarnos con servidores de aplicaciones Web y FTP en el mismo ordenador y ambos funcionarían correctamente, si bien un número elevado de Servicios en marcha podría ralentizar las respuestas a las peticiones de los clientes y aumentar el grado de insatisfacción de los mismos.

## 1.3 MÉTODOS DE PAGO POR INTERNET.

Como en el mundo real, en Internet se han establecido tres tipos de sistemas de pago distintos: sistemas prepagos, de pago inmediato y de pago diferido. Como el

término prepago lo indica, primero se paga y luego se puede adquirir un producto o servicio.

Los sistemas prepago funcionan básicamente a través del ahorro de dinero digital en el disco rígido o una tarjeta inteligente, podrían ser vistos como el equivalente digital del efectivo. El archivo que contiene el dinero electrónico se denomina *billetera virtual.* El dinero electrónico puede utilizarse en cualquier momento para pagar productos o servicios en línea. La ventaja del efectivo electrónico es que es anónimo. Nadie puede rastrear al pagador del producto o servicio. Si los productos deben entregarse físicamente, esta ventaja se pierde. La desventaja es el almacenamiento, si el archivo o la tarjeta se pierden, se pierde el dinero, como ocurriría si uno perdiera la billetera. Cualquiera que encuentre el contenido de la billetera, puede utilizarlo para pagar.

Los sistemas de pago inmediato se basan en el sistema de pago en el momento de la transacción. Son los más difíciles de implementar, ya que requieren acceso directo a las bases de datos de los bancos, para poder realizar el pago en un instante. Asimismo se requiere un sistema de seguridad más estricto que en los otros casos, ya que los sistemas de pago inmediato son los más potentes. Para esta solución es necesario establecer un límite para reducir las posibilidades de fraude.

En las transacciones prepagas o de pago diferido, el acceso al banco se realiza antes o después de ejecutarse el procesamiento de la orden misma. El dinero es debitado de la cuenta bancaria en el mismo momento en que tiene lugar la transacción. Por otro lado, los sistemas de pago diferido permiten comprar un producto y pagar mas adelante. Las tarjetas de crédito son uno de los sistemas de pago diferido más comunes tanto en el mundo real como en el cibernético.

Las tarjetas de crédito sirven en circunstancias particulares, pero son muy costosas. Esto se debe principalmente al bajo nivel de seguridad (que depende del

grabado en relieve, las bandas magnéticas, firmas y listas de inhabilitados), y el elevado y creciente costo del fraude resultante. Además, los costos de procesamiento de las transacciones son importantes.

Las tarjetas débito presentan una seguridad relativamente elevada, porque requieren del consumidor que confirme algo que solo el titular de la tarjeta debería saber: la clave. Pero si bien los costos por errores y fraude son muy bajos, los costos de comunicación asociados a transacciones íntegramente en línea son elevados.

### 1.3.1 Sistemas de pago diferido.

#### *1.3.1.1 Soluciones con tarjeta de crédito.*

El pago con tarjeta de crédito constituye hoy día el método de pago que mas se prefiere y utiliza en Internet. El uso de las tarjetas de crédito es simple, y se las acepta mundialmente.

El sistema de pago con tarjeta de crédito presenta algunas ventajas sobre otras formas de pago. Las tarjetas se emiten y aceptan en el mundo entero, y ofrecen a los consumidores la posibilidad de sumar todos los gastos y pagar el total mas adelante. El sistema de tarjetas de crédito ofrece buena protección al consumidor, ya que éste tiene derecho a devolver los productos en un plazo determinado y cuestionar los cargos, ya que no se debitan directamente de su cuenta. Las tarjetas de crédito no se hayan sujetas a monedas nacionales. Sin importar donde se efectúe la compra de los productos, el cambio de moneda se efectúa automáticamente para el cliente. El mecanismo de uso de las tarjetas de crédito por Internet se asemeja mucho al sistema de encargos por correo y teléfono, por cuanto cualquiera puede comprender por qué funciona en cuestión de segundos.

El este sistema de pago hay cuatro participantes: el consumidor, el comerciante, el emisor y el adquiriente. Para que una tarjeta de crédito pueda ser utilizada, el consumidor y el comerciante deben establecer relaciones con el emisor y el adquiriente, respectivamente. El emisor entrega al consumidor una tarjeta de crédito. El comerciante se acoge a un adquiriente para poder aceptar un tipo de tarjeta o varios.

Los consumidores que se dirigen entonces al comerciante deseando adquirir productos o servicios, le presentan su tarjeta de crédito. Éste verifica la validez de la tarjeta mediante el envío de la información de la misma al adquiriente. A través de la red financiera, se transmite la solicitud al banco del cliente. El banco verifica entonces la información y reenvía la autorización al comerciante por medio del adquiriente.

Aunque todavía existen compañías que solicitan el número de la tarjeta de crédito al del consumidor sin que se encripte la información, la mayoría de las empresas utilizan encriptación para proteger la información privada de la tarjeta de crédito, la orden y el cliente. Sin la encriptación sería muy fácil para los *hackers* interceptar los mensajes y utilizarlos o alterarlos para sus propios fines.

Mediante el uso de programas especiales, denominados *sniffers*, los delincuentes pueden copiar la información desencriptada y utilizarla para efectuar pagos. Mientras no se requiera una dirección de envío, la información de la tarjeta de crédito puede ser fácilmente utilizada en forma fraudulenta, para pagar servicios en línea, por ejemplo. Si bien el robo de información por Internet no es nada nuevo, Internet permite a los delincuentes robar más sistemáticamente. A fin de reforzar la seguridad de los pagos con tarjeta de crédito, se han establecido dos estándares en los últimos años: la encriptación SSL (Secure Sockets Layer), desarrollada por Netscape y SET (Secure Electronic Transactions)[1], desarrollada por Visa y Mastercard. Las diferencias entre SSL y SET son evidentes. SSL solo

[1] http://www.setco.com

encripta el tráfico entre el navegador de red y el servidor de red (la computadora del usuario y la computadora del comerciante). SET, por otro lado, ofrece una solución de pago completa, que abarca no solo al consumidor y al comerciante, sino también al banco necesario para el pago con tarjeta de crédito.

SET.

SET fue diseñado exclusivamente para asegurar las transacciones vía Internet, mientras que SSL es un sistema genérico de encriptación que puede emplearse para transmitir cualquier tipo de datos. SET combina tecnologías de seguridad existentes y encriptación de clave pública, con uso de certificados digitales tanto para los titulares de las tarjetas de crédito como para los comerciantes. La PKI (Public Key Infraestructure) se define dentro del rango de SET. La PKI se utiliza para verificar que el participante de la transacción sea realmente la persona o institución que dice ser. Esto es importante ya que Internet no ofrece ningún mecanismo estándar para la verificación de una persona o institución. Con este mecanismo es posible introducir el concepto de validación de las transacciones con base en Internet. Los consumidores que pagan vía SET no pueden cuestionar desconocer la transacción, ya que todas las órdenes quedan firmadas digitalmente. La firma digital no puede ser falsificada. Aparte de esta característica, la PKI se utiliza para enviar información encriptada vía Internet. Mediante el uso de una encriptación sólida es posible transmitir transacciones con tarjeta de crédito a través de redes públicas, como Internet.

