ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ESTUDIO DE REDES PRIVADAS DE TELECOMUNICACIONES COMO PLATAFORMA PARA REALIZAR TRANSACCIONES FINANCIERAS ELECTRÓNICAS SEGURAS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

ARMANDO RAMIRO REINOSO YEPEZ

DIRECTOR: ING. FERNANDO FLORES

Quito, agosto 2001

DECLARACIÓN

Yo, ARMANDO RAMIRO REINOSO YEPEZ, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Armando Ramiro Reinoso Yépez

AGRADECIMIENTOS

A Dios. A mis padres Armando y María Elena, por haberme sabido guiar y estar conmigo en todo momento y circunstancia. A Mario Hidalgo, por haber creído en mi y haberme dado la oportunidad de culminar mi carrera. Al Ing. Fernando Flores, por la ayuda recibida durante el desarrollo de este trabajo. Al Ing. Pablo Hidalgo, por haberme apoyado durante toda la tesis. A mi esposa Mariella, a mis hijos Andrés, Mateo y al Bebe, por haber tenido la paciencia de aguantarme todo este tiempo. A todo el CEPAR, por la incondicional ayuda y facilidades que me dieron para mi trabajo. A toda mi familia propia y política, que de una u otra manera estuvieron siempre pendientes.

Gracias.

CONTENIDO

Figuras	ix
Tablas	x
Resumen	xi
Presentación	xii
Capítulo 1. Comercio Electrónico: Definiciones y Principios	
1.1 Introducción	1
1.2 Definición y componentes del Negocio Electrónico	2
1.2.1 Definiciones	2
1.2.2 Componentes del Negocio Electrónico	4
1.3 Base para las Transacciones Electrónicas	5
1.4 Transacciones en Negocio Electrónico	6
1.5 Fundamentos del Negocio Electrónico	6
1.6 Infraestructura para Negocios Electrónicos	8
1.6.1 Proveedores	8
1.6.2 Al interior de la empresa	9
1.6.3 Clientes	9
1.7 Ventajas del Negocio Electrónico	10
1.7.1 Oferta y Demanda	11
1.7.2 Competitividad y Servicio	11
1.7.3 Atención generalizada y Venta personalizada	11
1.7.4 Entregas y Respuestas a necesidades mas rápidas	11
1.7.5 Costos y Precios menores	12
1.7.6 Oportunidades, Productos y Servicios Nuevos	12
1.7.7 Ventajas para el vendedor	12
1.7.8 Ventajas para el comprador	13
1.8 Desventajas del Negocio Electrónico	13
1.9 Modelos de Negocio Electrónico	15
1.9.1 Modelos Transplantados	16
1.9.2 Modelos Nativos	16
1.10 Categorías del Negocio Electrónico	17
1.10.1 Negocio Empresa-Consumidor	18

1.10.2 Negocio Empresa-Empresa 18
1.10.3 Negocio Empresa-Administración 18
1.10.4 Negocio Consumidor-Administración 18
1.11 Sistema de Negocio Electrónico 19
1.12 Proyección del Negocio Electrónico en el Mundo 22
1.13 Ámbito e Integración del Negocio Electrónico 24
1.13.1 Ámbito del Negocio Electrónico 24
1.13.2 Integración del Negocio Electrónico 26
1.14 Comunidades de Negocio Electrónico (EBC) 27
1.14.1 Tipos de EBC 29
1.14.2 Implementación de EBC 31
1.15 Diseño de un Negocio Electrónico 33
1.16 Análisis en Detalle 36
1.16.1Situación actual 36
1.16.2 Problemática de las Empresas 37
1.16.3 Beneficios 38
1.16.4 Metodología y Desarrollo para alcanzar el éxito en la gestión 39
1.16.4.1 Formación en el ámbito directivo de Internet y sus posibilidades 39
1.16.4.2 Definición del equipo que va a desarrollar el proyecto así como su alcance, plazos y recursos 39
1.16.4.3 Revisión del plan estratégico de la empresa para integrar en él la figura de Internet 40
1.16.4.4 Análisis de las necesidades de información y automatización para el proyecto y el grado de adecuación de los sistemas de información existentes 41
1.16.4.5 Definición de políticas y procedimientos de seguridad 41
1.16.4.6 Diseño de la presentación en Internet y tecnologías asociadas. Definición de la conexión 41
1.16.4.7 Reestructuración de procesos para adecuación a Internet 42
1.16.4.8 Promoción en Internet 42
1.16.4.9 Seguimiento y control 42
1.17 Banca y Negocio Electrónico 43
1.18 Logística 46

Capítulo 2. Redes Privadas: Tecnologías Inmersas

2.1 Introducción 48
2.2 Historia del Internet 49
2.3 Modelos de Referencia 52
2.3.1 Definiciones 52
2.3.2 Modelo de Interconexión de Sistemas Abiertos 54
2.3.2.1 Capa Física 55
2.3.2.2 Capa de Enlace de Datos 56
2.3.2.3 Capa Red 56
2.3.2.4 Capa Transporte 56
2.3.2.5 Capa Sesión 57
2.3.2.6 Capa Presentación 57
2.3.2.7 Capa Aplicación 57
2.3.3 Modelo de Referencia TCP/IP 58
2.3.3.1 Capa Host a Red 58
2.3.3.2 Capa Internet 58
2.3.3.3 Capa Transporte 59
2.3.3.4 Capa Aplicación 59
2.4 Objetivos y clasificación de las redes 59
2.4.1 Objetivos 59
2.4.2 Clasificación 61
2.4.2.1 Por la Tecnología de Transmisión 61
2.4.2.1.1 Redes de Difusión 61
2.4.2.1.2 Redes Punto a Punto 62
2.4.2.2 Por la Escala 62
2.4.2.2.1 Redes de Area Local 63
2.4.2.2.2 Redes de Area Metropolitana 63
2.4.2.2.3 Redes de Area Extendida 64
2.4.2.3 Redes Inalámbricas 64
2.5 Protocolos TCP/IP 65
2.5.1 Protocolo de Resolución de Direcciones 68
2.5.2 Protocolo Internet 68

2.5.3 Protocolo de Mensajes de Control de Internet 68
2.5.4 Protocolo de Control de Transmisión 69
2.5.5 Protocolo de Datagrama de Usuario 69
2.5.6 Protocolo Punto a Punto 69
2.5.7 Protocolo Sencillo de Transferencia de Correo 70
2.5.8 Protocolo de Transferencia de Hipertexto 70
2.5.9 Protocolo Sencillo de Administración de Redes 70
2.5.10 Protocolo de Transferencia de Archivos 71
2.6 Comunicación de Datos 71
2.6.1 SMDS 71
2.6.2 X.25 73
2.6.3 Frame Relay 74
2.6.4 ISDN 75
2.6.5 ATM 78
2.6.6 Tecnologías DSL 78
2.6.7 Redes Privadas Virtuales 80
2.7 Computación de Red 81
2.7.1 Primera Etapa 82
2.7.2 Segunda Etapa 82
2.7.3 Tercera Etapa 83
2.8 Redes con Tecnología IP 84
2.8.1 Intranets 85
2.8.2 Extranets 87
2.8.2.1 Beneficios 88
2.8.2.2 Desventajas 90
2.8.2.3 Aplicaciones de la Extranets 91
2.8.2.4 Construcción y Componentes de las Extranets 92
2.8.2.4.1 Construcción 92
2.8..2.4.2 Componentes 92
2.9 Negocio Electrónico y Redes de Información 93
2.9.1 Ventas y Mercadotecnia 93
2.9.2 Desarrollo de Producto 94

2.9.3 Servicios al Cliente 94
2.9.4 Recursos Humanos 95
2.9.5 Financieros 95
Capítulo 3. Transacciones Electrónicas Seguras
3.1 Introducción 96
3.2 Integridad y Seguridad de los Datos 97
3.2.1 Integridad 98
3.2.1.1 Amenazas Humanas 98
3.2.1.2 Errores de Hardware 98
3.2.1.3 Errores de la Red 99
3.2.1.4 Problemas de Tipo Lógico 99
3.2.1.5 Desastres 99
3.2.2 Seguridad 100
3.2.2.1 Amenazas Físicas 100
3.2.2.2 Basadas en los Cables 100
3.2.2.3 Autentificación 101
3.2.2.4 Programación 101
3.2.2.5 Puertas de Escape de los Sistemas 101
3.3 Criptografía 102
3.3.1 Algoritmos y Funciones Criptográficas 104
3.3.1.1 Algoritmo de llave simétrica 104
3.3.1.1.1 DES 104
3.3.1.1.2 IDEA 105
3.3.1.1.3 RC2 105
3.3.1.2 Algoritmo de llave pública 106
3.3.1.2.1 Algoritmo de intercambio de claves Diffie-Hellman 106
3.3.1.2.2 RSA- llave pública/llave privada 107
3.3.1.3 Criptosistemas híbridos 107
3.3.1.4 Funciones de síntesis o compendio de mensajes 107
3.3.2 Ataques contra algoritmos de encriptación y funciones de compendio 109
3.3.2.1 Contra algoritmos simétricos 109

3.3.2.1.1 Ataques de búsqueda de llaves (fuerza bruta) 109
3.3.2.1.2 Criptoanálisis 109
3.3.2.1.3 Ataques basados en el sistema 110
3.3.2.2 Contra algoritmos de llaves públicas 110
3.3.2.2.1 Ataques de factorización 110
3.3.2.2.2 Ataques algoritmicos 110
3.3.2.3 Contra funciones de compendio 110
3.3.3 Firmas digitales 111
3.3.4 Limitaciones de la criptografía 111
3.3.5 Sistemas de encriptación actuales 112
3.3.5.1 PGP 112
3.3.5.2 S/MIME 113
3.3.5.3 SSL 113
3.3.5.4 PCT 114
3.3.5.5 S-HTTP 114
3.3.5.6 SET y CyberCash 114
3.3.5.7 DNSSEC 115
3.3.5.8 IPSEC e IPv6 115
3.3.5.9 Kerberos 116
3.3.5.10 SHH 116
3.4 Identificación y Privacía 118
3.4.1 Identificación 118
3.4.1.1 Identificación mediante posesión 119
3.4.1.2 Identificación mediante características intrínsecas 119
3.4.1.3 Identificación mediante el conocimiento 119
3.4.2 Privacía 120
3.5 Principios y Políticas de Seguridad para Redes 120
3.5.1 Principios de Seguridad 120
3.5.2 Políticas de Seguridad 122
3.6 Capa de Conexiones Seguras 124
3.6.1 Características de SSL versión 3 125
3.6.1.1 Separación de responsabilidades 125

3.6.1.2 Eficiencia 125
3.6.1.3 Autenticación con base en certificados 125
3.6.1.4 Agnóstico en cuanto a protocolos 126
3.6.1.5 Protección contra ataques de hombre en el camino y de reproducción 126
3.6.1.6 Soporte de compresión 126
3.6.1.7 Compatibilidad retrospectiva 127
3.6.2 Funcionamiento de SSL 127
3.6.3 Estándar TSL 128
3.6.4 Desventajas de SSL 130
3.7 Seguridad y TCP/IP 131
3.7.1 Funcionamiento de IPSEC 132
3.7.2 VPN 134
3.8 Cortafuegos o Firewalls 135
3.9 Negocio Electrónico con Seguridad 140
3.10 Certificados y Pagos Digitales 142
3.10.1 Certificados Digitales 142
3.10.2 Pagos Digitales 146
3.11 Leyes y Negocio Electrónico 149
Capítulo 4. Estudio de Redes Privadas para Negocio y Transacciones Electrónicas Seguras.
4.1 Introducción 153
4.2 Caso de Estudio 155
4.3 Transformación hacia Negocio Electrónico 157
4.3.1 Aproximación a la economía digital 157
4.3.2 Diseño General 158
4.3.3 Orientación hacia el Negocio Electrónico 159
4.4 Servicio al Cliente 161
4.5 Descripción de Servicios 163
4.6 Planteamientos Técnicos para el ASP 166
4.6.1 Dispositivos de Red 167
4.6.2 Software 170
4.6.3 Canales de Comunicaciones y Cifrado 171

4.6.3.1 Canal de acceso ASP a ISP 171
4.6.3.2 Canal de acceso cliente a ASP 172
4.6.3.2.1 Canal de acceso cliente a ASP permanente 172
4.6.3.2.2 Canal de acceso cliente a ASP no permanente 172
4.6.3.3 Canal de acceso ASP a medio de pago 172
4.6.3.3.1 Canal directo con el medio de pago 173
4.6.3.3.1 VPN utilizando Internet 173
4.6.4 Protección de información 174
4.6.4.1 Protecciones físicas 174
4.6.4.2 Seguridades de la Información 175
4.6.4.3 Seguridades de cifrado 176
4.6.4.4 Seguridades contra piratas 176
Capítulo 5. Conclusiones y Recomendaciones
5.1 Conclusiones 177
5.1.1 Redes de Telecomunicaciones y Negocio Electrónico 177
5.1.2 Redes Privadas (Extranets) 178
5.1.3 Negocio Electrónico y sus servicios 178
5.1.4 Transacciones Electrónicas y Flujos de Información 179
5.1.5 Negocio Electrónico en el Ecuador 179
5.2 Recomendaciones 191
5.2.1 Por Hacer 181
5.2.2 Formación profesional 181
5.2.3 Proyecciones 182
5.3 Análisis FODA 183
5.3.1 Fortalezas 183
5.3.2 Debilidades 183
5.3.3 Oportunidades 184
5.3.4 Amenazas 184

Glosario de términos 185
Referencias Bibliográficas 202

FIGURAS

Capítulo 1. Comercio Electrónico: Definiciones y Principios

1.1 Categorías y actores del Negocio Electrónico 17
1.2 Crecimiento mundial del comercio electrónico 23
1.3 Pasos para llegar al Negocio Electrónico 25
1.4 Criterios para clasificar a las comunidades de Negocio Electrónico 29
1.5 EBC de Mercado Abierto 30
1.6 EBC Agregada 30
1.7 EBC de Cadena de Valor 31
1.8 EBC de Alianza 31
1.9 Transacciones bancarias minoristas 44

Capítulo 2. Redes Privadas: Tecnologías Inmersas

2.1 Diseño y protocolos de comunicación de la red ARPA 50
2.2 Modelo OSI 55
2.3 Modelo de referencia TCP/IP 58
2.4 Topologías de redes de difusión 61
2.5 Topologías de redes Punto a Punto 62
2.6 Protocolos TCP/IP y el modelo OSI 65
2.7 Clases de direcciones IP 67
2.8 Comparación de interconexión de LAN 71
2.9 Red DQDB 72
2.10 Primera etapa de la computación 82
2.11 Computación cliente/servidor 83
2.12 Modelo cliente/servidor, estructura y operación 83
2.13 Arquitectura de tres capas 84
2.14 Prioridades en Intranets 86

Capítulo 3. Transacciones Electrónicas Seguras

3.1 Amenazas a la integridad y seguridad de los datos 98
3.2 Técnicas de ubicación de firewall 137
3.3 Complejidad en la seguridad del Negocio Electrónico 141
3.4 Estructura esquemática del certificado X.509 típico 145

Capítulo 4. Estudio de Redes Privadas para Negocio y Transacciones Electrónicas Seguras.

4.1 Elementos sistemáticos estructurales 159

4.2 Negocio Electrónico de la empresa caso de estudio 164

4.3 Modelo jerárquico de redes para diseño 169

4.4 Estructura interna del ASP 170

TABLAS

Capítulo 1. Comercio Electrónico: Definiciones y Principios

1.1 Componentes físicos y digitales de los Mercados 5

1.2 Actores y roles en el Negocio Electrónico 15

1.3 Comparación de empresas tradicionales y orientadas al negocio electrónico 20

Capítulo 2. Redes Privadas: Tecnologías Inmersas

2.1 Tipos de servicios 53

2.2 Primitivas de servicio 53

2.3 Redes por su escala 62

2.4 Redes inalámbricas y computación Móvil 65

2.5 Rangos de direcciones IP 67

2.6 Tecnologías de acceso xDSL 79

2.7 Comparación de redes 85

Capítulo 3. Transacciones Electrónicas Seguras

3.1 Mejoramiento de la Integridad de datos 100

3.2 Mejoramiento de la seguridad de los datos 102

3.3 Comparación de sistemas de encriptación disponibles en la actualidad 117

3.4 Comparación de protocolos para VPN 135

3.5 Solicitud SET con firma dual 149

Capítulo 4. Estudio de Redes Privadas para Negocio y Transacciones Electrónicas Seguras.

4.1 Definición del caso de estudio 156

4.2 Recomendaciones generales para iniciar la transición 157

RESUMEN

El presente trabajo trata acerca del Negocio Electrónico en forma general, topando temas puntuales del Comercio Electrónico, como caso particular.

Inicialmente se dio el enfoque de Comercio Electrónico pero con el desarrollo del tema, se consideró que era mejor hablar sobre Negocio Electrónico y como las empresas pueden enfocar sus esfuerzos y hacer la transformación hacia la nueva era economía digital.

Los temas principales del presente trabajo se ven reflejados en cada uno de los capítulos los mismos que son:

- Capítulo I. Comercio Electrónico: Definiciones y Principios

  En este capítulo se trata de enfocar el comercio electrónico con todos los ingredientes que lo componen. Sin embargo, el comercio es un paso dentro de la economía digital, siendo el gran paraguas de la nueva era el Negocio Electrónico, por lo que este capítulo enfoca al Negocio Electrónico, sin dejar de lado las particularidades del comercio digital.

- Capítulo II. Redes Privadas: Tecnologías Inmersas

  Este capítulo hace referencia a todas las tecnologías de comunicación de datos que se usan actualmente, haciendo hincapié en los protocolos TCP/IP como base del intercambio de información. Se presenta la última tecnología de intercambio de información utilizando redes, la cual se llama extranet.

- Capítulo III. Transacciones Electrónicas Seguras.

  En este capítulo se enfocan criterios de cifrado de datos y de seguridad de la información. Así mismo se muestran los principales algoritmos utilizados para encripción de información, protocolos que manejan seguridad y cortafuegos o firewalls para protección contra piratas informáticos.

  Capítulo IV. Estudio de redes privadas para Negocio y Transacciones Electrónicas Seguras.

  Este capítulo presenta un caso particular y las recomendaciones basadas en los capítulos anteriores para poder convertir una empresa en e-business.

PRESENTACIÓN

Debido a que las formas de hacer negocios en todo el mundo están cambiando, Ecuador no puede quedarse atrás.

Los nuevos requerimientos y tendencias orientan tanto a las empresas como a todo el comercio a replantear estrategias y planes para encaminarse dentro de la economía digital. El comercio electrónico como la forma más simple dentro del intercambio electrónico, es la base en la que se fundamenta toda la infraestructura para desarrollar empresas de Negocio Electrónico.

Siendo esta una tendencia tan fuerte, todas la empresas y en general todas las personas se deben preparar de la mejor manera, para poder ser competitivos y lograr mantenerse dentro del mercado, que ahora comprende todo el mundo.

Este trabajo pretende dar a conocer otras alternativas de Negocios Electrónicos que se pueden adaptar a las diferentes necesidades y capacidades de las distintas regiones, sin perder el punto de vista de la globalización. Sin embargo, no representa el final de la investigación, sino más bien el inicio de todo un programa que puede ser la base para la implantación adecuada y coherente de esta actividad en el territorio ecuatoriano.

Queda claro, que el desarrollo del Negocio Electrónico se basa en un adecuado sistema de intercambio de información, con la cual se puede generar conocimiento. La base para este intercambio son las redes de datos, por lo que deben ser diseñadas adecuadamente, cuidando aspectos de seguridad de la información.

Los procesos involucrados dentro del Negocio Electrónico permiten definir los servicios, las tecnologías, los flujos de información y en general el diseño que más se ajuste a cubrir las necesidades que tiene el Negocio Electrónico, de las Tecnologías de Información y viceversa.

El poder agregar valor a las tareas cotidianas que desarrollan las empresas, utilizando la tecnología y basándose en el conocimiento, es el camino por el cual se debe caminar para poder dar el salto y pasar la frontera que divide los negocios tradicionales del e-business.

CAPÍTULO 1.

Comercio Electrónico: Definiciones y Principios

1.1 INTRODUCCIÓN

El Comercio Electrónico en particular y el Negocio Electrónico en general, son actividades que están creciendo en forma acelerada. Estados Unidos, Japón y Europa en general están liderando esta forma de hacer negocios pero no cabe duda tiene un ámbito universal. El impacto que está generando se hace sentir no solo en las empresas sino también en la sociedad en general. Cabe mencionar que las compañías que tomen en serio esta actividad serán las llamadas a tener éxito, para lo cual deben replantear sus planes estratégicos y la forma de acceder a sus clientes, orientando sus mercados y procesos comerciales de manera diferente.

En esta nueva era tecnológica, todas las empresas deben tener claro que solamente reuniendo la capacidad de su personal, es decir, su criterio y experiencia (vivida o aprendida) y los avances tecnológicos se pueden alcanzar estos objetivos con éxito. Este cambio tiene mucho que ver con las nuevas tecnologías de transmisión de datos y en general con lo más avanzado de las Tecnologías de la Información.

El alcance del Negocio Electrónico es tan grande que los ciudadanos normales verán como cambia su vida, en cuanto a los medios que se derivarán de esta actividad y las facilidades con las cuales podrán contar cuando necesiten adquirir bienes y servicios, tomando en cuenta que el factor geográfico no será más una restricción.

Asimismo, las tecnologías de telecomunicaciones y las tecnologías telemáticas que intervienen en el Comercio Electrónico son diversas y depende del tipo de transacciones comerciales que se desee realizar para elegir la más adecuada, esto incluye redes privadas e Internet.

"La computación por redes -la tecnología que define la nueva era económica- continúa transformando los modelos de negocios convencionales y obliga a

las empresas de todas las clases a reencaminar su forma de competir y enviar valor." J. Bruce Harreld. IBM Corporation.

También es muy importante que esta actividad se encuentre regulada por una ley, ya que básicamente las transacciones electrónicas serán financieras.

"El comercio electrónico, a través de redes compartidas, fortalecerá el crecimiento económico a largo plazo, no para todos los participantes sino para aquellos que se concentren en sus habilidades distintivas y respondan al cambio." Dennis H. Jones. Federal Express.

1.2 DEFINICIÓN Y COMPONENTES DEL NEGOCIO ELECTRÓNICO

1.2.1 DEFINICIONES

En principio el Negocio Electrónico o *e-business* (Electronic Business) se establece cuando varias partes interactúan por medios electrónicos para llevar a cabo una transacción comercial, en lugar del contacto físico o directo, incluyendo pagos con dinero electrónico como moneda de cambio. Realmente esta definición no toma en cuenta la esencia de esta actividad, la cual es revolucionar la forma de hacer negocios, tomando como base los avances de la tecnología y el impulso de cambio que estos avances generan.

Debido al fenómeno de la globalización y su influencia, ha surgido una gran competitividad en los mercados mundiales, así como también las exigencias de los consumidores han crecido. Por esta razón las empresas de todo el mundo deben cambiar su organización y sus estrategias, para lo cual se están dejando de lado las barreras que separan al interior de las empresas, a sus divisiones o departamentos y además los muros que estaban entre los proveedores, las empresas y sus clientes. Es claro que para que esto suceda, los planes y procesos comerciales deben replantearse, para hacer posible los cambios necesarios con la visión de globalización.

Los dos frentes que maneja una empresa son las relaciones con los clientes y con sus proveedores (internos o externos), las cuales a través del Negocio Electrónico se hacen más ágiles, flexibles y estrechas, cubriendo las expectativas de la organización.

Un aspecto muy importante de las empresas que incursionan en el Negocio Electrónico es el suministrar información internamente a todos sus empleados, la misma que puede ser presentada utilizando las tecnologías de Web.

Se puede enfocar al Negocio Electrónico desde algunos puntos de vista los mismos que no cubren todo el espectro de acción:

- Desde el punto de vista de bienes, se puede decir que es la cadena de valor de productos a través de redes de telecomunicaciones, es decir producción, promoción, ventas y distribución.
- Desde el punto de vista de servicios, el Negocio Electrónico usa a las transacciones electrónicas para el intercambio de información.
- Desde el punto de vista empresarial, la definición se amplía en el sentido de que se introduce el uso de las tecnologías de la información, para realizar los negocios entre la empresa, compradores, vendedores y socios, orientado a mejorar el servicio a los clientes, reducir los costos y consecuentemente, aumentar los réditos finales.

A continuación se da una definición general que recopila los tres puntos de vista expuestos.

