NOTAS DEL CURSO

MATERIA: COMERCIO ELECTRÓNICO
PLAN: 98
LICENCIATURA: ADMINISTRACIÓN
SEMESTRE: 9º
AREA: MERCADOTECNIA
COMPILADOR: DAVID KANAGUSICO HERNANDEZ
FECHA DE CREACIÓN: domingo, 25 de diciembre de 2005

OBJETIVO:

AL FINALIZAR EL CURSO, LOS ALUMNOS SERÁN CAPACES DE BRINDAR SOLUCIONES A LAS EMPRESAS QUE DESEEN INCURSIONAR A LOS NEGOCIOS POR INTERNET, ORIENTANDO SUS IDEAS DE NEGOCIOS HACIA EL COMERCIO ELECTRÓNICO.

INDICE

I. INTRODUCCIÓN A INTERNET

1. INTRODUCCIÓN

Internet fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado ARPANET (Advanced Research Project Network según su sigla en ingles) fue iniciado en 1969 y cuyo principal propósito era la investigación y desarrollo de protocolos de comunicación para redes de área amplia, para ligar redes de transmisión de información de diferentes tipos; capaces de resistir las condiciones de operación más difíciles y continuar funcionando aún con la pérdida de una parte de la red.

Estas investigaciones dieron como resultado el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) un sistema de comunicaciones muy sólido y robusto bajo el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet. Durante el desarrollo de este protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen así a la red de redes más grande del mundo, las funciones militares se separaron y se permitió el acceso a la red a todo aquel que lo requiriera sin importar de que país provenía la solicitud siempre y cuando fuera para fines académicos o de investigación (y por supuesto que pagara sus propios gastos de conexión), los usuarios pronto encontraron que la información que había en la red era por demás útil y si cada quien aportaba algo se enriquecería aún más el cúmulo de información existente.

Después de que las funciones militares de la red se separaron en una sub-red de Internet (llamada MILNET), la tarea de coordinar el desarrollo de la red recayó en varios grupos, uno de ellos, la National Science Foundation fue el que promovió bastante el uso de la red ya que se encargo de conectar cinco centros de contención de información a los que se accedía desde cualquier nodo de la red. Debido al trafico de datos se superaron las cargas de información que podía soportar, entonces se dio la concesión a Merit Network Inc. para que administrara y actualizara la red, se mejoraron las líneas de comunicación dando un servicio mucho más rápido, pero este proceso de mejora nunca termina debido a la creciente demanda de los servicios que se encuentran en la red.

El enorme crecimiento de Internet se debe en parte a que es una red basada en fondos gubernamentales de cada país que forma parte de Internet lo que proporciona un servicio prácticamente gratuito. A principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la red.

Internet ha influido en nuestras vidas y en nuestras costumbres, en nuestra forma de buscar información, de entretenernos, de comunicarnos y por supuesto han aparecido nuevas formas de comprar y vender bienes.

Estos cambios traen grandes beneficios, por ejemplo hoy en día las personas se comunican desde dos puntos muy distantes del planeta, ya sea a través del teléfono o de algunos de los medios que ofrece Internet; así mismo, las

empresas han encontrado grandes oportunidades en los desarrollos de las comunicaciones, destacando que los costos de las comunicaciones se reducen y que estas tecnologías están al alcance tanto de grandes empresas como de pequeñas empresas.

El desarrollo de estas tecnologías y de las telecomunicaciones ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada vez mas y creando nuevas formas de comercio, y en este marco se desarrolla el Comercio Electrónico.

2. SERVICIOS DE INTERNET

Los servicios mas importantes de Internet son los siguientes:

CONCEPTO DE TELNET
Telnet es la aplicación Internet para acceso remoto a otra computadora.
La sintaxis de telnet es: telnet://Nombre de la máquina. El puerto por estándar para telnet es el 23. Una vez se ha llegado se requiere tener cuenta y una password. Y se pueden utilizar los programas que estén autorizados para el usuario de dicha cuenta.
Un programa telnet, como casi todos los de Internet, consiste en dos piezas de un software que cooperan entre ellos: el cliente, que se ejecuta en el ordenador que solicita el servicio, y el servidor, que se ejecuta en el ordenador que proporciona el servicio.

Cuando hacemos telnet el cliente hace lo siguiente:

A. Crea una conexión de red TCP con un servidor
B. Acepta entrada de datos de una forma determinada
C. Reformatea esa entrada de datos a algún formato que pueda enviar al servidor
D. Acepta salida de datos del servidor en algún formato estándar
E. Reformatea esa salida para visualizarla en la pantalla/impresora, etc.

CONCEPTO DE FTP
FTP significa "File Transfer Protocol" o protocolo para la transferencia de archivos. Como implica su nombre, el trabajo del protocolo es mover archivos de una computadora a otra. Los servidores FTP son programas y máquinas que contienen un repositorio de archivos accesibles para un grupo restringido de usuarios o en el caso de los FTP anónimos, para todos los usuarios.
La sintaxis de FTP es: ftp://Nombre de máquina.
Una vez el cliente se conecta al servidor es necesario disponer de un nombre de usuario y una palabra clave para acceder a los recursos accesibles en el servidor FTP, generalmente programas o documentos aunque también pueden existir otro tipo de archivos.

La gran diferencia entre telnet y ftp es que con ftp la computadora cliente es capaz tanto de transferir archivos desde el servidor como de transferir archivos al servidor.

FTP ANÓNIMO

FTP anónimo es un FTP especial que a diferencia del FTP normal o identificado permite que todo el mundo pueda acceder al servidor sin necesidad de que el administrador de la máquina tenga que abrir una cuenta para cada usuario que desee acceder. En realidad se abre una cuenta pública, cuyo login es anonymous y que no requiere password o bien la password puede ser cualquier dirección de correo electrónica válida. En este tipo de servidores FTP generalmente no se pueden crear ni borrar directorios ni archivos y si se permite la transferencia de archivos al servidor suele estar limitada en cuanto al espacio y el tiempo que pueden estar dichos archivos en el servidor.

CORREO ELECTRÓNICO

El correo electrónico es uno de los servicios de Internet que más se utiliza. No obstante, el protocolo de correo de Internet, Simple Mail Transfer Protocol (SMTP, Protocolo de Transferencia de Correo Simple), está limitado a la transmisión de texto formateado en US-ASCII. Esto significa que los usuarios no pueden enviar, como parte de un mensaje electrónico, documentos con formateos más complejos, gráficos, archivos de sonido o, incluso, textos acentuados.

Una posible solución a este problema es la implantación de MIME o Multi-purpose Internet Mail Extensions (Extensiones del Correo de Internet a Múltiples-usos). Las extensiones de SMTP permitirían la transmisión de archivos de múltiples partes, con múltiples juegos de caracteres, multimedia, etc. como si fuesen partes de un mensaje electrónico. Los mensajes basados en las extensiones MIME preservarían su estructura, podrían contener imagen, voz y otros archivos binarios, no requerirían decodificación manual de los enlaces por el usuario, y podrían contener elaboradas ediciones de texto con distintas tipografías, pudiendo utilizar subrayados, negritas, cursivas, etc.

SMTP es el protocolo utilizado por las computadoras centrales para enviar correo electrónico a través de toda la red mundial Internet. SMTP es muy sencillo y muy popular. Es precisamente de su simplicidad de donde surgió la necesidad de MIME. SMTP está basado en documentos formateados en ASCII de 7 bits, lo que permite a éstos transmitiese por una gran variedad de computadoras con diferentes sistemas operativos y seguir teniendo un formato legible cuando llegan a su destino. No obstante, no se pueden transmitir archivos en formato binario como los "exe" de los programas, archivos producidos con procesador de textos, imágenes gráficas y/o formatos de sonido. El protocolo SMTP simplemente no sirve para el envío de mensajes electrónicos en formato binario (longitud de 8 bits).

Las limitaciones de Internet han provocado considerables frustraciones entre los usuarios de la red. El envío de archivos binarios tales como documentos de procesador de textos, gráficos, voz o cualquier otro tipo de datos, es sencillamente inviable a menos que se convierta el archivo a formato ASCII y que se esté dispuesto a sacrificar el formateo y cualquier gráfico asociado al documento.

MIME no es un nuevo protocolo en el sentido de que el usuario no necesita implementar nuevo software de correo electrónico para disponer de las funcionalidades de MIME. Es, por el contrario, un modo normalizado de intercambiar mensajes electrónicos multimedia compatible con todos los correos SMTP. MIME especifica un modo normalizado de codificar y asociar ficheros y mensajes a los mensajes electrónicos SMTP. De hecho, todos los mensajes MIME, incluso aquellos que contienen imagen en movimiento y sonido estéreo, se envían a través de Internet como un fichero ASCII de 7 bits completamente imprimible.

MIME es también compatible con diversas plataformas. Dado que MIME preserva el formato binario del fichero, un usuario puede enviar un fichero DOS a un Apple Macintosh sin tener que convertirlo previamente a ASCII. Asimismo, se pueden enlazar los siguientes tipos de archivos o Texto ASCII: conocido como texto plano, más la norma ISO 8859 [Partes 1-91 para lenguas europeas, hebreas y arábigas, así como la norma ISO 2022 para texto Kanji.

Texto editado: permite cambios de tipografías, utilización de subrayados, cursivas, negritas y otros mecanismos de formateo.
Multiparte: hay múltiples mensajes de distintos tipos enlazados y visualizados secuencialmente o en paralelo (una imagen gráfica y un sonido descriptivo al mismo tiempo).
Archivos de Imagen: GIF (formato de intercambio gráfico para imágenes), JPEG (norma de compresión de imágenes para imágenes estáticas) y Grupo 3 FAX, que se visualizan o se salvan en otro archivo para imprimir o visualizar posteriormente.
Audio: sonido de calidad de telefonía básica para anotar un mensaje electrónico.
Vídeo: MPEG (normas de compresión de imágenes para imágenes en movimiento).
Aplicación: PostScript y otros lenguajes de interpretación de escrituras que permiten diálogo interactivo y supervisión a través del correo electrónico.

3. WORLD WIDE WEB

El World Wide Web (Web) es una red de recursos de información. Se basa en tres mecanismos que permiten que estos recursos sean accesibles para su lectura a la mayor cantidad posible de audiencia.

- Un esquema uniforme de nombres para localizar los recursos en el web (ej: URI's)
- Protocolos, para acceder a los recursos nombrados y que están en la web (ej: http)
- Un lenguaje hipertextual, para navegar fácilmente entre los recursos (ej: html)

Los URI's
Todos los recursos disponibles en el Web, un documento html, una imagen, un video clip, un programa, etc, tiene una dirección que puede ser codificada

mediante el Identificador de Recurso Universal, URI (Universal Resource Identifier). Un URI consta de tres partes:

- El nombre del esquema del mecanismo que se utiliza para acceder al recurso. (ej: http)
- El nombre de la máquina en la que está el recurso. (ej: rayuela.uc3m.es)
- El nombre y la ruta del recurso. (ej:/cursos/clase1.html)

Sin embargo, el URI es un concepto mucho más amplio. Los alumnos deben familiarizarse más con el concepto de URL, Localizador de Recurso Universal (Universal Resource Locator). El URL es un subconjunto del esquema de nombres de URI.
Los URL se refieren normalmente a un recurso pero también se pueden referir a un fragmento, a una parte de ése recurso, en este caso el URL finaliza con el signo " #" al que le sigue un texto que representa el nombre de ese fragmento del texto. (ej: http://rayuela.uc3m.es/cursos/clase1.html#epígrafe-2)
Los URL pueden ser de dos tipos: absolutos y relativos. Son absolutos cuando se respeta la sintaxis completa del nombre del recurso. Son relativos cuando no contienen el esquema de nombres habitual sino tan solo el nombre del recurso (ej:clase2.html). En este caso se entiende que el recurso tiene el mismo esquema y está en la misma máquina que el documento que se está visualizando en ese momento. (ej: ../imágenes/hipertext.jpg).
En HTML los URL se utilizan para:

- Enlazar a otro documento o recurso.
- Enlazar a un hoja de estilo externa o a un script.
- Para incluir una imagen, un objeto o applets en una página.
- Para crear un mapa de imagen sensible.
- Enviar un formulario.
- Para crear un marco en un documento.
- Para citar una referencia externa.
- Para referirse a convenciones de metadatos que describen un documento.

LOS PROTOCOLOS
Reglas que siguen dos computadoras para comunicarse entre sí.
Ejemplos:

- http://porky.uc3m.es/tony/tony.html
- https://porky.uc3m.es/tony/tony.html
- ftp://porky.uc3m.es/pub/bdocu/ala.txt
- mailto:tony@porky.uc3m.es
- gopher://porky.uc3m.es/infoDAB/congreso/960129.txt
- telnet://sauron.uc3m.es

HTML
HyperText Markup Language. Lenguaje hipertexto de marcas que sirve para publicar información que pueda ser distribuida de forma global. Una especie de "lengua madre" que todas las computadoras pueden potencialmente entender y que es el que se utiliza en el Web.