SET fue desarrollado para la confidencialidad de la información de las órdenes y pagos. Toda la información en una transacción vía SET se halla encriptada. La integridad de los datos se ve asegurada a través del código digital de dispersión, que se anexa a cada mensaje y permite al receptor verificar que el mensaje no haya sido alterado en el camino. Mediante el uso de certificados digitales, es posible demostrar que el titular de una tarjeta de crédito es su legítimo usuario. También se requiere la autenticación del comerciante, para ser debidamente identificado por el banco adquiriente. El protocolo de SET no depende de las

medidas de seguridad del transporte y no impide su uso; por ejemplo, la encriptación SSL puede sumarse a la de SET. Como los programas con SET son desarrollados por numerosos vendedores de Software, la compatibilidad es muy importante.

SET ofrece algunas características de privacidad que dificultan la obtención de información del cliente. Sólo se revelará la información que un participante realmente requiera ver. Un comerciante, por ejemplo, no necesita verdaderamente conocer los detalles de la tarjeta de crédito. Esta información puede ser transmitida directamente al banco y éste puede confirmarle al comerciante la validez de la información y autorizar la transferencia del dinero. SET no solo define la encriptación. Los flujos de transacción, formatos de mensaje y algoritmos de encriptación, forman parte del estándar, para garantizar la integridad y confidencialidad de los mensajes y la autenticación de los usuarios.

En SET 2.0 se introducirá más seguridad, gracias al soporte para tarjetas inteligentes. Las tarjetas de crédito contarán entonces con un chip adicional en el plástico, que contendrá el certificado digital y la clave pública y privada del usuario, que se requiere para llevar a cabo una transacción vía SET. Actualmente solo algunas tarjetas débito cuentan con este chip. Las soluciones de tarjetas con chips ofrecen más seguridad y conveniencia para sus titulares. Esto también permitirá que mas personas la utilicen. Hoy día, sigue siendo difícil conseguir un certificado digital e instalarlo.

Mediante el uso de una tarjeta con chip, los consumidores podrán utilizar cualquier dispositivo de red habilitado por SET, en cualquier lugar, como computadoras y dispositivos *set-top* para televisión en el hogar, computadoras en la oficina y teléfonos públicos. Un beneficio adicional para la industria de las tarjetas, es la semejanza entre las transacciones vía SET y las transacciones convencionales por cajero automático y punto de venta (POS), con uso de tarjeta con chip. Esto simplificará los procedimientos de procesamiento y operación.

En este momento, varias pruebas piloto del C-SET (Transacciones electrónicas seguras aseguradas por chip) se hallan en curso en la Unión Europea. La comisión europea ha adoptado C-SET como especificación recomendada. La tarjeta inteligente ofrece autenticación y encriptación. El diseño también incluye una *gateway* bancaria mejorada, que maneja la mayor parte del proceso de pago, lo que reduce el costo y la complejidad para el comerciante.

A fin de resolver cuestiones legales relacionadas con la encriptación, las funciones criptográficas se hallan implementadas del lado bancario, para evitar regulaciones que prohíban una amplia distribución de software criptográfico.

Existen muchas otras formas posibles de pago con tarjeta de crédito. La desventaja de estas soluciones reside principalmente en que no son abiertas y se ven restringidas a un prestador de servicio determinado. La lista a continuación brinda un panorama sencillo de tres soluciones.

WIRECARD.

La solución WireCard[2] consiste en varios módulos que la hacen apta para transacciones *business-to-business* y *business-to-consumer*. El módulo de pago seguro en línea, que es lo que interesa en este punto, permite la transmisión segura de la información de la tarjeta de crédito de un consumidor a un comerciante, mediante un *applet* de Java que encripta la información utilizando 2.048 bits. El applet emplea los algoritmos RSA y Blow-Fish para la encriptación, lo que lo hace muy seguro. Con las tecnologías de hoy, llevaría aproximadamente $10^{22}$ (10.000.000.000.000.000.000.000) años decodificar la información de la tarjeta de crédito.

Como la compañía tiene su sede en Alemania, el software puede exportarse sin restricciones a cualquier otro país. Por otra parte, la solución no se ve limitada a

[2] http://www.wirecard.com

un determinado navegador o sistema operativo, lo que la convierte en una muy buena solución para el pago en línea con tarjeta de crédito.

Una vez que se ingresó la información de la tarjeta de crédito, el *applet* encripta los datos y los envía al servidor, que recupera la información y la transmite a un banco para su validación. Cuando se efectúa la validación, el comerciante recibe una notificación que le indica que proceda con la transacción. La validación de *back-end* es efectuada por el módulo de *clearing*, que permite que las tarjetas de crédito sean chequeadas en tiempo real (que es más seguro) o por lotes (que es más económico).

CYBERCASH.

La solución CyberCash[3] encripta detalles de tarjetas de crédito, como lo hacen SSL y SET, pero el procedimiento difiere un poco. La información de la tarjeta de crédito del cliente es enviada al comerciante, encriptada de tal forma que éste no pueda desencriptarla. El comerciante transmite la información al servidor de CyberCash, junto con el monto correspondiente al pedido del cliente. Desde el servidor de CyberCash, se inicia el pago a través de las redes financieras.

FIRST VIRTUAL.

First Virtual se fundó en 1994, y es el único sistema de pago seguro en línea sin encriptación. La seguridad en el sistema First Virtual[4] se ve garantizada por el requerimiento de una confirmación del cliente vía e-mail. Si el cliente no responde en un determinado plazo, con un determinado código, no se ejecuta la orden. A fin de evitar que se espíen las informaciones de las tarjetas de crédito, se intercambian identificaciones especiales en su lugar. Se requiere ingresar el número de la tarjeta de crédito una vez en el servidor First Virtual, al que se le asigna una clave virtual que se utiliza en las transacciones. El usuario debe llamar

[3] http://www.cybercash.com

[4] http://www.fv.com

a First Virtual y comunicar su número de tarjeta de crédito; la información nunca se envía por Internet. El servidor de First Virtual inicia la transacción de pago a través de las redes financieras.

Durante las fases más exitosas, en 1996 más de 2.000 comerciantes y 200.000 consumidores a nivel mundial utilizaron el sistema para el pago de productos. Hacia fines de 1998, el sistema de pagos con tarjeta de crédito vía First Virtual quedó en suspenso, ya que no había suficiente demanda porque muchos invertían en el estándar SET, que en aquel entonces estaba por convertirse en el sistema de pago con tarjeta de crédito, y en la tecnología de encriptación multipropósito SSL.

#### *1.3.1.2 Cheques de Internet.*

Hasta ahora, los cheques de Internet no gozan de gran repercusión en la red; aún así, es importante comprender la forma en que pueden utilizarse. Pueden ser valiosos para una determinada actividad comercial. Los cheques electrónicos funcionan como los convencionales. Los clientes reciben documentos digitales de sus bancos y deben ingresar el monto del pago, la moneda y el nombre del beneficiario para cada transacción de pago. Para el cobro del cheque electrónico, el pagador debe firmarlo digitalmente.

En los Estados Unidos el uso que se da a los cheques difiere del de Europa. La mayoría de las soluciones existentes de cheques electrónicos, están basadas en el sistema norteamericano, es decir, que el cheque debe ser firmado por el pagador y el beneficiario. El beneficiario lleva el cheque al banco, cobra el dinero y luego el banco remite el cheque al pagador.

NETCHEQUE

En 1995, el Instituto de Ciencias de la Información de la Universidad del Sur de California[5] desarrollo el sistema NetCheque, que implementa todos los requisitos mencionados anteriormente.