El Negocio Electrónico se basa en las tecnologías de la información orientadas a la compra/venta de bienes, servicios y otras formas de transacciones relacionadas con actividades comerciales de entidades o individuos, a través de redes de telecomunicaciones públicas o privadas, con la posibilidad de intercambiar la información digital necesaria, tal como texto, sonido e imagen, antes de que se cierre la negociación y realizar los pagos en forma electrónica, para poder brindar un servicio eficiente al cliente y aumentar las ganancias de una empresa.

A continuación se enuncian definiciones de organismos involucrados en el Negocio Electrónico:

- "Todas las transacciones de valor que involucren la transferencia de información, productos, servicios o pagos por medio de redes electrónicas" (ITAC, Noviembre 1997)
- "Se refiere generalmente a todas las formas de transacciones relacionadas con las actividades comerciales, incluyendo organizaciones e individuos, que están basadas en el proceso y transmisión de datos digitalizados, incluyendo texto, sonido e imagen" (OECD 1997)
- "Está basado en el proceso y transmisión de datos electrónicos, incluyendo texto, sonido y video. Esto involucra muchas actividades diversas, incluyendo negociación electrónica de bienes y servicios, envío de componentes digitales en línea, transferencia electrónica de fondos, negociación de segmentos electrónicos, conocimientos de embarque electrónicos, acciones comerciales, diseño e ingeniería cooperativa, fuentes en línea, compras, mercadeo directo al consumidor y servicio de posventa. Esto involucra ambos, productos (por ejemplo, artículos de consumo, equipo médico especializado) y servicios (por ejemplo, servicios de información, servicios financieros y legales); actividades tradicionales (por ej.: cuidado de la salud, educación) y nuevas actividades (por ej.: centros comerciales virtuales)" Comisión Europea, 1997.

1.2.2 COMPONENTES DEL NEGOCIO ELECTRÓNICO

Whinston, Stahl y Choi (1997) han conjugado tres aspectos que intervienen en el desarrollo de los negocios: agentes, productos y procesos, los mismos que pueden ser digitales (electrónicos) o manuales (no electrónicos).

La tabla 1.1 da las ocho combinaciones posibles y ubica el campo de acción del tipo de negocio.

AGENTE Compradores Vendedores Intermediarios	PRODUCTO Bienes intercambiados	PROCESO Interacción entre agentes	TIPO DE NEGOCIO Ejemplo
Manual	Manual	Manual	Comercio tradicional
Manual	Manual	Digital	Ventas en línea para productos físicos
Manual	Digital	Manual	Venta de productos digitales en stock
Manual	Digital	Digital	Venta en línea y despacho de productos digitales
Digital	Manual	Manual	Piso de intercambio de bienes
Digital	Digital	Manual	Piso de intercambio de stock
Digital	Manual	Digital	Oferta en línea de productos físicos
Digital	Digital	Digital	Principio de Negocio electrónico: intercambio de productos digitales en una base electrónica con interacciones electrónicas

Tabla 1.1 Componentes físicos y digitales de los Mercados
(Whinston, Stahl y Choi, 1997)

1.3 BASE PARA LAS TRANSACCIONES ELECTRÓNICAS

Para que las transacciones puedan llevarse a cabo, el Negocio Electrónico debe contar con tres niveles los que se basan en la conectividad de redes de telecomunicaciones y su adecuado diseño, los tres niveles son:

- Medios de acceso, que permitan a los participantes interactuar entre sí, así como también a los medios informáticos de cada uno.
- Aplicaciones, las mismas que corresponden a las fases de pedido, orden de compra, negociación y pago electrónicos, con las debidas seguridades en cada una de ellas.
- Servicios de red, referentes a seguridades como por ejemplo: autenticación de usuarios, control de acceso, pagos seguros, encripción de claves y transacciones financieras.

1.4 TRANSACCIONES EN NEGOCIO ELECTRÓNICO

Los expertos comentan que el impacto que generará en la forma de vida de la sociedad el Negocio Electrónico, será comparable al cambio producido por la introducción del teléfono o del automóvil.

El Negocio Electrónico no es un estándar mundial, sino más bien el conjunto de muchas tecnologías que interactúan entre sí para poder generar toda la gama de operaciones y transacciones electrónicas que están inmersas en esta actividad, entre las que se destacan[1]:

- establecimiento del contacto inicial, por ejemplo entre un cliente potencial y un proveedor potencial
- intercambio de información
- soporte pre y posventa (detalles de los productos y servicios disponibles, guía técnica del uso del producto, respuestas a preguntas de adecuación, etc.)
- ventas
- pago electrónico (usando transferencia electrónica de fondos, tarjetas de crédito, cheques electrónicos, caja electrónica)
- distribución, incluyendo tanto gestión de distribución y reparto para productos físicos, como distribución de los productos que puedan ser repartidos electrónicamente
- asociaciones virtuales, grupos de empresas independientes que aúnan sus competencias de manera que puedan ofrecer productos o servicios que van más allá de la capacidad de cada una de ellas individualmente
- Procesos empresariales compartidos que son llevados a cabo y de los que son propietario una empresa y sus socios.

1.5 FUNDAMENTOS DEL NEGOCIO ELECTRÓNICO[2]

Los fundamentos técnicos del Negocio Electrónico son bastos, debido a la gran cantidad de tecnologías que se encuentran inmersas, por lo que los administradores de este servicio necesitan gran cantidad de información para ser eficientes en su labor.

[1] http://www sopde.es/cajon/biblioteca/comercio/ambito.html
[2] http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html

Los autores Kalakota y Whinston en 1996 describen el marco tecnológico para manejar adecuadamente el Negocio Electrónico en su tratado para administradores denominado *Fronteras del Comercio Electrónico*, el mismo que consta en el siguiente listado:

- Marco de trabajo de Comercio Electrónico
- La Infraestructura de Red para Comercio Electrónico
- El Internet como una de las infraestructuras de red
- Seguridad de la red y "firewalls"
- Comercio Electrónico y Red Mundial o Red Privada
- Comercio Electrónico orientado al consumidor
- Sistemas de Pago del Comercio Electrónico
- Comercio interorganizacional y EDI
- Implementación del EDI, MIME y redes de valor agregado
- Comercio Electrónico dentro de la organización
- La Biblioteca Digital Corporativa
- Publicidad y Mercadeo en el Internet
- Búsqueda de Consumidores y Descubrimiento de Recursos
- Educación y Registros Digitales en demanda
- Agentes de software
- La "Suite" de protocolos de Internet
- Multimedia y video digital
- Telecomunicaciones de banda ancha
- Fundamentos de computación móvil y sin cable
- Documentos estructurados
- Arquitectura de documentos activa/componente

En la misma obra los autores enfocan las formas permitidas de Comercio Electrónico en una red de telecomunicaciones, las mismas que son:

- Fabricación de acuerdo a demanda
- Empresas virtuales y basadas en equipos
- Logística
- Videoconferencias en computadora

- Sistemas de flujo de documentos
- Correo electrónico
- Intercambio electrónico de datos

1.6 INFRAESTRUCTURA PARA NEGOCIOS ELECTRÓNICOS[3]

Se debe aclarar que la infraestructura que a continuación se detalla está orientada a negocios B2B (una de las categorías del Negocio Electrónico, punto 1.10 de este capítulo), debido al gran crecimiento que se espera en esta categoría, es la que se analizará en este punto.

Se va a enfocar la infraestructura del punto de vista lógico o aplicacional, más que desde el punto de vista de infraestructura de telecomunicaciones, que será objeto de estudio en capítulos posteriores.

Se listan las aplicaciones básicas que debe considerar tener una empresa para poder desarrollar la actividad de Negocio Electrónico de manera adecuada y para así integrar a sus clientes y a sus proveedores.

Existen algunos modelos que explican la base aplicacional que una empresa debe tener de cara a los Negocios Electrónicos; la que a continuación se detalla se ha obtenido de Jupiter Communications.

Este modelo divide en tres partes a la infraestructura de la empresa:

- proveedores
- al interior de la empresa
- clientes

Cada una de estas partes evidentemente tienen sus bloques funcionales los mismos que se desglosan a continuación.

1.6.1 PROVEEDORES

En esta parte se encuentran todas las aplicaciones de administración de compras, tanto de bienes relacionados con la *cadena de producción* (Supply Chain Management) como de las materias primas, y los no relacionados con la cadena de producción (Maintenance and Repair Ordering) como la papelería. Esta etapa no solamente se refiere a comprar y comparar ofertas

[3] Infraestructura para Comercio B2B, ITD Latinoamérica, Volumen 6-Edicion 1-Febrero 2001

de diferentes empresas y elegir la mejor, sino a todo un proceso en el sentido de estrategias de logística, de inventarios y de la producción en si misma, logrando de esta manera la mayor eficiencia posible para hacer frente a los cambios que el mercado dicte.

1.6.2 AL INTERIOR DE LA EMPRESA

Esta puede llegar a ser la más crítica de todas ya que se debe entender que se trata de rediseñar las estrategias de un negocio tradicional, orientándolo al Negocio Electrónico o arrancar de forma adecuada con un negocio directamente electrónico. Dentro de las aplicaciones al interior de la empresa se encontrará *planeación estratégica de recursos* (Enterprise Resource Planning), *administración del conocimiento* (Knowledge Management), *inteligenciación del negocio* (Business Inteligence), *colaboración* (Collaboration), *minería de datos* (Data Mining). Todas estas aplicaciones deben estar soportadas por una adecuada base de datos (Data Warehouse) que debe contener la información de la empresa, sus proveedores y sus clientes, así como también información respecto a estamentos gubernamentales.

1.6.3 CLIENTES

Para integrar un negocio de Comercio Electrónico Jupiter Communications identifica algunas aplicaciones del lado de los clientes, las mismas que se enfocan a mejorar el servicio y optimizar los recursos de la empresa, las aplicaciones recomendadas son:

- *Exhibición y catálogo* de productos (Storefront and Catalog) que permite interactuar con los clientes de manera de poder atender pedidos e informar sobre los productos que la empresa pone a disposición
- El Marketing permite realizar campañas y analizar resultados, lo que se orienta a dirigir ofertas y adaptar el negocio de acuerdo a los planes estratégicos que emerjan del estudio de mercado
- *Administración de la base de clientes* (Customer Relation Management) para poder brindar un servicio eficiente y sin pérdidas de tiempo, normalmente esta aplicación no se incluye en el diseño inicial de Negocio

Electrónico, ya que también existe fuera de este marco, por lo que se cree que con adaptar la *aplicación de legado* (Legacy System), es decir la heredada del negocio normal, es suficiente, pero es necesario realizar aplicaciones que puedan conjugar los dos mundos.

- Las aplicaciones de *personalización* (Personalization) permiten generar perfiles de usuario y de esta manera volver más ágil el negocio. Apoyada por la *administración de contenido* (Content Management) que permite visualizar desde varias fuentes y organizar toda la información para que los clientes puedan acceder a ella.
- Las aplicaciones de *órdenes de despacho* (Integrated Order Fulfillment) permiten enrutar los pedidos generados por los clientes a los departamentos correspondientes o en su defecto a la empresa encargada.
- Para poder llevar un control del sitio de Comercio Electrónico se utilizan aplicaciones de *control de desempeño* (Site Performance) con las que los clientes pueden expresar su percepción. Los factores que se toman en cuenta son de orden técnico y de orden estético
- Las *aplicaciones de pago electrónico* (Electronic Bill Presentment and Payment), que pueden ser las que decidan el futuro de un negocio, en el sentido de que la empresa que ofrece sus servicios sea confiable o no, cierran el ciclo. Están orientadas a la presentación y pago de facturas electrónicas, las cuales deben ser realizadas con la mayor seguridad ya que aquí se trabajará con tarjetas de crédito, números de cuentas corrientes y en general transacciones financieras de alto riesgo, y que al tratarse de negocios empresa-empresa se muevan grandes cantidades de dinero.

1.7 VENTAJAS DEL NEGOCIO ELECTRÓNICO

La ventaja principal del Negocio Electrónico es que es más rápido, barato y de mayor cobertura que un negocio tradicional. A continuación se describe las razones para hacer esta afirmación.

1.7.1 OFERTA Y DEMANDA

Los límites de un Negocio Electrónico están definidos por el área de cobertura de las redes de comunicaciones en las que operan, por lo que no importa el tamaño físico de las empresas que están en Negocio Electrónico, así como la ubicación de los clientes ya que éstos pueden elegir de diferentes proveedores un determinado producto o servicio, sin importar si se encuentra en su localidad o no.

1.7.2 COMPETITIVIDAD Y SERVICIO

La utilización de un Negocio Electrónico impulsa el incremento de la competitividad entre proveedores debido a que no se encuentran en contacto personal con sus clientes y deben estructurar sus departamentos de atención al público de una manera más eficiente en las etapas de pre y posventa, con un aumento de información, guías de ayuda en línea; de esta manera se ven beneficiados los consumidores al obtener una mejor atención a sus requerimientos.

1.7.3 ATENCIÓN GENERALIZADA Y VENTA PERSONALIZADA

Los proveedores pueden tener la información detallada de los gustos y preferencias de sus clientes ajustando su oferta de productos y servicios, lo que se refleja en productos a medida pero con un precio de mercado masivo.

1.7.4 ENTREGAS Y RESPUESTAS A NECESIDADES MAS RÁPIDAS

Generalmente las empresas que ingresan al comercio electrónico son mayoristas, por lo que el tiempo de entrega se ve reducido, además el costo de entrega es menor debido a que no existe almacenamiento intermedio; éste es un beneficio directo a los compradores en cuanto a precio y tiempo de entrega ya que no está dependiendo del stock de un distribuidor local. Para determinados productos la cadena de distribución se suprime totalmente; ese es el caso de empresas que venden libros, revistas, videos y software.

1.7.5 COSTOS Y PRECIOS MENORES

Este es sin duda el mayor aporte de esta modalidad de comercio. Una transacción comercial normal implica intervención de recurso humano, el cual representa dinero. La misma transacción electrónica, por tener esta característica, es de menor costo. Esto se traduce inmediatamente en reducción de precio para el cliente.

1.7.6 OPORTUNIDADES, PRODUCTOS Y SERVICIOS NUEVOS

Entre los servicios nuevos se puede anotar: información en línea, servicios de redes, contactos iniciales entre clientes y proveedores, etc.

Todo esto necesariamente se ve reflejado en dos aspectos muy importantes tanto para oferentes como para demandantes:

- Aumento de competitividad y calidad de servicios
- Reducción de costos y precios

De lo expuesto en este punto se describe a continuación las ventajas específicas para cada uno de los participantes de esta actividad:

1.7.7 VENTAJAS PARA EL VENDEDOR

- Disminución de costos de operación, debido a que la coordinación interna es menor al tener un solo almacén donde se exhiben sus productos y no necesitar de un equipo de ventas
- La competencia de precios se facilita ya que no existen distribuidores de los productos que se ofrecen
- Los costos para iniciar un negocio virtual son sustancialmente más bajos que en un negocio tradicional
- Los inventarios del negocio son mucho más manejables que mantener un negocio tradicional, debido a que se trabaja sobre pedidos y no se necesita tener un stock permanente
- Se reduce drásticamente la fuerza laboral tanto para ventas como administrativo

Para que las ventajas descritas sean realizables en una empresa que está incursionando en el comercio electrónico se deben tomar en cuenta dos aspectos muy importantes:

- El servicio al cliente es la pieza fundamental del negocio, ya éste se puede transformar en ininterrumpido, se debe contar con ayudas de consultas en línea sin operador, resolución de pedidos, etc.
- Se debe tomar en cuenta la marca y nombre de la empresa así como su imagen, ya que de esto depende el volumen de ventas que la empresa tenga

1.7.8 VENTAJAS PARA EL COMPRADOR

- Fácil y cómodo acceso a la información, sin restricción de horario
- Clasificación de bienes y servicios disponibles
- Menores costos de compra debido a la eliminación de intermediarios
- Características de los bienes y servicios y emisión de proformas
- Personalización del sitio de visita, con el objeto de satisfacer las necesidades del cliente, para cubrir condiciones particulares que hayan sido acordadas con anterioridad

1.8 DESVENTAJAS DEL NEGOCIO ELECTRÓNICO

Como es lógico, los avances tecnológicos también suponen problemas y tienen sus desventajas, y el Negocio Electrónico no puede ser la excepción. A continuación se citan algunas desventajas que pueden potencialmente convertirse en problemas al comparar el comercio tradicional con el electrónico:

- Se debe tener cuidado con la legalidad de las transacciones sin papel, ya que al ser electrónicas no cabe la existencia de documentos físicos
- El no contar con una sola ley de Comercio Electrónico a escala mundial, ya que siendo ésta una actividad global deben cuidar asuntos de impuestos y demás tributos que varíen de un país a otro, así como también la propiedad intelectual

- El control sobre uso indebido de datos personales, contenidos ilegales y publicidad maliciosa y atentatoria contra el ser humano, así como también el fraude
- La poca facilidad de evaluar en el Internet ofertas y de poder comparar la fiabilidad de los proveedores de bienes y servicios electrónicamente
- La falta de seguridad en lo que se refiere a transacciones monetarias y pagos electrónicos
- El no contar con estándares mundiales para normar esta actividad y el número cada vez mayor número de aplicaciones dispersas de comercio electrónico
- La congestión cada vez mayor del Internet y la falta de facilidad para los usuarios de acceder con suficiente capacidad, sobre todo en el caso de países del tercer mundo

Como se ve el Negocio Electrónico tiene componentes legales y también tecnológicos, que se deben pulir cada vez más, para que no se trabaje como hasta hoy, es decir con soluciones a medida que no permiten una interrelación adecuada y ágil entre ellas, haciendo que surjan soluciones adaptables entre sí y que no sean incompatibles a futuro.

Es necesario crear sitios que ofrezcan soluciones especialmente para la mediana y pequeña industria, los cuales estén orientados a procedimientos sencillos y adaptados a sus necesidades, pero que al mismo tiempo sean lo más estándar posible para poder interactuar entre diferentes proveedores de servicios.

Para el caso de los consumidores el riesgo se encuentra en la cantidad de sitios que hacen uso indebido de números de tarjetas de crédito y además de los datos que proporcionan los usuarios para poder hacer sus compras, incurriendo en procedimientos engorrosos para alcanzar cierta seguridad.

La limitación de acceso con capacidad adecuada al Internet, hace que las respuestas de elementos multimedia sean pobres, con la obvia insatisfacción de los clientes, lo que ocasiona que esa tienda virtual sea menos visitada y por lo tanto sus ventas bajen con resultados conocidos. En 1998, un estudio de grupo GVU (Graphics, Visualization, & Usability) del Instituto de Tecnología de Georgia, indicaba que el 65% de las quejas sobre sitios Web

en el Internet se debía a la lentitud en la respuesta cuando el usuario accedía, lo que ocasiona que el 53% de los usuarios abandonen la búsqueda de la información del producto o servicios requeridos. Otro de los problemas mencionados en este mismo estudio era el de los enlaces caídos, es decir cuando un enlace o *link* apunta a páginas inexistentes.

1.9 MODELOS DE NEGOCIO ELECTRÓNICO

Al hablar de modelos de negocios se hace referencia al diseño por medio del cual se mueve un producto o servicio. En la tabla 1.2 se presenta además los elementos que lo conforman y sus funciones, es decir, se describen el origen de los ingresos que sustentan un determinado negocio.

Actores	Roles
Cuerpos Multinacionales	Fomentar la Sociedad de la Información
	Eliminar barreras globales
Gobiernos Nacionales	Asegurar el campo de actuación
	Eliminar barreras nacionales
Sectores Representativos	Promocionar la difusión y la adopción
	Proporcionar tecnologías disponibles
Suministradores de Tecnología	Reorganizar los negocios
	Adoptar las tecnologías
Empresas	Aprovechar las oportunidades
Consumidores	

Tabla 1.2 Actores y roles en el Negocio Electrónico[4]

Para el caso del Negocio Electrónico se manejan dos grupos:

- Modelos transplantados
- Modelos nativos

[4] http://www.sopde.es/cajon/biblioteca/comercio/actores.html

1.9.1 MODELOS TRANSPLANTADOS

Son aquellos que siendo tradicionales han sido modificados para poder soportar transacciones electrónicas. Como ejemplos se pueden citar:

- Librerías que se basaban en venta por catálogo y correo tradicional
- Sistemas de publicidad, los mismos que son pagados por terceros y donde el atractivo es proporcional al éxito
- Negocios en los cuales se da mayor atención a los servicios alrededor de un producto que el producto mismo
- Mercadeo directo: envío masivo de publicidad informativa, envío de información personalizada con consentimiento del usuario

El cambio del modelo transplantado no solamente supone un cambio de tecnología sino también cambios profundos en la organización misma, que si no son manejados adecuadamente pueden llevar al fracaso por el riesgo que implica. Por otra parte, el cambio también puede suponer el innovar en nuevas líneas de servicios y servicio al cliente.

1.9.2 MODELOS NATIVOS

Estos negocios han surgido dentro de las tecnologías de Internet, sin las cuales sería muy difícil desarrollarlos. Citando algunos ejemplos de este modelo se tienen:

- *Internet Service Providers* ISP (proveedores de acceso a Internet) y proveedores de comercio; entre los servicios que brindan están el web hosting, e-mail, salida al Internet, transacciones seguras. Estos servicios se basan en conexión, procesamiento y transacciones.
- Subastas en el Web, facilitando la interacción entre clientes con diferentes ofertas, siguiendo reglas muy claras en el sitio para la ejecución de la subasta y el cierre de la compra. Estas subastas pueden ser públicas (Internet) o no (redes privadas). Otra modalidad es aquella en la que el sistema guarda los datos para su procesamiento y no permite ver a los participantes sino cuando ya se tiene un resultado para cerrar el proceso de compra/venta.
- En la categoría de negocio empresa-empresa están apareciendo las redes privadas destinadas a agrupar proveedores, empresas y clientes

para realizar transacciones tales como proformas, pedidos, compras, ventas de productos o servicios que tengan relación con grupos afines de empresas.

- Repositorios de información que son aquellos sitios que se dedican a capturar información, procesarla y venderla a terceros. Están destinados a relacionar a compradores y vendedores en áreas específicas y procesar esa información para toma de decisiones en compras futuras.

1.10 CATEGORÍAS DEL NEGOCIO ELECTRÓNICO

Para poder categorizar de manera adecuada al Negocio Electrónico se debe tomar en cuenta los participantes en el mismo. Esta categorización se la hace sin importar si el negocio se lo desarrolla en Internet o en una red privada.
Se tiene cuatro tipos de negocios, de los cuales los más desarrollados son los dos primeros de la lista:

- Negocio empresa-consumidor (B2C-Business to Consumer)
- Negocio empresa-empresa (B2B-Business to Business)
- Negocio empresa-administración
- Negocio consumidor-administración

En la figura 1.1 se ilustran las categorías del Comercio Electrónico.

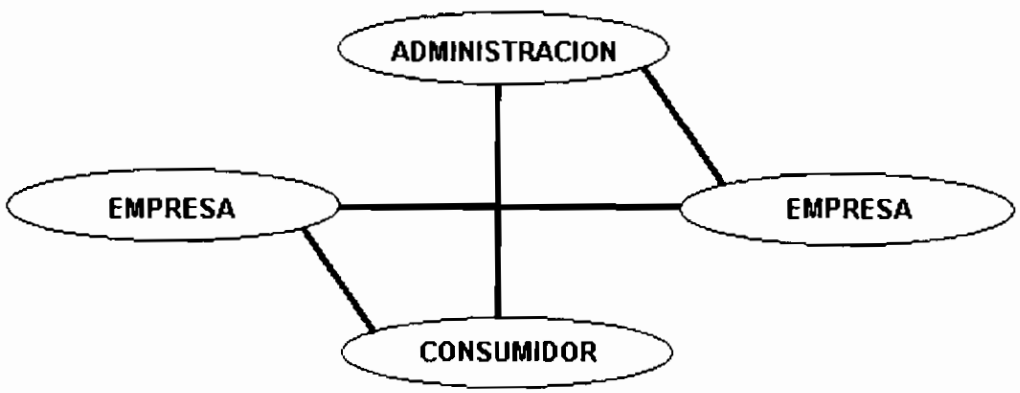


Figura 1.1 Categorías y actores del Negocio Electrónico[5]

[5] http://www.internautas.org/documentos/pista.htm

1.10.1 NEGOCIO EMPRESA-CONSUMIDOR

Es lo mismo que la venta electrónica, la cual se ha visto expandida con la popularización del Word Wide Web, lo que ha permitido la existencia de galerías virtuales comerciales en el Internet, las mismas que ofrecen todo tipo de productos de consumo como flores, dulces, computadoras, automóviles, etc.

1.10.2 NEGOCIO EMPRESA-EMPRESA

Se describe esta categoría con una empresa que hace los pedidos a sus proveedores y al mismo tiempo vende a sus clientes, haciendo y recibiendo los pagos, todo esto en forma electrónica.