El HTML fue desarrollado por Tim Berners-Lee en el CERN y se popularizó mediante el programa Mosaic, desarrollado por el NCSA en 1990. HTML (2.0) fue aprobada en Nov. 95. HTML (3.2) fue aprobada en Enero de 1997. HTML 4.0 en abril de 1998.

ANCLAS

Un enlace es una conexión de un recurso web a otro, este concepto tan simple ha sido uno de los factores claves del éxito del Web.

Un enlace tiene dos puntos, llamados "anclas", y una dirección. El enlace comienza en el "ancla fuente" y apunta al "ancla destino", que puede ser otro recurso web o una zona o fragmento del mismo nodo o página.

La conducta asociada por defecto a un enlace es la recuperación de otro recurso web.

Para activar un enlace sólo hay que pulsar sobre él con el ratón (un click).

El elemento HTML que permite incluir anclas es el elemento <A, uno de cuyos atributos más importantes es el **"href"** que se encarga de especificar la dirección (URL) del ancla destino.

Aunque el uso más común de un enlace es la recuperación de otro recurso Web también es posible expresar otras relaciones entre recursos.

II. CONCEPTOS BÁSICOS DEL COMERCIO ELECTRÓNICO A TRAVÉS DE INTERNET

1. DEFINICIÓN DE COMERCIO ELECTRÓNICO

El comercio, es la actividad ancestral del ser humano, ha evolucionado de muchas maneras, pero su significado y su fin siempre es el mismo.

El comercio es "el proceso y los mecanismos utilizados, necesarios para colocar las mercancías, que son elaboradas en las unidades de producción, en los centros de consumo en donde se aprovisionan los consumidores, último eslabón de la cadena de comercialización. Es comunicación y trato".

El comercio electrónico se entiende como cualquier forma de transacción comercial en la cual las partes involucradas interactúan de manera electrónica y no de la manera tradicional por medio de intercambios físicos o trato físico directo.

Algunos expertos opinan que en cierta forma, el comercio electrónico comenzó antes de Internet, mediante transacciones comerciales por teléfono, fax y lasa redes privadas, pero el desarrollo de la WEB motivó que alcanzara mayor auge. Su acepción más general es "acercar el comprador al fabricante por medios electrónicos", lo cual implica eliminación de intermediarios, reducción de costos y una filosofía diferente en la forma de comprar y vender, y lo que es más importante, de obtener información para esas gestiones.

Para especialistas como Juan Fernández, coordinador de la Comisión Nacional de Comercio Electrónico de Cuba, puede definirse como "cualquier forma de transacción de negocios en la cual las partes interactúan electrónicamente en lugar de mediante intercambios materiales o contacto físico directo", y agrega que su esencia se capta mejor si afirmamos que es "uno de los casos poco

frecuentes en que se unen las nuevas necesidades con las tecnologías nuevas para revolucionar la forma en que se realizan los negocios."

2. PANORAMA ECONOMICO MUNDIAL SOBRE COMERCIO ELECTRÓNICO

Actualmente la manera de comerciar se caracteriza por el mejoramiento constante en los procesos de abastecimiento, y como respuesta a ello los negocios a nivel mundial están cambiando tanto su organización como sus operaciones. El comercio electrónico es el medio de llevar a cabo dichos cambios dentro de una escala global, permitiendo a las compañías ser más eficientes y flexibles en sus operaciones internas, para así trabajar de una manera más cercana con sus proveedores y estar más pendiente de las necesidades y expectativas de sus clientes. Además permiten seleccionar a los mejores proveedores sin importar su localización geográfica para que de esa forma se pueda vender a un mercado global.

3. COMERCIO ELECTRÓNICO EN LATINOAMERICA

Diversos estudios y estadísticas (cantidad de usuarios, cantidad de host, páginas) muestran que los mayores mercados para el comercio electrónico en América Latina son: Brasil, México, Argentina y Chile con una demanda de productos y servicios en línea de $160 millones al finalizar el año 1999, siendo $77 millones facturados por compañías y sitios de Latinoamérica. Brasil se presenta como el mercado más grande y de más rápido crecimiento, representado el 88 por ciento de las ventas del tipo negocio-consumidor. Este dominio de Brasil en el comercio electrónico no es una sorpresa ya que se ha podido llegar a una masa crítica de usuarios domésticos de Internet que dan soporte a este mercado electrónico. Con una representación del 50% de los usuarios en toda la región Brasil se sitúa a la cabeza, seguido por México con un 18%, Argentina con un 9% de los usuarios, complementados por Chile Colombia, Perú y Venezuela.

Fuente: http://www.idrc.ca/en/ev-68562-201-1-DO_TOPIC.html

4. CATEGORÍAS Y MODELOS DE SITIOS COMERCIALES EN INTERNET

CATEGORÍAS DEL COMERCIO ELECTRÓNICO

EMPRESA – EMPRESA (B2B)

Se trata de todas aquellas actividades en las que un proveedor vende algún producto o servicio a un cliente industrial o profesional.

Se puede extraer un gran rendimiento a la Red en este sentido ya que Internet hace posible la disminución de los costes de transacción entre las empresas, en otras palabras, encontrar proveedores, negociar con ellos y coordinar los suministros puede hacerse más barato mediante Internet.

De esta forma, un proveedor puede poner en su web todo un catálogo de productos de manera que sus clientes puedan hacer sus pedidos de manera más cómoda y personalizada. Incluso pueden crearse páginas con catálogos personalizados para cada cliente en las que se especifiquen los productos que

adquiere habitualmente y los precios a los que se ofrecen dichos productos en función de su volumen de compras.

EMPRESA – CONSUMIDOR (B2C)
Es la modalidad de comercio electrónico más conocida popularmente, debido a los sectores que involucra: la empresa y sus clientes, se trata del método más conocido como venta electrónica, que usualmente se realiza a través de la World Wide Web de Internet. Existen ya en la actualidad muchos tipos de galerías que ofrecen a través de Internet todo tipo de bienes consumibles, desde computadores a vinos, vehículos, materiales, libros, etc.
Existen tres modelos de negocios diferentes:
1. Tienda virtual (e-Shop).
Se trata de un establecimiento instalado en la red en la que se actúa como intermediario en la venta de productos propios o de terceros. Estas compañías resuelven todo lo relativo al acto de compra: oferta del producto, disponibilidad del producto en almacén, entrega física del producto, sistemas seguros de pago, etc.
Entre sus beneficios destacan la posibilidad de creación de nuevas oportunidades de ventas e ingresos; la recuperación a corto plazo de la inversión inicial y la reducción de costes directos de ventas en personal, teléfono, etc

CONSUMIDOR – CONSUMIDOR (C2C)
Se refiere a las transacciones privadas entre consumidores que pueden tener lugar mediante el intercambio de correos electrónicos o el uso de tecnologías P2P (Peer to Peer)
Un método sencillo para que las empresas se inicien en el comercio electrónico consiste en colocar una oferta especial en el sitio Web y permitir a los clientes realizar sus pedidos on-line. No es preciso hacer los pagos vía electrónica.

EMPRESA – ADMINISTRACIÓN (B2A)
Aquí se cubre todo tipo de transacciones entre las empresas y las organizaciones gubernamentales. Esta categoría es bastante importante ya que se piensa que a través de ella se podrá promover la calidad, la seriedad y el crecimiento del comercio electrónico.

MODELOS DE NEGOCIO EN INTERNET

Un modelo de negocio define una arquitectura alrededor de la cual gira un producto o servicio y un flujo de información en una actividad que crea valor. Este modelo también presenta a los actores y sus roles respectivos, así como los beneficios esperados que se obtendrán siempre que se organicen de forma adecuada. En definitiva, un modelo de negocio describe las fuentes de los ingresos que sustentan dicho modelo.

En el caso de *e-Business*, los diferentes modelos de negocio se pueden clasificar en dos grandes grupos: **Modelos «transplantados» y Modelos «nativos».**

MODELOS DE NEGOCIO «TRASPLANTADOS».

Los modelos trasplantados son aquellos modelos de negocio tradicionales que han sido modificados y llevados al mundo *web*.

Ejemplos de este tipo de modelo de negocio son:

Librerías y similares de ***venta al detalle*** cuyo núcleo básico de negocio es el mismo que la venta por correo.

Sistemas de ***publicidad*** donde un tercero soporta los costes de un servicio gratuito y cuyo éxito dependerá de lo atractivo que sea el servicio ofrecido.

Suscripciones para acceder a bases de datos durante un tiempo o por un número determinado de consultas.

Promocionales, en donde se presenta un producto y el negocio está en los servicios que se prestan alrededor de dicho producto, o bien en permitir la prueba gratuita y sin compromiso por un periodo de 30 días, siguiendo modelos de venta al detalle clásica.

Marketing directo en sus dos vertientes: la primera, el envío masivo de información no solicitada con el riesgo de provocar un efecto de rechazo generalizado a dicho envío, y la segunda, siguiendo pautas de fidelización, aceptar la publicidad directa o información personalizada solicitando la conformidad del usuario, explícitamente o a través de un regalo, ventajas por contestar a encuestas, etc.

El hecho de traspasar modelos de negocio estándar a entornos Internet no es en sí mismo un efecto pernicioso para el negocio actual, e incluso puede verse como una línea nueva o complementaria, sin embargo, la transición de uno a otro medio no es una cuestión puramente de tecnología sino que también conlleva un nivel de riesgo asociado a dicho cambio.

MODELOS DE NEGOCIO «NATIVOS».

Los modelos nativos son aquellas actividades que surgen dentro de los entornos tipo Internet y no tienen un paralelo en otras áreas. Estos modelos serían inconcebibles o al menos muy complicados si no existiera la *web*. Ejemplos de este tipo de modelo de negocio son:

Proveedores de acceso (*hosting*, *e-mail*, etc.) a Internet y proveedores de servicios de comercio. Sin embargo, éste no constituye realmente un nuevo modelo de negocio, ya que está basado en servicios de conexión, procesado y transacciones.

Subastas basadas en web, que se podrían clasificar en función de la audiencia y la forma en que se lleva el mercado a la *web*, dando lugar a subastas que facilitan las transacciones entre un cliente con otro cliente, clientes con ofertas de empresas. El modelo consiste en ofrecer dos o más ítems para la venta con el mismo precio y en función de las reglas (mejor oferta, mejor ofertante, etc.) se cierra la subasta y se ejecuta la compraventa.

Subasta moderada, que consiste en una subasta en la que se guardan las identidades y las pujas que se hayan realizado. Al final, el sistema interactúa

con todos los datos obtenidos y presenta al ganador de la subasta, ejecutándose la acción pertinente.

Subasta business to bussiness: el mercado del *business to business*, esta comenzando a aparecer en sitios *web*, donde se enfocan algunos aspectos de la empresa, tales como: proveedores, pedidos, compras o ventas de productos y/o servicios, etc., y se actúa sobre ellos.

Intermediarios de información: son aquellos negocios cuya fuente de ingresos procede de capturar información y determinar perfiles detallados, para ser usados por terceros. También se pueden definir como los que relacionan múltiples compradores y vendedores en áreas muy especí-ficas, que recogen información precisa, consistente y comparable de los vendedores y proporcionan herramientas para la ayuda a la decisión de una compra determinada.

III. ASPECTOS GENERALES DE NEGOCIO A CONSIDERAR ANTES DE INCURSIONAR EN EL COMERCIO ELECTRÓNICO.

1. OBJETIVOS DEL NEGOCIO.

Dependiendo del giro del negocio cambiará la planeación estratégica.

Por ejemplo, en la industria de bienes raíces se estima que una transacción típica involucra cerca de 100 personas que manipulan más de formularios, modelos y papeles. Por medio de Internet, pueden ahorrarse (estimado para EE.UU) cerca de 2 mil millones de dólares anuales. General Electric ha perfeccionado la gestión comercial de varias de sus divisiones cambiando a un sistema de órdenes basados en Internet, reduciendo los costos en un 30%, lo cual a escala de una compañía tan grande significan decenas de millones de dólares. Por su parte, la multinacional petrolera Exxon está ahorrando 50 millones de dólares anuales utilizando Internet como eje de un sistema de órdenes de compra, pago y servicio en sus comercios de combustible y artículos generales, como resultado del procesamiento electrónico de la información de operaciones en sustitución del papel.

2. PRODUCTOS.

Lo que una tienda vende es a veces más importante de cómo lo vende. Lo primero que se debe tener en consideración es escoger productos o servicios que se puedan vender por el mercado electrónico.