El comprador y el vendedor deben tener una cuenta en NetCheque. A fin de que esta sea realmente segura, se utiliza una identificación de tipo Kerberos y una contraseña. Para pagar por cheque, es necesario instalar un software especial de cliente que funciona como una chequera. Gracias a este software, el cliente puede enviar un cheque encriptado al comerciante.

El comerciante puede recibir el dinero a través de un banco o bien puede utilizar el cheque en una transacción con un proveedor. Una red contable especial verifica los cheques, y envía el visto bueno al comerciante, que entonces entrega los productos. Si bien el sistema también es apto para micropagos, nunca prosperó en realidad. El principal inconveniente es la infraestructura de clave pública que se requiere para intercambiar certificados y firmar los cheques. En 1995, esa infraestructura no estaba disponible, y simultáneamente comenzaron a prosperar las transacciones con tarjeta de crédito. Otro punto débil de NetCheque fue asimismo su reducida base inicial de consumidores y comerciantes.

PAYNOW

El servicio PayNow, desarrollado por CyberCash, brinda soporte para micropagos mediante cheques electrónicos. La billetera CyberCash para Internet contiene los cheques PayNow, que pueden utilizarse en comercios en línea que admitan el estándar CyberCash. El cheque electrónico funciona similar a las tarjetas con chip con capital almacenado; el consumidor carga previamente capital en una billetera CyberCash, aunque el verdadero dinero permanece en el banco.

ECHECK

[5] http://www.usc.edu

El cheque electrónico FTSC (*echeck*)[6] se hallaba hasta hace poco en fase piloto en el departamento del tesoro de los Estados Unidos. El *echeck* logra una migración del sistema de pago del mundo real al virtual, con una menor cantidad de pasos manuales. Se adapta a las actividades comerciales actuales, eliminando la necesidad de costoso procesos de reingeniería. El sistema *echeck* es muy seguro y pueden utilizarlo todos los clientes bancarios con cuentas corrientes. Estas cuentas existen en Estados Unidos y solo hasta este momento están ganando reconocimiento en Europa.

Los *e-checks* contienen la misma información que los cheques impresos y se basan en el mismo esquema legal. Los cheques electrónicos pueden intercambiarse directamente entre las partes y reemplazar todas las transacciones a distancia en las que hoy día se utilizan cheques impresos. Los *echecks* funcionan de la misma forma que los cheques tradicionales. El cliente completa el *echeck* y lo remite electrónicamente al beneficiario. Éste último deposita el cheque electrónico, se le acredita, y el banco del beneficiario efectúa el "*clearing*" del *echeck* con el banco pagador. El banco pagador valida el *echeck* y deduce el monto del cheque de la cuenta del cliente.

Los *echecks* ofrecen la posibilidad de llevar a cabo transacciones bancarias en forma segura, vía Internet. El banco puede verificar la validez de los *echecks* automáticamente, lo cual reduce las pérdidas por fraude para las partes involucradas. El uso de FSML (Financial Service Mark Language), de las firmas digitales y de los certificados hace que el sistema sea muy seguro.

#### *1.3.1.3 Pago Contra Entrega.*

[6] http://www.echek.org

Otro modelo de pago diferido que funciona *off-line* es el de pago contra entrega (COD). Los clientes pueden encargar productos y servicios en línea y abonarlos al recibirlos en el domicilio. Jeans & Jackets[7], emplea este método para su negocio en línea. Los clientes pueden explorar el catálogo en línea o el impreso, encargar por teléfono, fax, e-mail o directamente en la página web y recibir los productos en su domicilio. En caso de no tener oficina en la localidad, el empleado del servicio postal es el encargado de recibir el efectivo luego de entregar la mercancía. La ventaja de esta sistema para Jeans & Jackets es que utiliza un datáfono inalámbrico cuando se trata de pagos domiciliarios con tarjeta débito en localidades con oficina, y en otro caso, recibe el dinero del servicio postal y no requiere verificar en cada caso que el cliente quiera pagar por los productos. Si el cliente no quiere pagar al recibir el paquete, éste se reenvía al remitente normalmente.

Este sistema facilita la venta de productos y servicios a personas desconocidas que por algún motivo no desean pagar con tarjeta de crédito. Por otra parte, no hay espera en el pago de la factura por el cliente. El COD suele ser más costoso, ya que comprende el servicio postal. Normalmente, los costos de COD corren por cuenta del cliente.

#### *1.3.1.4 Requerimientos de Software.*

Para permitir el pago mediante tarjeta de crédito con uso de encriptación SSL, lo único que hace falta es un certificado digital en el servidor web que encripta el tráfico entre el consumidor y el comerciante. El certificado puede ser generado por un servidor de certificados, que puede instalarse en el sitio del comerciante independientemente del sistema, o se lo puede comprar, por ejemplo, VeriSign[8],

[7] http://www.jeans&jackets.com

[8] http://www.verisign.com

ya que estos certificados son aceptados por todos los navegadores. En el caso de certificados creados por entidades no reconocidas, como un comercio, los consumidores deben aprobar el certificado antes de utilizarlo por primera vez. El problema de SSL es que no existe ningún mecanismo estándar en los servidores que permita comunicarse con los bancos. Esta cuestión debe resolverse caso por caso.

Muchos bancos ofrecen la tercerización de los métodos de pago. La empresa dispone de un sitio de venta y ellos se ocupan del pago. Ésta es la mejor solución, especialmente para pequeñas empresas. Existen muchos proveedores de servicios de pago como NetBanx, MasterMerchant[9], que ofrecen servicios de pagos especiales para libros, sitios web para adultos y casinos en línea. El estándar SET requiere la instalación de software especial en la computadora del cliente, el servidor del comerciante y la *gateway* del banco. Este software regula la comunicación requerida para la transacción con tarjeta de crédito entre las partes implicadas. Hewlett Packard e IBM ofrecen soluciones completas para el estándar SET. La solución de Hewlett Packard se basa en el software de Verifone[10], que la empresa adquirió en 1997, denominado vSuite[11]. Contiene cuatro productos: vWallet para el cliente, vPOS para el comerciante, vGate y omnihost para el banco. IBM ofrece su IBM Payment Suite[12], que abarca los siguientes productos: IBM Consumer Wallet, IBM Payment Server, IBM Payment Gateway e IBM Payment Registry. Existen muchos otros vendedores, de menor envergadura, del software SET. Puede hallarse una lista completa en el sitio de SetCo[13].

Verifone ha desarrollado un nuevo producto llamado Pay Works, que puede actuar como base y *hub* central para cualquier configuración de aplicación IPS

[9] http://www.mastermerchant.com

[10] http://www.verifone.com

[11] http://www.verifone.com/solutions/internet

[12] http://www.software.ibm.com/commerce/payment

[13] http://www.setco.org/matrix.html

(Intagrated Payment Solution), el componente de aplicación IPS Switch que traslada los mensajes de pago de un componente u opción IPS a otro. El software maneja una amplia variedad de información, incluyendo transacciones con tarjeta de crédito (mediante SET o SSL, por ejemplo), transacciones de débito, pagos y otros mensajes relacionados con pagos. El IPS Switch es apenas uno entre muchos componentes que forman parte de la IPS: también contiene otros que manejan créditos y débitos, captura y liquidación de órdenes de pago, líneas de crédito privadas, interfaces de emisor e incluso seguridad para Internet.

### 1.3.2 Sistemas de Pago Inmediato.

#### *1.3.2.1 Tarjetas Débito.*

Las tarjetas débito también se utilizan frecuentemente, de hecho se usan más en Europa que en Estados Unidos donde las tarjetas de crédito son más comunes. La diferencia entre tarjetas de crédito y débito es que para pagar con las segundas hay que conocer el Número de Identificación Personal (PIN), y se requiere de un dispositivo hardware que pueda leer la información almacenada en la banda magnética al dorso, mientras que en las tarjetas de crédito, toda la información está escrita al frente.