Esta categoría se ha establecido hace varios años, utilizando en principio el intercambio electrónico de datos EDI (Electronic Data Interchange), sobre redes privadas o de valor agregado.

1.10.3 NEGOCIO EMPRESA-ADMINISTRACIÓN

Esta categoría abarca todas las transacciones que deben hacer las empresas con los estamentos gubernamentales. En otros países las disposiciones del gobierno son publicadas en el Internet, así como los formularios de declaración y pago de impuestos y demás deberes para con el estado, los mismos que las empresas pueden llenar y enviar en forma electrónica.

Esta categoría se está implementando, y su potencial de crecimiento es grande, si los gobiernos usan la tecnología para agilitar, dar valor agregado a sus transacciones y brindar un servicio de calidad.

1.10.4 NEGOCIO CONSUMIDOR-ADMINISTRACIÓN

Se trata de la categoría menos desarrollada del Negocio Electrónico, en la que se tiene la combinación del negocio empresa consumidor y de empresa administración. Para que esta categoría surja los gobiernos deben extender los servicios e interacciones electrónicas como pago de impuestos individuales, pensiones, etc. Además la penetración del Internet, en los hogares de todo el mundo, debe ser mayor.

1.11 SISTEMA DE NEGOCIO ELECTRÓNICO

Los sistemas normales de negocios resultan ser ineficientes frente a las alternativas electrónicas que existen hoy en día, en el sentido de que toman mucho tiempo y gasto de recursos. Por ejemplo, cuando se realiza una venta de un bien o servicio:

- se emite una factura por la venta
- la factura debe ser enviada al cliente
- en el departamento financiero del cliente debe ingresar la factura recibida a cuentas por pagar
- emitir un cheque o disponer el giro bancario a nombre del proveedor del bien o servicio
- dar conocimiento por parte del cliente al proveedor que la deuda correspondiente a tal factura ha sido cancelada, de lo contrario hacer el seguimiento por parte del proveedor si la factura enviada ha sido cancelada o no
- ingresar a las contabilidades de las dos empresas involucradas en la compra/venta del bien o servicio

Todo este proceso implica papeleo y que los papeles pasen de una persona a otra, con el bien conocido problema de pérdidas que esto puede ocasionar.

El mismo proceso dentro del Negocio Electrónico es bastante más eficiente y rápido, sin la posibilidad de errores, solamente los que se podrían generar de una mala programación del sistema que controla el negocio electrónico (para lo cual se hacen pruebas de control de calidad antes de salir con un servicio). Además, la idea de mejorar el servicio al cliente y proporcionar seguridad, agilidad y la posibilidad de interactuar en línea son los objetivos y beneficios del Negocio Electrónico.

Los servicios que se ofrecen en este campo para agilitar el proceso de compra/venta y pago, todo esto en línea, son:

- catálogo de productos y precios e inventario en formato web
- accesibilidad por parte del cliente para realizar pedidos electrónicos
- emisión de facturas electrónicas

- emisión de créditos/débitos bancarios, los que afectarán las cuentas del proveedor y cliente respectivamente
- servidores de autorización para pago con tarjeta de crédito
- emisión de guías en las empresas que transportan mercadería, en forma nacional o internacional, en forma electrónica (no se necesita de personas que llenen guías de remisión)

Todos estos servicios deben tener el respaldo de poder ser verificados por las partes en cualquier momento, pero solamente por los interesados más no por cualquier persona, lo que implicará que no se pueden hacer cambios a los datos de órdenes de pedido y/o facturas. Esto da como resultado un sistema de alta seguridad.

A continuación se comparan los dos tipos de empresas a las que se ha hecho mención, una tradicional y otra orientada al negocio electrónico. La "nueva" empresa difiere de la "antigua" en la forma de ver sus clientes y en el servicio de valor que les brinda.

La tabla 1.3 muestra las diferencias entre los dos tipos de empresas, que básicamente se puede resumir en los objetivos y prioridades que se da a cada una de ellas, además a las virtudes que presenta una empresa tradicional se añaden las habilidades adquiridas en el negocio electrónico.

	EMPRESA TRADICIONAL	**EMPRESA ORIENTADA AL NEGOCIO ELECTRÓNICO**
Prioridades organizacionales	Mantener múltiples divisiones o unidades operativas.	Establecer nuevas comunidades complementarias, es decir, nuevos entornos de negocio.

Tabla 1.3 Comparación de empresas tradicionales y orientadas al negocio electrónico[6]

[6] "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economía Digital", Don Tapscott, McGraw Hill, 1999, pag. 85-86

	EMPRESA TRADICIONAL	EMPRESA ORIENTADA AL NEGOCIO ELECTRONICO
Prioridades del mercado	Conservar la partición en los segmentos de mercados existentes.	Crear y establecer nuevos mercados.
Definición de liderazgo	Triunfar sobre los competidores directos.	Liderar la coevolución de jugadores importantes.
Relación con los mercados y las compañías no básicas del *espacio en blanco*[7]	No ver los aspectos ni las oportunidades el *espacio en blanco*.	Enfocarse en los aspectos y oportunidades del *espacio en blanco*.
Método para la selección y segmentación del cliente, desarrollo del mercado, inversiones en proceso y tecnología, relaciones organizacionales, grupos de interés externo y financiación, y relaciones con el gobierno.	Aislarse en silos funcionales, sin poder para integrar la acción.	Integrarse alrededor de las oportunidades de mercado y la creación de entornos, con poder para la acción.
Política de operación financiera	Se espera que cada unidad de negocios produzca retornos en el mercado.	Puede optimizar los rendimientos totales de la compañía a partir del entorno, aunque esto implique tomar rendimientos de una unidad e invertir en otra.
Tipos de recursos que se consideran básicos para formular la estrategia.	Principalmente aquellos recursos que existen dentro de la empresa u organización bajo el control directo de la persona que formula la estrategia.	Todos los recursos que pueden dirigir el mercado y el entorno, especialmente los controlados por otros poderosos participantes.

Tabla 1.3 Comparación de empresas tradicionales y orientadas al negocio electrónico (continuación)

[7] Don Tapscott, McGraw Hill, 1999, pag 79 "Espacio en blanco" es la porción de negocio que surge entre los mercados existentes y las operaciones de la compañía

	EMPRESA TRADICIONAL	EMPRESA ORIENTADA AL NEGOCIO ELECTRONICO
Grado de control asumido por los gerentes	Control directo de las actividades del negocio y de las prioridades de inversión.	Influencia indirecta sobre actividades de negocios y prioridades de inversión.
Campo de acción de las actividades	Múltiples segmentos de mercado existentes, dirigidos por compañías con operaciones múltiples y activos.	Múltiples espacios de mercado, al igual que segmentos de mercado, atendidas por entornos con distintos niveles de madurez, con diversos temas y desafíos.
Promoción, marcas y relaciones públicas.	Busca captar la imaginación tradicional del cliente, a través de actividades de promoción convencionales centradas alrededor de los productos o la imagen de la empresa.	Capta la imaginación de los contribuyentes potenciales y existentes en el entorno, sabe que la percepción ayuda a crear realidad, moviliza "enjambres".

Tabla 1.3 Comparación de empresas tradicionales
y orientadas al negocio electrónico (continuación)

1.12 PROYECCIÓN DEL NEGOCIO ELECTRÓNICO EN EL MUNDO

Según estudios del Organización para la Cooperación y el Desarrollo Económico OECD (Organisation for Economic Cooperation and Development), el movimiento del comercio electrónico ha sufrido un incremento muy grande desde casi cero a $25.000 millones, entre 1995 y 1997. Se estima que para los años 2001 y 2002 esta cifra aumentará a $300.000 millones y para el 2005 se colocará en $1´000.000 millones. De estas cantidades la categoría de Negocio Electrónico empresa-empresa cubre el 80% como lo muestra la figura 1.2[8].

[8] http://www internautas.org/documentos/pista.htm

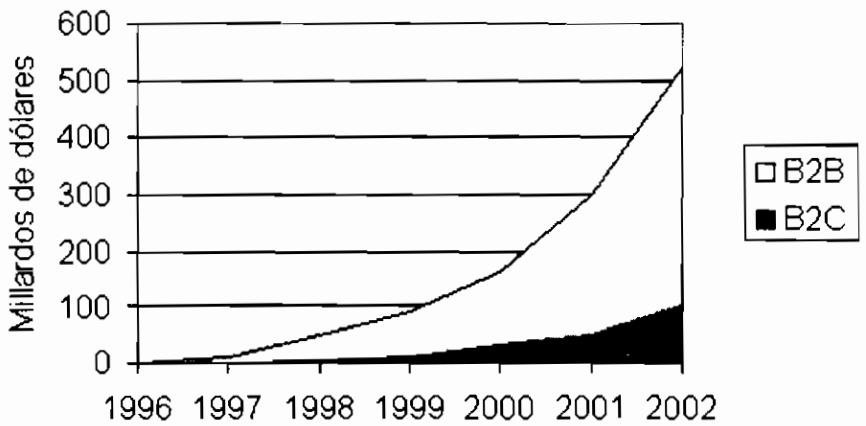


Figura 1.2 Crecimiento mundial del comercio electrónico

Otros estudios afirman que el crecimiento y proyección del comercio electrónico en los siguientes años serán mayores, por ejemplo IDC (International Data Corporation) indica que en el año 2000 se llegó a cursar en comercio electrónico $272.000 millones de dólares y proyecta para el 2004 unos $2´600.000 millones, de los cuales, ellos estiman, 2.2 billones serán generados por transacciones entre empresas.

Otros estudios y proyecciones son mucho más alentadores, según Giga Information Group, el segmento B2B arrojará en el 2004, $5´200.000 de ventas, realizando a través de EDI, combinaciones de EDI y redes de comercio electrónico, alianzas estratégicas en Internet y mercados electrónicos privados. Sin embargo, la necesidad de varias interacciones electrónicas que implican fiabilidad, seguridad y costo, puede afectar a este mercado. La solución a este inconveniente es adaptar el canal de comunicaciones adecuado de cara con cada cliente o grupo de éstos, es así como se cuenta con algunas alternativas, como son redes privadas para grandes empresas y para relaciones estratégicas o bien EDI adaptado para Internet en las medianas y pequeñas empresas o cuando la relación no sea de estrategia alta.

1.13 ÁMBITO E INTERGACIÓN DEL NEGOCIO ELECTRÓNICO

1.13.1 ÁMBITO DEL NEGOCIO ELECTRÓNICO

El Negocio Electrónico, contrariamente a lo que se pueda pensar, no solamente tienen que ver con actividades de compra y de venta utilizando medios telemáticos, sino también las transacciones de pre y posventa utilizando las mismas facilidades tecnológicas. Estas otras actividades son:

- publicidad y promoción
- información de productos, búsqueda en catálogos
- negociación de precios y condiciones de pago entre compradores y vendedores
- atención a clientes
- trámites administrativos al realizarse la transacción electrónica
- colaboración entre empresas afines a corto o largo plazo
- créditos y débitos monetarios en forma electrónica
- compensación electrónica de cuentas

Cabe mencionar que estas transacciones no necesariamente se presentan todas al mismo tiempo, y algunas no están siempre presentes en transacciones financieras de Negocio Electrónico. A continuación se muestra un posible camino para llegar a una transacción completa, es decir que incluya todas las transacciones anotadas. La figura 1.3 nos indica una implantación gradual del Negocio Electrónico.

Toda la información que generan ciertas actividades al interior de una empresa puede ser tomada desde los tres puntos de vista siguientes:

- información
- privacidad de la información
- compartición de la información

Figura 1.3 Pasos para llegar al Negocio Electrónico

Estos tres enfoques son tomados dentro del principio de que se debe entregar en tiempo real la información a los individuos que la necesitan, cuando la necesiten, como ellos la necesiten y de acuerdo a las circunstancias del momento. (Avaya Inc. IW-EBS 1034, 2000)

El Negocio Electrónico usa esa información apoyándose en el hecho de que las telecomunicaciones permiten el intercambio de la misma en forma instantánea, este intercambio se conoce como *flujo de información*.

La optimización y máxima eficiencia de una empresa comienza cuando se logra que el principio antes mencionado se cumpla, para lo cual se utilizan los flujos de información. Debe estar claro que para esta tecnología las personas deben estar suficientemente preparadas y dispuestas a darle uso, de lo contrario todo el planteamiento no tendrá ningún sentido.

Las nuevas metas del negocio deben tomar en cuenta que la tecnología y el Negocio Electrónico permiten que se tenga mayor presencia, que se amplíe el mercado, que se aumente el número de proveedores, que se deban hacer alianzas estratégicas, y que se cuente con la opción de tercerizar, brindar o contratar, este servicio (Outsourcing).

Otra forma de ver la figura 1.3 desde el punto de vista de flujos de información es introducir el Negocio Electrónico en tres etapas:

- "oficinas cero papel"
- adecuado diseño o rediseño de flujos de información
- uso de los flujos de información en forma dinámica

La sustitución de los sistemas basados en papel, tanto dentro de una empresa, como entre ellas, produce pocos beneficios reales. Es cierto que reduce los costos administrativos y mejora el nivel de precisión en el intercambio de datos, pero no aborda las cuestiones relacionadas a que las actividades comerciales se hagan eficientemente a la primera. Las aplicaciones del Negocio Electrónico ayudan a reformar las maneras de realizar las actividades comerciales, y con frecuencia, actúan como un catalizador para que las empresas utilicen la reingeniería de procesos empresariales (BPR, Bussines Process Reengineering. Year-X Ltd, 1996).

1.13.2 INTEGRACIÓN DEL NEGOCIO ELECTRÓNICO

Todas las empresas dentro del mercado están en posibilidades de ofrecer sus servicios a través del comercio electrónico, pero está claro que las que tienen mayores oportunidades son las más grandes, debido especialmente a situaciones de presupuesto y a aspectos técnicos.

Entre los aspectos técnicos se destacan la integración de aplicaciones, la seguridad, y la administración. Siendo la primera la más crítica, debido a la existencia previa de sistemas de administración, contabilidad, inventarios y atención a cliente, todos estos conocidos normalmente como procesos internos (Back Office).

La integración debe tomar dos puntos de vista: a) conocer las aplicaciones ofrecidas por varios proveedores de tecnología, estudiarlos y armar una solución con los mejores módulos de las aplicaciones; o, b) trabajar basándose en una aplicación global que enmarque todas las aplicaciones necesarias.

Cualquiera de los dos caminos tiene un alto costo, debido a lo cual muchas empresas están tercerizando (Outsourcing) este proceso. Al realizar el outsourcing se puede contar con soluciones ajustadas a las necesidades puntuales de cada empresa, en cuanto a presupuesto e implementación adecuada y fácil, debido a que ahora es posible tener la parte de Negocio

Electrónico fuera de la empresa, utilizando los servicios de hosting que ofrecen muchas compañías hoy en día. Sin embargo, como es lógico las aplicaciones de back office están al interior de la empresa, por lo que es importante contar con un canal de comunicaciones de alta seguridad, entre el sitio del hosting y la empresa, creando de esta manera redes privadas para realizar transacciones electrónicas igualmente seguras.

1.14 COMUNIDADES DE NEGOCIO ELECTRÓNICO EBC[9]

Para poder alcanzar las expectativas de la organización en cuanto al Negocio Electrónico, su infraestructura y todas las ventajas que éste ofrece, es necesario trabajar en unión a los clientes y proveedores. Necesariamente esta unión se basa en redes telemáticas, a las cuales se añadirán innovaciones tecnológicas, dando como resultado un valor agregado al simple intercambio de información.

A este conjunto formado por las redes de telecomunicaciones entre la empresa, sus clientes y sus proveedores, con el valor agregado que se ha mencionado, se lo conoce como *Comunidad de Negocios Electrónicos* EBC (e-business community). Este concepto según Alliance for Converging Technologies, extiende y amplía el alcance de comercio electrónico.

"Las EBC son redes de abastecedores, distribuidores, proveedores comerciales y clientes que utilizan Internet y otros medios de comunicaciones electrónicas como plataformas de colaboración y competencia" David Ticoll y Alex Lowy, Alliance for Converging Technologies.

Toda esta nueva forma de hacer negocio está desarrollando nuevas estrategias e incluso reglas de competencia que favorecen a todas las partes que intervienen en una EBC, dando como resultado relaciones a largo plazo bajo el esquema de *ganar-ganar*, es decir que el beneficio se da tanto para los clientes, empresa y proveedores.

En la actualidad la competencia entre empresas en el Negocio Electrónico se enfoca desde el punto de vista de que es mejor integrar una EBC con empresas que han sido competencia en la industria tradicional, que enfrentar

[9] "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economía Digital", Don Tapscott, McGraw Hill, 1999, pag.19 a 32.

aislados el mercado, tomado en cuanta además que no basta solamente vender masivamente bienes y servicios, sino que además es necesario dar un valor adicional que sea significativo.

Como en todo cambio o revolución, existen fuerzas o corrientes que rigen la nueva forma de hacer negocios[10], cada una es poderosa pero conjuntamente son una herramienta con la cual se puede trasformar destruir una empresa:

- *Redefinición del valor.* La generación de utilidades, las telecomunicaciones, el comercio y la distribución se han unido, dejando si bases a la industria que definía sus estrategias tomando en cuenta las fronteras. Esta transformación genera la necesidad de buscar, lo que puede ser la esencia del Negocio Electrónico, la creación de valor como ingrediente principal de sus operaciones.
- *Las economías del conocimiento digital.* Son fundamentalmente diferentes y están pobremente entendidas, tomando en cuenta que la base para una implantación adecuada en el Negocio Electrónico es el compartir el conocimiento, tomando como definición de conocimiento que es la información analizada profundamente y puesta dentro del contexto, lo cual implica que es valiosa para la organización. Todo lo que se origine a través del conocimiento aumentará el rendimiento de la empresa y mientras más se lo utilice, incrementará el valor agregado, lo que indica que las empresas que ingresaron en sus inicios a la economía digital tienen una ventaja competitiva, del mismo modo que la tuvieron las empresas pioneras en la era industrial.
- *Ritmo de crecimiento.* El vertiginoso cambio de la tecnología marca el paso para los nuevos negocios, por lo que los mandos medios y altos de las empresas deben adaptarse rápidamente a la innovación y dinamismo de la industria de las tecnologías de información, para poder convertir este punto en otra ventaja que puedan ofrecer en el mercado.
- *Eliminar la intermediación.* Cuando se realizan negocios en forma electrónica se eliminan las fricciones en las transacciones en el sentido de reducción de costos, tiempos de entrega y errores. Al mismo tiempo los

[10] "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economía Digital", Don Tapscott, McGraw Hill, 1999, pag. 20-21

clientes tienen acceso a información, la cual al ser realimentada al negocio, aumenta el valor a todo el proceso.

- *La era digital en los negocios*. Los avances digitales de los últimos tiempos han originado que la concepción tradicional de un negocio vertical u horizontal sea desechada. La información no es solamente para ser manejada dentro de un departamento en una empresa sino que al ser capital de todos genera riqueza y al mismo tiempo agrega valor a un producto o servicio, por medio de la innovación, ampliación y adaptación en su ciclo de producción.

1.14.1 TIPOS DE EBC

De un estudio realizado por Alliance for Converging Technologies sobre 170 EBC, se desprende que existen algunos tipos básicos, los mismos que se clasifican según la figura 1.4, tomado en cuenta dos ejes fundamentales:

- Control económico: este eje se mueve desde el control jerárquico hasta empresas que son auto-organizables, desde líderes que manejan las estrategias del negocio, hasta democracias estructuradas con liderazgo distribuido para manejo de las reglas del negocio.
- Integración de valor: dependiendo del tipo de negocio se ofrecen productos o servicios originados desde varios puntos, de lo contrario se tiene una oferta simple.

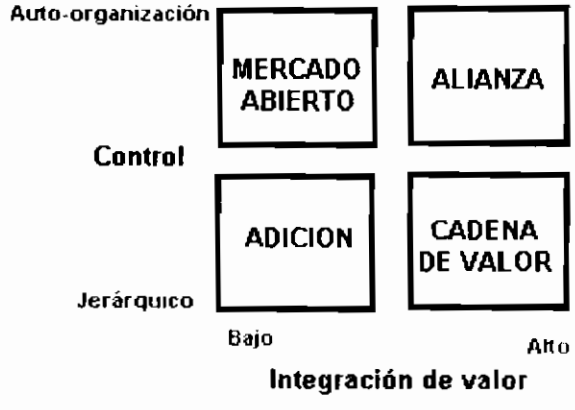


Figura 1.4 Criterios para clasificar a las comunidades de Negocio Electrónico

En la realidad ninguna EBC es *pura*, sino más bien mezclan características de cada una de las cuatro, pero básicamente cada comunidad tiene un principio que se lo puede clasificar utilizando los criterios mencionados.

- EBC de Mercado Abierto: en esta comunidad cualquier participante puede ser comprador o vendedor, es comparable a la bolsa de valores. No existe integración de valor en gran medida y ninguno de los participantes tiene el control absoluto. En definitiva el negocio se rige por estar en el lugar correcto con la solución adecuada y a un precio razonable. La figura 1.5 muestra este tipo de EBC.

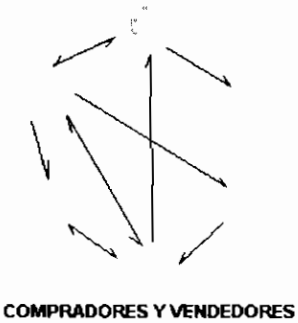


Figura 1.5 EBC de Mercado Abierto

- EBC Agregada: existe una empresa que se maneja como intermediaria entre los productores y los clientes. Al utilizar las tecnologías disponibles para manejar y controlar la cadena de suministros, se logra mayor eficiencia y efectividad en cuanto a costos. Al igual que la anterior no se tienen una mayor agregación de valor. La figura 1.6 muestra una EBC agregada.

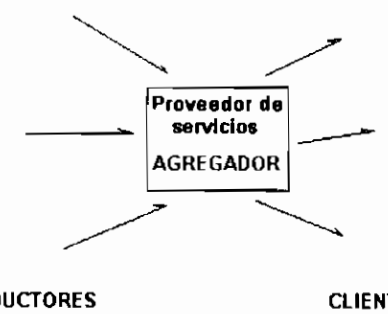


Figura 1.6 EBC Agregada

- EBC de Cadena de Valor: es similar a la agregada, pero ahora su punto principal es la optimización de procesos con la efectividad operacional, maximizando la integración de valor. La figura 1.7 muestra una EBC de cadena de valor.

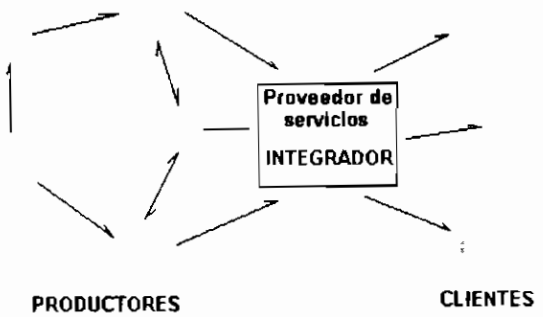


Figura 1.7 EBC de Cadena de Valor

- EBC de Alianza: la integración de valor en esta EBC es alta ya que no hay un control jerárquico, contando con uno o más líderes. Está orientada a satisfacer los requerimientos específicos del cliente, contando con amplias soluciones, las que pueden ser integradas fácilmente. La figura 1.8 muestra una EBC de alianza.

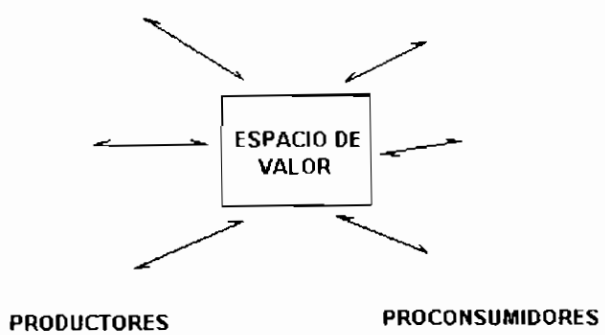


Figura 1.8 EBC de Alianza

1.14.2 IMPLEMENTACIÓN DE EBC

Como es de suponer la creación de EBC no se parece en nada a la creación de negocios tradicionales, al igual que liderar un grupo de este tipo no tiene nada que ver con gerenciar una empresa *privada* ya que todos dentro de la

comunidad son responsables por igual, además el hecho de no contar con intereses convergentes es un aspecto fundamental para el entorno. Dentro de las prácticas usuales dentro de la comunidad están: alta colaboración, respeto mutuo, confianza, intercambio de información, uso de marcas conjuntas, lo que hace que las EBC sean en realidad muy humanas.