3. COMPETENCIA.

El ciclo de vida de un producto requiere un estudio detallado. Todos los productos pierden con el tiempo su atractivo inicial derivado de la novedad. Los

productores también pueden acelerar la caducidad del producto al introducir otros nuevos con características más modernas. Hoy los consumidores no sólo esperan que aparezcan productos novedosos, sino que reaccionan de modo positivo a las mejoras e innovaciones productivas. Esto influye en la duración de los artículos que, a su vez, repercute en los costes y, por tanto, en el precio final. La competencia entre productores que fabrican artículos parecidos acelera la aparición de otros con nuevas características.

Los dos determinantes principales del precio son los costos de producción y la competencia. No resulta rentable vender un producto a un precio inferior a los costes de producción, pero es imposible hacerlo a un precio superior al de los bienes similares. No obstante, existen muchos otros factores que determinan el precio final. La política de la empresa puede exigir que se venda a un precio que minimiza los beneficios en las nuevas líneas de productos, o se puede bajar mediante descuentos para vender mayor cantidad.

Existen normas sobre la competencia que impiden a los productores fijar una cuantía máxima del precio de venta final. No obstante, algunos fabricantes logran controlar el precio de venta final al ser propietarios de los puntos de venta al por menor, pero esto sólo ocurre en contadas ocasiones.

Por otra parte, algunos gobiernos intentan limitar la competencia en precios para favorecer a los pequeños empresarios que no pueden competir con las grandes empresas. Por ello, las decisiones que toma el departamento de mercadotecnia sobre precios deben ser revisadas por el departamento jurídico de la compañía.

Es cierto que muchas empresas virtuales tuvieron que cerrar y que otras tantas aún no logran salir de los números rojos. En todos estos casos se ha dicho que los modelos de negocios no cumplieron con una o más de las reglas de la vieja economía, a lo que obedece su fracaso.

Sin duda es cierto, pero también es verdad que en muchos casos falló la estrategia de mercadotecnia, si es que la hubo más allá de un impresionante derroche de recursos en publicidad, lo que nunca permitió tener un flujo de efectivo positivo y mucho menos reportar ganancias para esas empresas.
Basado en la incomparable eficiencia y eficacia del Internet como medio de comunicación, el comercio electrónico es ya una realidad probada y comprobada en diversos contextos y para muchas líneas de productos. Dentro de pocos años la mayoría de la población estará haciendo ciertas transacciones comerciales por el Internet de manera cotidiana, las que le signifiquen mayor comodidad y economía.
FUENTE: http://www.cimm.com.mx/cimm/comercio.html

4. ATENCIÓN A CLIENTES.

Los requerimientos del cliente pueden analizarse examinando el proceso de compra. Una tienda con buen medio para el proceso tiende a ser más atractiva para los consumidores. Se pueden elegir varios modelos existentes en este trabajo se adopta el modelo EKB para definir las necesidades de los consumidores.

El modelo EKB divide el proceso de decisión en cinco etapas: reconocimiento del problema, búsqueda de la información, evaluación de las alternativas, elección y evaluación outcome. Cuando un problema se reconoce se buscan por ciertos productos que pueden eliminar el problema determinado. La información del producto se selecciona y productos alternativos se evalúan. Una vez que una alternativa se elige el consumidor evalúa la outcome, y guarda la experiencia para el futuro.
De aquí los requerimientos para el comercio electrónico en cada etapa puede ser realizada como sigue:

Reconocimiento del problema: Es común si el sistema puede identificar las necesidades del cliente, estimular la demanda, y generar un medio para que él reconozca sus problemas.
Recolección de información: La tienda necesita ayudar a los consumidores a colectar información de ayuda durante el proceso de selección. Esta información puede ayudarlos a evaluar productos y a influenciar su criterio de decisión.
Evaluación Alternativa: Es común tener funciones que ayuden a los clientes a evaluar alternativas basadas en la información recolectada.
Elección: En la etapa de elección el cliente frecuentemente hace tradeoffs entre varios criterios. Es necesario tener funciones que le ayuden a hacer decisiones.
Transacciones y servicios de Post-Venta: Las amigables líneas del proceso de transacción, servicios de post-venta y otras funciones que hacen la transacción mas fácil son también importantes para la atracción del cliente.

5. LOGÍSTICA DE DISTRIBUCIÓN.

La logística son las acciones y medios destinados a prever y proporcionar los recursos necesarios que posibiliten realizar una actividad de forma eficiente y eficaz.

E-LOGÍSTICA
La distribución debe ser capaz de responder en tiempos mucho menores a los acostumbrados y adecuarse a nuevos horarios y condiciones. Y además hacerlo barato. En el mundo Internet, en el que la información de los precios de productos es una realidad, los márgenes se estrechan y tener la mejor de las estructuras logísticas, que ahorre costes, es fundamental.
No olvidemos que comercio electrónico es comercio a distancia. De ahí la importancia de la logística. Muchas empresas no están preparadas para la venta a distancia o por teléfono ni tienen experiencia en ello por lo que fracasan al abordar un proyecto de comercio electrónico.
Se dice que, en la actualidad, la logística es el cuello de botella del desarrollo del comercio electrónico. Según un artículo publicado en octubre del 2000 en Ciber Estrella "El 19,5% de las compras realizadas por Internet en España no llegaron a entregarse". El informe muestra que "sólo un 10 por ciento de los comercios en la red ofrece al cliente información sobre las existencias del producto en el momento de la compra." "El 72 por ciento de los sitios no ofrece fecha de entrega aproximada".

FACTORES CLAVE EN LA E-LOGÍSTICA

- El coste del servicio
- El alcance de la red de distribución
- Los costes adicionales de embalaje y seguro
- Los tiempos de entrega prometidos
- La política de la empresa ante los posibles problemas de entrega
- Más servicio: que el cliente pueda elegir el plazo y forma de entrega
- Información sobre el seguimiento del pedido

E-FULLFILMENT

El e-fullfilment trata de "desarrollar una metodología para integrar sistemas de información entre las tiendas virtuales y el operador logístico, y ver que capacidades tienen los operadores en aspectos como las entregas urgentes, la gestión de los pedidos, el cobro contrareembolso las entregas o las devoluciones entre otras funciones".

6. CONVENIOS - CONTRATOS

Hay un día nadie puede negar el impacto que produjo la revolución informativa en todos los campos de la vida humana; la ciencia del derecho en repuesta de esta realidad tiene que dar nuevas reglas para evitar que se produzcan daños y abusos en aquellas relaciones comerciales que día a día se realizaron en la red. Por lo tanto cabe delimitar cuales el campo del a informática y el derecho en cuanto a la contratación.

Dentro del derecho informático encontramos la contratación informática que es aquella cuyo objeto es un bien o servicio, informático o ambos; y la contratación electrónica es aquella con independencia de cual, sea su objeto, que puede ser también la informática aunque no necesariamente, se realiza a través de los medios electrónicos.

Es decir los contratos electrónicos son aquellos para cuya celebración el hombre se vale de la tecnología informática pudiendo consistir su objeto en obligaciones de cualquier naturaleza.

CONCEPTO

Los contratos son actos jurídicos que son celebrados por dos o mas partes para cual, modificar regular o extinguir una relación jurídica patrimonial. La diferencia con los contratos electrónicos es que estos se realzan sin la presencia física simultánea de las partes, prestando su consentimiento, por medio de equipo electrónico de tratamiento y almacenaje de datos de datos conectados por medio de cable, radio, medio óptico o cualquier otro medio cuando nos referimos a las partes nos referimos 2 o más sujetos intervinientes en al contracción; tomarse en con declaración además que la sola existencia de dos partes, con intereses iguales no da lugar a la formación de la relación jurídica, para ello es necesario que dichas partes se pongan de acuerdo y que ambas tengan la voluntad común de celebrar el contrato.

IV. DISEÑO DE SITIOS COMERCIALES PARA INTERNET

1. INTRODUCCIÓN

Una tienda virtual (también llamada una tienda electrónica) es una dirección de la web en la cual las homepages dan información acerca de sus productos o servicios y asiste procesos básicos de transacciones Existen dos tipos de tiendas la tienda electrónica y el portal. La tienda electrónica tiene su dirección para comerciar ciertos productos o servicios. Por ejemplo Amazon Un portal es una dirección de web que combina muchas tiendas electrónicas para crear un synergy. El portal también proporciona funciones comunes consejos, ordenes y pago para sus tiendas. El portal es mas atractivo por la cantidad de productos que muestra.

Los productos que muestran las tiendas electrónicas pueden ser físicos o digitales. Productos digitales los que pueden ser descargados de la red. Productos físicos que son ordenados electrónicamente y pueden ser entregados por medios tradicionales.

Las ventajas para el propietario de una tienda virtual es por ejemplo el costo de operación es menor que una tienda tradicional. También da un acceso en línea económico y efectivo para los usuarios. Los consumidores tienen la opción de comparar productos y costos electrónicamente. La tienda electrónica puede crear nuevos tipos de negocios.

Entre las tiendas electrónicas existen aquellas que son exitosas y aquellas que no lo son. Existen varios productos que pueden afectar el éxito de su operación como las características del producto, diseño, precio y promoción de la tienda. El diseño de la tienda puede afectar la decisión si compra o no electrónicamente.

2. ANÁLISIS DE REQUERIMIENTOS

Es un procedimiento para determinar los requerimientos funcionales de una tienda.

Para el cliente la tienda electrónica es el canal de venta. Existen 4 preocupaciones principales: producto, precio, lugar y promoción.

Producto
Productos o servicios que se puedan vender por el mercado electrónico.

Precio
Los medios electrónicos tienen gran flexibilidad en precio dinámico. Los productos o servicios pueden ser etiquetados a diferente precio en diferentes veces a diferentes clientes a veces en diferentes áreas. Una buena tienda electrónica debe tener facilidades para ajustar el precio.

Lugar

La localización de la tienda electrónica puede afectar sus costos y desarrollo. Una de las mayores limitaciones es el ancho de banda. Ejecutar una tienda virtual debe tener un servidor apropiado y cuando se necesite “espejos” para incrementar el desarrollo de la diseminación de la información. Seleccionar el espejo adecuado es similar a seleccionar una tienda en negocios tradicionales. Es necesario utilizar varios lenguajes para varios mercados.

Promoción
Además de las técnicas tradicionales de promoción, la tecnología de la web otorga un medio interactivo con capacidades analíticas bastante fuertes. Nuevas técnicas de promoción como bases de datos interactivas comerciales pueden utilizarse con mayor eficiencia. De acuerdo a las preocupaciones el diseño de una tienda electrónica necesita tomar cuidado del diseño de una página web, buena distribución, procesos de transacciones y operación administrativa.

3. PROCESO PARA LA CONSTRUCCION DE SITIOS WEB COMERCIALES

Diseño de páginas web
Desde que las tiendas electrónicas podrían no tener almacenes físicos accesibles a los consumidores en línea, Las páginas web son las tiendas que percibe el cliente. De aquí, diseñar paginas web atractivas para que los clientes en línea deseen visitar mas frecuentemente y quedarse en ellas más tiempo.

Distribución
La administración de distribución es importante en las tiendas tradicionales. En las tiendas electrónicas la organización de productos es la distribución que percibe el cliente. Es necesario diseñar una distribución amigable y bien organizada.

Procesos de Transacciones
La venta de productos se hace por procesos de transacciones, los cuales incluyen ordenes, pago, entrega de productos, entrega del producto y procesos para devolución de bienes. Se necesita que el proceso sea seguro, confiable flexible y cómodo para los clientes

Obtener un dominio
Tener dominio propio o no tenerlo no es una cuestión de capricho, es una decisión importante a tomar. Veamos que significa esto a nivel general, si su empresa está conectada a Internet con un determinado proveedor y no tiene dominio propio, la URL de su página web será:

- www.proveedor.mx/empresa
- www.proveedor.com/empresa

Si por el contrario registramos un dominio propio la dirección será:

- www.empresa.mx
- www.empresa.com.mx

Aparte de ser una cuestión de imagen, la no posesión de dominio propio puede ocasionar una gran pérdida en el número de visitas a nuestro sitio, es más fácil acordarse de www.empresa.mx que de www.empresa.mx/renault, y aunque solo fuese por esto necesitamos el dominio.

Los nombre de dominio se pueden registrar a nivel nacional, con terminación .mx, en el caso o a nivel internacional con dominio .com (empresa comercial, aunque hay otros dominios como .edu, .mil, .org y .net). Para registrar un dominio .com acudiremos a NIC de México cumpliendo los siguientes requisitos:

Condiciones para registrar un dominio .com

- El dominio no estará registrado.
- Para el nombre solo se podrán utilizar letras americanas, números y guiones.
- El nombre no podrá empezar o terminar por guión.
- La longitud del nombre será de 2 a 22 caracteres.
- Puede ser registrado por empresas, organizaciones o personas físicas.
- Deben configurarse dos servidores de dominios (DNS) que respondan a las peticiones de dicho dominio antes de hacer la solicitud.