Hasta ahora no existe el comercio con tarjetas débito en Internet, dado que ninguna computadora viene equipada con un dispositivo que pueda leer la banda magnética. Al bajar los precios de estos dispositivos, se venderán con cada computadora. La tendencia indica una migración de las tarjetas con bandas magnéticas a las tarjetas inteligentes con chips electrónicos. Hoy día, estas últimas se utilizan principalmente para el efectivo electrónico, pero en el futuro reemplazarán a las tarjetas débito y a las de crédito.

#### *1.3.2.2 Débito Directo.*

El débito directo es otra solución de pago diferido que se utiliza en las transacciones en línea. PureTec[14], proveedor alemán de servicios de Internet, emplea este sistema para el pago de sus servicios, que abarcan registros de dominio y ofrecimientos de sitios web. En lugar de solicitar el número de tarjeta de crédito del usuario, PureTec le pide su número de cuenta bancaria y el código del banco. El dinero puede ser debitado directamente de la cuenta bancaria. El único problema con este sistema es la firma.

Para obtener dinero de un banco, se necesita una firma válida del cliente en la nota de pedido. Como no se ha establecido aún una legislación para las firmas digitales, es necesario imprimir la nota completa, firmarla y enviarla por fax a PureTec.

El débito directo no constituye todavía una solución de pago inmediato, pero con la elaboración de leyes de certificación digital en curso, en poco tiempo los primeros sitios web y bancos aceptarán las firmas digitales de sus clientes para el débito de sus cuentas.

#### *1.3.2.3 Requerimientos de Software.*

Para el débito directo o se requiere ningún software especial, ya que en la mayoría de los países los bancos aún no aceptan las firmas digitales. En Alemania está a punto de establecerse el estándar HBCI, que no solo permite el débito directo, sino también otras aplicaciones bancarias. Un formulario web especial alcanza para

[14] http://www.puretec.de

reunir toda la información relevante de los clientes, que luego deben imprimir y enviar por fax al comerciante. Todo el proceso es manual, pero los datos ingresados en el formulario pueden ahorrar tiempo, puesto que los detalles bancarios se guardan en formato digital. El formulario enviado por fax se utiliza para autorizar la transferencia de dinero. Una vez aceptadas las firmas digitales, un software especial en el servidor del comerciante transmitirá la transacción al banco, donde la transferencia de dinero se iniciará en un instante.

### 1.3.3 Sistemas de Prepago.

#### *1.3.3.1 Efectivo Electrónico.*

Las soluciones de efectivo electrónico utilizan software para guardar el equivalente del efectivo en un disco rígido o en un disquete. Las monedas y billetes son reemplazados por archivos con firma digital. La ventaja de este sistema es que el costo de transferencia del dinero es prácticamente nulo (el único costo real en el que se incurre estaría constituido por el valor del tiempo que dura la conexión a Internet). Para obtener dinero debe recurrirse a un cajero automático virtual en Internet, o a uno en el mundo real, donde se puede obtener efectivo electrónico mediante débito directo a la cuenta bancaria o pago con tarjeta de crédito. El problema del efectivo electrónico reside en lograr implementarlo con suficiente seguridad. Como el dinero se almacena en archivos, se debe garantizar que la copia de los archivos no aumentará el capital, ni se podrá alterar el monto del dinero digital en el disco rígido. Las monedas y billetes electrónicos deben poseer marcas digitales que hagan imposible su uso más de una vez. El uso de tecnologías de encriptación y firmas digitales y electrónicas contribuye a reducir la posibilidad de fraude.

DIGICASH

El efectivo electrónico de DigiCash[15] se denomina eCash. DigiCash intentó establecerlo junto con una red de proveedores de servicios y productos que lo aceptaran. Las librerías, los casinos y los periódicos en línea han aceptado este dinero a cambio de productos, juegos e información. La solución de dinero electrónico de DigiCash es muy exitosa.

Para poder usar eCash, el consumidor debe abrir una cuenta en un banco adherido a DigiCash, luego debe transferir una determinada suma a esa cuenta y recibe el dinero en forma de efectivo electrónico, que puede almacenar en su disco rígido. El dinero se almacena en forma de fichas. El efectivo electrónico que los consumidores obtienen del banco también se transfiere a una cuenta bancaria especial a través de la cual los comerciantes cobran las transacciones financieras. El sistema eCash es un sistema de sentido único, con fichas, que permite que el dinero se utilice una sola vez. El comerciante no puede utilizar el dinero electrónico recibido del cliente para pagar otra cosa: debe llevarlo al banco para cobrarlo. Las transacciones de igual a igual, entre consumidores, son posibles, pero requieren un banco intermediario para la conversión de las fichas. Cada ficha contiene la ficha que representa, un número aleatorio que se usa como número de serie y la firma digital del banco emisor, el banco puede validar el efectivo electrónico sin saber quién lo utilizó, lo que permite el uso anónimo del dinero electrónico. Esto se logra mediante un sistema llamado *blind signature* (firma ciega), esta es un algoritmo cuya patente está en trámite, inventado por David Chaum, el fundador de DigiCash. En términos simples, digamos que un consumidor que adquiere dinero electrónico genera fichas en crudo. A cada ficha se le agrega un número de serie y luego se las envía al banco del consumidor. El número de serie resulta invisible para el banco, porque se lo multiplica por otro número al azar (el factor ciego). El banco le agrega una firma digital a la ficha y la reenvía al consumidor. Este último puede dividir el número de serie entre el factor ciego y obtener el número de serie original nuevamente. Mediante este mecanismo, el banco no puede rastrear las fichas hasta los consumidores, al no

[15] http://www.digicash.com

poder ver los números de serie originales. El consumidor puede entonces, visitar un sitio web que admita eCash y pagar con los archivos de su disco rígido. Un comerciante que desee aceptar eCash debe también abrir una cuenta en un banco adherido a DigiCash, para poder cobrar el dinero aceptado. Los costos de transacción son nulos con el modelo de DigiCash. En 1998, más de 150 sitios web aceptaron eCash, hasta que DigiCash quebró a fines de ese año. Las transacciones con tarjeta de crédito han destruido el negocio de DigiCash, aunque están en la búsqueda de nuevos inversionistas para reconstruir el servicio con un mejor modelo comercial.

CYBERCOINS

Además de la solución de CyberCash para tarjetas de crédito, existe asimismo un sistema para los micropagos denominado CyberCoins. Este sistema permite a comerciantes y consumidores comprar y vender productos digitales vía Internet. Los CyberCoins pueden tener un valor de 0,25 a 10 dólares, lo cual es demasiado bajo para su uso en compras con tarjetas de crédito.

En un servidor especial de Internet se provee “contenedores de efectivo” especiales para cada consumidor y comerciante, que funcionan como cuentas CyberCoin. Mediante el uso de la billetera CyberCash, es posible transferir dinero a la cuenta CyberCoin. Para poder pagar, un comando especial del navegador web se comunica con la billetera, y solicita al cliente que acepte el pago. Una vez aceptado, el dinero es transferido electrónicamente de la cuenta del cliente a la del comerciante. La comunicación se ve asegurada mediante encriptación. El encargo del cliente es enviado al comerciante, que le agrega sus datos y envía la orden completa a la *gateway* de CyberCash, la que entonces efectúa el movimiento del dinero entre las cuentas.