Las comunidades al ser una recopilación de varias empresas deben tener normas claras, bien difundidas y suficientemente entendidas, estas reglas son tanto para el manejo del negocio como para emitir las estrategias del mismo.

Dentro de las áreas estratégicas de las EBC están:

- estandarizar sus productos o servicios dentro del mercado, para poder penetrar dentro del mismo
- dictar normas para que sus socios de negocios se encuentren motivados y atraídos y de esta manera conservarlos
- moverse dentro de un perfil del mercado y mantener su marca
- dictar normas que conduzcan a la efectividad y eficiencia en el servicio al cliente y en general en todos los proceso que tengan que ver con el producto o servicio
- manejar adecuadamente el conocimiento, crearlo y mostrarlo

Para crear un ambiente favorable dentro de una EBC una vez definidos los campos estratégicos, deben dictarse reglas de acuerdo a los objetivos que persiguen los directivos de la comunidad. En principio tales reglas pueden ser autocráticas, altamente participativas, pero la tendencia es encontrar un punto medio. Antes de formular cada regla se debe reflexionar en cada uno de los siguientes puntos:

- debe existir un grupo de participantes par cada regla (clientes, socios, canales, proveedores)
- controles internos compartidos para lograr transacciones activas y con suficiente información
- procedimiento para formulación de más reglas, sin caer en burocracias innecesarias

Una vez que se han emitido las reglas, debe existir un método para verificar su cumplimiento para lo cual se deben fijar parámetros, los mismos que son:

- obligatoriedad de cumplimiento de las normas
- motivaciones para el cumplimiento y sanciones por incumplimientos
- procedimientos formales o no para verificar el cumplimiento de las normas
- implicaciones competitivas de la emisión de las normas
- asuntos jurídicos de las normas

1.15 DISEÑO DE UN NEGOCIO ELECTRÓNICO

"A largo plazo, tener más capital que capacidad para usarlo realmente entorpecerá la construcción de una empresa sostenible y resistente." Paul Woolner, Alliance for Converging Technologies.

El principio por el que se rigen los negocios electrónicos o empresas con esta tendencia, es llevar con suficiente velocidad al mercado nuevos productos o servicios, desarrollando otras estrategias de ventas, de mercadeo y de servicio al cliente.

Cabe mencionar que pese al nuevo enfoque, las empresas no son capaces de crecer con un modelo libre de formato organizacional, por el contrario deben desarrollar un diseño algo más formal que contenga la esencia del espíritu y el éxito empresarial y que pueda respaldar un crecimiento sostenido.

Para desarrollar un negocio electrónico, la empresa debe pasar de una etapa de formación a una etapa de desarrollo organizacional. Sin embargo existen tres factores que afectan dicha transición:

- La ventaja competitiva sobre la base del conocimiento
- La agilidad organizacional
- La velocidad de cambio

Otra inquietud que se formulan los gerentes de las empresas es que *cual es el momento más adecuado para practicar el cambio*. Una transición muy temprana no es aconsejable ya que la atención se puede diluir entre el desarrollo del producto y otras actividades que generen ingresos; por otra

parte la transición tardía puede provocar que el desempeño sea bajo debido a que la organización no es efectiva.

Asimismo el cruce parcial es desastroso, debido a que los empleados de la empresa no tienen claro las reglas de la organización, lo que ocasiona que se pierda tiempo y además de la ventaja inicial, ya que como se ha dicho el nuevo mercado electrónico cambia y evoluciona de una manera muy rápida.

A continuación constan 7 puntos en los que Paul Woolner[11] se basa para poder establecer estrategias de la nueva empresa digital, asimismo da parámetros para futuras transiciones, en conjunto lo siete puntos crean las condiciones necesarias para la transición a la era digital:

Empresa dirigida por la visión y basada en el valor

Tomando en cuenta que lo único cierto en la era digital es el cambio, la visión y el valor son los argumentos para dar dirección a una empresa.

Elaboración rápida de un prototipo de organización

Tomando como base la tecnología, las empresas deben ser capaces de ir a nuevos y más grandes mercados, para lo cual la capacidad de elaborar prototipos adecuados promete un alto crecimiento, de lo contrario, la empresa no podrá cubrir demandas de desempeño, personal, liderazgo, experiencia, y gerencia. Los responsables de la organización, no deben pensar que una organización fuerte, puede hacer frente a la nueva ola, sino más bien que el cambio continuo es una norma, por lo que organizaciones demasiado rígidas, no pueden responder adecuadamente, esta capacidad de cambio debe verse reflejada en el personal que trabaja en la empresa, el mismo que debe convivir con responsabilidades cambiantes.

Sistemas organizacionales estructurados

Para la elaboración del prototipo se debe tener claro el marco de referencia del sistema de una organización. Este marco debe permitir que los sistemas o elementos centrales de la organización, se sitúen adecuadamente con respecto a la visión, a ellos en sí y con el ambiente externo.

[11] "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economía Digital". Don Tapscott. McGraw Hill. 1999. pag 101-109.

Según Paul Woolner, "el éxito está en establecer el modelo de los sistemas (estrategias, programas y herramientas) de la empresa y el objetivo estratégico de cada uno de ellos", dependiendo de las prioridades y necesidades del negocio. Se conoce que los sistemas estructurados arrojan una cultura organizacional fuerte y resistente, lo que permite proyectar la empresa a un mayor tamaño, sin que su personal pierda la perspectiva de la organización.

Conocimiento, información e infraestructura tecnológica

Como se ha mencionado anteriormente el conocimiento es la base de una empresa en la era digital, por lo que una de las principales estrategias de una organización es incluir el aprendizaje y el conocimiento, tanto su creación como su diseminación. La empresa digital debe estar orientada a optimizar los niveles de conocimiento y aprendizaje, debido a lo vertiginoso de los cambios que la tecnología produce. La implementación de redes (intranets, extranets) para intercambio de conocimiento es fundamental para poder realizar la transición desde la formación al desarrollo de la organización, la tecnología funciona como facilitadora de la transición.

Mapa extendido de la empresa

Se debe tener claro los alcances de las relaciones con socios de negocios así como también las responsabilidades al interior de la empresa. La estrategia de la comunidad da en gran medida la estrategia de la empresa, y esta última debe decidir el grado de colaboración externa, así como el grado de agregación de valor interna. Todo esto debe verse reflejado en el mapa de las relaciones al interior de la comunidad.

Liderazgo de profesionales reflexivos

Según Paul Woolner, "las nuevas empresas digitales necesitan líderes que puedan trabajar bien en entornos ambiguos. Ellos deben demostrar capacidades efectivas para el trabajo en equipo, transmitir con voz carismática la visión de la empresa, establecer y mantener relaciones efectivas caracterizadas por la inteligencia emocional". Es difícil para una persona contar con todos los atributos necesarios para ser un líder efectivo, por lo que el ser un profesional reflexivo es una característica esencial.

El líder debe tener como prioridad el beneficio de su empresa más no la satisfacción personal.

La reflexión provee valor a una experiencia volviéndole a dar forma para mejorar la acción futura, esto conduce a la implementación, elaboración de un prototipo y luego se regrese a la reflexión, ciclo basado en el conocimiento y en la acción mental.

Estructura organizacional innovadora

El entendimiento de la organización y el lenguaje con el que se la describe son piezas clave para el desarrollo de culturas organizacionales, de alto desempeño en territorios desconocidos. Las nuevas y recién formadas culturas corporativas se modelan haciendo uso de diversas herramientas como son: limitar el uso de títulos tradicionales, el lenguaje, los iconos e incluso hacen uso de organigramas tradicionales.

1.16 ANÁLISIS EN DETALLE[12]

A continuación se describe una metodología para la adaptación de PYMES (pequeña y mediana empresa) hacia la economía digital. Este estudio lo elaboró la empresa Improven Consultores de España. Está orientada hacia los portales en el Internet, pero sus principios son perfectamente aplicables si se parte de la premisa que el Negocio Electrónico no es solamente la Web.

Esta metodología es interesante ya que se refleja que fue hecha para una situación de mercado como la del Ecuador y por eso se ha considerado que debe mencionársela en el presente estudio.

Consta de varios puntos, los que se desglosan a continuación.

1.16.1 SITUACIÓN ACTUAL

El planteamiento de varias empresas es como manejar y mejorar sus resultados luego de la gestión dentro del Negocio Electrónico. Frente a esta consideración se tienen tres casos:

1. La empresa aún no implanta el Negocio Electrónico y no tienen presencia en el Internet.

[12] http://www.winred.com/colaboradores/colaborador28.htm

2. La empresa tiene presencia en el Internet y ha implantado el Negocio Electrónico, pero no tienen mejores resultados que antes de hacerlo.
3. La empresa ha implantado el Negocio Electrónico, tiene presencia el en Internet y está obteniendo muy buenos resultados.

Normalmente el resultado que están obteniendo la pymes no son de los mejores, por lo que en esta metodología se exponen la alternativas de soluciones.

1.16.2 PROBLEMÁTICA DE LAS EMPRESAS

Las consideraciones de este punto están hechas tomando como base que las empresas son reales, de ahí que se habla de la implantación del Negocio Electrónico, si la empresa se crearía íntegramente para comercio electrónico algunas consideraciones deberían ser diferentes.

Las causas más comunes para que la pequeñas y medianas empresas no estén consiguiendo los resultados esperados, pueden provenir de una o varias de las razones que a continuación se detallan:

- Desconocimiento total o parcial de las oportunidades importantes que ofrecen las nuevas tecnologías, lo que se refleja poco apoyo por parte de la directiva.
- Se subestiman las posibilidades que brinda el Negocio Electrónico.
- Falta de planificación en el proceso de implantación del Negocio Electrónico.
- Falta de personal cualificado en esta área.
- No se remodelan los procesos de la empresa para la correcta adecuación del negocio.
- No se ve a esta actividad como algo prioritario.
- Incorrecto desarrollo de la imagen de la empresa.
- Incorrecto desarrollo de estrategias de promoción de la empresa.
- La empresa no tiene una cultura innovadora.
- No se cuenta con una metodología adecuada para el desarrollo del proyecto.

1.16.3 BENEFICIOS

Las mejoras que se pueden hacer para aprovechar los beneficios de la tecnología, el Internet, y el Negocio Electrónico, se pueden concretar en las siguientes:

- Mejoras en el área comercial y en la relación con los clientes:
  - Incremento de las ventas
  - Disminución de los costos de comercialización
  - Incremento de los márgenes comerciales
  - Mejora de la atención a clientes y automatización
  - Captación de nuevos clientes
  - Medición del incremento de la satisfacción del cliente
  - Interacción todo el tiempo
  - Acciones de mercadeo y comunicaciones personalizadas
  - Mayor conocimiento de las necesidades del cliente
  - Mejora de la comunicación a los clientes y la información que tienen de los productos o servicios
  - Fidelización de los clientes
  - Posibilidad de acceso a mercados dispersos geográficamente
  - Expansión internacional con un bajo costo
  - Velocidad para alcanzar nuevos mercados
  - Acciones de comunicaciones con bajo costo
  - Autoservicio de los clientes
- Mejora de los procesos de la empresa
- Aprovechamiento de nuevas oportunidades de negocio
- Desarrollo de nuevas ventajas competitivas
- Mejoras en el área de relación con los proveedores:
  - Existencias, pedidos, envíos, pagos, JIT (del inglés *just in time*)
  - Area de administración
- Mejora de la utilización y distribución de la información interna
- Mejora de la comunicación interna
- Ofrecer productos diferenciados
- Reducir costos de infraestructura

- Suministro online
- Refuerzo de la imagen de marca
- Aprovechamiento de las oportunidades de colaboración

Como se puede observar estas son las ventajas del Negocio Electrónico, las cuales fueron enunciadas con más detalle en el punto 1.7 de este capítulo. Es claro que como existen ventajas, las desventajas también están presentes, por lo que se deben analizar en conjunto para poder evaluar el proyecto en su real magnitud. Se hace referencia a las desventajas en el punto 1.8 de este capítulo.

1.16.4 METODOLOGÍA Y DESARROLLO PARA ALCANZAR EL ÉXITO EN LA GESTIÓN

En este punto se desarrolla con un poco más de detalle las recomendaciones enunciadas en el punto 1.15 de este capítulo, lo que se complementa con temas de seguridad y de telecomunicaciones que serán analizados en los capítulos posteriores.

La metodología y su desarrollo se han estructurado de la siguiente manera:

1.16.4.1 Formación en el ámbito directivo de Internet y sus posibilidades

La correcta formación hace que ésta se convierta en un elemento motivador para el proyecto, además, si los directivos no tienen claro lo que se busca y cómo buscarlo, difícilmente podrán transmitir lo que requieren de su grupo de colaboradores.

1.16.4.2 Definición del equipo que va a desarrollar el proyecto así como su alcance, plazos y recursos

Este punto es muy importante, debido a los cambios que se presentarán.

El equipo de trabajo puede ser totalmente interno, totalmente externo o mixto, dependiendo de las necesidades y recursos de la empresa y de los objetivos planteados, debiendo contar con el apoyo directivo. Según Improven lo óptimo es normar equipos mixtos, el personal interno aporta con su conocimiento de la empresa y el personal externo aporta con su experiencia en este tipo de proyectos.

Lamentablemente en el Ecuador no existe todavía el personal nacional lo suficientemente preparado en proyectos de implantación de Negocio Electrónico, por lo que los cambios deben hacerse con personal interno y con referencias de países vecinos en los cuales se han llevado a cabo con éxito la transformación, esto implica un gran trabajo de investigación.

1.16.4.3 Revisión del plan estratégico de la empresa para integrar en él la figura de Internet

Revisión de las áreas de mercadeo, económico, recursos humanos y tecnológico, para tener una idea clara de los mercados, las inversiones y los recursos con los que se cuenta.

El componente estratégico que implica el Internet y el Negocio Electrónico son fundamentales en el sentido de conocer: el mercado, el comportamiento de los "nuevos clientes" (en el sentido de que su atención no es la tradicional), los nuevos canales de distribución, nuevas acciones de marketing, análisis de la competencia, las nuevas necesidades de recursos humanos, y económicos.

Es importante que el plan estratégico se vea reflejado en un documento formal de conocimiento general de todos los empleados, la mayoría de las empresas los planes son informales y se encuentran en la mente de los directivos.

En este punto existen varias alternativas para realizar el proyecto:

- Desarrollar el proyecto internamente.
- Desarrollar el proyecto externamente.
- Emplear alianzas para la rápida integración del Internet y del Negocio Electrónico.
- Crear una nueva empresa para la presencia en el Internet y la implantación del Negocio Electrónico.

Esta decisión se la tomará en función de los recursos y de la cultura de la empresa.

1.16.4.4 Análisis de las necesidades de información y automatización para el proyecto y el grado de adecuación de los sistemas de información existentes

Las necesidades de información son básicas para el buen desenvolvimiento del proyecto.

Se pueden tener sistemas de comercio electrónico, sistemas de seguimiento de clientes CRM (Customer Relationsip Management), sistemas de seguimiento de socios PRM (Partner Relationship Management), personalización y de esta manera aprovechar todo el potencial del Negocio Electrónico.

Los sistemas de información deben ser analizados desde varios puntos de vista como tecnologías empleadas, bases de datos, escalabilidad.

1.16.4.5 Definición de políticas y procedimientos de seguridad

La seguridad informática es fundamental, como se indica en el capitulo 3 de este trabajo. Para saber que este punto es crítico, basta hacerse la pregunta de qué pasaría si la información que se tiene se perdiese o cayera en manos indebidas.

Las políticas, planes y procedimientos de seguridad se vuelven muy importantes.

1.16.4.6 Diseño de la presencia en Internet y tecnologías asociadas. Definición de la conexión

Analizando las necesidades de nuestros clientes se determina el diseño, los contenidos y la tecnología que mejor se acoplen a dichas necesidades. Este es un concepto muy importante, no solamente en el Internet, ya que lo valorado son visitantes fieles y habituales y no las visitas esporádicas y sin repetición. El sitio web debe ser *customer focused*, es decir, enfocado completamente al cliente, dando confianza, proporcionando valor agregado, permitiendo la realimentación o *feedback,* y emitiendo profesionalismo, rapidez, sencillez de uso, facilidad de acceso a la información. Para poder concebir un sitio tan complejo se deben enumerar las necesidades de los clientes y describir como se va a cubrir cada una de ellas y con cuales herramientas se lo realizará.

Asimismo, la definición del equipo de comunicaciones, servidores, seguridad, deben ser parte del planteamiento final, así como también el dimensionar las líneas de comunicaciones que se emplearán para comunicar a los clientes y los proveedores.

En general, los métodos de acceso, tipo de conexión, configuración y características del software y del hardware, deben contenerse en este punto.

1.16.4.7 Reestructuración de procesos para adecuación a Internet

La reingeniería de procesos mejorará la eficiencia y eficacia de todas las áreas de la empresa como son: relaciones con clientes, compras, ventas, administración, utilizando las posibilidades que ofrecen los sistemas de información.

1.16.4.8 Promoción en Internet

En ese punto pueden fallar algunas estrategias. Se debe tomar en cuenta que se está hablando de una promoción a escala mundial, y si no se hace de la forma adecuada los clientes nunca encontrarán el sitio.

Las herramientas que se pueden emplear son múltiples y todo depende de los recursos con los que cuente la empresa.

Evidentemente las acciones publicitarias pueden ser llevadas a cabo en el mundo real al mismo tiempo, con publicaciones en los diferentes medios de comunicación social.

1.16.4.9 Seguimiento y control

Los resultados del proyecto deben ser seguidos y controlados con minuciosidad, no tienen nada que ver con el mantenimiento del sitio web.

Se recomienda hacer un cuadro que contenga parámetros de seguimiento como por ejemplo: ventas por el portal, % de ventas por el portal frente al total de ventas, ventas por tipo de producto por el portal, % de ventas por producto por el portal, % de clientes nuevos adquiridos por el portal, etc.

Cada empresa deberá obtener los parámetros con los cuales realice el seguimiento.

Una vez definidos los parámetros se debe llevar el control, comparándolos contra los planificados y de existir desviaciones tomar los correctivos que sean necesarios.

1.17 BANCA Y NEGOCIO ELECTRÓNICO

Un papel fundamental dentro del Negocio Electrónico es el que tiene que ver con los bancos y su interacción con la EBC y en general con las empresas digitales.

Todo el manejo financiero que se deriva de una transacción de comercio electrónico debe ser manejada por empresas cuyo negocio principal sea justamente el manejo de dinero, de ahí que en esta actividad también haya incidido en la forma de trabajo tradicional de los bancos en el ámbito mundial, a tal punto que la gran mayoría de ellos se han visto obligados a replantear sus estrategias para enfrentar de manera adecuada los nuevos retos que la era digital les presenta.

Matthew W. Barrett, presidente y COE de Bank of Montreal Group of Companies, hace alusión a este fenómeno cuando escribe: "Necesitamos enfrentar con firmeza las nuevas realidades que están transformando la banca con tal sutileza, que analizarlas sería como tratar de hacer un mapa de las nubes. Globalización, cambios demográficos y explosión de información y tecnología de comunicaciones ya han causado cambios masivos en la manera como se realizan las transacciones bancarias. No obstante, estoy seguro de que nosotros sólo estamos pasando el umbral de un nuevo mundo. Es como si acabáramos de inventar la imprenta o e motor de vapor."

Es tan profundo el cambio en el ámbito bancario que realmente está produciéndose una explosión, la cual arrastrará a los bancos que no se adapten a las nuevas tendencias tecnológicas, de esta explosión surgirán entidades literalmente reinventadas, capaces de brindar sus servicios vía Negocio Electrónico y como hoy las conocemos.

La *banca digital* se debe reorientar al cliente que será su modus operandi de aquí en adelante, tomando en cuenta que ahora el mercado es global y que en negocio financiero no será exclusivo de los bancos ni de economías nacionales, esa pérdida de fronteras representa una amenaza y una

disminución de ventajas competitivas, además el dinero no es el verdadero capital en la era digital, sino más bien el conocimiento.

Las transacciones financieras comunes que suceden hoy en una oficina, y en horas de oficina, ahora pueden ocurrir a cualquier hora y usando cualquier medio, como son: cajeros automáticos, teléfonos, computadoras y hasta televisores.

La figura 1.9 indica el cambio en el comportamiento de usuarios bancarios en Estados unidos y en Canadá, respecto a transacciones bancarias en oficinas.

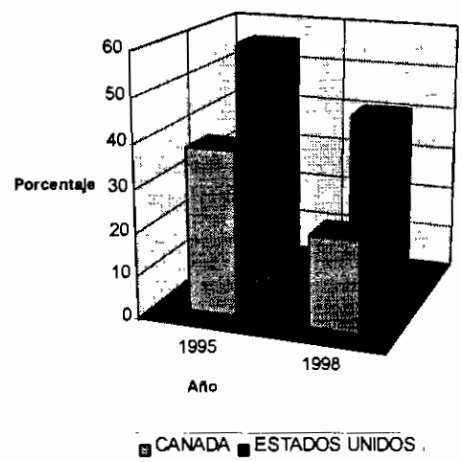


Figura 1.9 Transacciones bancarias minoristas[13]

De la figura 1.9 se desprende que la banca debe prestar más servicios de valor a sus clientes, estos servicios solamente se los puede ofrecer en el campo digital del ciberespacio.

Los retos son grandes pero también lo son las oportunidades. Es claro que el capital necesario para poner en funcionamiento un banco en la Web es mucho menor que el que se necesita para uno tradicional, como se lo conoce hoy. Así fuera del Ecuador, en 1997 el costo de abrir un banco *virtual* era igual que el de abrir una nueva oficina, es decir cerca de un millón de dólares. Ese mismo banco virtual puede llegar a atender aproximadamente a 16 millones de hogares en Norteamérica, si esa misma cantidad de clientes se pretenden alcanzar con oficinas en la "esquina de los barrios", se necesitarían cerca de 900 millones de dólares; las cifras demuestran el abismo que separa

[13] Fuente. *Fifth Annual Special Report on Technology in Banking – Creating the Value Network 1996.* Ernst & Young, 1996

la banca electrónica de la tradicional. Sin embargo no se debe descuidar las otras opciones de atención al cliente, ya que como se ha mencionado anteriormente, el Negocio Electrónico está orientado a satisfacer las necesidades de los usuarios, en este caso, antes que las de la empresa, desde ese punto de vista los clientes de los bancos utilizarán los canales de conexión con el banco que mejor se adapten a sus necesidades y no los que al banco le resulten más rentables. Otro punto a tener en cuenta es el costo de las transacciones basadas en tecnología así por ejemplo: el costo de una transacción realizada por teléfono es de $0,35, frente a $1,07 si se la realiza en una oficina, si se la hace en un cajero automático es de $0,27, si es hecha con una tarjeta de débito $0,10, pero realizada la transacción vía red el costo es casi cero. Estos costos son de cara al cliente, no se toma en cuenta la fuerte inversión que los bancos deben hacer en tecnología, para buscar la satisfacción de sus depositantes.

La credibilidad de algunos bancos tradicionales y la confianza que sus depositantes les tienen no son suficientes para que estos incursionen de manera exitosa en la banca virtual (multicanales), ni tampoco es conveniente, por ahora, crear bancos del todo virtuales; esa credibilidad de cara a los clientes está dada literalmente por la última transacción que una persona realizó en una institución financiera, en cualquiera de los dos tipos.

Otra amenaza para la banca virtual es la seguridad y privacidad, las cuales siempre estarán en tela de discusión mientras los piratas cibernéticos sigan navegando en el mar de la información y buscando sitios dónde poder realizar sus prácticas, todos saben que eso nunca terminará, lo único que se puede hacer es seguir perfeccionando las seguridades, para que a su vez éstas sean violadas y comenzar nuevamente el ciclo.

Lo cierto es que la banca virtual está naciendo, las cifras de personas que están conectadas en línea con sus bancos no son altas, así en Estados Unidos solamente el 10% de los hogares estaban conectados a su banco para obtener información sobre servicios financieros en 1996, y solamente el 2% estaban realmente en línea; mientras que en Canadá las cifras son del 5% y del 2% respectivamente.

Definitivamente la banca debe adaptarse a los veloces cambios que seguirán produciéndose sobre la base del Negocio Electrónico, solamente la capacidad de cambiar con las tendencias y basándose en las necesidades de los clientes podrán asegurar a las instituciones financieras un futuro con rentabilidad.

1.18 LOGÍSTICA

Para iniciar el tratamiento de este punto se debe indicar que la logística es la clave para un *negocio virtual.* Se la compara con temas financieros y al igual que estos, ella es básica para el desarrollo del Negocio Electrónico. No basta tener un web site que venda cualquier cosa si no se tiene como recibir los pagos y peor aún como enviar el producto o bien que ha sido adquirido.