4. CATALOGO ELECTRÓNICO DE PRODUCTOS

Hablar de catálogo electrónico es una temática nueva que a partir de ahora se presentará constantemente. Son importantes sus beneficios en la cadena de abasto.

El "*Strategic Leadership Forum*" expresó que actualmente el operar mejor, generando mas utilidades y rentabilidad es una necesidad de la empresa. Eso implica adoptar nuevas herramientas gerenciales, cambios y mejoras.

Estos cambios y mejoras requieren de herramientas como la realización de benchmarking, costeo basado en actividades, retención de los clientes, la satisfacción de los mismos, pago en base a desempeño, reducción de los tiempos en los procesos, llegar a una calidad total, reingeniería, planeación estratégica, alianzas estratégicas. Todo esto pretende maximizar satisfacción, minimizar los costos, aplicar tecnología a la cadena de abasto, disminución de tiempos, promociones exitosas, lanzamientos exitosos de nuevos productos y mejora continua.

El catálogo electrónico debe de ser un sistema de referencia que de manera uniforme y automatizada, en la que podamos confiar para un manejo de información importante, nos ayude en la toma de decisiones.

Esto se refuerza con tecnologías actuales tales como el código de barras sacándole provecho a la información que contiene el código.

Al encuadrar el comercio electrónico y la mercadotecnia virtual dentro de las compras por catálogo y mercadotecnia directa, esto brinda una cierta

orientación a los empresarios virtuales a la hora de buscar apoyo para encausar su estrategia de mercadotecnia de manera más efectiva.

Una ventaja de este enfoque simplificador es que no descarta la explotación de la interactividad y personalización, al contrario. Aún está por verse si podrá aceptarse como el marco conceptual de la mercadotecnia virtual por una mayoría de sus practicantes.

5. SEGURIDAD EN SISTEMAS DE COMERCIO ELECTRÓNICO

Tal y como avanzan las tecnologías cada vez es más frecuente encontrarnos con portales que nos ofrecen productos y servicios a través de la Red. Y poco a poco los usuarios empezamos a dar uso a este tipo de servicios, aunque todavía nos sentimos reticentes a revelar nuestros datos privados y bancarios así como así.

Esto puede deberse a la falta de seguridad que en unos casos está ausente y en otros no sabemos hasta que punto es fiable.

Pero también se corre un riesgo cuando se compra en una tienda normal o se come en un restaurante y se paga con la tarjeta de crédito. De hecho existen muchos fraudes al respecto. Cada transacción que se realiza en el comercio tradicional y en el comercio electrónico está expuesta a un riesgo.

Cuando se realiza una transacción por Internet y se envían los datos personales (nombre, dirección, número de tarjeta de crédito, etc.) deberíamos plantearnos si pueden ser interceptados durante la transmisión (entre comprador y vendedor) por alguien que no sea el vendedor. Ese "alguien" ¿Podría utilizar estos datos para suplantar nuestra identidad?.

Igualmente el vendedor quiere asegurarse de que los datos que recibe son verdaderos, es decir, necesita saber que el comprador es quien dice ser. Es por estas razones que se han desarrollado los sistemas de transacciones seguras.

La incorporación de mecanismos, técnicas y algoritmos adecuados para realizar transacciones electrónicas se hace necesaria para evitar los riesgos a los que nos exponemos. La firma digital, por ejemplo, no es más que un tipo de encriptación, en la cual se realiza un control sobre el flujo de información (por ejemplo de un contrato, de un número de tarjeta de crédito, etc.). Se usan para verificar al proveedor de una determinada información y que la información firmada (el pedido, el número de tarjeta, etc.) no ha sido alterada.
Se puede hablar en este sentido de cuatro aspectos básicos de seguridad: **autentificación, confidencialidad, integridad y el no-repudio.**

CONFIDENCIALIDAD
La confidencialidad es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. Igual que antes, los usuarios pueden ser personas, procesos, programas, etc.
Para evitar que nadie no autorizado pueda tener acceso a la información transferida y que recorra la Red se utilizan técnicas de encriptación o codificación de datos.

INTEGRIDAD

La integridad de la información corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales.

Mediante una firma digital se codifican los mensajes a transferir, de forma que una función, denominada hash, calcula un resumen de dicho mensaje y se añade al mismo.

La validación de la integridad del mensaje se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se añadió al final del mismo cuando se calculo por primera vez antes de enviarlo.

Mantener la integridad es importante para verificar que en el tiempo de viaje por la Red de la información entre el sitio emisor y receptor nadie no autorizado ha modificado el mensaje.

AUTENTIFICACION

La autentificación es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información. Por entidad se entiende tanto personas, como procesos o computadoras.

Existen varias formas de poder autentificarse:

- basada en claves
- basada en direcciones
- criptográfica

De estas tres posibilidades la más segura es la tercera, ya que en el caso de las dos primeras es posible que alguien escuche la información enviada y pueden suplantar la identidad del emisor de información.

Desde otro punto de vista se puede hablar de formas de autentificarse, como puede ser a través de la biometría (huellas digitales, retina del ojo, la voz, etc.), por medio de passwords o claves, y por último utilizando algo que poseamos, como un certificado digital.

Se llama autentificación fuerte a la que utiliza al menos dos de las tres técnicas mencionadas en el párrafo anterior, siendo bastante frecuente el uso de la autentificación biométrica, que como se indicó antes se basa en la identificación de personas por medio de algún atributo físico.

NO-REPUDIO

Los servicios de no-repudio ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida.

Con este aspecto conseguimos que una vez que alguien ha mandado un mensaje no pueda renegar de él, es decir, no pueda negar que es el autor del mensaje.

Para el comercio electrónico es importante ya que garantiza la realización de las transacciones para las entidades participantes.

Se aplica en ambos lados de la comunicación, tanto para no poder rechazar la autoría de un mensaje, como para negar su recepción.

Es necesario identificar la información que debe conocer cada una de las entidades participantes en el proceso de comercio electrónico y con ello permitir la privacidad de forma fraccionada a las partes autorizadas para su uso.

El no repudio se consigue mediante los certificados y la firma digital.

La combinación de estos cuatro aspectos mencionados, que son la confidencialidad, integridad, autentificación y no-repudio, garantiza en cierto grado la seguridad en las transacciones electrónicas.
Conocer y aplicar conceptos, técnicas y algoritmos para implementar un sistema de seguridad es imprescindible para minimizar riesgos y así poder asegurar al usuario que el comercio electrónico es un mecanismo seguro en el cual puede confiar siempre que se trate con la delicadeza que requiere.

Confidencialidad-> Encriptación
Integridad -> Firma Digital
Autenticidad -> Certificado Digital
No-repudio -> Certificado y Firma Digital

ENCRIPTACION
El futuro del comercio electrónico, de las comunicaciones electrónicas y del almacenamiento digital de datos dependerá en gran medida de la capacidad de los sistemas para proteger la información y controlar los accesos, asegurar la integridad de los datos transmitidos o almacenados y proporcionar garantías de autenticidad. Estos requisitos ya existían en la etapa preinformática y se inventaron soluciones adecuadas para ellos. Sin embargo, la velocidad y el alcance universal de la economía digital incrementan la importancia de estos temas. En particular, si se quiere que el comercio electrónico se afiance, los usuarios se tienen que fiar de los sistemas y confiar en que no van a correr riesgos inaceptables. Hay que recalcar que la elevada velocidad de los sistemas electrónicos y su capacidad para enviar rápidamente grandes cantidades de datos exigen todavía más la necesidad de protección.
Aunque cierta regulación para proteger la información y limitar el acceso, conforme con la ley y ampliamente aplicable (como la relativa al fraude) puede ser de gran valor, la regulación por sí sola, ya sea por parte de los gobiernos o por parte de industria (autorregulación) no puede dar una solución adecuada a las necesidades de la protección de los datos y de la protección de la infraestructura de la información.
La codificación criptográfica es el medio más práctico para evitar accesos no deseados o no autorizados a los datos e información almacenados en ordenadores o transmitidos por las redes informáticas y los sistemas de telecomunicaciones. También es un medio de asegurar la integridad de los datos o de la información y la autenticidad de la fuente, y lo que quizá sea más importante, permite a los individuos proteger sus propios datos e informaciones, más que confiar en otros o confiar en los sistemas jurídicos para solucionar los problemas.
Además, esta codificación puede ser integral para los datos/información -en vez de una defensa periférica- es en cierto modo más fiable que los "firewalls" (cortafuegos) y proporciona mayores garantías. También se puede utilizar para proteger los sistemas utilizados en las redes privadas.

Dada su importancia para numerosos usos, entre los que se encuentra el comercio electrónico, es probable que en el futuro se produzca una fuerte demanda comercial de codificación. El enorme crecimiento y desarrollo del comercio electrónico, del que ahora somos testigos, y el gran interés mostrado por el sector empresarial ponen de manifiesto que lo que se necesita en este

sector se podrá conseguir. La potencia del mercado lo impulsa y la proliferación de capacidades y productos lo asegura.

METODOS DE ENCRIPTACION

La criptografía tradicional se basa en el concepto de que tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave secreta.

Los métodos de *cifrado simétrico* usan una misma clave para cifrar y descifrar. Suponiendo que dos interlocutores comparten una clave secreta y de longitud suficientemente grande, el cifrado simétrico permite garantizar la confidencialidad de la comunicación entre ellos. Este esquema es poco adecuado cuando una parte establece comunicaciones ocasionales con muchas otras con las que no tenía una relación previa, como ocurre frecuentemente en el comercio electrónico, ya que antes de poder establecer cada comunicación sería necesario intercambiar previamente por algún procedimiento seguro la clave que se va a utilizar para cifrar y descifrar en esa comunicación. Por ejemplo, un consumidor que quisiera comprar a través de Internet necesitaría intercambiar una clave secreta diferente con cada uno de los vendedores a los que quisiera acceder.

Gráfico. Cifrado / descifrado simétrico

El principal problema consiste en conseguir que ambas partes conozcan la misma clave sin que ningún tercero se entere. Si la clave es interceptada, quien la conozca podrá luego utilizarla para leer todos los mensajes encriptados.

La Criptografía con clave secreta ha tenido dificultades para brindar la seguridad necesaria en este aspecto.

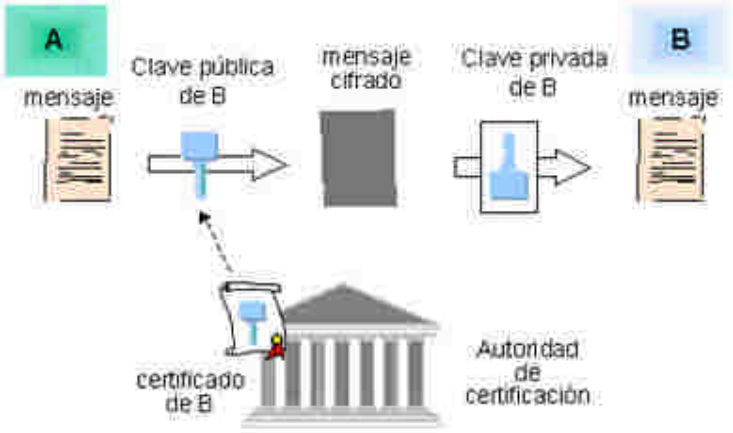
Existe un acuerdo generalizado acerca de que el sistema que mayor seguridad brinda en la actualidad a las transacciones electrónicas e intercambio electrónicos de datos, es el de la Criptografía de Clave Pública, basado en algoritmos asimétricos. Nace en 1976 en la Universidad de Standford, Estados Unidos, con el propósito de resolver el problema de la administración de claves.

Los métodos de *cifrado asimétrico* usan parejas de claves con la propiedad de que lo que se cifra con una cualquiera de las claves de una pareja sólo se puede descifrar con la otra clave de la pareja. En el caso más simple, con este sistema un interlocutor sólo necesita tener una pareja de claves que puede utilizar para comunicarse de forma segura con cualquier otro interlocutor que disponga a su vez de otra pareja de claves. Cada interlocutor hace pública una de sus claves (será su clave pública) y mantiene en secreto la otra (su claveprivada). Por ello, el cifrado asimétrico se denomina también cifrado de clave pública. La clave privada (o las claves privadas si el usuario utiliza varias parejas de claves para diferentes propósitos) puede guardarse en el ordenador del usuario o en una tarjeta inteligente.