MICROPAGO IBM

El sistema desarrollado por la división de pagos de IBM Israel en Haifa[16] es un sistema de micropago que permite transformar vínculos HTML simples en vínculos de pago. Por ende es necesario que haya proveedores de servicios de Internet entre consumidores y comerciantes. El sistema utiliza la infraestructura de pago existente en los ISP. Los clic en un vínculo dado se registran en los archivos *log* del comerciante y pueden atribuirse a un consumidor determinado. El pago requerido se transfiere luego al ISP, que debita el dinero de la cuenta bancaria del cliente. Por ahora existen algunas pruebas piloto en Internet.

MILLICENT

MilliCent[17] ha sido desarrollado por DEC (Digital Equipment Corporation). Se basa en el sistema de cupones, que permite pagos por debajo del límite del centavo. Estos cupones se denominan *scrip*. Se requieren intermediarios para el pago en el comercio electrónico. Los intermediarios son típicamente ISP o entidades financieras. Estos venden vales de intermediario a los consumidores y administran los *scrips* de los comerciantes, que difieren en cada caso. Para pagar, el cliente debe canjear un *scrip* de intermediario por un *scrip* de comerciante. Los *scrips* se administran entonces en la billetera MilliCent. Con un *scrip* de comerciante, el consumidor puede pagar productos, información y servicios en un comercio dado, sin intervención de un tercero. Esto hace que MilliCent sea una solución económica para los negocios con micropagos. Aunque hay varias pruebas piloto en curso, no queda claro si el sistema prosperará, principalmente porque no garantiza el anonimato.

### *1.3.3.2 Tarjetas Inteligentes.*

Las tarjetas inteligentes son muy populares en Europa y su aceptación aumenta en los Estados Unidos. Las tarjetas telefónicas, de cobertura médica y débito poseen chips incorporados que contienen dinero, información médica y bancaria.

[16] http://www.hrl.il.ibm.com/mpay

[17] http://www.millicent.digital.com

Cada tarjeta débito emitida en Europa (llamada EC Card) contiene información sobre el titular y su cuenta. Los sistemas han sido desarrollados para almacenar efectivo en el chip, además de los otros datos. El dinero de la tarjeta se halla encriptado y protegido mediante una contraseña, en pos de la seguridad de esta solución. Para pagar mediante tarjeta inteligente, es necesario introducir la tarjeta en un terminal hardware. El dispositivo requiere una clave especial del banco emisor para iniciar una transferencia de dinero en un sentido u otro.

Las tarjetas inteligentes ofrecen a los comercios la ventaja de evitar el transporte de mucho dinero en el momento del cierre diario; pueden en cambio transferir el dinero electrónicamente a su cuenta bancaria en el momento del pago. De hecho, el dinero virtual utilizado para pagar productos puede ser transferido en un instante al banco del comerciante. La mayor ventaja de las tarjetas inteligentes es que se pueden utilizar tanto en el mundo real como en el cibernético. Con la tarjeta inteligente, es posible ir a un banco, cargarlo y pagar en Internet. Lo contrario también es posible: un comerciante ofrece un servicio en Internet, les cobra a los clientes que transfieren su dinero a la tarjeta que le pertenece, y puede cobrar el dinero en su banco o transferirlo en pago de otro servicio.

Sus dos grandes ventajas son su relativa seguridad y la simplicidad de las operaciones *off-line*. Juntas, se traducen en bajos costos de transacción.

### 1.3.4 El Futuro de los Pagos

#### *1.3.4.1 SEMPER*

En el futuro existirán estructuras altamente integradas que contribuirán a hacer negocios seguros vía Internet. Las soluciones de pago serán solo un segmento de la infraestructura, puesto que el pago no afecta el proceso de “comercialización”

general en forma abierta y extensible. La comercialización abarca más que la realización de los pagos; incluye, por ejemplo, ofertas, recibos, comprobantes de pago y atención al cliente, componentes que los consumidores reclaman en el mundo real y que por ende deben estar presentes en el virtual. Esta sección se concentrará en cuatro proyectos: dos para el área de transacciones *business-to-consumer* (SEMPER y el Protocolo de Comercialización Abierta), y los dos restantes, más concentrados en las transacciones *business-to-business* (Global Trust Enterprise y OBI). En cada caso se identificarán las soluciones de pago utilizadas.

SEMPER (Secure Electronic Marketplace for Europe)[18] es un proyecto de investigación fundado por la Unión Europea para permitir el pago con dinero electrónico vía Internet. El proyecto SEMPER intenta identificar la infraestructura requerida para el entorno. El proyecto que lo precedió, CAFÉ (Conditional Access for Europe), ya identificó los requerimientos para pasaportes electrónicos, registros de conducir digitales y dinero electrónico en aplicaciones del mundo real. Los terminales y cajeros automáticos pueden identificar al usuario y permitir el almacenamiento de dinero electrónico.

Muchos sistemas de pago por Internet, diferentes e incompatibles, compiten entre sí. La mayoría de los comercios en línea acepta sólo un subgrupo limitado, y algunos aceptan un solo sistema de pago. Idealmente, cada comercio en línea debería poder brindar soporte para cualquier método de pago disponible, pero sin un incremento de los costos para el comerciante. Sin una estructura de pago unificada, el arquitecto de la solución para un comercio en línea, debe implementar cada método de pago, uno tras otro, lo que incrementa los costos. En consecuencia, se requiere una estructura general de servicios de pago que desligue el modelo comercial del modelo de pago. La estructura debe lograr que los diferentes modelos de pago sean transparentes para la aplicación comercial.

[18] http://www.semper.org

La estructura SEMPER consiste en un núcleo de seguridad y diferentes servicios a su alrededor. Los servicios se dividen en módulos. En este momento existen módulos de encriptación, certificación y pago. Es posible comunicarse con estos módulos desde aplicaciones comerciales, a través del núcleo de seguridad, mediante una API especial.

La conexión entre el proceso de pago y el comercial consiste en un núcleo de seguridad debe definirse a través de una jerarquía de API que represente los modelos de pago, como tarjeta de crédito o dinero electrónico. Es preciso implementar lo siguiente para complementar las API: los modelos de pago deben seleccionarse automáticamente para que las aplicaciones no se ocupen de ello; deberían ocuparse solo del valor del pago y del beneficiario, y habría que crear herramientas que permitan la incorporación de modelos de pago en éste modelo genérico de servicios de pago.

Para el sistema SEMPER, se ha creado un servicio genérico de pago basado en Java. Puede ampliarse bastante fácilmente, mediante la adición de nuevas clases a la clase genérica de pago. Hasta ahora, se han implementado SET y DigiCash; así, los usuarios del servicio genérico de pago pueden realizar transacciones financieras con gente que utilice SET o DigiCash. Sólo es cuestión de esperar a que aparezcan otros módulos que le den valor a todo el sistema. Gracias a la condición modular de Java y a la estructura abierta, la implementación no constituye un problema. Resulta más difícil convencer a los propietarios de los estándares patentados que admitan una infraestructura de estándar abierto, ya que esto implica que revelen el código fuente.

#### *1.3.4.2 El Protocolo de Comercialización Abierta.*

El Protocolo de Comercialización Abierta (OTP)[19] complementa los protocolos de pago electrónico actuales al abordar el proceso de realización de negocios. El OTP ofrece medios para negociar la comercialización y la compra y venta, apelando a los protocolos de pago subyacentes.