"El dominio de la logística es tan vital para triunfar en la economía digital como lo fue para el extraordinario éxito del imperio romano." Frederick W. Smith. Director, presidente y CEO de FDX Corporation.

Utilizando las tecnologías de telecomunicaciones y de información, es posible mantener una logística que abarca desde el manejo de la cadena de suministro hasta los puntos de distribución, cuando se trata de productos no digitales, como es lógico estos procesos incluyen el servicio al cliente, transporte, procesamiento de pedidos, manejo de inventarios, estrategias de producción y compra. Todo esto conjugado en una cadena de valor en la cual la información sea la esencia de la logística.

El objetivo de la logística, desde el imperio romano, es saber dónde se encuentran los bienes en determinado momento y cuánto tardarán en llegar a su destino, minimizando la necesidad de tener un inventario en bodega como reserva. Como resume Dennis H. Jones de Federal Express "la cantidad se reemplaza con la información", lo que hace que se reduzca la inversión monetaria y reduce los costos de los productos, haciendo que la logística sea una de las estrategias principales cuando de Negocio Electrónico se trata, nuevamente basándose en el pensamiento reflejado en el conocimiento.

La nueva visión de la logística hace que las empresas cambien sus herramientas y utilizando las redes de telecomunicaciones se conviertan en la clave del comercio actual.

La tercerización de esta actividad es lo más recomendable, de esta forma las empresas se dedican exclusivamente a su negocio y pueden concentrar sus energías en las ventas, el marketing y el diseño. De hecho las empresas digitales se enfocan en habilidades limitadas, para poder utilizar todo su potencial, mientras que las demás funciones son delegadas a otras empresas. La razón fundamental es que casi ninguna empresa que se dedique a este negocio puede tener el capital necesario para poder mantener toda la parafernalia necesaria para poder competir en la economía global y además agregar valor.

La logística integrada agrega valor a la cadena de suministro entre el fabricante y el vendedor, al obtener estos últimos los productos directamente de sus productores y al mismo tiempo distribuirlos del mismo modo a sus clientes, de una manera personalizada. Esta forma de comercializar productos es la base para la masificación de la venta personalizada de bienes y servicios, en el sentido más amplio del concepto.

Nuevamente retornamos a las ventajas citadas del Negocio Electrónico, las que tienen que ver con los compradores: menores costos, conveniencia por el despacho directo y posibilidad de elección debido a la personalización.

Las empresas de logística deben tener claro su negocio y nunca competir con las empresas que están contratando sus servicios. Al tener contacto con los clientes de sus clientes, las compañías de correspondencia tienen acceso a información estratégica: códigos postales, hábitos de compra, valores, etc. Al usar esta información para sacar ventaja, la logística pierde valor y esto se ve reflejado en una baja de rendimiento y el descenso de los beneficios mutuos. Cada empresa se dedica a la porción de la cadena de valor que le corresponde y toda la comunidad funciona de manera adecuada es ahí cuando los beneficios mutuos se ven reflejados.

CAPÍTULO 2.

Redes privadas: Tecnologías Inmersas

2.1 INTRODUCCIÓN

Este capítulo está orientado a emitir un marco teórico de referencia para un nuevo fenómeno en el mundo del intercambio de información y de las telecomunicaciones, denominado *extranet*. Este marco conjuga tecnologías de transmisión de datos, criterios de diseño de redes privadas (¿qué tan privadas?) y el tratamiento de la tecnología más comúnmente usada en el mundo de las redes de computadoras, que es TCP/IP.

El avance de la tecnología ha originado una estrecha relación entre el software, el hardware y las telecomunicaciones, dando lugar a las denominadas *Tecnologías de la Información (TI)*. El surgimiento de TI ha influido en la manera de cómo los sistemas de cómputo se organizan, de este modo la plataforma de trabajo actual en tecnología digital conjuga:

- Sistemas de telecomunicaciones: como la base en dónde se desarrollan todos los procesos de intercambio de información
- Técnicas informáticas: mediante las cuales se tienen las interfaces necesarias para que el intercambio de información sea entendido por las personas que utilizan tal o cual servicio

Esta es la forma de dar valor a la información y así crear el conocimiento necesario para poder interactuar en el ámbito del Negocio Electrónico.

Antes de iniciar el estudio de las redes privadas y todo lo relacionado con ellas, se debe hacer un paréntesis histórico, esto servirá para ubicarse en el momento tecnológico actual y poder proyectar ese momento sobre el Negocio Electrónico y las transacciones financieras que están revolucionando al mundo. Se iniciará el estudio de la historia del Internet que es la base de la era global digitalizada y sobre la cual se ha desarrollado un sinnúmero de tecnologías y de protocolos de comunicaciones que son motivo de este capítulo. Luego de ello se analizará los tipos de redes y los

principales modelos de referencia que se utilizan dentro de este ámbito, para poder entender de mejor manera algunos términos comunes y cómo se encuentran estructuradas las tecnologías de transmisión de datos más usadas. Antes de terminar este capítulo se tratará sobre la familia de protocolos TCP/IP, lo que dará el fundamento teórico para entender el desarrollo de las comunicaciones actuales y del futuro.

Con toda esta base teórica se podrá emitir criterios de redes privadas y su influencia dentro del Negocio Electrónico.

2.2 HISTORIA DEL INTERNET

Los orígenes del Internet se remontan a la década de los 60, cuando el Departamento de Defensa (DoD) de los Estados Unidos recurrió a ARPA (Advanced Research Projects Agency), su rama científica. El objetivo fue iniciar un proyecto ambicioso para montar una red de datos a prueba de guerras, para lo cual acudieron a las universidades para poder plasmar el proyecto. La idea era contar con una red que no dependiera del hardware y que su operación no se interrumpiera, es decir, que la transmisión de datos entre dos máquinas permanezca pese a que el equipo o línea de transmisión sufriera algún daño grave. A inicios de los años 60, Paul Baran había sugerido una red de conmutación de paquetes, esa idea fue acogida por ARPA y así se inició la primera red de conmutación, cuyos componentes son una subred y computadoras o hosts.

La subred tenía computadoras denominados *IMP* (Interface Message Processors) conectados por lo menos a otros dos, lo que permitía tener varias rutas para los datagramas que cursaban por la red; además, cada IMP estaba conectado a un host, lo que se muestra en la figura 2.1, así como los protocolos que manejaba la red de ARPA.

Esta red se denominó *ARPANET*, la que tuvo un crecimiento muy acelerado y en 1972 cubría todos los Estados Unidos. ARPA también financió investigaciones en el campo de la transmisión de datos vía satélite y redes de radio, para de esta manera poder ayudar al crecimiento de Arpanet, lo que demostró que los protocolos existentes no eran lo suficientemente

poderosos para manejar varios tipos de redes. Esto culminó con la invención de los protocolos TCP/IP (Cerf y Kahn, 1974) que servía para llevar a cabo la comunicación entre redes de diferente naturaleza, lo que se popularizó cuando más redes ingresaban a la ya muy extensa Arpanet. En 1983, con TCP/IP adoptado y con más de 200 IMP y miles de host conectados, ARPA concede la operación de su red a la Agencia de Comunicaciones de la Defensa (DCA) y esta agencia decide separar la parte militar de la red y denominarla *MILNET*. En la década de los 80, se hizo muy costoso encontrar un determinado host entre los miles que existían, por lo que se creó el, sistema de designación de nombres *DNS* (Domain Name System), para establecer una relación entre la dirección IP de una máquina (dirección única dentro de toda la red) y su nombre. En 1990 Arpanet fue desmantelada debido a la existencia de varias redes más nuevas que ya utilizaban los protocolos que se generaron en Arpanet.

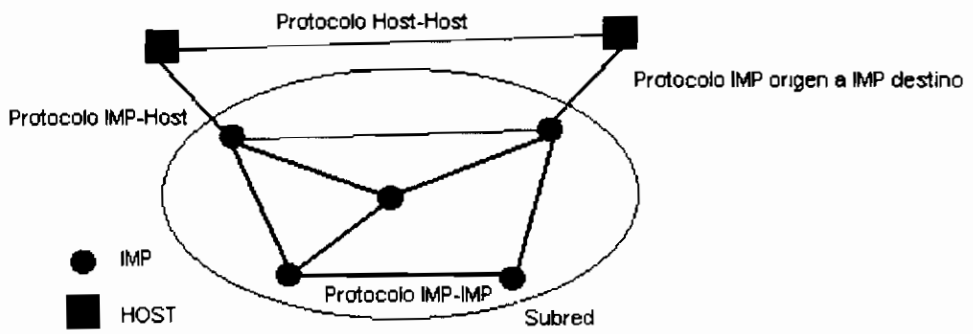


Figura 2.1 Diseño y protocolos de comunicación de la red ARPA[1]

Sin embargo, la primera red WAN que usó TCP/IP desde su inicio, fue la *CSNET*, que surgió de la necesidad de conexión que tuvo la Fundación Nacional de la Ciencia de los Estados Unidos NSF (National Science Fundation) en 1970, debido a que algunas universidades no tenían contratos con ARPA y no podían entrar en su red. Esta red contaba con un *backbone* y redes regionales que enlazaban museos, universidades, bibliotecas y

[1] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra Ed., pag 48

laboratorios de investigación, se llamó al final *NSFNET*, la que necesariamente se conectó a Arpanet. Debido a que ésta era una red que funcionaba con fondos no privados y su crecimiento era muy acelerado, la NSF sugirió a MERIT, MCI e IBM formar un consorcio para la operación de la red, de ahí se formó la *ANSNET* (Advanced Network and Services). En 1995 ANSNET fue vendida a America On Line, la que tuvo que contratar servicio comercial IP para conectarse. Luego la NSF otorgó contratos a diferentes operadores para establecer puntos de acceso a la red, esta nueva columna vertebral no se encontraba administrada por una sola compañía, sino que ahora se había convertido en un mercado regido por el precio y la competencia.

Es así como el 1 de enero de 1983, TCP/IP se convierte en el único stack de protocolos para redes nacionales y continentales y nace la red de redes hoy conocida como *Internet*. Para 1990 la Internet contaba con 3.000 redes y algo como 200.000 computadoras, para 1992 se unió la computadora número un millón. En 1995 la Internet contaba con varias columnas vertebrales de alta velocidad, cientos de redes regionales, miles de redes locales, millones de computadoras y decenas de millones de usuarios. Estos números crecen cada año.

"Una máquina está en Internet si opera con la pila de protocolos de TCP/IP, tiene una dirección IP y es capaz de enviar paquetes IP a todas las demás máquinas de Internet." A.S Tanenbaum, *Redes de Computadoras*, Prentice Hall, 3ra. Ed., pag.53.

Las aplicaciones principales de que disponía el Internet en sus inicios eran:

- Correo Electrónico (e-mail)
- Noticias (news)
- Sesión Remota (Telnet)
- Transferencia de Archivos (FTP)

Hoy en día la cantidad de aplicaciones que están disponibles en el Internet es muy grande, entre las más sobresalientes están:

- WWW, World Wide Web o telaraña mundial de la información

- Teletrabajo
- Negocio Electrónico

Todos estos servicios se basan en los protocolos TCP/IP que tienen sus orígenes en la Arpanet.

2.3 MODELOS DE REFERENCIA

Para iniciar el estudio de los diferentes modelos de referencia para las redes, es necesario precisar algunos conceptos.

2.3.1 DEFINICIONES

Todos los modelos se dividen en capas o niveles. Las capas tienen definidos su nombre función y protocolos. Entre las capas existen interfaces, las mismas que permiten el intercambio de información entre un nivel superior y uno inferior. Esta información debe ser la mínima indispensable para que se realice la comunicación sin pérdidas ni mutilaciones. Los datos van de una capa a otra hasta llegar al medio físico, en el cual son enviados a su destino.

La conjunción de protocolos y capas define una arquitectura de red, la que permitirá a un diseñador implementar el software y el hardware necesario para que cada nivel cumpla las funciones de diseño.

El diseño también debe contemplar otros aspectos:

- Posibilidad de múltiples destinos
- Tráfico en una vía o en dos vías (símplex, semidúplex o dúplex)
- Detección y corrección de errores
- Desensamblaje y reensamblaje de información, en el caso de que ésta sea dividida en paquetes de menor tamaño
- Saturación de receptores lentos contra transmisores rápidos
- Multiplexación y demultiplexación de canales lógicos

Dentro de un modelo de referencia existen servicios que las capas ofrecen, la tabla 2.1 muestra los servicios disponibles, los mismos que pueden ser: orientados a conexión y sin conexión.

	SERVICIO	EJEMPLO
Orientado a conexión	Flujo de mensajes confiable	Secuencia de páginas
	Flujo de bytes confiable	Ingreso remoto
Sin conexión	Conexión no confiable	Voz digitalizada
	Datagrama no confiable	Correo electrónico chatarra
	Datagrama con acuse de recibo	Correo registrado
	Petición/respuesta	Consulta de base de datos

Tabla 2.1 Tipos de servicios[2]

Los servicios que una capa ofrece a su superior están compuestos por operaciones o *primitivas* que son las que indican qué acción se debe realizar.

La tabla 2.2 indica una posible clasificación de los tipos de primitivas u operaciones para servicios confirmados.

Para los servicios no confirmados solamente existen dos primitivas: petición e indicación.

PRIMITIVA	SIGNIFCADO
Petición	Una entidad quiere que el servicio haga el trabajo
Indicación	Se le informa a una entidad acerca de un suceso
Respuesta	Una entidad quiere responder a un suceso
Confirmación	Ha llegado una respuesta a una petición anterior

Tabla 2.2 Primitivas de servicio[3]

Las peticiones y respuestas son de la entidad origen, éstas generan indicaciones o confirmaciones en la entidad destino.

A continuación se analizan los modelos más difundidos en el campo de las redes.

[2] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra. Ed., pag.25
[3] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra. Ed., pag.25

2.3.2 MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS

En 1983 la Organización de Estándares Internacionales ISO (International Standard Organization), junto con la CCITT (Comité Consultivo Internacional de Telecomunicaciones y Telefonía), hoy UIT (Unión Internacional de Telecomunicaciones), propusieron un grupo de estándares y recomendaciones para interconexión de sistemas.

Los criterios en los que se basaron para el diseño de este modelo son:

- Cada capa supone una función específica
- La función se debe basar en protocolos estandarizados a escala mundial
- Las funciones se limitan tomando en cuenta un mínimo de información entre las capas
- No se debe agrupar funciones distintas en una misma capa, lo que dará el número total de niveles

Esos criterios permiten que los avances tecnológicos no afecten a todo el modelo, sino más bien a capas específicas.

Normalmente las tareas de las capas inferiores son realizadas por hardware, mientras que las de capas superiores son asuntos de software.

Una de las desventajas de aplicar el modelo OSI (Open System Interconection) es que éste dispone de siete capas (figura 2.2), lo que implica que el mensaje entregado al medio físico se encuentra con muchos encabezados, los que son colocados por las capas para poder llevar el control y la comunicación con los niveles pares. El resultado es que solamente el 15% del mensaje es información útil, el resto es sobrecarga.

En general las tres primeras capas se ocupan del movimiento de los bits por el medio físico, mientras que las cuatro capas superiores permiten la comunicación entre dos host.

El modelo OSI en si no es una arquitectura de red, ya que no se especifican los servicios y protocolos que cada capa debe tener, sin embargo, existen protocolos para cada nivel, los que han sido publicados por separado.

A continuación se exponen las características principales de cada una de las capas que componen el modelo OSI.

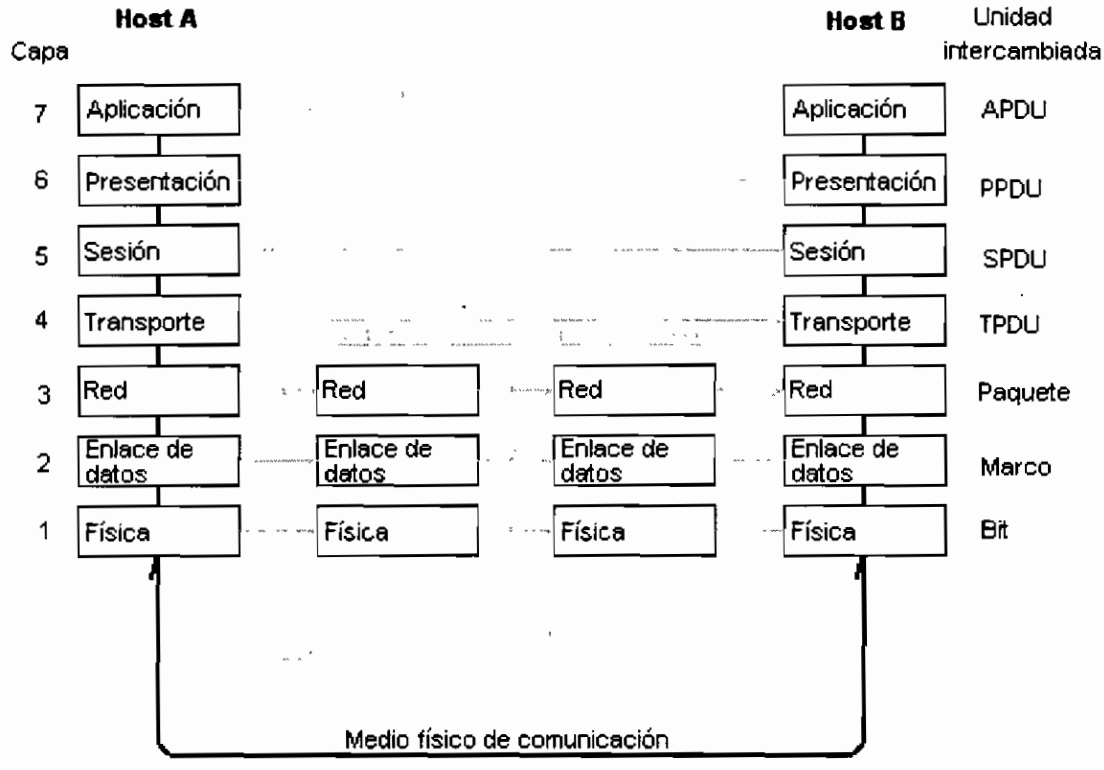


Figura 2.2 Modelo OSI[4]

La figura 2.2 indica que las capas 4 a la 7 son de extremo a extremo, mientras que las capas 1 a 3 son encadenadas, es decir, que la *conversación* entre pares correspondientes de 1 a 3, se da entre cada nodo de la subred, empezando desde el host de origen y terminando en el host de destino.

2.3.2.1 Capa Física

Este nivel tiene que ver con la transmisión de bits por el canal de comunicaciones. Especifica los estándares físicos, eléctricos, funcionales

[4] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra. Ed., pag.29

y de procedimiento para ingresar al canal. La unidad de datos que maneja esta capa es el bit.

2.3.2.2 Capa de Enlace de Datos

Tienen que ver con las comunicaciones entre los nodos en la red y proporciona un medio de activar, mantener y desactivar la comunicación por el canal, además, proporciona un canal libre de errores para la transmisión.

La unidad de datos que maneja esta capa es el *marco* o *frame*, los que transmite en forma ordenada y una vez entregados, los procesa. De esta manera puede controlar errores como: frames no recibidos, duplicidad de frames y frames dañados. Asimismo, debe tener el control acerca de la regulación el tráfico entre emisor y receptor.

En redes de difusión, ésta dispone de un nivel bajo dentro de sí misma, la que se conoce como *subcapa de acceso al medio*, la cual negocia la compartición de un mismo canal de comunicaciones.

2.3.2.3 Capa Red

La unidad de datos de esta capa es el paquete. Se encarga del funcionamiento de la subred y la configuración más apropiada de la misma. Esta capa se encarga de dividir la información de las capas superiores en paquetes, los que son enrutados dentro de la subred, analizando la congestión y gestionando los canales más adecuados.

Sin embargo, la función principal de la capa red es *interconectar* redes diferentes, con distintos protocolos, distintas formas de direccionar los paquetes y diferentes tamaños de paquetes.

2.3.2.4 Capa Transporte

La integridad de la información de un extremo a otro es la función de la capa transporte, lo que supone que este nivel se encarga de los mensajes de ruteo, la segmentación de la información y la recuperación de errores. Se puede decir que desde el punto de vista de comunicaciones es la última capa. Por esta razón este nivel actúa como frontera entre los aspectos de aplicaciones que se relacionan con capas superiores y con

aspectos de red que se relaciona con las capas inferiores, es decir, que esta capa aisla de los cambios tecnológicos del hardware a las capas superiores.

Basándose en la carga de información de la capa de sesión, esta capa puede multiplexar varias conexiones en la conexión de red, haciendo este proceso transparente para el nivel superior. La capa transporte libera y establece las conexiones por las que va a enviar los datos, además, controla el flujo de información previniendo saturaciones. Debemos distinguir el control de flujo entre nodos e la subred, que lo hace la capa de red, con el control de flujo entre origen y destino que es trabajo de este nivel.

2.3.2.5 Capa Sesión

Entre las funciones de esta capa se encuentra el almacenamiento de *buffers*, la capacidad de procesamiento, en definitiva la disponibilidad de la red, así como también el inicio y abandono de sesiones, y la autenticación de usuarios. Es una instancia temporal que se *levanta* cuando los datos están listos para su transmisión.

La sincronización es otra de las funciones de la capa de sesión, esta función utiliza puntos de verificación para transmisión de datos.

2.3.2.6 Capa Presentación

Maneja la sintaxis y semántica de los datos hacia la red, es decir, que la información se encuentre en un modo adecuado para su transmisión. Se ocupa de la encripción y desencripción, compresión y sincronización de mensajes. Los códigos de representación de información más usados por la capa de presentación son ASCII, EBCDIC, Unicode.

2.3.2.7 Capa Aplicación

Controla las actividades dentro de una aplicación y se comunica directamente con la aplicación que está siendo utilizada por el usuario de una máquina. La transferencia de archivos es otra función de esta capa, al igual que el correo electrónico, la carga de trabajo remota, las búsquedas, etc.

2.3.3 MODELO DE REFERENCIA TCP/IP

Este modelo de referencia es el utilizado por la red ARPANET y lógicamente por su sucesora, la red Internet.

La figura 2.3 compara las capas del modelo OSI con la que se encuentran presentes en el modelo TCP/IP.

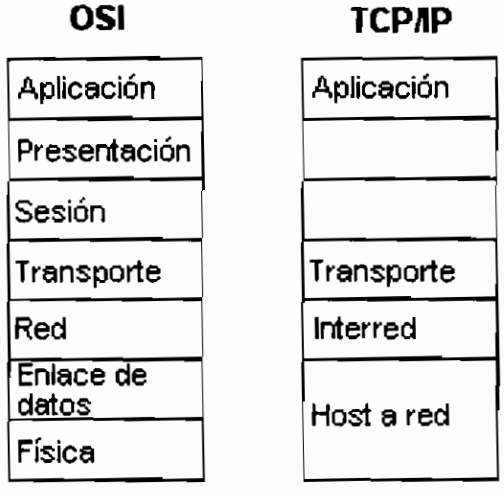


Figura 2.3 Modelo de referencia TCP/IP[5]

A continuación se describen las capas que conforman el presente modelo.

2.3.3.1 Capa Host a Red

Este modelo no proporciona especificaciones concretas sobre esta capa. Lo único que indica es que el medio debe poder aceptar paquetes IP.

2.3.3.2 Capa Internet

Esta capa es la principal y el eje de todo el modelo, permite que los nodos transmitan y reciban paquetes, en forma independiente cada uno.

Esta capa define un protocolo y un formato de paquete denominado protocolo de interred, conocido como IP (Internet Protocol[6]).

Las funciones principales de este nivel son: entregar paquetes IP a su destino y también gestionar el canal para evitar congestiones.

[5] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra. Ed., pag.36

[6] Aquí el término *Internet* se refiere a interredes en inglés (internetwork), más no a la red mundialmente conocida el Internet

2.3.3.3 Capa Transporte

Su función es similar a la capa transporte del modelo OSI.

Tiene definidos dos protocolos:

- *TCP* (Transmission Control Protocol): éste es el protocolo de control de transmisión, está orientado a la conexión y es confiable, es decir, que los bits que una máquina entrega a otra serán recibidos sin errores. Además, fragmenta la información en el origen y luego arma nuevamente los datos en el destino, de igual forma gestiona el flujo a ser transmitido para evitar saturación.
- *UDP* (User Datagram Protocol): es el protocolo de datagrama de usuario, no está orientado a conexión y es no confiable. Se puede decir que es contrario a TCP. Las aplicaciones pueden hacer uso de sus propios controles de flujo y demás servicios que no presta UDP. Se lo utiliza para peticiones y respuestas simples en el modelo cliente-servidor y para aplicaciones que no necesiten entregas libres de errores, sino más bien entregas rápidas.