Por la propiedad de las parejas de claves citada antes, para enviar un mensaje de forma confidencial a un destinatario basta cifrarlo con la clave pública de ese destinatario. Así sólo él podrá descifrarlo mediante la clave privada que mantiene en secreto. No es necesario que el remitente y el destinatario

intercambien previamente ninguna clave secreta. El remitente sólo necesita averiguar la clave pública del destinatario. Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

Gráfico. Cifrado asimétrico con consulta de clave pública a autoridad de certificación y descifrado con clave privada del destinatario



Por este medio, se obtienen transacciones seguras y auténticas, con la certeza de la integridad de los datos y la imposibilidad de repudio por parte del emisor. Pero para poder cumplir con estos principios, la Criptografía de Clave Pública debe basarse en una adecuada infraestructura de manejo de claves y productos adecuados, que permita identificar en forma indubitada a particulares y corporaciones con sus claves públicas, a través de terceras partes confiables (las Autoridades Certificantes).

El sistema requiere una infraestructura grande y compleja, pero esencial: sin ella los usuarios no podrán saber con quién están tratando en la red, a quién le están enviando dinero, quién firmó un documento, o si la información fue interceptada y alterada durante la transmisión.

Por ello, los usuarios demandarán una fuerte infraestructura de administración o manejo de claves basadas en autoridades certificantes que operen bajo estrictas normas predeterminadas.

Otro método es la encriptación mediante códigos de integridad, en el cual se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos (una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital; pero la probabilidad es ínfima. Si se manipulan los datos la huella cambia; y modificar los datos de forma tan sabia para obtener la misma huella es algo computacionalmente inabordable en un plazo razonable.

Y complementando éste método se encuentra la encriptación mediante firma digital, método mediante el cual dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser(autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de emisión (y posiblemente la fecha de vencimiento de validez) suelen proporcionarse en texto claro, e incorporarse al cálculo de la huella digital, para ligarlas irrenunciablemente.

FIRMA DIGITAL

Desde el punto de vista técnico, como alternativa a la firma manuscrita sobre papel se ofrecen las firmas electrónicas y/o digitales.
En el comercio electrónico el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas, que pueden ser remplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica, dentro del que tiene cabida, como categoría particular, el de firma digital.
Las firmas digitales basadas sobre la criptografía asimétrica podemos encuadrarlas en un concepto más general de firma electrónica, que no presupone necesariamente la utilización de las tecnologías de cifrado asimétrico. Aunque, generalmente, varios autores hablan indistintamente de firma electrónica o de firma digital.
La firma digital tiene los mismos cometidos que la firma manuscrita, pero expresa, además de la identidad y la autoría, la autentificación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL, PGP, DSA, LUC, etc.), técnicas de sellamiento electrónico y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe (no es constante), pero que la hace absolutamente inimitable mientras no se tenga la clave privada con la que está encriptada, verdadera atribución de la identidad y autoría. La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no-violación del secreto.
Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. En este concepto amplio y tecnológicamente indefinido de firma, tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (p. ej. la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje.
Algunas definiciones más exactas de firma digital podrían ser podrían ser:

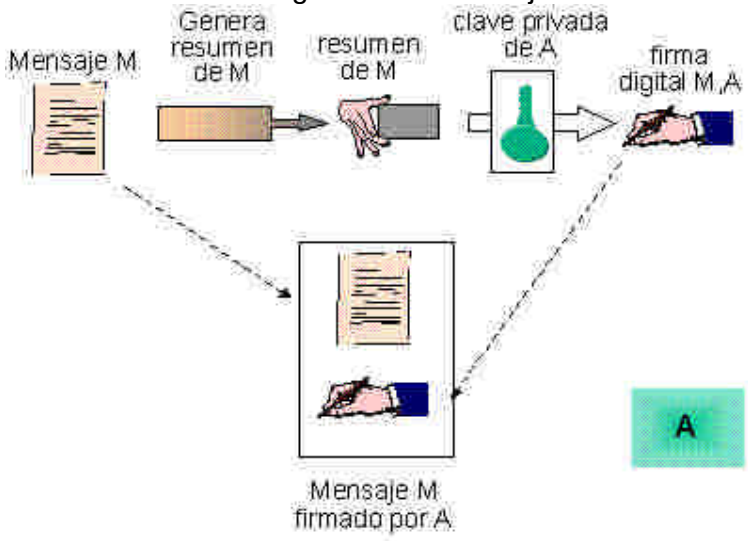
“La firma digital supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.”

“Es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina entidad de certificación que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, sino también jurídica.”

FIRMA, VERIFICACION Y ADMINISTRACION DE CLAVES

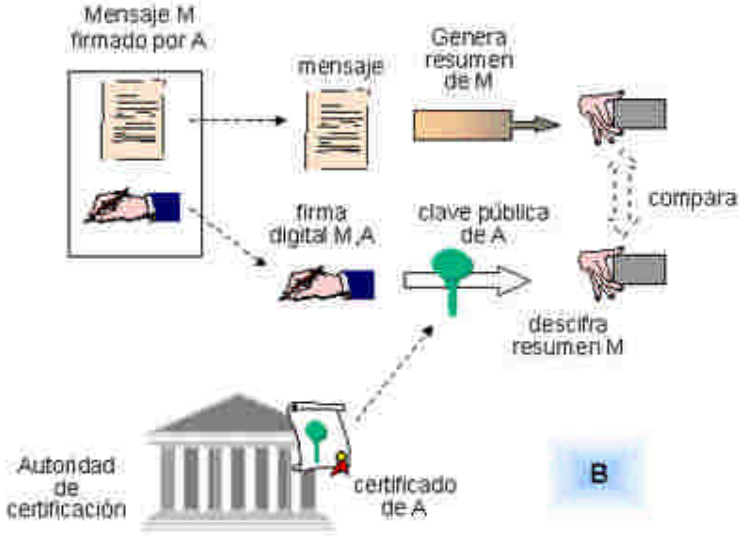
Según los técnicos, la firma digital es en la actualidad el único mecanismo que permite asegurar en un medio tan inseguro como las redes abiertas (Internet, por ejemplo), la identidad de las personas o computadoras que contratan o

intercambian mensajes e información, y que dicha información no ha sufrido alteraciones durante la transmisión.
Para comprender su funcionamiento y utilización debemos apartarnos por un momento de la idea de un documento en soporte papel y su firma. La firma digital es utilizada para todo tipo de información, ya se trate de texto, sonido o imágenes.
Como adelantáramos, la firma digital está basada en la utilización de la criptografía de clave pública, es decir, en algoritmos matemáticos que operan a través del juego de un par de claves, privada y pública, las que se encuentran íntimamente vinculadas.
Toda persona que quiera "firmar" digitalmente información para su posterior transmisión debe generar su propio par de claves. Recalcamos que la bondad de la criptografía de clave pública radica en que no se necesita compartir la clave: la clave privada queda en poder del usuario y es la utilizada para "firmar". Sólo la clave pública se publicita y es utilizada para verificar la firma.
La firma digital no se asemeja en nada a la firma tradicional. El proceso de creación del par de claves lo realiza un software especial: en general, la clave privada queda almacenada en el hardware del usuario y se activa por medio de una contraseña, aunque también puede ser almacenada en otros dispositivos como una tarjeta inteligente.
Las claves no son otra cosa que una combinación de letras y números, es decir un conjunto de bits, que a su vez constituyen un conjunto de ceros y unos. La creación de una firma digital implica combinar los caracteres que conforman la clave privada del usuario con los caracteres del documento o información al que se le quiere adosar la firma. Este nuevo conjunto de caracteres obtenido a partir de la mezcla de los caracteres del documento/información con los de la clave privada, es lo que constituye la firma digital. En dicha mezcla quedan comprendidos todos los caracteres que conforman el documento, incluso los espacios en blanco, de forma tal que cada combinación (clave privada más documento, es decir, firma) es única para cada documento. Como se advierte, también es muy importante la longitud de la clave.
Una vez obtenida la firma, el suscriptor / emisor la transmite conjuntamente con el documento. Asimismo transmite su clave pública para ser utilizada en el proceso de verificación.
Gráfico. Generación de la firma digital de un mensaje



El destinatario recibe el documento con la firma digital y la clave pública del suscriptor. Procede entonces a iniciar el proceso de verificación de la firma digital adosada al documento recibido. Aplica la clave pública del suscriptor a la firma digital. Como resultado de este proceso se obtiene una serie de caracteres que son comparados con los que conforman el documento transmitido. Si los caracteres coinciden, la firma es válida, y garantiza que fue aplicada por el titular de la clave privada que se corresponde con la clave pública utilizada para la verificación y que el documento no ha sido alterado. Cabe señalar que todo este proceso se realiza automáticamente y en pocos segundos.

Gráfico. Comprobación de una firma digital



Si la firma es válida, el titular de la clave privada utilizada para firmar el documento/información no puede desconocerla. Pero podría suceder que alguna persona se haya apoderado de su clave privada y haya firmado por él. De allí que resulte indispensable la existencia de un sistema de administración de claves que establezca reglas claras y concretas sobre el funcionamiento y utilización de las claves, de forma tal que se puedan atribuir válidamente efectos a determinadas situaciones preestablecidas.

La administración de claves se realiza a través de “Autoridades Certificantes”. Aquél que desee ingresar en el sistema deberá registrar su clave pública ante la autoridad certificante.

ENTIDADES CERTIFICADORAS

La creciente interconexión de los sistemas de información, posibilitada por la general aceptación de los sistemas abiertos, y las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas principalmente de la digitalización, están potenciando formas de intercambio de información impensables hace pocos años. A su vez, ello está conduciendo a una avalancha de nuevos servicios y aplicaciones telemáticas, con un enorme poder de penetración en las emergentes sociedades de la información. Así, el teletrabajo, la teleadministración, el comercio electrónico, etc., están modificando revolucionariamente las relaciones económicas, administrativas, laborales de tal forma que en pocos años serán radicalmente distintas de como son ahora.

Todos estos nuevos servicios y aplicaciones no podrán desarrollarse en plenitud a no ser que se les dote de unos servicios y mecanismos de seguridad fiables. Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento a seguir.
Existen diferentes tipos de protocolos en los que intervienen terceras partes confiables (Trusted Third Party, TTP):

¿QUE ES UNA AUTORIDAD DE CERTIFICACION?
Es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actuaría como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Sin embargo ¿quién autoriza a dicha autoridad?, Es decir, ¿cómo sé que la autoridad es quién dice ser?, ¿Deberá existir una autoridad en la cúspide de la pirámide de autoridades certificadoras que posibilite la autenticación de las demás?.
En USA la ley de Utah sobre firma digital da una importancia fundamental a las Autoridades Certificantes, definidas como las personas facultadas para emitir certificados. Pueden ser personas físicas o empresas o instituciones públicas o privadas y deberán obtener una licencia de la Division of Corporations and Commercial Code. Están encargadas de mantener los registros directamente en línea de claves públicas.
Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser fiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave. Esta solución da origen a diferentes niveles o jerarquías de CAs.
En cuanto a los Certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.
Contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un Registro (Repository), considerado como una base de datos a la que el público puede acceder directamente en línea para conocer acerca de la validez de los mismos. Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.
La Autoridad Certificante puede emitir distintos tipos de certificados:

FUENTE: http://www.cybertesis.cl/tesis/uchile/2004/acevedo_f/html/index-frames.html

6. LA CADENA DE SUMINISTRO

Se puede afirmar de manera rotunda que el ciberespacio es una canal de distribución, e incluso que es el canal con mayor potencial de crecimiento de los conocidos en la actualidad.

Es evidente que hay artículos que no se pueden distribuir a través de la red, pero hay otros que es especialmente fácil, algunos ejemplos pueden podrían ser música, ya que podemos comprar canciones y recibirlas directamente en tu PC, otro artículo de distribución fácil en la red es el software, ya que podemos comprar nuestro programa o actualización e inmediatamente recibir el programa solicitado, los webmaster pueden adquirir al instante sus imágenes y fotografía en Internet, incluso podemos reservar billetes de avión o tren, también habitaciones de hotel en la red y muchos otros productos que se pueden distribuir físicamente.

Hay otro tipo de artículos que no se pueden enviar/recibir por la línea telefónica pero que afectan y mucho más en el futuro a los canales de distribución, y que van a intentar reducirla a la mínima expresión. En el mundo editorial prensa y libros tienen unos costes de distribución para las editoriales en principio prohibitivos, pues bien, podríamos llegar al caso que esos costes de distribución se acercaran al coste cero. En la actualidad la mayoría de las editoriales venden en su web de manera directa con lo que se ahorran los costes ocasionados por la distribución, aunque deberán hacer frente a los costes de envío y de la propia venta electrónica (casi nulo en la mayoría de los casos).

Un ejemplo actual de empresas de distribución comercial es Wal-Mart algunos proveedores tienen la responsabilidad de reponer los artículos en sus supermercados. En otras ocasiones, algunos distribuidores se ocupan de la gestión integral de las marcas propias. En Internet puede aplicarse este modelo: los portales alquilar su espacio (visitado por muchos usuarios) a los fabricantes y recibir una comisión por cada venta.