El objetivo de OTP es reducir el costo de comercialización. Esto se logra mediante el uso de Internet como canal de distribución coherente, económico y seguro. La estructura requerida se describe como parte del OTP. Este protocolo habilita nuevos modelos de comercialización disponible solamente en Internet. La estructura permite modelos de pago de dos (pago directo) o tres partes (pago indirecto). El protocolo es abierto, flexible, extensible, robusto y neutro con respecto a los vendedores, lo cual lo hace ideal para Internet. Que sea abierto significa que las especificaciones no son secretas, la flexibilidad permite la creación de ofertas de servicios diferenciadas; el carácter extensible implica que pueden integrarse modelos de comercialización y pago nuevos o mejorados, sin interrumpir el servicio de los demás componentes; la robustez del protocolo alude a que toda la infraestructura puede cubrir errores o tiempo de inactividad de los servidores y clientes participantes. Como el protocolo es abierto, cualquier vendedor de software independiente puede crear software compatible con el estándar. Esto ofrece a los comercios la capacidad de elegir entre una gama de productos con características similares, independientemente del vendedor de software independiente.

Los costos de atención al cliente pueden reducirse significativamente mediante el OTP, ya que presenta un método muy flexible, aunque estándar, de ofrecer información sobre un pago determinado. La información puede extraerse luego para resolver cuestiones de pago. El OTP brinda soporte para la entrega digital y física de productos. Toda la cadena de comercialización se ve conectada por la información; así, la información de entrega y la de pago pueden asociarse.

[19] http://www.otp.org

#### *1.3.4.3 Compra Abierta en Internet (OBI)*

OBI[20] es una estructura íntegramente disponible para las transacciones entre comercios. El estándar contiene una arquitectura detallada, especificaciones técnicas y normas concisas, e información sobre compatibilidad y cuestiones de implementación. Cualquier organización o individuo puede adquirir una copia del estándar OBI y utilizarla para crear un producto, servicio o solución.

La arquitectura de OBI está basada en la idea de que los propietarios de los procesos comerciales deben ser responsables de la información vinculada a estos. Los proveedores, por ejemplo, deben ser responsables del contenido del catálogo en línea y los precios, mientras que las organizaciones de compras, deben ser responsables de la información sobre perfiles y códigos contables.

La arquitectura normalmente involucra a tres organizaciones: el proveedor, el comprador y la autoridad de pago. El solicitante que efectúa el encargo vía Internet forma parte de la organización adquiriente. Para identificar al solicitante, se utiliza un certificado digital. La organización de compras maneja el servidor, como el servidor OBI, para recibir los encargos y darles curso, junto con la información sobre el perfil de los solicitantes. El departamento de compras también mantiene la relación con los proveedores y se ocupa de los precios.

La autoridad de pago brinda los procesos necesarios para la autorización del pago entre el comprador y el proveedor. La autoridad de pago es, en la mayoría de los casos, una institución financiera, por ejemplo un banco.

La comunicación entre las partes en la negociación se efectúa mediante un protocolo http estándar y encriptación SSL, con uso de navegadores web

[20] http://www.openbuy.org

estándar, para que los costos para el comprador sean bajos. La información se transmite vía Internet. Cuanto mayor sea el número de compañías que adapten el estándar OBI, más económica será la compra. Hasta ahora se realizan pruebas piloto con OBI, pero no se ha visto una implementación concreta en Internet. Queda por verse si el estándar OBI tendrá éxito en el negocio MRO/ORM (Mantenimiento, Reparación y Operación / Administración de Recursos Operacionales).

#### *1.3.4.4 Global Trust Enterprise.*

Global Trust Enterprise (GTE) ha sido desarrollado por CertCo[21] de los Estados Unidos, junto con varios bancos asociados de todo el mundo. Fuero varios los motivos que dieron lugar a la creación del servicio, pero la idea original fue crear una herramienta potente para habilitar las transacciones entre comercios. La idea se basa en el principio de la participación abierta de instituciones financieras, y cada vez más bancos se están adhiriendo a la iniciativa. Aparte de las transacciones entre comercios y consumidores en Internet, que dependen de modelos de autenticación bilateral, GTE busca llevar este modelo a un entorno multilateral (múltiples participantes), ya que los comercios suelen tener más de un empleado. El mayor obstáculo para la implementación de redes mundiales intercomerciales es la cuestión de la confianza en la identidad. A través del nuevo sistema, las compañías que efectúen negocios electrónicos podrán identificar al socio comercial. CertCo emite certificaciones de identidad que permiten a compradores y vendedores manejar el riesgo. Esta confianza en los socios comerciales permite a las empresas efectuar transacciones de alta integridad, autenticadas y confiables, con socios comerciales conocidos o no, vía Internet.

[21] http://www.certco.com

El comercio internacional, las compras corporativas y la entrega de contenidos representan algunas de las típicas transacciones intercomerciales cubiertas por GTE. Un ejemplo podría ser una mediana empresa caucana de artesanías que desea expandir su mercado, minimizar los costos y desarrollar negocios con varios importadores de Europa y Norteamérica. Los certificados digitales emitidos por los bancos participantes permiten que se genere una confianza mutua entre exportadores e importadores para negociar los precios y firmar los contratos. Los certificados también pueden usarse para auditar las transacciones. Una vez que las compañías participantes han obtenido los certificados de sus bancos, están en condiciones de emprender negocios vía Internet con cualquier otra compañía registrada en alguna de las instituciones participantes.

A través de la estructura GTE, los clientes corporativos podrán utilizar los servicios provistos por los bancos participantes. Una típica transacción de compra y venta requeriría del vendedor que solicite a la entidad financiera que verifique la firma digital del comprador. El banco del comprador y el del vendedor se pondrían en contacto automáticamente a través de la red e intercambiarían las informaciones requeridas. En este caso, el banco del comprador verificaría la firma y enviaría una certificación de validez; lo mismo ocurriría si el comprador deseara que se verificara el certificado digital del vendedor. Para habilitar la comunicación entre participantes, se ha establecido un sistema y proceso estándar para la certificación de identidad. El sistema GTE actúa como autoridad certificadora de base para las entidades financieras y puede realizar una auditoria para controlar la adhesión a una serie de reglas del sistema y prácticas comerciales predefinidas.

# 2 ARQUITECTURA DE INTERNET.

## 2.1 INTRODUCCIÓN.

Internet es una red de redes de computadoras. Toda red que desee conectarse a Internet debe utilizar un conjunto de protocolos de comunicación denominados IP (Protocolos de Internet). Las redes están constituidas por nodos y canales que proveen la infraestructura básica de comunicación. Existen dos tipos básicos de nodos: los terminales y los intermediarios. En la mayoría de los casos, los nodos terminales son los servidores y los clientes, que proveen o solicitan un conjunto de servicios. Generalmente los clientes son computadoras que los usuarios utilizan para comunicarse con otros nodos, mientras que los servidores son proveedores de servicios centralizados que, entre otras cosas, ofrecen funciones de servidor web o de correo a los clientes.

Los nodos intermediarios suelen ser computadoras de funciones reducidas que reenvían tráfico entre segmentos de red. Estos dispositivos que se denominan *enrutadores (routers)* y *puentes (bridges)*, pueden utilizarse en ciertas ocasiones para filtrar ciertas solicitudes o para restringir el acceso a ciertos dispositivos de una red. Sin embargo, ni los clientes ni los servidores pueden acceder a los servicios que ofrece un nodo intermediario.