2.3.3.4 Capa Aplicación

Esta capa contiene los protocolos de *alto nivel*, entre los que se cuenta: terminal virtual TELNET, transferencia de archivos FTP, correo electrónico SMTP, resolución de nombres de host y nodos DNS, transferencia de noticias NNTP, recuperación de páginas de la World Wide Web HTTP.

2.4 OBJETIVOS Y CLASIFICACIÓN DE LAS REDES

2.4.1 OBJETIVOS

Generalmente las empresas tienen un gran número de máquinas interconectadas entre sí, con el objeto de poder tener información en línea, extraer y correlacionar la misma, de esta forma hacer más productiva su organización. Con ese punto en mente se puede enumerar algunos objetivos/ventajas de los sistemas de redes:

- Compartir recursos: Es decir, que todos los datos, archivos y recursos estén disponibles para cualquier persona en la organización, independientemente de la localización geográfica del usuario.
- Alta confiabilidad: no depender de un solo procesador para las diferentes tareas y disponer de un respaldo de la información, es decir, no para los procesos productivos o aplicaciones críticas, si se ocasiona una falla de hardware.
- Ahorrar dinero: Debido al gran costo de computadoras centrales (mainframes), no es posible que las organizaciones tengan este tipo de procesadores en todas sus oficinas, por lo que se ha optado por hacer redes en oficinas, sucursales, las que se conectan con un servidor central en la oficina principal.
- Escalabilidad: ampliar la capacidad de procesamiento y rendimiento de la red, esto se aplica con mayor énfasis a la red, no así a los sistemas distribuidos, ya que el actualizar un mainframe es demasiado costoso y al ampliarlo significa hacer una nueva inversión en un equipo mayor, por otro lado, en una red se puede añadir más servidores y clientes dependiendo de las necesidades creadas en la empresa.
- Medio de comunicación: para mantener constantemente comunicados a empleados que se encuentran distantes y que necesitan hacer tareas en común.

Como se puede observar, las características técnicas no se encuentran como prioridad importante y a ser tomada en cuenta como factor determinante en el momento del diseño, incluso a futuro se puede llegar a dar más énfasis al hecho de conectar y mantener grupos de cooperación que a mejorar la confiabilidad. El cambio radical del uso de los mainframes a las computadoras personales se debe a la ventaja de estas últimas en lo que se refiere a la relación precio/rendimiento.

2.4.2 CLASIFICACIÓN

2.4.2.1 Por la Tecnología de Transmisión

Las redes se clasifican en:

- Redes de difusión
- Redes punto a punto

No es una regla general pero normalmente las redes ubicadas dentro de un área geográfica pequeña suelen utilizar difusión, mientras que las geográficamente distantes son punto a punto.

2.4.2.1.1 Redes de Difusión

Son las que tienen un solo canal de comunicaciones, por lo que los mensajes que envía una máquina son recibidos por todas. Estos mensajes se conocen como *paquetes*, y un campo dentro de éstos indica la máquina a la que van dirigidos los datos (dirección), el resto al no ser destinatarias, desechan los datos. También existe la posibilidad de direccionar, utilizando el mismo campo, el paquete a todas las máquinas lo que se domina *broadcasting*. Asimismo colocando una secuencia especial en el campo de dirección el paquete es enviado a un grupo de máquinas haciendo *multicasting*.

La figura 2.4 muestra dos ejemplos de topologías de redes de difusión.

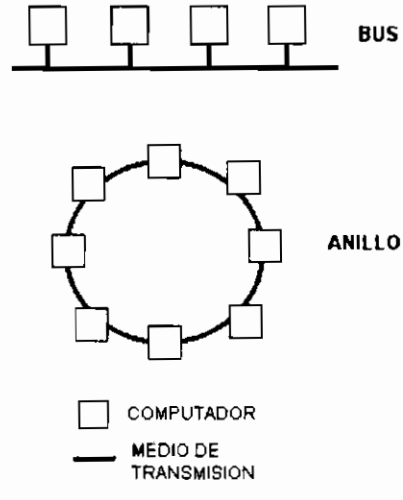


Figura 2.4 Topologías de redes de difusión

2.4.2.1.2 Redes Punto a Punto

Estos tipos de redes manejan múltiples conexiones entre pares de máquinas, por lo tanto un paquete de información puede pasar por varias máquinas para llegar a su destino, como consecuencia se puede tener varias rutas para que la información viaje del origen al destino, por lo que se hace necesario introducir una técnica que se denomina ruteo de información. La figura 2.5 ejemplifica dos topologías que pueden ser utilizadas en estos tipos de redes.

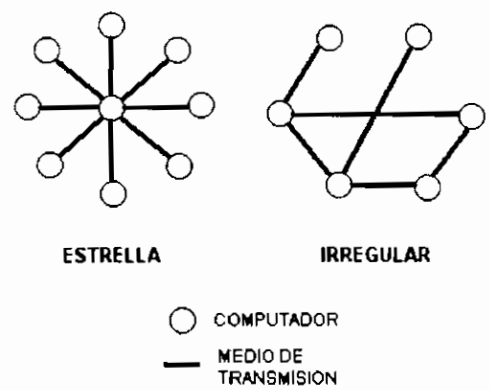


Figura 2.5 Topología de redes Punto a Punto

2.4.2.2 Por la Escala

La tabla 2.3 muestra las redes de acuerdo con su extensión física.

Distancia entre los procesadores	Ubicación de los procesadores	Nombre
10 cm	Tarjeta de circuitos	Máquina de flujo de datos
1 m	Sistema	Multicomputadora
10 m	Cuarto	
100 m	Edificio	Red de área local
1 km	Campus	
10 km	Cuidad	Red de área metropolitana
100 km	País	Red de área amplia
1000 km	Continente	
10000 km	Planeta	Red de redes

Tabla 2.3 Redes por su escala[7]

[7] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra. Ed., pág. 8.

Esta clasificación se basa en que un procesador es una unidad independiente de procesamiento de datos

A continuación se dará una definición de cada una de ellas.

2.4.2.2.1 Redes de Area Local

Son conocidas como redes LAN (Local Area Network).

Normalmente son redes privadas que utilizan las empresas dentro un mismo edificio o campus. Conectan computadoras personales con el objeto de compartir recursos tales como archivos, impresoras, bases de datos.

Se distinguen de otros tipos de redes por su tamaño, topología y tecnología de transmisión, por estas razones se puede conocer de antemano los tiempos de transmisión, facilitando de esta manera su administración.

Son redes de difusión y entre las más utilizadas se tiene:

- IEEE 802.3, conocida como Ethernet
- IEEE 802.4, conocida como Token Bus
- IEEE 802.5, conocida como Token Ring
- IEEE 802.12, conocida como VG-AnyLAN y Prioridad de demanda

2.4.2.2.2 Redes de Area Metropolitana

Son conocidas como redes MAN (Metropolitan Area Network).

Son muy similares a las LAN, incluso en su tecnología, pueden abarcar oficinas de una misma organización ubicadas dentro de una misma cuidad, pueden ser públicas o privadas, no tienen elementos de conmutación y pueden transmitir video y datos, normalmente están relacionadas con redes de televisión por cable.

El estándar más utilizado para este tipo de redes es el IEEE 802.6, conocido como Bus Dual de Cola Distribuida, DQDB (Distributed Queue Dual Bus), al igual que las anteriores estas también son redes de difusión.

2.4.2.2.3 Redes de Area Extendida

Son conocidas como redes WAN (Wide Area Network).

Son redes punto a punto, y su cobertura puede extenderse a un país o a un continente. Está constituida por máquinas conectadas entre sí con el objeto de ejecutar programas de usuario, a éstas se las conoce como *host*. Los host están conectados por medio de la denominada subred de comunicaciones, la cual se encarga de transportar los mensajes de un host a otro. Las telecomunicaciones se encuentran separadas del software aplicacional, lo que simplifica el diseño y manejo de este tipo de redes.

La subred tiene dos elementos bien definidos, el medio de comunicaciones o líneas de transmisión (canales o circuitos) y los equipos de conmutación (nodos centrales o centrales de conmutación), más conocidos como ruteadores. Los host no forman parte de la subred. Las líneas de comunicaciones unen dos ruteadores, si dos nodos necesitan comunicarse y no comparten el mismo canal, el mensaje deberá buscar una ruta que pase por uno o varios ruteadores para que la información pueda ser entregada a su destino. Esto conforma la red de conmutación de paquetes, y casi todas las WAN son de este tipo, exceptuando las que tienen canales de comunicaciones satelitales que son redes de difusión.

2.4.2.3 Redes Inalámbricas

Debido a que las ventas de computadoras portátiles han sufrido un incremento considerable, es necesario mencionar este tipo de redes para intercambio de información. Las redes inalámbricas pueden ser desde LAN hasta WAN dependiendo del lugar desde dónde se acceda. Sus usos son diversos, desde llamadas, faxes, correo electrónico, acceso a servidores remotos.

Se debe hacer una distinción entre redes inalámbricas y redes móviles, la tabla 2.4 indica sus diferencias.

Inalámbrica	Móvil	Aplicación
No	No	Estaciones de trabajo en oficinas
No	Sí	Uso de una portátil en un hotel
Sí	No	LAN en edificios viejos sin alambrado
Sí	Sí	Oficina portátil

Tabla 2.4 Redes inalámbricas y computación Móvil[8]

2.5 PROTOCOLOS TCP/IP

Un protocolo es un conjunto de normas, en cuanto a formato y modos de intercambio, que existen entre los equipos de cómputo, de tal manera que puedan *conversar* e intercambiar información.

TCP/IP viene de las siglas en inglés *Transmission Control Protocol* e *Internet Protocol*.

La figura 2.6 indica la relación entre los protocolos TCP/IP y el modelo de referencia OSI.

<table>
<tr><td>Aplicación
Presentación
Sesión</td><td colspan="2">TELNET</td><td>FTP</td><td>SNMP</td><td>SMTP</td><td>DNS</td><td>HTTP</td></tr>
<tr><td>Transporte</td><td colspan="7">TCP</td></tr>
<tr><td>Red</td><td colspan="7">IP</td></tr>
<tr><td rowspan="2">Liga de Datos</td><td colspan="5">802.2</td><td>X.25</td><td>LLC/SNAP</td></tr>
<tr><td>802.3</td><td colspan="2">802.5</td><td colspan="2">LAPB</td><td>ATM</td></tr>
<tr><td>Física</td><td>Ethernet</td><td>Token Ring</td><td>FDDI</td><td colspan="2">Línea Síncrona WAN</td><td>SONET</td></tr>
</table>

Figura 2.6 Protocolos TCP/IP y el modelo OSI[9]

[8] "Redes de Computadoras", A.S Tanenbaum, Prentice Hall, 3ra. Ed., pag.14.
[9] http: //uca.edu.sv/investigacion/tutoriales/tcp_ip.html

Como indica la figura 2.6 los protocolos TCP/IP ofrecen independencia del medio físico, pero como es lógico deben existir protocolos bien definidos en la capa host a red.

Objetivos

Esta arquitectura ofrece independencia de la tecnología que se use en niveles bajos así como también del tipo de computadora que se desee interconectar, de esta manera se logra una conectividad universal. Debido a que los protocolos de capas bajas no son de interés para TCP/IP, el reconocimiento de la conexión se establece extremo a extremo y se dispone de protocolos al nivel de aplicación estándares.

Características

- Para el nivel de red los protocolos son no orientados a conexión
- La tecnología de transmisión utilizada es la conmutación de paquetes
- En el nivel de transporte los protocolos tienen funciones de seguridad
- Las aplicaciones son comunes a todos los host
- La comunicación entre redes se realiza mediante *gateways* o pasarelas
- Todas las redes que se conectan son consideradas iguales

Direcciones

Este es un aspecto sumamente importante dentro del funcionamiento del protocolo TCP/IP. Debido a la gran cantidad de máquinas conectadas en red, el direccionamiento y reconocimiento de cada host es un asunto muy delicado, por lo que se dispone de direcciones que siguen reglas diseñadas para tratar de hacer la tarea de "poner nombre" a cada máquina sea menos difícil.

La identificación de las máquinas se realiza con direcciones lógicas (de niveles altos) que consisten en números de 32 bits, escritos en forma de cuatro octetos decimales separados por puntos. La información que lleva este formato toma en cuenta la máquina y la red a la que ésta pertenece.

Existen cuatro clases de direcciones IP, las cuales indica la figura 2.7.

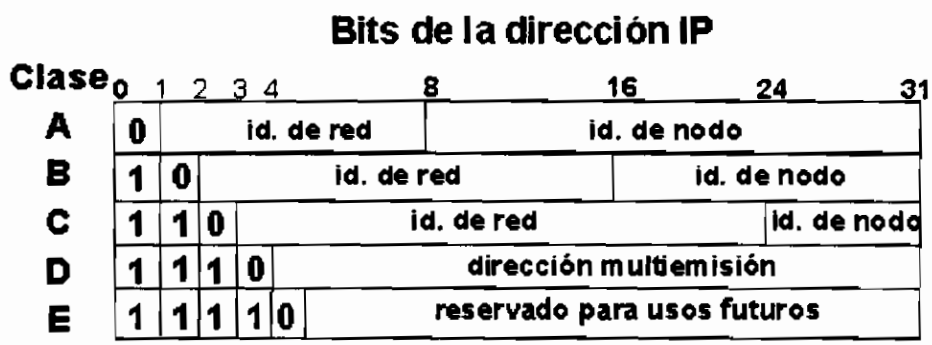


Figura 2.7 Clases de direcciones IP

A continuación, la tabla 2.5 especifica la cantidad de redes y de máquinas dentro de esas redes, que pueden direccionar cada una de las clases de la figura 2.7.

CLASE	REDES	HOST	RANGO DE DIRECCIONES
A	127	16'777.215	1.0.0.0 a la 127.255.255.255
B	4.095	65.535	128.0.0.0 a la 191.255.255.255
C	2'097.151	255	192.0.0.0 a la 223.255.255.255
D			244.0.0.0 a la 239.255.255.255
E			240.0.0.0 a la 247.255.255.255

Tabla 2.5 Rangos de direcciones IP

Una vez definidas las direcciones IP y sus clases, se pueden diseñar *subredes*, utilizando las denominadas *máscaras*, las mismas que tienen el igual formato de las direcciones IP, es decir, cuatro octetos separados por puntos. No se debe confundir el concepto de estas subredes con las que se mencionó cuando se trataba la ARPANET. Ahora subredes son redes físicas distintas que comparten la misma dirección IP de una red principal. Cada clase de direccionamiento (figura 2.7) puede tener subredes.

El objetivo de la máscara es identificar a la subred. El número de la subred se lo obtiene haciendo un AND lógico entre la máscara y una dirección IP de

cualquier máquina. Todas las máquinas que formen parte de una subred deben tener la misma máscara.

2.5.1 PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES

Los protocolos usados para la transmisión de datos en las capas inferiores utilizan un direccionamiento físico, debido a esto debe existir una correspondencia entre las direcciones IP y las direcciones físicas, esto se consigue utilizando el protocolo ARP (Address Resolution Protocol).

Este protocolo de bajo nivel permite obtener la dirección física de una máquina a partir de la dirección IP, lo que posibilita una conversión dinámica de direcciones que es guardada en una tabla temporal, optimizando la carga de la red para transmisiones repetidas.

2.5.2 PROTOCOLO INTERNET

El IP (Internet Protocol) es un protocolo no orientado a conexión y no fiable, lo que significa que los paquetes que se entregan a la red se los trata como entidades autónomas, pudiendo viajar por diferentes caminos y, además, no se garantiza su entrega. Fragmenta los paquetes de información, siendo el tamaño máximo de 65635 bytes. Utiliza las direcciones IP de 32 bits. Hace verificación por suma solamente al encabezado del paquete no así a los datos.

La unidad que intercambia el protocolo IP es el datagrama, que contiene un encabezado y una parte para datos, esta última puede usarse arbitrariamente por la capa de transporte.

2.5.3 PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET

El ICMP (Internet Control Message Protocol) es el protocolo de mensajes de control de Internet, es el que reporta sobre destinos inalcanzables, controla el flujo de datagramas y congestión de la red, controla el cambio de rutas entre gateways, cuando éstas son demasiado grandes y si existe ruta entre dos puntos y el estado de la misma. Es un protocolo eminentemente de notificación y no se encarga de corrección de errores.

2.5.4 PROTOCOLO DE CONTROL DE TRANSMISIÓN

El TCP (Transmission Control Protocol) es el protocolo que brinda la comunicación bidireccional utilizando circuitos virtuales. Es un protocolo de nivel alto cuya función principal es que la información llegue a su destino en forma correcta, con una función adicional que es el recobrar paquetes que se puedan haber perdido. Asegura la confiabilidad de datos:

- Asigna un número secuencial a cada uno de los paquetes segmentados
- Realiza la verificación por suma
- Hace el reconocimiento de los paquetes recibidos
- Hace uso de las ventanas deslizantes para intercambiar información

A cada paquete que se envía se le asigna un identificador, para que el equipo que lo reciba devuelva una notificación de que ese paquete en particular ha llegado. Si luego de un tiempo predeterminado no se ha recibido la notificación del paquete, éste es reenviado a su destino nuevamente, pudiéndose producir la duplicidad si fue la notificación la que no llegó.

2.5.5 PROTOCOLO DE DATAGRAMA DE USUARIO

El UDP (User Datagram Protocol) proporciona los mecanismos para que los programas de aplicación se comuniquen con sus respectivos en otras máquinas, utilizando los *puertos*. Es un protocolo no confiable no orientado a conexión, en el que los programas de aplicación pueden utilizar sus propios controles de flujo y corrección de errores.

2.5.6 PROTOCOLO PUNTO A PUNTO

Este es un protocolo para líneas punto a punto. El PPP (Point to Point Protocol) proporciona una clara marcación de inicio y fin entre cada marco transmitido, detección de errores, un protocolo de control de enlace LCP (Link Control Protocol), y, además, un protocolo de control de red NCP (Network Control Protocol).

2.5.7 PROTOCOLO SENCILLO DE TRANSFERENCIA DE CORREO

Para que las máquinas intercambien correo se necesita que existe una comunicación TCP entre la máquina de origen y la de destino. El SMTP (Simple Mail Transfer Protocol) es un protocolo ASCII sencillo en donde la máquina emisora trabaja como cliente y la receptora como servidor. Esta última le indica a la primera si está o no apta para recibir el correo. Existen mensajes de confirmación de recibido o de error en la transmisión.

2.5.8 PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO

Este es el protocolo estándar de transferencia en el Web, el HTTP (HyperText Transfer Protocol) tiene dos elementos: las solicitudes de los vizualizadores a los servidores y el grupo de respuestas, cada solicitud recibe una respuesta que consiste en una línea de estado e información adicional. Este grupo de estándares describen cabeceras y cuerpos de mensajes con suficiente detalle.

Las páginas para Web se escriben con el HTML (HyperText Markup Language) que es un lenguaje de marcación, lo que quiere decir que se dispone de comandos específicos para el formateo del documento. Lo que permite que cualquier navegador sea capaz de leer el documento y reformatearlo según sea el caso. Este lenguaje permite incluir texto, gráficos y enlaces dentro de un documento.

2.5.9 PROTOCOLO SENCILLO DE ADMINISTRACIÓN DE REDES

El SMNP (Simple Network Management Protocol) proporciona una manera de administración y gestión de redes de información basadas en TCP/IP. Se basa en cuatro componentes: nodos administrados (cualquier equipo que sea capaz de informar su estado y correr un agente SNMP), estaciones administradoras (comunicación consulta-respuesta con los agentes), información de administración (la información se da en la estructura conocida como MIB *Management Information Base*, que es una base de información de administración) y un protocolo de administración.

2.5.10 PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS

El FTP (File Transfer Protocol) permite descargar archivos de servidores remotos hacia un host. El Web ha hecho más sencillo el manejo de FTP ya que en un principio este protocolo tenía una interfaz poco amistosa.

2.6 COMUNICACIÓN DE DATOS

Con base en los puntos anteriores, se analizarán las tecnologías más usadas dentro de la transmisión de datos digitales. Básicamente las tecnologías que se anotan a continuación están componiendo la subred, que es propiedad de las empresas que brindan el servicio de transmisión de datos, ya que son empresas que venden estos servicios, las redes son públicas.

2.6.1 SMDS

El servicio de datos conmutado de multimegabits SDMN (Switched Multimegabit Data Service) está diseñado para conectar varias LAN. Su diseño lo hizo *Bellcore* en 1980 y se lo puso a disposición del público a partir de 1990 y fue el primer servicio conmutado de alta velocidad. La figura 2.8 ejemplifica el uso de SDMS al conectar varias LAN.

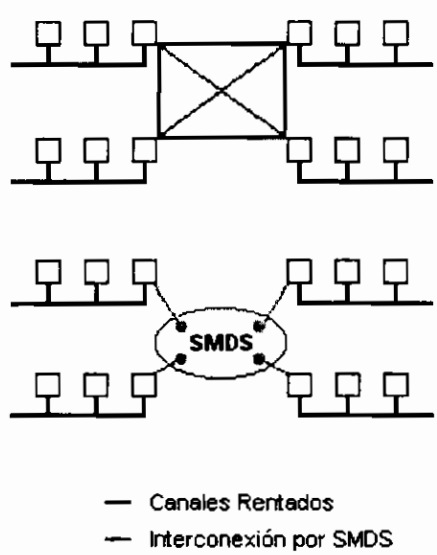


Figura 2.8 Comparación de interconexión de LAN

En la figura 2.8 se puede observar que es mejor contar con cuatro conexiones vía SMDS en lugar de con seis canales privados.

Por lo general los canales a SMDS forman parte de una MAN y usan DQDB, el mismo que se muestra en la figura 2.9.

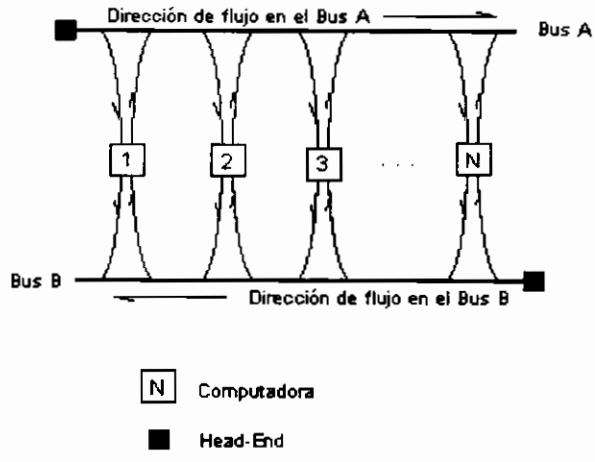


Figura 2.9 Red DQDB

El tráfico que maneja SMDS es un tráfico en ráfagas, lo que quiere decir que la transmisión de paquetes de una LAN a otra no se da en forma continua y la mayor parte del tiempo no hay datos para transportar. Esta es la razón para que resulte ineficiente y costoso tener líneas rentadas de datos. La velocidad estándar de una línea SMDS es de 45 Mbps. Para conectar varias LAN utilizando una MAN es necesario disponer de un cable que conecte la primera con la segunda, ésta con la tercera y así sucesivamente. Por otra parte utilizando SMDS, cada LAN debe conectarse al conmutador SMDS más cercano, con lo cual los paquetes serán ruteados a través de todos los conmutadores de la red, siendo éste un servicio sin conexión, es decir, sin garantía de entrega. La tecnología que utiliza es difusión.

Utilizando la función de preselección de direcciones, los usuarios pueden llegar a formar verdaderas redes privadas entre sus socios, sin dejar que usuarios ajenos lean mensajes privados o puedan enviar a destinos no autorizados.

2.6.2 X.25

La ex CCITT hoy UIT, emitió un estándar en 1970 para la comunicación en redes de conmutación de paquetes. En la capa física se encuentra el protocolo X.21, que utiliza señalización digital por lo que muchas redes telefónicas analógicas no pueden utilizar este protocolo, para solucionar este inconveniente se ha diseñado otro estándar muy parecido a RS-232.

En la capa enlace se han diseñado protocolos para controlar errores de transmisión.

La capa red se ocupa de asignar direcciones y de controlar el flujo, entrega y recepción de paquetes (lo que lo hace protocolo confiable) además de las interrupciones, esta característica permite contar con circuitos virtuales en los que viajan paquetes de información de hasta 128 bytes, con velocidades no mayores de 64 kbps.