V. MERCADOTECNIA EN INTERNET

1. MEZCLA DE MERCADOTECNIA.

La mezcla de la mercadotecnia la podemos definir como el conjunto de estos cuatro factores

Plaza
La localización de la tienda electrónica puede afectar sus costos y desarrollo. Una de las mayores limitaciones es el ancho de banda. Ejecutar una tienda virtual debe tener un servidor apropiado y cuando se necesite “espejos” para incrementar el desarrollo de la diseminación de la información. Seleccionar el espejo adecuado es similar a seleccionar una tienda en negocios tradicionales. Es necesario utilizar varios lenguajes para varios mercados.

Precio.
Podríamos preguntarnos ¿Internet va a tener influencia en la política de precios? y por muy sorprendente que pueda parecer, sí que va a tener

influencia y en algunos casos mucha. Algunos de los factores que influirán en la política de precios son:

- Añadimos valor a nuestros productos.
- Reducimos costos de publicidad.
- Reducimos costos en el proceso de distribución.
- Es muy posible aumentar el número de clientes.
- Podemos vender las 24 horas del día.

Producto.
Respecto a él Internet nos ofrece un amplio abanico de posibilidades como son la realización de estudios de viabilidad, ofrecer promociones, realizar publicidad, etc.

Promoción
Dentro del Marketing-Mix quizás sea la publicidad la parte que más cambios puede sufrir con el uso de la nueva herramienta aparecida, ya que una de las primeras aplicaciones que todo el mundo ha pensado de la red es la realización de publicidad usando los nuevos servicios que se nos ofrecen.

2. PROMOCIÓN Y PUBLICIDAD POR INTERNET.

Aun no podemos hablar en sentido estricto de "CiberMarketing" o "Marketing para la *red*". Internet no cambia el conjunto de acciones a desarrollar dentro de la empresa por la aparición de un nuevo medio de comunicación. Nunca hemos oído hablar de "TVMarketing" o "RadioMarketing", ya que el Marketing abarca muchos más aspectos que la publicidad, incluso podríamos decir que la publicidad sólo es una pequeña herramienta que el Marketing utiliza para lograr sus objetivos.

La aparición de un interesante nuevo medio de comunicación hace que se deba estudiar como utilizarlo para lograr nuestros objetivos. Parece innegable que Internet ha despertado muchas expectativas en todo el mundo y que se empiezan a atisbar algunas de las posibilidades que el medio ofrece. Pero ello no nos debe hacer caer en la trampa de que la *red* es el único medio a utilizar, o que el es mejor, ni incluso creer que es el medio con más futuro para utilizar, ya que ello dependerá de la evolución que Internet sufra con el tiempo (desde hace años ya se habla de Internet2) y de las características de las empresas y sus objetivos en el tiempo.

A principios del siglo XXI el número de usuarios de Internet superará los 1.000 millones. En 1998 la cifra de venta de computadoras en la mayoría de los países desarrollados superó la venta de aparatos de televisión y elevados porcentajes de estas computadoras se conectan a Internet.

Se estima que a comienzos del 2001 más del 15% de las ventas mundiales se realizarán por computadora, cifra que irá creciendo de manera exponencial durante varios años. El siguiente cuadro nos ofrece 10 razones para utilizar Internet como herramienta a utilizar por parte del Marketing:

10 RAZONES PARA USAR INTERNET EN MARKETING

i. Por estar presentes en todo el mundo los 365 días del año durante las 24 horas del día.

ii. Vender on-line sin necesidad de intermediarios.

iii. Facilitar a nuestros clientes actuales y potenciales el acceso a la información de nuestra organización.

iv. Abaratar los costos de comunicación, catálogos, anuncios, comunicados a clientes y proveedores.

v. Podemos realizar estudios de mercado, sin movernos de la oficina.

vi. Para poder afrontar la globalización de los mercados en buena situación.

vii. Podemos hacer llegar nuestro mensaje llegue solo a nuestro público objetivo.

viii. Prepararse para la Sociedad de la Información.

ix. Para el cliente es mas fácil encontrar el producto, pues no tiene que desplazarse.

x. Mejorar nuestros servicios de atención al cliente.

Alguna diferencia entre la publicidad clásica y la realizada en la red puede ser, que mientras que los medios actuales, televisión, prensa y radio utilizan tecnología push, es decir la publicidad se lleva al destinatario, en Internet se utiliza tecnología pull, o lo que es lo mismo el usuario acude a la publicidad.

Por ello la publicidad online no será una intromisión, sino que será una elección del usuario/consumidor.

Otra diferencia interesante es que mientras que Internet es Multimedia, la mayoría de los otros medios no.

Una de las tareas más importantes dentro del Marketing es la promoción, no solo de productos o servicios, que se realizaría de la manera convencional, sino también de nuestra página web en el ciberespacio. ¿Quién vista una página que no conoce? En este apartado vamos a dar una serie de pistas para promocionar nuestro web.

Como en cualquier promoción los principios a seguir son:

Realizar un estudio previo de lo que se pretende conseguir.
Conseguir el mayor número de visitantes objetivos (target Marketing), no es tan importante tener un gran número de visitas, como que dichas visitas sean las que queremos.

Segmentar y seleccionar el público objetivo, identificando nichos de mercado si ello es posible.

Crear páginas atractivas, que posibiliten que el visitante compre y posteriormente repita vista el mayor número de veces que sea posible.

Hacer que nuestras páginas sean vivas, y por lo tanto actualizarlas tantas veces como sea necesario.

Para conseguir los objetivos de promoción de nuestros productos realizaremos campañas de promoción, dichas campañas pueden ser de dos tipos:

i. Campañas de reconocimiento de marca: sirven para el lanzamiento de una marca o producto.
ii. Campañas de posicionamiento estratégico: se utilizan para aumentar las ventasen un periodo de tiempo determinado.

Para lograr promocionar adecuadamente nuestra página web, lo que hará de efecto multiplicador en la promoción del producto podemos realizar las siguientes acciones (no se descartan otras imaginativas):

i. Incluiremos la dirección web y los e-mail necesarios en nuestra papelería corporativa, papel de carta, tarjetas de visita, albaranes, facturas, saludas, felicitaciones, catálogos de productos.

ii. También incluiremos las direcciones en todo tipo de campañas publicitarias que realicemos, sean en prensa, radio, televisión o cualquier otro medio utilizado.

iii. Enviaremos una carta a nuestros clientes y proveedores indicándoles la puesta en marcha de nuestro web.

iv. En los anuncios de páginas amarillas también pondremos como datos de interés las direcciones.

v. Si es posible debemos añadir en el etiquetado de nuestros productos este dato.

Al conjunto de las acciones anteriores las llamaremos promoción online. Existe otro tipo de promoción de nuestro web, es la llamada promoción online, ésta abarca todos los pasos a realizar en la red para dar a conocer nuestro site.

Algunas de las acciones más relevantes de este tipo de promoción son:

i. Enviar un e-mail a nuestro cliente notificando la puesta en escena del web site.

ii. Haciéndolo con delicadeza ya que los correos no deseado no gustan en Internet.

iii. Enviar mensajes a las News que tengan relación con nuestra página.

iv. Enviar mensajes a las Listas de Distribución que lo permitan, ya que en la mayoría no se admite publicidad y están moderadas. Hacer llegar nuestra dirección en las conversaciones que mantengamos en los chats relacionados.

v. Presentar nuestra página a concursos y premios.

vi. Establecer links recíprocos con otras páginas del sector.

vii. Introducción de nuestra URL en todos los buscadores posibles, hay miles de ellos en todo el mundo.

VI. ASPECTOS LEGALES Y ÉTICOS EN EL COMERCIO ELECTRÓNICO

1. LEGISLACIÓN EN EL COMERCIO ELECTRÓNICO.

El Derecho, considerando como tal a los textos o principios legales y la puesta en acción de los mismos por las instituciones o los operadores jurídicos, ha tenido que preservar en el comienzo del Estado de Derecho, fase liberal, la confianza de que en caso de que suceda algún conflicto en las relaciones sociales el ciudadano o la persona implicada en el mismo encontrará el procedimiento adecuado para alcanzar la reparación del daño. Con esta actitud el Derecho también garantizaba que su mera existencia, como instancia capaz de resolver problemas, impediría causarlos, al temer los causantes de los mismos sufrir las consecuencias establecidas en el ordenamiento.

En la actualidad esta confianza en el mecanismo ha quedado ampliada por el hecho de que ella ha de extenderse no tan sólo a la prevención o solución de conflictos sociales concretos, sino a la circunstancia de que funcionen todos los mecanismos que permiten la convivencia social: el suministro de energía, el agua, las redes de comunicaciones. Esta es una consecuencia del cambio de caracterización del Derecho: de ser una solución de carácter sancionador o represivo para con conflictos concretos, concepción propia del Estado liberal, ha pasado a formar parte, como ámbito representativo de la discusión política diaria, de la promoción, desarrollo y mantenimiento de los individuos y la sociedad en su conjunto, concepción propia del Estado social o del de bienestar.

Todo ello ha acarreado la necesidad de contar con la colaboración de profesionales de formación diferente a la jurídica en la solución de los problemas sociales. Ellos son los expertos de diferentes ámbitos de acción y trabajo que son necesarios para que se produzca el estudio y la solución de los problemas de subsistencia y supervivencia que tienen los individuos y la sociedad diariamente. Son los profesionales formados en la Universidad y en la práctica profesional desde el siglo XIX, con el progresivo desarrollo del conocimiento y las ciencias, y la aplicación práctica de los mismos mediante la técnica.

Esta circunstancia es particularmente destacable cuando, como sucede en estos momentos, nos encontramos en la fase de aparición de fenómenos desconocidos como el hecho de que en un instante, mediante Internet, podamos comunicarnos, utilizando el habla, la escritura y las imágenes, con personas que desarrollan su vida en otros lugares del mundo. El fenómeno

requiere, como cualquier otro, una regulación normativa que prevea tanto su implantación como la solución de los diferentes problemas sociales que él mismo pueda causar. En la propuesta de solución han de intervenir, como en la del resto de los problemas sociales, expertos en Derecho y en otros conocimientos y técnicas.

Todo ello obliga a la Filosofía del Derecho, disciplina experta en el estudio de las actividades jurídicas, los principios del ordenamiento, el conocimiento del Derecho y el ámbito de la argumentación jurídica, a discurrir sobre las características del nuevo mecanismo, y proponer visiones del mismo y perspectivas regulativas al jurista, a efectos de que éste pueda participar en la provisión de soluciones a la implantación de Internet que den confianza a sus usuarios por ser soluciones respetuosas con el ordenamiento. Esta propuesta paliaría un problema social: el hecho de que por ahora la confianza en el uso de Internet reside, especialmente, en el contenido de protocolos o reglas técnicas, siendo que éstas, como vamos a ver, resultan marcadamente insuficientes para dar a los usuarios de Internet, a la hora de comunicarse entre si, las garantías establecidas por el ordenamiento en su conjunto a cualquier actividad social.

La promulgación de regulaciones está justificada por el hecho del comienzo de la expansión de Internet, el consenso existente acerca de su relevancia para el desarrollo económico y social en cuanto instrumento capaz de crear riqueza y nuevos empleos, y también por la conciencia de que la red, tal y como está concebida y opera, tiene fuertes riesgos técnicos y consecuencias jurídicas que requieren normas que propicien su uso a la vez que superen dichas debilidades. De ahí que las primeras normas sobre Internet promulgadas estén referidas al uso de las técnicas de cifrado en lo relativo a la firma electrónica y fomentar la expansión del uso de Internet.

EL PAPEL DEL DERECHO EN EL MUNDO VIRTUAL.

El Derecho también se ve afectado por estos cambios, solo que la intensidad y el grado del giro, superan ampliamente lo ocurrido luego de la revolución francesa o la revolución industrial. La imagen del Abogado casi siempre se ha asociado a un papel o un libro, o a una pluma de escribir, o a un maletín, aunque algunos ya los asocian con el teléfono móvil en uso constante.

Pues bien no solo es la imagen del Abogado la que se asocia al medio escrito, sino que el Derecho mismo se sustenta en el uso y abuso del medio escrito, incluso algunos contratos tienen dicha solemnidad bajo sanción de carecer de efectos jurídicos. En el medio procesal se utilizan aforismos como “lo que no esta en el expediente, no existe en el mundo” y en el argot popular la frase “me han empapelado” denota el fastidio de recibir documentos de incidencia legal para una persona. La prueba por excelencia para acreditar una transacción es el papel con firmas manuscritas de las personas que intervienen.