No es necesario utilizar otros dispositivos como nodos terminales o intermediarios: los servidores también pueden funcionar como clientes o como *routers* en forma simultánea. Cada nodo cuenta con un identificador único llamado dirección IP. Los sistemas de mayor envergadura pueden llegar a tener varias direcciones IP, a las

que se les suele asignar un nombre de dominio para que sean más fáciles de recordar.

Los canales necesarios para la comunicación entre nodos pueden implementarse de diferentes maneras. En la mayoría de los casos se utiliza un sistema de cables que conecta los nodos terminales a través de los intermediarios. El cable utilizado puede ser coaxial, de fibra óptica o el tradicional de cobre. Las velocidades de conexión varían de acuerdo al tipo de cable utilizado. No obstante, ya que se utilizan los mismos protocolos de transmisión, no es necesario rescribir las aplicaciones para los diferentes canales. Además de las conexiones físicas, es posible transmitir en forma inalámbrica. Estas transmisiones electromagnéticas se realizan en diferentes frecuencias: sistemas infrarrojos, *links* de microondas, telefonía celular y comunicación por *link* satelital.

En líneas generales, todos los nodos se comunican entre sí a través de Internet, dado que esto no siempre es deseable por cuestiones de seguridad, algunos nodos intermediarios pueden denegar la conexión con ciertos nodos. Dispositivos denominados *firewalls,* impiden que el público acceda a las redes exclusivas de empresas (intranets). Debido a que las intranets utilizan el mismo conjunto de protocolos, cualquiera podría acceder a los datos confidenciales de las empresas. Los *firewalls* también se emplean para proteger datos de los gobiernos y todo tipo de información que se desee incluir en una red para el uso de un grupo en particular.

Teniendo en cuenta que Internet aparentemente no pertenece a nadie, resulta sorprendente que todavía funcione a la perfección. Una de las razones para ello es que en la actualidad las redes ya no se conectan en forma directa entre sí, sino que utilizan *backbones;* con esta estructura se ha logrado organizar las redes y normalizar el tráfico. Estos sistemas son conexiones de alta velocidad que vinculan segmentos de red separados y que ofrecen conexiones a redes ajenas mediante puntos de intercambio o *gateways.* En realidad, se puede decir que los

*backbones* de Internet son la verdadera autopista informática. Las redes locales son más bien como ciudades, en las que las calles están más congestionadas y son más estrechas.

Los protocolos básicos de Internet se planifican y controlan en forma jerárquica. Aunque cualquiera puede contribuir al desarrollo de nuevas tecnologías y protocolos, solo unas pocas organizaciones tienen influencia sobre lo que se incluye en el grupo de protocolos de Internet.

El IETF (Internet Engineering Task Force)[22] es el impulsor de los nuevos estándares. Este organismo está constituido por una comunidad internacional de empresas que diseñan y operan redes, investigan nuevas tecnologías y venden productos desarrollados a partir de esas investigaciones. Aunque es un organismo abierto, está dirigido por compañías que intentan acordar nuevos estándares para proveer más servicios de Internet y a la vez mejorar su funcionamiento. Los estándares de Internet propuestos por el IETF se denominan RFC (Request For Comments)[23]. Aunque los estándares RFC son borradores, una vez que se convierten en estándares conservan su nombre.

El IESG (Internet Engineering Steering Group)[24] es el responsable de la administración técnica de las actividades del IETF y del proceso de estándares en Internet.

El tercer grupo que ejerce influencia sobre los nuevos estándares es la ISOC (Internet Society)[25], una organización constituida por expertos de Internet que aporta su opinión con respecto a políticas y usos. Se preocupa de supervisar otras

[22] http://www.ietf.org

[23] http://www.ietf.org/rfc

[24] http://www.ietf.org/iesg.html

[25] http://www.isoc.org

comisiones y grupos especiales relacionados con cuestiones vinculadas a políticas de Internet.

El famoso W3C (World Wide Web Consortium)[26] no tiene injerencia directa sobre los estándares de Internet. Esta organización es responsable de los estándares de la web, que se establecen por sobre los de Internet. Cabe aclarar que Internet y la web no son lo mismo.

## 2.2 GRUPO DE PROTOCOLOS DE INTERNET.

Para lograr una comunicación estable entre nodos conectados a Internet, se estableció un conjunto de reglas que contienen una gran cantidad de funciones agrupadas en protocolos. Esa familia de protocolos se denomina IPS (Internet Protocols Set).

Los protocolos se basan en las capas del modelo OSI/ISO (Interconexión de Sistemas Abiertos / International Standards Organization). Las capas inferiores de este modelo desarrollan funciones alojadas de carácter técnico, mientras que las capas intermedias son utilizadas por las aplicaciones y se sustentan en el buen funcionamiento de las capas inferiores, sin necesidad de conocer en detalle su forma de operación. Los protocolos de las capas superiores están basados en la funcionalidad que requiere una aplicación, por lo que reducen drásticamente la complejidad de las aplicaciones. Cualquier aplicación puede establecer una conexión a Internet con facilidad, sin necesidad de saber nada del hardware utilizado para el acceso, ya sea un módem o un enrutador.

[26] http://www.w3.org

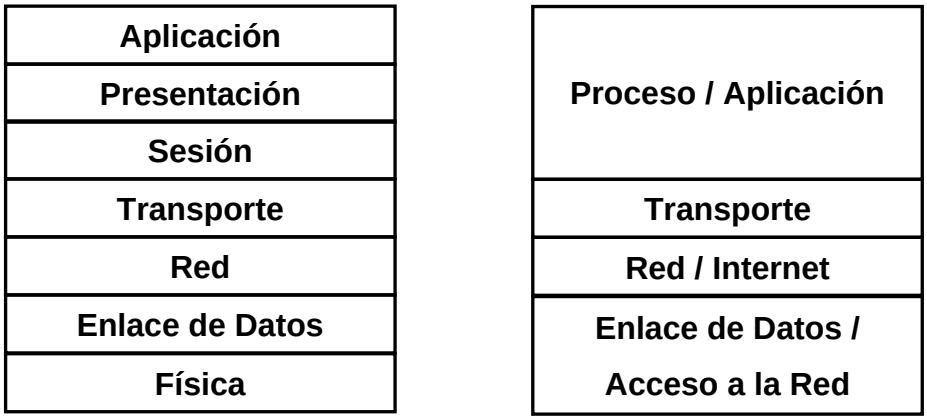


**Figura 4.1 Comparación del modelo de referencia OSI y del modelo del protocolo Internet**

El IPS utiliza, solo cuatro de las siete capas del modelo OSI/ISO: las de enlace, de red, de transporte y de aplicación. La capa inferior, la de enlace es la responsable del acceso a la red: se encarga de conectar el nodo con el canal y de especificar como se realiza dicha conexión. El resultado es la transmisión de una señal convertida en paquetes constituidos por bits que contienen la información. Esa señal parte desde un puerto físico (por ejemplo, un puerto paralelo o un RJ-11) hacia un canal, que puede ser una cable de fibra óptica o de cobre. Los protocolos mas comunes para la capa de enlace son la FDDI (Fiber Distributed Data Interface), utilizada para crear redes ethernet, y el PPP (Protocolo Punto a Punto), para redes token ring. El software utilizado para la capa de enlace se conoce también como administrador de dispositivos; generalmente está incorporado a la tarjeta de red.

La capa siguiente a la de enlace, es la capa de red. Es responsable del direccionamiento de los datos y de la transmisión de la información. Los protocolos definen la manera en que los paquetes se desplazan por la red, es decir, la forma en que se dirige la información desde el nodo inicial hasta el terminal. La información se representa como segmentos y paquetes, y estos últimos están constituidos por segmentos de bits o bytes. La capa de red utiliza el protocolo IP.