Este protocolo hace el control de información de tal modo que un emisor de mayor velocidad no sature a un receptor de baja velocidad.

X.25 trabaja con dos tipos de circuitos virtuales:

- *permanentes* que son los que siempre están presentes y no requieren una llamada para que se establezcan y usarlos, se lo puede comparar con una línea rentada
- *conmutado* cuando una computadora envía un paquete y solicita que se llame a una host remota, una vez establecida la conexión se envía en orden los paquetes

Como se debe notar, no todas las host "hablan" X.25 para lo cual se emitieron los estándares conocidos como *triple X* dentro de los cuales están:

- X.3: trata del funcionamiento del ensamblador/desensablador de paquetes PAD (Packet Assembler Desassembler), que son equipos que conectan terminales con una red X.25
- X.28: define el protocolo entre un PAD y la terminal
- X.29: define el protocolo entre el PAD y la red

Este protocolo trabaja en las tres primeras capas del modelo OSI con las siguientes funciones:

- Física - Conexión física
- Enlace - Control de enlace
  - Creación de tramas
  - Control de errores
  - Control de flujo de enlace
  - Fiabilidad
- Red - Establecimiento del circuito
  - Control del circuito
  - Control de flujo del circuito
  - Direccionamiento

2.6.3 FRAME RELAY

Este protocolo de retransmisión de frame, es un sistema económico que maneja velocidades razonables, orientado a conexión que ofrece soluciones de comunicación entre dos puntos.

Es un protocolo simple, hace uso de los avances tecnológicos como son: la existencia de líneas digitales de comunicaciones libres de error, y computadoras rápidas y de bajo costo.

Son líneas virtuales permanentes entre dos puntos, igualmente es posible hacer conexiones punto a multipunto, en cada paquete se indicará que circuito virtual utilizar, lo que convierte a *frame relay* en un protocolo para conexiones punto a punto.

Como indica Andreu S. Tanenbaum, en su obra *Redes de Computadoras* "La diferencia entre una línea rentada real y una virtual es que, con una real, el usuario puede enviar tráfico durante todo el día a máxima velocidad. Con una línea virtual se pueden enviar ráfagas de datos a toda velocidad, pero el uso promedio a largo plazo deberá ser inferior a un nivel predeterminado." Por esta razón los proveedores de líneas de transmisión de datos cobran menos cuando se trata de una línea virtual, en comparación a una línea real.

Un circuito de frame ralay trabaja normalmente a 1,5 Mbps y a diferencia de los mismos circuitos de X.25 ofrece muchas menos funciones. Como por ejemplo ofrece un servicio básico de determinar el inicio y fin de un

frame y de detección errores, tal es así que si se recibe un marco errado es función del usuario detectarlo y volver a enviarlo, es decir, que no proporciona mensajes de recepción de marcos, ni control de flujo.

Este protocolo trabaja en las dos primeras capas del modelo OSI, con las siguientes funciones:

- Física - Conexión física
- Enlace - Direccionamiento
  - Creación de tramas
  - Control de errores
  - Gestión de interfaces

2.6.4 ISDN

Esta es una red diseñada con el objetivo de proporcionar una sola plataforma para intercambiar información en formato de: datos, video y voz. Esta característica da el nombre a esta red: *Red Digital de Servicios Integrados* ISDN (Integrated Services Digital Network).

"Esencialmente, ISDN es la integración de un rango amplio de servicios a una red sencilla de múltiples propósitos". Wayne Tomasi, *Sistemas de Comunicaciones Electrónicos.*

Los lineamientos básicos para este tipo de redes, fueron enunciados en 1984 por el CCITT en su recomendación CCITT I.120, en donde se mencionan los siguientes principios básicos y evoluciones de ISDN[10].

Principios

1) La característica principal del concepto ISDN es apoyar a un rango amplio de aplicaciones de voz (teléfono) y sin voz (datos digitales) en la misma red usando un número limitado de facilidades estandarizadas.
2) Las ISDN apoyan a una gran variedad de aplicaciones incluyendo conexiones conmutadas o no conmutadas (dedicadas). Las conexiones conmutadas incluyen conexiones de conmutación de circuito y de paquetes así como sus concatenaciones.
3) Siempre que introduzca nuevos servicios y prácticas una ISDN deben ser compatibles con conexiones digitales conmutadas de 64 kbps. La

[10] "SISTEMAS DE COMUNICACIONES ELECTRONICAS", Wayne Tomasi, Pentice Hall, 2da.Ed , 1996, pág. 595

conexión digital de 64 kbps es el bloque de construcción básico de ISDN.

4) Una ISDN contendrá inteligencia para proporcionar características de servicio, mantenimiento y funciones de manejo de la red. En otras palabras, de ISDN se espera que proporcione servicios más allá del simple establecimiento de llamadas de circuitos conmutados.
5) Una estructura de protocolo en capas debe usarse para especificar los procedimientos de acceso a una ISDN y puedan ser mapeados dentro del modelo de interconexión de sistemas abiertos (OSI). Los estándares ya desarrollados para las aplicaciones relacionadas con OSI pueden usarse para ISDN, tal como X.25 capa 3 para acceso a servicios de conmutación de paquetes.
6) Se reconoce que las ISDN pueden implantarse en una variedad de configuraciones de acuerdo a situaciones nacionales específicas. Esto acomoda una política nacional de fuente simple o competitiva.

Evolución

1) Las ISDN se basarán en los conceptos desarrollados para las ISDN telefónicas y pueden evolucionar progresivamente incorporando funciones adicionales y características de la red, incluyendo aquellas de cualquier otra red dedicada tal como conmutación de circuito y de paquetes para datos así como para proporcionar servicios a los existentes y nuevos.
2) La transición de una red existente a una ISDN comprensible puede requerir un período de una o más décadas. Durante este período, los cambios deben desarrollarse para la interconexión de servicios con ISDN y servicios de otras redes.
3) En la evolución hacia ISDN, la conectividad de extremos a extremo digital se obtendrá por medio de planta y equipo usados en las redes ya existentes, tal como la transmisión digital, multicanalización por división de tiempo y/o conmutación multiplexada de división espacial. Las recomendaciones relevantes existentes para esos elementos dispositivos de una ISDN están contenidas en la serie apropiada de

recomendaciones de CCITT y CCIR, hoy UIT-T y UIT-R respectivamente.

4) En las primeras etapas de la evolución de las ISDN, tal vez necesiten adoptarse algunos arreglos de red de usuario intermedio en algunos países para facilitar una penetración temprana de las capacidades del servicio digital.
5) Una ISDN evolucionando también puede incluir en sus etapas posteriores conexiones conmutadas a velocidades de bit mayores y menores de 64 kbps.

Existen tres tipos de canales que se pueden utilizar en una ISDN:

- Canal B de 64 kbps
- Canal D de 16 ó 64 kbps
- Canal H de 384, 1536 ó 1920 kbps

Para el caso de usuarios residenciales el acceso a ISDN contempla tres canales multiplexados por división en el tiempo TDM (Time División Multiplexing) full dúplex: dos canales B y un canal D de 16 kbps. A este enlace se lo conoce como *acceso básico*, 2B+D o interfaz de velocidad básica BRI (Basic Rate Interface). Uno de los canales B se utiliza para voz codificada digitalmente, el otro para aplicaciones como video, voz codificada PCM (Modulación por Codificación de Pulsos) y datos y el canal D para información de señalización y de control de red. La disponibilidad de canales BRI llega a 192 kbps incluidos los dos canales B, el canal D, tramas, sincronización y bits de encabezados. Se puede utilizar canales H para aplicaciones como audio de alta calidad y datos de alta velocidad.

Otro servicio que brinda ISDN en el *servicio primario* o interfaz de velocidad primaria PRI (Primary Rate Interface), el que proporciona múltiples canales B, siendo los más comunes:

- T1, 23B+D, utilizado en Estados Unidos, Canadá, Japón y Corea, velocidad de 1,544 Mbps
- E1 30B+D, utilizado en Europa, velocidad de 2,058 Mbps.

2.6.5 ATM

El *Modo de Transferencia Asincrónico* ATM (Asynchronous Transfer Mode) fundamenta la tecnología denominada ISDN de *banda ancha* o BISDN (Broadband ISDN). En 1988 el CCITT emite las recomendaciones de la serie I sobre BISDN: I.113, vocabulario de términos para los aspectos de banda ancha de ISDN, e I.121, aspectos de banda ancha de ISDN. BISDN surge de la necesidad de mayor ancho de banda para aplicaciones para las que ISDN *de banda angosta* (concepto original de ISDN) no era suficiente. Los servicios que se puede ofrecer en BISDN son:

- Interactivos, cuando el intercambio de información se realiza entre el usuario y el proveedor de servicio o entre dos usuarios, en los dos sentidos al mismo tiempo
- Distribución, cuando la información normalmente viaja desde el proveedor de servicios hasta el usuario

Una característica importante de BISDN es que los datos pueden transmitirse a diferentes velocidades dependiendo de las necesidades de la red, es decir, que la velocidad desde el usuario al proveedor es diferente que existe desde el proveedor al usuario, esta característica se denomina *transmisión asimétrica.*

Concretamente ATM es una forma de enviar y recibir datos desde BISDN en una forma independiente del tiempo. Una vez que los datos se encuentran en la red forman *celdas* que son ranuras fijas de tiempo. El canal de transmisión es virtual por lo que la ruta física y el tiempo de salida del paquete dependan de la disponibilidad de la red y derechos de acceso.

2.6.6 TECNOLOGÍAS DSL

Las tecnologías de *línea digital de suscriptor* DSL (Digital Subscriber Line) permiten conexiones de alta velocidad utilizando líneas telefónicas, además son conexiones dedicadas. El sistema se basa en el envío de información utilizando frecuencias diferentes a las utilizadas en el envío de voz (entre 300 Hz a 3400 Hz). DSL trabaja en un rango que va desde 25 kHz hasta 1.1 MHz.

Las cuatro técnicas dentro de la familia de xDSL son:

- HDSL: La denominada línea digital de suscriptor de alta tasa de bits HDSL (High bit-rate DSL), al contrario de la anterior HDSL es simétrica, es decir, que el ancho de banda es igual en las dos direcciones. Es una técnica mejorada para transmitir T1 y E1 sobre pares de cobre.
- SDLS: La denominada línea simple digital de suscriptor SDLS (Single line DSL), es la versión de HDSL para transmitir por un solo par de cobre líneas T1 y E1.
- VDSL: La línea digital de suscriptor de muy alta tasa de bits VDSL (Very high bit-rate DSL) permite velocidades muy superiores que el resto de la familia pero a distancias muy cortas.

La tabla 2.6 indica cada una de la tecnologías.

Nombre	Significado	Velocidad	Modo	Aplicación
DSL	Digital Subscriber Line	1.2 a 33.6 kbps	Dúplex	ISDN (voz y comunicación de datos
HDSL	High data rate Digital Subscriber Line	160 kbps	Dúplex	Servicios T1/E1, acceso a LAN y WAN, conexión de PBX
SDLS	Single line Digital subscriber Line	1.544 a 2.048 Mbps	Dúplex	Igual que HDSL más acceso para servicios simétricos
ADSL	Asymmetric Digital Subscriber Line	1.5 a 9 Mbps 16 a 640 kbps	Descendente Ascendente	Acceso a Internet, video bajo demanda, multimedia interactiva

Tabla 2.6 Tecnologás de acceso xDSL[11]

2.6.7 REDES PRIVADAS VIRTUALES

Una red privada virtual es una red de datos que hace uso de la infraestructura pública de telecomunicaciones, manteniendo la privacidad a través del uso de protocolos de túnel y procedimientos de seguridad.

Los servicios de comunicación de datos que ofrecen las redes privadas virtuales son gestionados extremo a extremo, consisten unir empresas y sus

[11] http://www.iies.es/teleco/publicac/publbit/bit107/quees.htm

2.6.7 REDES PRIVADAS VIRTUALES

Una red privada virtual es una red de datos que hace uso de la infraestructura pública de telecomunicaciones, manteniendo la privacidad a través del uso de protocolos de túnel y procedimientos de seguridad.

Los servicios de comunicación de datos que ofrecen las redes privadas virtuales son gestionados extremo a extremo, consisten unir empresas y sus socios, proveedores y clientes. Teniendo en cuenta aspectos de comunicación, configuración, mantenimiento, rendimiento y seguridad.

La forma de transporte de los datos se realiza mediante la técnica de tunelización, en donde los protocolos más utilizados son: GRE (Generic Routing Encapsulation), L2F (Layer 2 Forwarding), PPTP (Point to Point Tunneling Protocol) y L2PT (Layer 2 Tunneling Protocol).

La seguridad que mantienen una red privada virtual VPN (Virtual Private Network) se basa en la encripción de los datos, tema que será estudiado en el siguiente capítulo, para lo cual se utilizan, entre otros los siguientes algoritmos de encripción: DES, 3DES, RC-4.

Las aplicaciones que se pueden utilizar en una VPN son las siguientes:

- Interconexión de redes (LAN)
- Acceso a Internet de las sucursales sin tener que enrutarse por la oficina central
- Videoconferencia
- Redes privadas virtuales de Voz sobre IP
- Formación de Intranets
- Televigilancia
- Aplicaciones host-terminal
- Aplicaciones cliente-servidor
- Acceso remoto a bases de datos
- Construcción de bases de datos distribuidas

El *Tunneling*, es el procedimiento mediante el cual la información de un cierto protocolo es encapsulada dentro de otro protocolo. El tunneling tienen tres componentes:

- Protocolo Interno, protocolo viajero o protocolo de carga (Payload Protocol), que es el protocolo que está siendo encapsulado
- Protocolo Encapsulador (Carrier Protocol), que es el protocolo que se encarga de encapsular
- Protocolo de Transporte, protocolo extreno (Delivery Protocol), que es el protocolo que se encarga de transportar tanto al protocolo interno como al encapsulador

2.7 COMPUTACIÓN DE RED

La *computación de red* es la base para compartir la información hoy en día, ha cambiado la forma de manejarse de las empresas en todos los ámbitos: editorial, entretenimiento, ventas y tecnología. Raymond J. Lane de Oracle Corporation indica que "la computación de red es una manera más fácil, menos costosa y más confiable de manejar la información". Asimismo indica que la computación de red ha cambiado la forma de comunicación, como lo hizo en su tiempo el teléfono o la televisión, y se basa en utilizar las tecnologías de Internet junto con las tecnologías de comunicaciones disponibles, por lo que asegura que la computación de red es la conjunción de las computadoras y las redes de telecomunicaciones.

El intercambio de información hoy en día se realiza mediante el uso de software estándar en máquinas que están conectadas a redes en las que se manejan protocolos de Internet.

La computación como se la conoce hoy en día es el fruto de una constante evolución y una cambio sustancial desde los inicios de la era computacional. En la actualidad se está atravesando por la tercera etapa en lo que se refiere a redes de computadoras y de hecho por la interacción con los tres elementos que conforman los datos de computación[12]:

- La información que se recopila y usa
- Las aplicaciones como herramientas para manipular los datos
- Las interfaces que son la manera de presentar los datos

[12] "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economía Digital", Don Tapscott, McGraw Hill, 1ra. Ed., 1999, pág. 241.

2.7.1 PRIMERA ETAPA

La primera etapa de la computación hace referencia a los mainframes (figura 2.10) en la década de los 70, cuando toda la información, aplicaciones, presentación de la información, capacidad de almacenamiento y procesamiento, se encontraba en la misma máquina. La arquitectura que manejaban los mainframes era de relación única. Para acceder a la información los usuarios disponían de terminales no inteligentes las cuales presentaban la información en formato de texto.

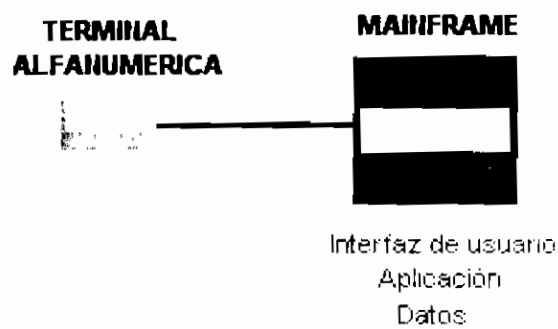


Figura 2.10 Primera etapa de la computación

Los mainframes eran escalables, confiables seguros pero sin tecnología para optar por una interfaz gráfica.

2.7.2 SEGUNDA ETAPA

El aparecimiento del microcomputador, las máquinas independientes y el *computador personal* originaron la segunda etapa, denominada cliente/servidor (figura 2.11). Esta base es muy utilizada hoy en día por muchas empresas. Los datos están compartidos en una máquina, la misma que puede ser un mainframe, minicomputador o incluso PC. Sin embargo, las aplicaciones y las interfaces se encuentran en las máquinas de los usuarios o clientes.

Esta etapa ha agregado dificultad al manejo de las aplicaciones y los datos. Lo negativo de este modelo es que las PC tienden a fallar y bloquear los datos, por lo que la logística es un asunto crítico en la administración de este tipo de modelo de red.

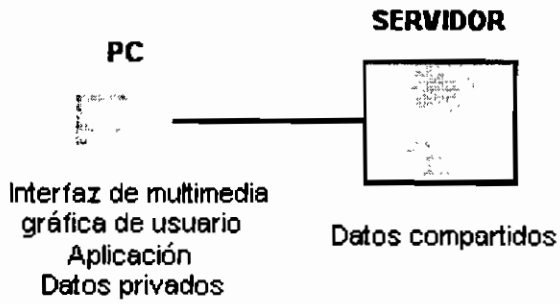


Figura 2.11 Computación cliente/ servidor

Consiste en sistemas en los cuales existen computadoras y, además, servidores; cada computadora generalmente se la asigna a un usuario y toma el nombre de cliente, en tanto que las máquinas que comparten su espacio se llaman servidores, de aquí se tiene el modelo cliente/servidor, su estructura y operación se puede observar en al figura 2.12. En este modelo el cliente envía una solicitud a un servidor para que realice un determinado trabajo, luego de lo cual el servidor envía la respuesta al cliente solicitante, generalmente los clientes tienen acceso a más de un servidor para realizar sus tareas.

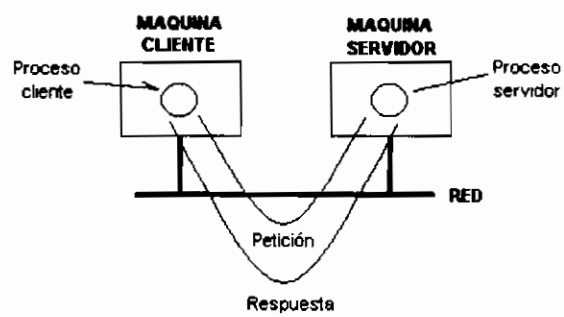


Figura 2.12 Modelo cliente servidor, estructura y operación[13]

2.7.3 TERCERA ETAPA

La tercera etapa es la computación de red, la misma que ha conjugado lo mejor de las dos etapas anteriores, haciendo más manejable la computación y mejorando la experiencia de los usuarios.

[13] "Redes de Computadoras", A S. Tanenbaum, Prentice Hall, 3ra. Ed., pág.4

Los costos de esta etapa son bajos por lo que es más asequible para muchas empresas.

Separa al cliente en dos pares, la interfaz está en la computadora del usuario sea éste un PC o una computadora de red NC (Network Computer). Las aplicaciones por su parte se encuentran en un servidor específico llamado *servidor de aplicaciones* y los datos están alojados en el *servidor de datos*. Se la ha denominado *arquitectura de tres capas*, como lo indica la figura 2.13.

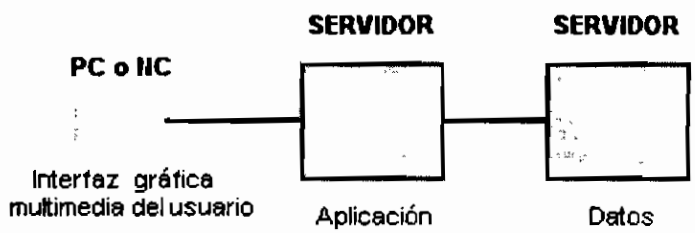


Figura 2.13 Arquitectura de tres capas

"Este modelo se aprovecha de la tendencia principal de la década: el traslado del valor del computador a la red". Raymond J. Lane, Oracle Corporation. Antes el valor lo daba la computadora, debía ser la más rápida, debía tener el mejor sistema operativo y las aplicaciones más actuales. Hoy el valor de la computadora está dado por la red a la cual está conectada. Para los usuarios y en general para las empresas, el tener acceso a la información en redes corporativas o públicas, como el Internet, es el principal objetivo.

2.8 REDES CON TECNOLOGÍA IP

Como se ha visto en la sección anterior, la tendencia tecnológica ha ocasionado que la información deba ser presentada de una manera ágil y al mismo tiempo sencilla, para que los usuarios puedan acceder a ella desde cualquier parte y con cualquier sistema. Con este antecedente, las empresas deben diseñar sus redes para que la información contenida en ellas la utilicen sus trabajadores.

Sin lugar a dudas la tecnología que se está utilizando con este propósito es la tecnología de Internet, por lo que es esta sección se analizan las tendencias de redes de información que utiliza las tecnologías mencionadas. La tabla 2.7 indica los tres tipos de redes que utilizan tecnología TCP/IP, definiéndolas utilizando sus diferencias.

	INTERNET	INTRANET	EXTRANET
Tipo de acceso	Abierto	Privado	Controlado
Usada por	Público	Miembros de la organización	Socios comerciales
Tipo de información	General	Propietarios	Compartida por selección

Tabla 2.7 Comparación de redes[14]

"Internet es divertida. Una Intranet ayuda a los empleados a hacer mejores trabajos. Una Extranet ayuda a la compañía a realizar un mejor trabajo." Richard H Baker, "EXTRANETS", 2000.

2.8.1 INTRANETS

Las *intranets*, como lo explica la tabla 2.7, es una red diseñada para un entorno privado, en donde la información está disponible solamente para los miembros de la organización.

Sin embargo, estas redes no solamente permiten el acceso interno sino también el externo debido a que algunas aplicaciones son orientadas a compartir información con empresas y profesionales que se encuentran fuera de las instalaciones de una empresa, y por lo tanto fuera del *cortafuegos* (firewall).

En un inicio las intranets no se diseñaron para compartir información. La existencia de un servidor de datos, no fue una solución práctica para poder disponer de la información de manera ágil, así mismo las aplicaciones de

[14] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág. 3.

cliente como por ejemplo hojas de cálculo, procesadores de palabras, son aplicaciones de uso individual.

La figura 2.14 da una idea de las aplicaciones que se han diseñado para la intranets, en donde se observa que algunas de ellas se orientan también al medio externo.

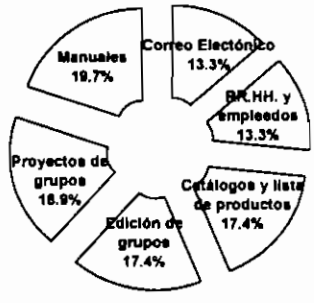


Figura 2.14 Prioridades en intranets[15]

Las tecnologías Web permiten el intercambio más fácil de información, por lo que los servidores de datos deben ser reemplazados por servidores web, en donde la información residirá y podrá ser encontrada de manera fácil. El repositorio de archivos y la compartición de espacio en disco más que de información, representan los servidores de datos.

La seguridad y niveles de acceso para edición y lectura de documentos web es un asunto de control administrativo de red.

Las ventajas de poner la información en una intranet son:

- Poder compartir información con menor esfuerzo, debido a que la actualización de los documentos se los realiza en un servidor Web, el cual actualiza de manera inmediata la información, que puede ser consultada en línea por otro usuario.
- La búsqueda de información se realiza con menor dificultad, con la ayuda de las herramientas de búsqueda se puede encontrar información independientemente de donde ésta se encuentre.

[15] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra Ed., 2000, pág. 4.

- Se reducen los costos de impresión y gasto de papel.

Más tarde o más temprano una intranet ofrecerá acceso controlado para el ingreso de clientes, proveedores y socios de negocios, convirtiéndose de esta manera en una extranet.

2.8.2 EXTRANETS

Las extranets tienen un potencial muy grande, ya que la división entre comunicación interna y comunicación externa, tomado a la comunicación como la relación entre personas y entre empresas y no orientada a las telecomunicaciones, tiende a desaparecer. Al formar redes con proveedores y clientes, las empresas tiene todavía una leve línea de división entré que debe ser externo y qué debe ser interno.