Sin embargo el paradigma del documento escrito con firmas manuscritas esta siendo dejado de lado por el uso del documento digital con o sin firma electrónica sobre el mensaje. Las transacciones, la publicidad y la información se viabilizan en un formato ajeno al medio escrito. Para muchas personas incluyendo a las empresas el cambio de paradigma significa una facilitación en la búsqueda de información, acceso a mercados mundiales, a nuevas

tecnologías e incluso facilita la compraventa de mercancías. El cambio hacia el mundo digital es relativamente bajo en comparación con los beneficios que este ofrece, en consecuencia el uso de tecnologías de la información no es tan traumante para el común de las personas, como lo es para el mundo del Derecho.

Para el ordenamiento legal, el uso de tecnologías de la información se convierte en un uno de los mayores retos que tiene que enfrentar y superar, si es que quiere cumplir con sus objetivos de establecer las reglas de convivencia social.

El Derecho tiene que tener las respuestas adecuadas para facilitar la transición del medio físico al mundo virtual, de lo contrario la convivencia social en Internet sería una suerte de anarquía que puede llevar a su propio aniquilamiento. Claro esta, que todo ordenamiento legal surge cuando existe un grupo social, y de hecho en Internet ya existen reglas de convivencia y códigos de conducta que están regulando a la mayoría de los internautas. Lo que sucede en Internet es que los propios actores tienen internalizadas sus normas y no la toman como impuestas por terceras personas, tal como sucede con algunas comunidades campesinas respecto al derecho occidental.
El reto del Derecho es, pues, flexibilizar sus instituciones e incorporar aquellas normas surgidas dentro del Internet para que todos los actos jurídicos que se den dentro del mundo virtual tengan idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios tenga los mismos efectos legales.

Por tanto resulta de suma importancia revisar nuestros ordenamientos jurídicos y reorientarlos hacia la esfera digital tal cual lo vienen haciendo las administraciones gubernamentales, empresas y personas de todo el mundo. Nosotros no somos de la opinión de “crear” una nueva rama del Derecho, como es el Derecho Laboral, o el derecho Penal, puesto que el cambio atraviesa a todas las especialidades jurídicas, con distintos niveles de afectación, es decir, no pretendamos definir el objeto de estudio de esta “especialidad” porque no existe como tal. Este cambio subyace a todas las especialidades del Derecho.
Cabe mencionar que no debemos confundir lo expresado con la aparición del Derecho informático que si tiene un objeto de estudio, sin embargo en la medida que el cambio se generalice y en la medida que el objeto de estudio de esta especialidad aumente, su importancia en la nueva configuración del Derecho va ser muy valiosa. Su importancia será equivalente a la que tiene el Derecho Civil para el sistema romano – germánico. Para aquellos lectores que pertenecen al sistema del Common Law, el sistema que predomina en América Hispana es el sistema de codificación o sistema romano – germánico, donde el Derecho Civil codificado en un solo cuerpo legal irradia sus efectos a las demás áreas del Derecho.

Ante ello nos surge la pregunta si la actual convergencia digital de la sociedad puede originar la creación de un sistema jurídico propio o unificar los ya existentes, el tiempo nos lo dirá, lo es cierto es que los cambios actuales modificarán los sistemas jurídicos ya existentes en el mundo.

2. ASPECTOS ÉTICOS EN EL COMERCIO ELECTRÓNICO.

Las dificultades éticas particulares del comercio electrónico normalmente giran alrededor de tres cuestiones: la intimidad o privacidad y la identidad, ambas referidas al comprador, y la no-refutabilidad de la transacción (Baum 1998: 65; Suprina 1997: 8-12; Joyanes 1997: 277-281). Sin embargo, pienso que habría que introducir una cuarta cuestión, la de "allanamientos, intrusiones, entradas abusivas o no autorizadas" ("trespass" o "break-ins" según la tradición legal anglosajona, en un sentido metafórico) en los equipos informáticos, páginas web, buzones electrónicos, etc. Quizá la palabra inglesa "hacking", en su reciente acepción de lograr algo en principio difícil con gran facilidad, burlando el sistema de protección o defensa, sea la que mejor capte el concepto. Los actos de "hacking" se distinguen de las violaciones de intimidad, no obstante, porque la red es un "lugar público", un sistema abierto. Al igual que un lugar comercial físico y convencional, nadie discute que una dirección electrónica comercial sea propiedad privada; pero el acceso ha de estar abierto al público, como su propia naturaleza y finalidad exige. Es decir, por principio y a priori, no se puede prohibir la entrada a cualquiera; de otra forma se correría el riesgo de caer en una discriminación ilegal, si no, al menos, abusiva. O sea, por el hecho de entrar en una página web o en un buzón electrónico, no se atenta contra la intimidad del propietario; pero una vez allí, pueden realizarse actividades inapropiadas.

"Hacking", "cracking" y "page-jacking" (allanamientos y secuestros informáticos)

El "hacking" atenta contra la misma computadora, contra un sistema informático particular o contra la red en general, en cuanto almacén de datos o medio de comunicación; pone en peligro la confidencialidad, la integridad o la disponibilidad de la información almacenada en la computadora o de los servicios que la computadora presta (US Department of Justice 2000: 10). Antiguamente, como diversión de adolescentes y demás gentes especialmente dotadas para la informática, no tenía necesariamente finalidad criminal o delictiva alguna; si acaso, sólo se trataba de gastar una broma pesada al dueño o al administrador del equipo informático señalado como objetivo, descifrando ("cracking") sus códigos secretos de acceso. Como forma de protesta, los "hackers" "secuestraban" una página web ("page-jacking"), dirigiendo a los visitantes a otra dirección mediante un cambio de servidor. Por ejemplo, el 21 de junio de 2000, los visitantes de la página web de Nike fueron reconducidos a la de "S 11 Alliance", una organización australiana que lucha contra la globalización y las grandes multinacionales (Richtel 2000). Los "hackers" demostraban de esa manera su habilidad superior, al vencer los retos y los obstáculos que los sistemas de seguridad del ordenador les planteaban; era algo así como superar una marca olímpica deportiva.

Sin embargo, desde hace unos años, se han llevado a cabo actos de "hacking" con una malicia más que presumible; de modo que se ha convertido en una actividad accesoria a un delito, si no en un delito mismo. Así fue, supuestamente, el caso de Jeffrey Hirschorn, un reportero de IPO.com, empresa informativa que cubre la salida en bolsa de nuevos valores en Nueva York (Bloomberg News 2000). Anteriormente, Hirschorn trabajaba para Wall Street Source, competidora de IPO.com. En septiembre de 1999, Wall Street Source despidió a Hirschorn, según él, en un acto de discriminación anti-semita. Unos meses después, Hirschorn, valiéndose de la contraseña de un empleado a tiempo parcial, logró meterse en el

sistema informático de Wall Street Source y borró datos de su página web. En consecuencia, Wall Street Source tuvo que rehacer todo su sistema de seguridad. En mayo de 2000, Wall Street Source puso un pleito contra Hirschorn y IPO.com por sabotaje, por el que pedía $100.000 de compensación y $5 millones de daños punitivos.

¿Cómo operan este tipo de “hackers”? En primer lugar, se burlan del sistema de seguridad informática para acceder sin autorización a archivos confidenciales: es el robo de información. Los blancos preferidos son las computadoras del gobierno, sean del servicio de policía o militar, por ejemplo. Es fácil imaginar el interés que pueden tener grupos criminales, terroristas o espías de estados enemigos en acceder a esos archivos. En otros contextos, el meterse en las computadoras de los ministerios de economía o de hacienda también puede presentar alicientes similares. Los equipos informáticos de instituciones y empresas privadas son igualmente susceptibles de este tipo de ataques. Un “hacker” puede entrar en un sistema de reservas hoteleras para sustraer informaciones referentes a tarjetas de crédito, por ejemplo. O también lo podría hacer para robar distintas formas de “propiedad intelectual”: desde enterarse de secretos comerciales hasta reproducir materiales sujetos a copyright, como son los programas de copmutadora. Por último, el “hacker” puede realizar por este procedimiento lo que ha dado en llamarse “ciber-acoso”: busca información confidencial referente a un sujeto, bien para extorsionarle, bien para satisfacer una curiosidad malsana (US Department of Justice 2000: 12). Especialmente vulnerables para este fin son los sistemas que almacenan historiales clínicos, crediticios, números telefónicos y direcciones que no aparecen en listas públicas, etc.

En segundo lugar, los “hackers” abordan un sistema informático para controlar las operaciones que regula. Así pueden aprovecharse de los servicios de una empresa sin pagar, o venderlos a terceros, quedándose con los pagos: es el robo de servicios. Ha habido intrusiones en sistemas de telefonía para realizar llamadas gratis, o en computadoras de gran capacidad para descifrar claves y contraseñas de tarjetas de cajero automático, por ejemplo. Los “hackers” más sofisticados pasan por diversos medios de telecomunicaciones —teléfonos fijos, teléfonos móviles, computadoras personales, computadoras institucionales, Internet— para poder ocultar así su identidad. En noviembre de 1999, la Guardia Civil española desarticuló la primera red de estafa a través de Internet en la Unión Europea, que afectó a más de 30.000 personas (ABC 1999c). La Benemérita recibió denuncias de usuarios que habían recibido mensajes en su correo electrónico en los que se les cargaban 78.000 ptas. en sus tarjetas de crédito por supuestos pedidos. El cargo era a favor de Plssl Software, Inc., cuyo número de teléfono de información gratuita aparecía en los mensajes. Resultó que dicho número de teléfono correspondía a Entel Telecomunicaciones, una empresa chilena. Luego, los agentes descubrieron que los cargos se realizaban desde la cuenta de correo electrónico de E.V.L., un argentino residente en Málaga, mediante conexiones telefónicas desde el domicilio del empresario británico J.C., en la localidad de Alhauín de la Torre. Finalmente, los dos sospechosos fueron detenidos y se intervinieron en sus casas cinco computadoras y abundante documentación incriminatoria.

En tercer lugar, los “hackers” pueden causar daño al colapsar una computadora personal, un servidor o una parte de la red: por ejemplo, con los ataques que

provocan el “fuera del servicio” (denial of service) (The Economist 2000a; Sager et al. 2000). Se lleva a cabo mediante el “bombardeo de correo electrónico” (mailbombing), el envío de un aluvión de mensajes a una cuenta o dirección electrónica al mismo tiempo, causando la sobrecarga del servidor. El “hacker” sólo tiene que copiar un pequeño programa, fácil de conseguir en la red, e instalarlo en varias computadoras donde haya logrado entrar, o mejor todavía, en las computadoras de los proveedores de servicios de Internet (ISPs), para hacer asaltos con mayor eficacia y anonimato. Esta fue la técnica empleada para inutilizar los servicios de los principales comercios virtuales, como Yahoo, Amazon, EBay y Buy, en febrero de 2000. El interrumpir deliberadamente los servicios de una red informática está tipificado como crimen federal en los EE.UU., y puede suponer un castigo de cinco años de carcel, más una multa de $250.000 y daños. (Bonner 2000).

Por supuesto que las redes informáticas también pueden colapsarse mediante la difusión maliciosa de “virus” y “gusanos”. Los “gusanos” se distinguen de los “virus” en que no sólo se autorreproducen, como éstos, sino en que también son capaces de autopropagarse o autoenviarse por la red (Markoff 2000b). El gusano “Melissa” costó alrededor de $80 millones en pérdidas de tiempo, esfuerzo, datos y oportunidades de negocio a usuarios de todo el mundo (Markoff 1999b). El gusano “I love you”, por su parte, podría haber provocado en mayo de 2000 daños valorados en torno a $10.000 millones (Reuters 2000a).

Asuntos relacionados con la privacidad

Double Click es la principal agencia publicitaria de Internet (Green, Alster & Borrus 2000). Sus computadoras insertan mensajes publicitarios en las páginas web de unas 1.500 empresas. Esos mensajes tienen una extraordinaria puntería en sus destinatarios gracias a los “cookies” (“galletas”), pequeños archivos que las empresas instalan en el disco duro de los visitantes de su página web, permitiéndoles seguir sus hábitos de navegación. Con los “cookies”, Double Click elabora un perfil de cada usuario basado en información valiosísima para la dirección comercial, como las páginas que éste frecuenta, el tiempo que pasa en cada una de ellas, la fecha de su última visita, etc.

El 27 de enero de 2000, Harriet Judnick, una administrativa de California, puso un pleito contra Double Click por violaciones del derecho a la intimidad y prácticas comerciales fraudulentas. Unos meses antes, en noviembre de 1999, Double Click había comprado Abacus Direct, una empresa convencional de “comercialización en directo” (“direct marketing”) por $1.700 millones. Abacus Direct contaba con importantes bases de datos de nombres y direcciones de clientes que compraban por catálogo. Según Judnick, Double Click había cambiado de política comercial: la información acerca de los usuarios de Internet que antes recogía de forma anónima, ahora se iba a combinar con los verdaderos nombres y direcciones postales, gracias a los datos de Abacus Direct. Así, Double Click podría averiguar el nombre, la dirección postal, el número de teléfono y otros datos del usuario real de Internet, cuyo perfil de navegación se había elaborado mediante los “cookies”. Judnick pensaba que de esta manera, Double Click estaba traficando con datos personales y confidenciales sin conocimiento ni consentimiento de los consumidores afectados. Esta situación, que representaría un verdadero paraíso para los agentes comerciales, sin embargo significaría un auténtico infierno para cualquier persona celosa de guardar su intimidad o privacidad.