Otro protocolo utilizado en este nivel se encarga del *multicasting*, es decir, el envío de un mismo mensaje a destinatarios múltiples, lo que reduce el ancho de banda necesario para transmitir la información. Este protocolo, denominado IGMP (Internet Group Management Protocol), se utiliza para transmisiones de audio y video en Internet.

El nivel siguiente es la capa de transporte, se encarga de la distribución de los datos a un nodo en particular. Esta capa verifica si se puede garantizar la recepción de mensajes completos y exactos. La información se representa en mensajes y segmentos; los primeros están constituidos por grupos de paquetes. La capa de transporte divide los mensajes más grandes en segmentos para su posterior distribución. Existen dos protocolos importantes en esta capa: el TCP, que es el principal, provee un servicio de transmisión de mensajes confiable.

La capa de aplicación se ocupa de la distribución de los datos de una a otra aplicación ubicada en el mismo o en otro nodo de la red. Esta capa utiliza mensajes para encapsular la información. Entre los protocolos de este nivel se incluye el HTTP (Hypertext Transfer Protocol), que se ocupa de la transmisión de documentos HTML; el SMTP (Simple Mail Transfer Protocol), que transfiere mensajes desde y hacia cualquier nodo; y el FTP (File Transfer Protocol), que transfiere archivos entre nodos.

Aunque esta estructura puede parecer complicada, en realidad simplifica la implementación del IPS. Al segmentar la información en mensajes, paquetes, bytes, bits y señales según la capa que se utilice, se facilita el desarrollo de software que contenga el protocolo requerido. Cada capa puede implementarse en forma individual, sin conocimiento detallado de las otras capas, lo que hace que el software resulte más sencillo y robusto. Además también facilita la integración de paquetes de software de diferentes proveedores, aunque operen en distintos niveles. El uso de protocolos comunes permite que se los utilice en forma transparente.

## 2.3 IPV6.

En la actualidad, Internet se basa en el IPv4 (Protocolo de Internet versión 4), que administra alrededor de 4 mil millones de direcciones IP. En 1990, ya se habían asignado alrededor del 20% de las direcciones IP disponibles, y la cantidad de asignaciones se duplicaba cada 14 meses. Sin un cambio de paradigmas, todo el espectro de direcciones IP se habría acabado antes de 1994. Para esa época se empezó a trabajar en IPv6.

En 1999, la mayor parte de Internet todavía utilizaba al IPv4, y aún quedan direcciones disponibles, gracias a la introducción de direcciones IP dinámicas para usuarios de Internet que no tienen una conexión permanente. En la actualidad, los ISP utilizan una reserva de direcciones IP que se asignan a los usuarios en el momento de conectarse a la red.

Aunque no se prevé una escasez de direcciones IP en el futuro próximo, todavía hay muchas razones para implementar una nueva generación del protocolo de Internet. En el RFC1726[27] se define el estándar IPv6. El motivo original de la creación de esta nueva versión era el espacio limitado para las direcciones IP. Con el IPv6, el espacio ha aumentado de $2^{32}$ (4.294.967.296, un número de 10 dígitos) a $2^{128}$ (una cifra enorme de 39 dígitos), lo que permite el soporte de $10^{12}$ nodos y $10^{9}$ redes.

Para posibilitar la transición hacia el IPv6, es necesario que éste brinde soporte para paquetes IPv4. El nuevo estándar debe tener compatibilidad retroactiva para permitir que los sistemas y dispositivos antiguos funcionen con la nueva pila de protocolos.

[27] http://www.ietf.org/rfc/rfc1726.txt

La implementación actual del protocolo de Internet parte de la premisa de que los dispositivos y las redes no son móviles. Sin embargo, cada vez existen más dispositivos móviles que se conectan a Internet, como los teléfonos celulares y los PDAs. Incluso hay redes completas que están adquiriendo movilidad. Un automóvil provisto de computadoras, impresoras y scanners es un ejemplo de una red móvil. La conexión a Internet debe ser dinámica; con el IPv4 es necesario interrumpir y reanudar la conexión. El IPv6 debe soportar protocolos de depuración y control con el fin de mejorar la administración de la red.

Sobre la base de esta propuesta, muchas empresas involucradas en las tecnologías de red crearon software y dispositivos compatibles con el IPv6. El proyecto Internet 2[28] que se está desarrollando en los Estados Unidos se basa en la nueva pila de protocolos para permitir la introducción, el desarrollo y el análisis de nuevos servicios y aplicaciones.

## 2.4 REDES DE ATM.

Otra tecnología interesante que ha emergido en los últimos años es la de ATM (Modo de Transferencia Asincrónico), una nueva tecnología de red diseñada especialmente para comunicaciones multimedia de última generación, como la telefonía, el video o los datos generados por computadora.

Además del TCP/IP, el ATM ofrece nuevos protocolos diseñados para administrar datos sensibles a las demoras, como los de audio y video. Estos nuevos protocolos aportan una red homogénea para todo tipo de tráfico y son independientes del contenido que se transporta.

[28] http://www.internet2.edu

La información se transporta en células de tamaño constante que permiten una conmutación rápida, lo que facilita la transmisión de datos sensibles a los retardos a través de las mismas redes que se utilizan para el tráfico de datos informáticos. En vez de funcionar con una tasa de datos fija, cada aplicación decide el ancho de banda que necesita y lo solicita en la red. El ancho de banda bajo demanda se ha transformado en una realidad.

Los protocolos de ATM son muy escalables. Aunque esta tecnología se emplea principalmente para *backbones,* en la actualidad se basa en cableado de fibra óptica. Es posible implementar ATM sobre OC-48 (Optical Carrier de 2,5 Gbps), que ofrece un ancho de banda de 2488 Gbps. Sin embargo, la tecnología ATM no se limita a la fibra óptica. Si se la implementa de la manera correcta, puede funcionar sobre cualquier medio de transmisión.

El ATM Forum[29] es el organismo encargado de desarrollar y preservar los protocolos de esta tecnología. Esta organización sin fines de lucro se constituyó con el fin de acelerar la utilización de productos y servicios basados en ATM mediante una veloz convergencia de especificaciones de interoperabilidad. Una vez que se desarrolla y se aprueba un estándar, se lo presenta ante la ITU (International Telecommunications Union).

Hay muchos motivos para pensar que ATM será la tecnología de redes del futuro. Uno de ellos es que fue diseñada en forma proactiva para enfrentar los problemas inherentes a las próximas generaciones de redes.

Gracias a la proliferación de aplicaciones multimedia, las tecnologías de este tipo han tenido mucho éxito, debido a su capacidad de administrar todos los aspectos relacionados con el audio, el video y los datos. Otro motivo es que las mejoras de la capacidad que pueden aportar son de una magnitud tal que justifican la inversión necesaria. La escalabilidad del ancho de banda permite establecer redes

[29] http://www.atmforum.com

que transmitan a velocidades de giga bits por segundo. También se cuenta con la posibilidad de aumentar la cantidad de nodos de red, gracias a la arquitectura de red conmutada.

El motivo más importante del éxito futuro de la tecnología ATM es que se basa en estándares, los que, junto con la interoperabilidad, son el factor de más importancia para el *internet-working*. El desarrollo de estándares robustos aplicados de manera estricta es más importante que las limitaciones técnicas que pueda tener un sistema.