Finalmente, debido a la avalancha de críticas que recibió, en parte por la atención que los medios habían dirigido al pleito de Judnick, Double Click decidió dar un paso atrás en sus planes. Su director general, Kevin O'Connor, con un tono compungido, lamentaba "haberse adelantado a los sucesos", intentando realizar unas actividades sin que existieran todavía claras normas éticas y legales (Seglin 2000a). No obstante, estos acontecimientos fueron suficientes para desencadenar una discusión pública intensísima sobre la protección de la privacidad en Internet, concretamente, la de los consumidores frente a las empresas "prospectoras de datos" (data-mining, data-profiling), probablemente carentes de escrúpulos (Clausing 1999b).

La privacidad es deseable en cuanto permite a un sujeto reafirmar su individualidad, separándose del grupo y reclamando un espacio o dominio propio. El problema de la privacidad en el comercio electrónico se refiere a la dificultad de transmitir, de manera segura, los datos necesarios para una transacción por la red (Suprina 1997). Se trata de evitar que la información que se envía, considerada económicamente valiosa o en cierta medida confidencial, no sea interceptada ni quede disponible para otra persona que no sea la destinataria. Proteger la privacidad de la comunicación supone un gran reto por la misma naturaleza del medio, que es una red abierta de telecomunicaciones digitales. De hecho, es imposible, tanto desde el punto de vista técnico como económico, tapar todos los posibles agujeros por donde pueden realizarse intrusiones desautorizadas en las transmisiones por la red (Coleman 1999a). Además, como la misma experiencia enseña, cada vez hay una mayor variedad o picaresca en los modi operandi de quienes se empeñan en minar los derechos a la intimidad de los usuarios de Internet (Garfinkel 1999; The Economist 1999e; Rosen 2000). No existe, por tanto, una privacidad absoluta; y todo esfuerzo en este sentido debe dirigirse, más bien, hacia la obtención del grado de privacidad adecuada, consensuada por las partes implicadas, para cada tipo concreto de transacción (The Economist 1999b).

Las medidas para la protección de la privacidad son de tres tipos:

i. las que pertenecen a la estructura o disposición física de la red
ii. las que utilizan protocolos, programas o aplicaciones especiales para este fin
iii. las que derivan de determinadas pautas de conducta o comportamiento, de carácter ético y legal.

Las primeras pueden englobarse en el conjunto de técnicas que se llaman "firewalling"; o sea, en la construcción de una especie de "muro de seguridad o contención" en el sistema informático y de telecomunicaciones (Stewart 1998a). En general, se trata de decidir, con la privacidad como criterio, qué equipos poner en qué red ("LAN" (local area network) o red local, "intranet" o red privada de una empresa u organización, Internet público), así como el control de las vías de acceso y salida de cada uno de ellos (las líneas telefónicas, fijas o móviles, los "ISP" (Internet Service Providers) o proveedores de servicio de Internet, los portales), evitando "puertas traseras" inseguras (Freedman 1999). Puede que se destinen equipos concretos para determinado tipo de comunicaciones o transacciones, en función del grado de privacidad que requieran. La mejor aliada de la privacidad sigue siendo la separación física, junto con la ausencia de cables,

antenas, portales de infrarrojo y receptores de cualquier otra forma de energía electromagnética por la que la información digitalizada pueda viajar.

Las segundas son de dos tipos; en primer lugar está el empleo de claves, contraseñas, números personales de identificación, etc., que restrinjan el acceso a cuentas, documentos y archivos; y en segundo término aparece el uso de la criptografía, por la que los mensajes en tránsito se vuelven indescifrables, excepto para los destinatarios y aquellos que estén debidamente provistos de las claves, aplicaciones y capacidades informáticas oportunas. Debido a sus implicaciones para los servicios de inteligencia, la defensa de los estados y el sector militar, la criptografía es, en sí misma, una tecnología muy protegida y regulada por los gobiernos.

Aunque en un sentido, las medidas que se refieren al comportamiento son las que menos garantías ofrecen, en otro, pueden ser las más eficaces, porque tanto el respeto como la violación de la privacidad, al fin y al cabo, siguen siendo actos humanos, no informáticos. El objetivo, por tanto, es llegar a un acuerdo sobre los criterios de acción: cuáles son las conductas que deben prohibirse, evitarse, permitirse, fomentarse y por qué (Nail, Prince & Schmitt 2000). En esta tarea es imprescindible la colaboración entre el sector público y el privado; aunque sólo sea porque la salvaguarda de la privacidad siempre lleva consigo un coste para las fuerzas de seguridad del estado, que tendría que contrastarse con los beneficios empresariales esperados. La reglamentación estatal de Internet y del comercio electrónico es tan deseable como es necesaria, aunque la autorregulación es lo mejor (Consejo Pontificio para las Comunicaciones Sociales 2002: 16).

Las iniciativas del sector público en los EE.UU. derivan de las directrices de la Secretaría de Salud, Educación y Bienestar de 1973 y de la “Privacy Act” de 1974, que establecían criterios para la recogida y utilización de datos personales por parte del gobierno federal. Estas prácticas fueron adoptadas luego por la OECD en sus “Guidelines for the Protection of Personal Data and Trans-border Flows of Personal Data” de 1980. Estas normas fueron reafirmadas en lo sustancial para el nuevo medio de Internet, con el documento “Implementing the OECD Privacy Guidelines in the Electronic Environment” de 1998. Ese mismo año entró en vigor una norma europea según la cual las empresas sólo podrían transmitir los datos de los consumidores comunitarios allí donde recibiesen un grado adecuado de protección, similar al que tienen dentro de la Unión. Los EE.UU. —donde la legislación en esta materia se ha paralizado y se ha optado más bien por la autorregulación— quedaban excluidos de este ámbito seguro (Stewart 1998a: 2). Esta política europea provocó múltiples protestas por parte de las empresas norteamericanas, y las más beligerantes han amenazado con elevar este asunto a la Organización Mundial de Comercio, como ejemplo de medida discriminatoria ilegal. En julio de 2000, la credibilidad de los estados a la hora de proteger la privacidad o intimidad de sus ciudadanos recibió un duro golpe al descubrirse la utilización de programas de “escucha” —como el “carnivore” por parte del FBI— en varios proveedores de servicio de Internet (Reuters 2000b). Estos sucesos sirven para subrayar la necesidad de la cooperación y del consenso internacional de cara a la formación de criterios y el establecimiento de mecanismos para promover y proteger el bien de los ciudadanos en todo el mundo (Consejo Pontificio para las Comunicaciones Sociales 2002: 17).

El sector privado también ha puesto en marcha varias iniciativas a favor de la privacidad, a pesar de que cuenta con una barrera difícil de superar, el cumplimiento obligatorio, ya que sólo puede emplear compromisos o acuerdos voluntarios. El World Wide Web Consortium (W3C), organismo internacional que desarrolla protocolos para Internet, propone la “Platform for Privacy Preferences” (P3P), unas especificaciones técnicas que permiten a los consumidores elegir y decidir qué datos quieren revelar acerca de sí mismos y, en cierta medida, controlar su uso (Stewart 1998a: 2-3). El consumidor configura sus preferencias en el navegador y, siempre que los niveles de protección de la página visitada se adecuen a lo previsto, no habrá ningún problema. Cuando la página visitada solicita más datos de los inicialmente permitidos, el programa alerta al usuario y le da dos opciones: salirse o dar más información para poder continuar. Otra medida consiste en la organización de entidades independientes, sin ánimo de lucro, cuya finalidad es velar por el cumplimiento de los acuerdos sobre la confidencialidad de los datos del consumidor. Las empresas firman contratos con esas organizaciones —la más conocida de las cuales es “Trust-e”— y les pagan una cuota, a cambio de poder llevar en su página el “sello de garantía”.

En abril de 1999, la Asociación de Autocontrol de la Publicidad (AAP) de España elaboró —según normativa europea— un código ético sobre la publicidad en Internet (ABC 1999a). Este documento de adhesión voluntaria fue el primero que se redactó en Europa, y puede resumirse, sustancialmente, en el siguiente “decálogo”:

i. La publicidad y el anunciante deben identificarse.
ii. Se debe respetar la legislación vigente de protección de datos.
iii. Los menores no pueden facilitar información on-line sin autorización paterna.
iv. Los contenidos publicitarios dirigidos exclusivamente a los adultos deben estar identificados.
v. No se debe incitar directamente a los menores a la compra de un producto o servicio.
vi. No se admitirá el envío de publicidad por correo electrónico si no ha sido solicitada por el destinatario (anti-spam).
vii. No pueden utilizarse los grupos de noticias para captar los datos con finalidad publicitaria.
viii. La publicidad en la world wide web (www) no puede impedir la libre navegación del usuario.
ix. Si las interrupciones publicitarias son inevitables para acceder al contenido editorial de una página web, el usuario debe ser advertido.
x. Deben identificarse las páginas web patrocinadoras.

Algo similar a la relación de los gobiernos con sus ciudadanos sucede con las empresas, en lo que respecta a la intimidad de empleados y trabajadores. Mas los esfuerzos legítimos por parte de los empleados de evitar abusos tendrán que buscar su equilibrio con los de la empresa, en su autodefensa. En los EE.UU., algunas empresas han tenido que enfrentarse a acusaciones de discriminación racial o acoso sexual, porque en el correo electrónico de los empleados aparecían comentarios a este efecto: la empresa es propietaria del equipo informático, y por ello es responsable de todo lo que ahí se publica (Seglin 1999; Guernsey 2000a).

En otro orden de cosas, un empleado desde hacía 30 años de la Deutsche Bank en Barcelona fue despedido por el abuso del correo electrónico: desde su puesto de trabajo, mandó 140 mensajes en cinco semanas; y en la mayoría de ellos, se incluían chistes sexistas y obscenos (Diario de Navarra 2001). Anteriormente, ya había sido advertido de que las herramientas de trabajo sólo debían utilizarse con fines profesionales. En noviembre de 2000, el Tribunal Superior de Justicia de Cataluña avaló el despido, porque según su parecer, el empleado incurrió en "una falta de disciplina grave y reiterada": o sea, la empresa no había vulnerado ningún derecho a la intimidad del trabajador en el escrutinio de su correo electrónico.

Teniendo en cuenta que la privacidad nunca puede ser absoluta, y que el grado de privacidad adecuada para cada transacción virtual depende de múltiples factores, se recomienda, sin embargo, la observancia de los siguientes principios (Green, Alster, Stepanek & Borrus 2000):

i. Aviso. Las empresas deben avisar en su página web si recogen o no información sobre el usuario, para qué sirve esa información y quién la va a utilizar.
ii. Opción. Los consumidores han de poder controlar sus datos personales y el uso que las empresas hacen de ellos; por eso, se les presentará la posibilidad de negarse ("opt-out") a la recogida de sus datos, así como al traspaso y venta de éstos a terceros.
iii. Acceso. Los consumidores han de poder acceder a los archivos que las empresas guardan de sus datos personales y revisarlos, para corregir errores, retirar aquello con lo que no están de acuerdo, etc. O sea, los datos personales de los usuarios nunca pasan a ser propiedad de la empresa.
iv. Seguridad. Las empresas deben asumir la responsabilidad de la seguridad de los datos, y cuando ésta no se respeta, deben someterse a sanciones y castigos proporcionados. Incluso han empezado a comercializarse aplicaciones, BeFree y AbiliTec, para la difícil tarea de, por un lado, permitir a los consumidores acceder a sus datos, y por otro, permitir a las empresas mantener niveles adecuados de seguridad en sus archivos (Tedeschi 2000b).

Estas disposiciones recogen, sustancialmente, el acuerdo de "puerto seguro" (safe harbor) jurídico entre Europa y los EE.UU. (Agence France Press 2000b).

FUENTE:
http://www.unav.es/empresayhumanismo/3prog/profesorado/ajgsison/publications/journal/49/49.html

FUENTES CONSULTADAS:

http://www.idrc.ca/en/ev-68562-201-1-DO_TOPIC.html
http://www.monografias.com
http://www.lawebdelprogramadaror.com
http://www.unav.es/empresayhumanismo/3prog/profesorado/ajgsison/publications/journal/49/49.html
http://www.cybertesis.cl/tesis/uchile/2004/acevedo_f/html/index-frames.html
http://www.cimm.com.mx/cimm/comercio.html
http://mktglobal.iteso.mx/numanteriores/2001/sep01/sep04.htm