Las aplicaciones que se integran en una extranet, están orientadas a grupos de trabajo en donde se otorga valor a la información que se comparte, convirtiéndola en conocimiento. Así, tomando como base las intranets, el potencial de las extranet se observa en diferentes ámbitos:

- Hoy en día los grupos de trabajo en las empresas se conforman con personal que pertenece a diferentes departamentos, por lo que disponer de la información generada por ellos es fundamental, siendo la manera más eficiente las páginas web. Las extranets ayudan a conformar grupos de trabajo con personas ubicadas en diferentes ciudades e incluso en diferentes organizaciones, con lo que compartirán información de interés para las empresas involucradas.
- La información cruzada entre departamentos dentro de una misma empresa, es fundamental para lograr un eficiente desempeño de la organización. Las extranets dan la base para compartir información con socios orientado a mejorar procesos internos.
- La comunicación con trabajadores externos a la empresa es muy importante. La extranet es una forma de obtener información de primera mano de su oficina principal. Asimismo, los empleados externos pueden tener información de sus clientes, la cual alimentará la extranet realimentando los procesos de la empresa, las extranets permiten que

este proceso sea llevado a cabo por los mismos clientes y en forma directa.

Las aplicaciones disponibles para extranets son numerosas. Todas las aplicaciones diseñadas para una intranet pueden tener componentes externos, perteneciendo a alguno de los siguientes grupos:

- Comunicación de uno a varios equipos, departamentos o corporaciones, colocando la información en un página web.
- Aplicaciones que requieren de una interacción hacia ambos lados, por ejemplo cuando se trata de help desk (servicio al cliente) y soporte técnico.
- Colaboración que requiere interacciones de muchos a muchos, en el caso de foros de discusión, en los que se debe poner atención a quien debe y quien no debe intervenir, es decir, privacidad.

2.8.2.1 Beneficios

Richard Vallis de IDC indica refiriéndose a las extranets, que éstas "deben satisfacer una o más necesidades específicas de una mejor manera que cualquier otra alternativa".

Los diseñadores están convencidos de que al entregar navegadores, en lugar de un software complicado para intercambiar información, llegarán a más personas y éstas se adaptarán más fácilmente al modelo web.

Las extranets son útiles desde algunos puntos de vista[16].

Acceso inmediato a la información

La información que se puede presentar en una extranet la hace el medio de comunicación, tanto interna como externa, más adecuado. La información se la puede tener de manera inmediata, a un costo bajo y en una forma fácil de usar.

[16] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág.21-24

Libertad de elección

Al utilizar la tecnología de Internet, las extranet no se cierran sobre un solo fabricante sino que sus aplicaciones se pueden instalar en cualquier sistema operativo y sobre cualquier hardware.

Seguridad

La seguridad de hecho es mayor que en Internet, todo depende de las políticas de los administradores de la red deseen implantar, el siguiente capítulo se analizará las posibilidades de seguridad para ser implantadas en una extranet.

Facilidad de uso

El uso del protocolo HTTP facilita la *navegación* por la extranet, además este sistema es único y los usuarios no necesitan de ninguna otra herramienta para poder realizar su trabajo.

Costo de instalación moderado

Dependiendo del alcance y seguridades que se deseen brindar el costo de una extranet varía. Netscape considera que el costo promedio de instalación de una extranet es de $40,00 por usuario, lo cual resulta cómodo.

Costo de impresión y procesamiento más bajos

El ahorro de papel se ha presentado desde las intranets. El ejemplo más claro de este ahorro son los manuales de procedimientos de las empresas, antes se llegaba incluso a imprimir uno por empleado, hoy basta con publicarlo en la extranet, ya que es un documento en línea, todos tendrán acceso a él, al igual que a los cambios que el manual tenga.

Flujo de trabajo más simplificado

Los flujos de trabajos burocráticos se pueden mejorar con el uso de las extranets. Entre los trámites más comunes se puede mencionar: pedido de suministros, solicitudes (vacaciones, permisos, salidas, help desk, etc.) archivos de informes, etc.

Costos de capacitación más bajos

La capacitación es un factor muy importante y al utilizar tecnología Web resulta cómodo entrenar al personal cuando y en dónde lo necesite, por ejemplo se evita la movilización de empleados de las sucursales a la matriz.

Mejor dinámica de grupo

La información disponible en línea, los grupos de discusión, el correo compartido, ayudan a las personas a aprender de otros, lo que hace que los *grupos de colaboración* realmente funcionen. Estos grupos se pueden extender a los socios de negocios de la empresa, es decir, clientes, proveedores e incluso a la *competencia* que como se mencionó en el capítulo anterior ahora se deben considerar como aliados de negocios.

2.8.2.2 Desventajas

Naturalmente no todo es color del oro, también existen algunas dificultades con la tecnología web y con la implantación de las extranets.

La primera y mayor dificultad con la que se puede topar una empresa, es la relación costo beneficio y las utilidades que se generarían al ingresar en una extranet.

Para obtener los costos más reales de implantación de una extranet se deben tomar en cuenta los tiempos del personal, capacitación, soporte técnico a los usuarios y el desarrollo de aplicaciones. Todo esto unido al costo del hardware según Meta Gruop multiplica por más de 100 el valor mencionado por Netscape, llegando a la cantidad de $4.100,00 por usuario.

Los costos ocultos pueden estar dentro de alguna de las siguientes categorías[17]:

- Soporte para múltiples navegadores
- Actualizaciones necesarias del hardware
- Diseñar nuevamente los procesos comerciales
- Firewalls
- Administración del sistema
- Integración de bases de datos y otras aplicaciones existentes
- Complicaciones de todo tipo
- Desarrollo y mantenimiento del contenido
- Control de la versión del navegador
- Instalación y mantenimiento de líneas de comunicaciones de alta velocidad
- Administración de bibliotecas de aplicaciones de Internet
- Aumento en los costos de producto

Esto convierte a los 4.100 en una cifra cercana a los $16.400,00 por usuario.

2.8.2.3 Aplicaciones de las Extranets

Como las extranets se basan en tecnología web existen aplicaciones propias de ella como son: correo electrónico, colaboración de grupo, comunicación de audio y video en tiempo real, publicar información, búsquedas, directorios. Todas éstas se aplican a las extranets, siendo aplicaciones rutinarias o aplicaciones diseñadas a medida y que cumplen una función específica.

- Registrar de pedidos, recibir facturas, rastrear embarques, procesar pagos.
- Compartir información orientada a desarrollos de proyectos conjuntos, entre personal de distintas organizaciones, lo que hace que trabajen como un solo grupo.

[17] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág.25.

- Comunicación clara, las extranets proporcionan una plataforma estándar para divulgar la información.
- Help desk, en donde los clientes pueden encontrar información de soporte y de apoyo orientados a solucionar sus problemas más frecuentes.
- Las corporaciones multinacionales pueden llegar a tener varios sistemas de correo electrónico incompatibles entre sí, la base de una extranet puede solucionar este problema estandarizando el servicio de mensajería hacia todos los sistemas dispersos de la organización.
- Acceso a las bases de datos distribuidas de una organización, naturalmente este acceso lo tendrán las personas autorizadas.

2.8.2.4 Construcción y Componentes de las Extranets

2.8.2.4.1 Construcción

La extranet depende del control de acceso que se le otorgue a una intranet, ya que las dos tiene muchas similitudes en principio la diferencia es que la intranet es principal y exclusivamente hacia el interior de la organización, no así la extranet que ve también hacia el exterior.

Para poder diseñar una extranet se deben tomar en cuenta los siguientes aspectos:

- Utilizar protocolos de comunicaciones conocidos (TCP/IP)
- Utilizar estándares conocidos (HTML, FTP, SMTP)
- Utilizar métodos conocidos (administración y seguridad)

2.8.2.4.2 Componentes

Independientemente de cómo se acceda a la extranet, la siguiente es una lista de componentes clave[18]:

- Una distribución universal de TCP/IP
- Navegador Web
- Servidor Web

[18] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág.79.

- Servidor de acceso remoto
- Software cliente para uso telefónico
- Dispositivo de conexión a Internet
- Seguridad de firewall

2.9 NEGOCIO ELECTRÓNICO Y REDES DE INFORMACIÓN

Las aplicaciones que se han diseñado para extranets son:

- Ventas y mercadotecnia
- Desarrollo de productos
- Servicio al cliente
- Recursos humanos
- Financieros

Como se puede ver, todas las aplicaciones mencionadas tienen que ver, de una manera u otra, con el Negocio Electrónico. A continuación se analiza cada una de ellas.

2.9.1 VENTAS Y MERCADOTECNIA

Poder contar con información actualizada en cualquier parte del mundo es un reto grande.

Desde el punto de vista de las ventas la información en forma correcta y en el momento justo hace la diferencia entre el éxito y el fracaso. La extranets puede proporcionar información sobre:

- Productos y catálogos
- Prospectos para portafolio de ventas
- Información de la competencia
- Calendario de actividades relacionadas con ventas
- Capacitación para el momento preciso
- Material de ventas

Para la gente de mercadeo la información básica gira en torno a los clientes de su empresa y sus prospectos. Los sistemas de ventas y mercadeo se encuentran muy relacionados, es así como en cada paso de las ventas debe haber un proceso logístico. Las extranets permiten

mantener comunicados la fuerza de ventas, con la oficina principal usando páginas web, además, compartir información contable de una manera segura.

2.9.2 DESARROLLO DE PRODUCTO

La aplicación de extranets, no necesariamente llega a los clientes en forma directa, sino más bien por medio del personal de la empresa que tienen acceso a la red. Al igual que el punto anterior, los grupos de desarrollo de productos necesitan información actualizada y en línea, básicamente para poder manejar los proyectos adecuadamente y tener la perspectiva de los clientes acerca de sus productos, es aquí donde funciona la extranet. La información relacionada con productos que puede *publicarse* en una extranet es:

- Cambios de diseño, catálogos, cambios de cronogramas
- Grupos de trabajo, desarrolladores, áreas de responsabilidad
- Sugerencias y comentarios de clientes
- Especificaciones de productos de la competencia

2.9.3 SERVICIOS AL CLIENTE

De hecho éste es un aspecto de más contacto externo para la empresa. Es muy importante que por medio de las extranets, una organización pueda tener realimentación por parte de sus clientes, así como también es importante para los clientes que puedan dar sus opiniones en forma sencillas y sin complicaciones, además de saber que sus inquietudes van a ser contestadas con prontitud.

Las extranets, en lo que tiene que ver con servicio al cliente pueden proporcionar información acerca de:

- Consultas puntuales sobre temas de interés para sus clientes
- Problemas frecuentes y orígenes de los mismos
- Intercambio de soluciones entre los empleados, sobre problemas repetitivos o experiencias aisladas
- Cambios sobre alguna información importante, originados en los grupos de noticias

2.9.4 RECURSOS HUMANOS

Esta en una aplicación típica para una intranet, pero esto no implica que sea solamente para ese tipo de red. El personal es el principal uso de esta aplicación, las personas pueden poner su currículum en la red y vía correo electrónico enviar y recibir peticiones. Esto se hace más sencillo cuando se utilizan formas realizadas con formato HTML.

Las aplicaciones de recursos humanos menos *externas* son:

- Información de prestaciones y paquetes opcionales
- Manuales de procedimientos y políticas
- Estrategias de las empresas
- Promociones internas de puestos de trabajo
- Teléfonos importantes internos
- Informes e información de departamentos y de personal
- Encuestas realizadas a los empleados
- Información de asistencia y faltas del personal

2.9.5 FINANCIEROS

El componente externo de esta aplicación es la administración de las compras. El departamento de adquisiciones puede publicar una página en donde se encuentren los suministros y equipos disponibles para uso interno, así, como también un sistema de administración de compras que centralice los pedidos de una organización y al mismo tiempo solucione asuntos de facturas, cuentas por pagar y facturación. Las finanzas de una organización son principalmente internas, pero siempre existe el flujo de información hacia el exterior, por ejemplo los informes a las instituciones públicas.

CAPÍTULO 3

Transacciones Electrónicas Seguras

3.1 INTRODUCCIÓN

La seguridad ha sido un dolor de cabeza para los administradores de redes de telecomunicaciones, como indica un estudio realizado en 1997 por la firma Strategic Focus Inc, el cual dice que la principal preocupación de los administradores es, justamente, la seguridad.

Ningún sistema es totalmente seguro, todas las seguridades que el hombre pueda inventar, más tarde o más temprano serán violadas, y se deberá volver a pensar en otras que a su vez caerán. La idea es tener sistemas que pongan obstáculos a los agresores, de tal manera que el tiempo que tengan entre el inicio del ataque y su terminación sea el mayor posible. De esta manera se pueden generar las alarmas del caso y alertar de que el sistema está siendo atacado, para en último de los casos desconectarlo y así defender la integridad de la información.

Los riesgos de realizar Negocio Electrónico son grandes, desde el punto de vista de seguridad, lo que se persigue es minimizarlos, ya que como se ha indicado su anulación total es imposible.

Algunos puntos de vista a ser tomados cuando se planifica la seguridad son, por ejemplo: controlar el acceso a la información, reducir el riesgo de que el servidor sufra un ataque, tener procedimientos de contingencia en el caso de un ataque, temas legales acerca de la seguridad y privacidad.

La gran cantidad de datos que residen en una red de información pueden sufrir alteraciones o daños, por lo que se debe tener muy claro las fuentes de donde pueden provenir, para de esta manera tener planes de acción así como estrategias de seguridad y planes de contingencia adecuados. Todas estas estrategias y estos planes deben estar orientados a que los sistemas tengan un *tiempo de caída* que sea el menor posible y que éste no afecte de ninguna manera las operaciones de la organización.

Además, se debe tener claro que es más costoso recuperarse de un incidente relacionado con la seguridad, que implementar medidas preventivas. La seguridad es un conjunto de prácticas, políticas, procedimientos y tecnologías orientadas a proteger una organización de comportamientos inesperados, tanto de las personas como de los equipos.

En este capítulo se analizará las técnicas y protocolos más utilizados para realizar las transacciones electrónicas seguras y poder garantizar la mayor privacidad o reserva que el Negocio Electrónico necesita para funcionar de manera adecuada. Todos los procedimientos deben estar sustentados por leyes, para lo cual se observarán las leyes que en este sentido existen en el Ecuador.

3.2 INTEGRIDAD Y SEGURIDAD DE LOS DATOS

La *integridad* de los datos se refiere a su estado en relación con la pérdida o alteración de la información, es decir, los datos almacenados están seguros y son los correctos. Se habla de un estado inalterado y completo, la cualidad de ser indivisible.

"El objetivo de la integridad de los datos es mantener los datos y la información de los sistemas de computadoras en un estado completo e inalterado."[1]

La *seguridad* se refiere al estado de los datos en cuanto a su pérdida o destrucción intencional, es decir, que los datos están libres de daños. Además, la seguridad tiene que ver con medidas de protección contra espionaje, sabotaje, crimen, ataque y fuga.

La figura 3.1describe las posibles amenazas a la integridad y seguridad de los datos.

[1] "LAN TIMES: GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J Hsu, McGraw Hill, 1ra. Ed., 1998, pág. 14

Figura 3.1 Amenazas a la integridad y seguridad de los datos

3.2.1 INTEGRIDAD

3.2.1.1 Amenazas Humanas

El mayor obstáculo para que los sistemas sean completamente fiables son las personas que los utilizan, tanto los usuarios finales como los administradores de las redes. Entre las amenazas humanas se tiene:

- Accidentes
- Inexperiencia
- Estrés y pánico
- Falta de comunicación
- Venganza
- Avaricia

3.2.1.2 Errores de Hardware

Estos errores se producen debido a que los aparatos físicos no tienen una vida indefinida, incluidos los equipos de cómputo.

Los errores de hardware más comunes son los siguientes:

- Fallos de disco
- Fallos de controladores de entrada/salida
- Fallos de energía
- Fallos de memoria
- Fallos en medios y dispositivos
- Mal funcionamiento del chip y de la placa base

3.2.1.3 Errores de la Red

Las fallas de una red se puede presentar en cualquier momento, debido a que las líneas de comunicaciones están expuestas a una serie de riesgos que incluyen interferencias y averías.

Las amenazas para los datos que generan los errores en la red son:

- Fallos en los controladores y en las tarjetas de interfaz de red
- Problemas en componentes de red
- Problemas de radiación e interferencia

3.2.1.4 Problemas de Tipo Lógico

El software es otro factor que puede afectar a los datos. Los problemas en cuanto al software se enumeran a continuación:

- Errores
- Corrupción de archivos
- Errores de intercambio
- Errores de almacenamiento
- Errores del sistema operativo
- Requisitos mal definidos

3.2.1.5 Desastres

Es probablemente la amenaza más devastadora contra la integridad de los datos. Ha sido motivo de estudio por más de quince años, el cómo recuperar los datos luego de producirse un desastre natural o provocado.

Los desastres que afectan a los datos pueden son los siguientes:

- Incendios
- Inundaciones
- Tormentas
- Accidentes industriales
- Sabotaje y terrorismo

La tabla 3.1 indica las herramientas que se pueden utilizar para mejorar la integridad de los datos. Como se puede observar existen dos tipo de técnicas: las preventivas y las correctivas. Las primeras están orientadas a

mantener la integridad de los datos cuando éstos surgen, es decir, cuando ocurren. Las correctivas son para recuperar los datos una vez ocurrida la falla y la pérdida de los datos.

TECNICA	TIPO
Copias de seguridad	Correctiva
Técnicas de espejo	Preventiva
Archivado	Preventiva
Custodia	Correctiva
Administración jerárquica del almacenamiento	Preventiva
Chequeo de paridad	Preventiva
Planificación de recuperación frente a desastres	Correctiva
Análisis predictivo de fallos	Preventiva
Alimentación ininterrumpida	Preventiva
Implementación de técnicas de seguridad	Preventiva

Tabla 3.1 Mejoramiento de la integridad de datos[2]

3.2.2 SEGURIDAD

3.2.2.1 Amenazas Físicas

Se trata de no permitir que otras personas u organizaciones tengan lo que es de otros, ni que tampoco espíen información ajena. Las amenazas físicas más comunes son:

- Robo
- Dumpster diving (escarbar en los basureros)
- Espionaje
- ID falsos

3.2.2.2 Basadas en los Cables

Las redes de computadoras han aportado amenazas de seguridad adicionales, a continuación se listan algunas:

[2] "LAN TIMES: GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J Hsu, McGraw Hill, 1ra Ed., 1998, pág. 34

- Escuchas
- Marcación de un número de teléfono
- Imitación

3.2.2.3 Autentificación

Esta propiedad de las redes indica que usuarios pueden solicitar o incluir información dentro de un servidor. Las amenazas más comunes en lo que se refiere a la identificación de usuarios son:

- Captura de contraseñas
- Averiguación de contraseñas
- Suposiciones hechas en algoritmos
- Edición de contraseñas

3.2.2.4 Programación

Las amenazas contra la seguridad más interesantes provienen de códigos de programación, siendo los más probables:

- Virus
- Códigos bomba
- Caballos de Troya
- Actualizaciones y cargas

3.2.2.5 Puertas de Escape de los Sistemas

Fueron creadas para resolver problemas de usuarios, pero eventualmente puede ocasionar problemas de seguridad, los más conocidos son:

- Piggybacking
- Servicios no seguros
- Configuración en iniciación

La tabla 3.2 indica las herramientas más utilizadas contra la falta de seguridad de los datos. El ámbito de implementación de las recomendaciones está dado por políticas en el ámbito de todo el sistema, o por políticas que deben ser comunicadas al personal para que éste las ponga en práctica.

RECOMENDACIÓN	AMBITO
Eliminación de las puertas traseras del sistema	Sistema
Chequeo de virus	Sistema
Seguridad física	Empleados
Política de máquinas desatendidas	Empleados
Política de eliminación de basura	Empleados
Política de contraseñas	Empleados
Cifrado	Sistema
Obligación de identificación	Sistema
Cortafuegos para acceso a Internet	Sistema
Trampas para intrusos	Sistema

Tabla 3.2 Mejoramiento de la seguridad de los datos[3]

3.3 CRIPTOGRAFÍA

El principal objetivo de la criptografía es la confidencialidad. La confidencialidad de la información se convierte en un problema cuando ésta viaja por una red a la cual están atadas muchas computadoras o peor aún si viaja por el Internet. La información debe ser alterada para que pueda ser reconocida exclusivamente por las máquinas a las que va dirigida, este proceso de conoce como *cifrado de la información*.

Cifrar la información significa revolver los datos para que parezca que los bits han sido generados en forma aleatoria y sin sentido, pero que tengan la posibilidad de ser recuperados. Esta es la base de la criptografía (escritura secreta).

Desde hace miles de años se ha utilizado la criptografía basada en dos técnicas que son la sustitución y la trasposición. La primera cambia las letras de un mensaje por otras siguiendo un esquema determinado, la segunda revuelve los caracteres del mensaje.

En la actualidad las computadoras han permitido tener encriptación utilizando los dos métodos al mismo tiempo.

[3] "LAN TIMES: GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J Hsu, McGraw Hill, 1ra Ed., 1998, pág. 37

La forma de cifrar los datos, para que no sean interpretados por cualquier ente, es un *algoritmo*, el cual es de conocimiento general. Estos algoritmos de cifrado toman la información original y utilizando un operador denominado *llave,* la transforman, originando el texto o mensaje cifrado. Aunque otras personas conozcan el algoritmo, si no poseen la llave correcta no podrán acceder a la información o texto original.

Dentro de la encriptación o codificación de mensajes existen dos procesos que son complementarios:

- Encriptación: este proceso toma el texto original o normal y lo transforma en un mensaje cifrado utilizando una función conocida como algoritmo de encriptación y una llave de codificación o encriptación especial.
- Desencripción: este proceso es el inverso del anterior, es decir, se toma el texto cifrado y se lo convierte nuevamente en el texto normal utilizando una llave de desencripción. En algunos sistemas las llaves de encripción y desencripción son las mismas y en otros sistemas no.

"La idea básica es que la confidencialidad de la información cifrada se encuentra a salvo porque existen tantos posibles valores de llaves diferentes que es 'completamente imposible' probarlos todos para descubrir el correcto."[4]

Las funciones de la criptografía pueden resumirse en estas cuatro características:

- *Confidencialidad*: cuando la información viaja por medios de telecomunicaciones debe ser protegida de cualquier intento de interceptación y de acceso al contenido de los datos de forma no autorizada.
- *Autenticación*: el uso de las firmas digitales sirven para identificar a los autores de los mensajes.
- *Integridad*: la verificación de si un mensaje ha sido modificado en la ruta hacia su destino tiene varios métodos, la firma digital o el compendio de mensajes.
- *No-repudiación*: para evitar que el autor de un mensaje niegue su envío.

[4] "LAN TIMES· GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J Hsu, McGraw Hill, 1ra Ed , 1998, pág 222

3.3.1 ALGORITMOS Y FUNCIONES CRIPTOGRÁFICAS

3.3.1.1 Algoritmo de llave simétrica

Utilizan la misma llave para cifrar y descifrar los mensajes. También se conocen como algoritmos de llaves secretas. Normalmente estos algoritmos son más rápidos y fáciles de implementar que los de llave pública. El problema es que si dos puntos desean intercambiar información utilizando este tipo de llaves, primero deben intercambiar de forma segura la llave con la cual se realizará la comunicación.

Encriptan flujos o bloque de datos, son muy rápidos y tienen un número elevado de llaves.

Los algoritmos de bloque cifran los datos por bloques, en cambio los de flujo cifran byte por byte.

3.3.1.1.1 DES

Fue desarrollado por IBM en los años 70, se encuentra aceptado por la ANSI y la Oficina Nacional de Estándares de los Estados Unidos de Norteamérica.

El *Estándar de Cifrado de Datos* DES (Data Encrytion Standard) es un algoritmo de llave simétrica o llave secreta, utiliza 56 bits, fragmentando los datos en grupos de 64 bits, estos valores constituyen un secreto de estado. Los bloques de 64 bits son sometidos a 16 fases de transformación, cada fase cuenta con una llave de transformación de 48 bits cuyo valor se obtienen de la llave completa de 56 bits. En cada fase los datos y el valor de la llave se introducen en cajas "S" que se encargan de revolver los datos siguiendo una función. A la salida se tiene un flujo de bits *desordenado* y sin ningún sentido, sin embargo, el flujo original de 64 bits se puede volver a obtener aplicando en orden inverso el proceso de cifrado, es decir, descifrando el grupo con la misma llave maestra de 56 bits que se utilizó en un inicio.

Por causa del desordenamiento de los bits, DES es más eficiente realizarlo por hardware que por software, por este motivo los piratas cibernéticos han encontrado dificultades para realizar sus ataques, debido

que para hacerlo deben contar con el hardware diseñado para este propósito.

Pese a las bondades del algoritmo DES, hoy en día se deberían invertir varios cientos de miles de dólares para construir una computadora que sea capaz de romper las llaves de cifrado y obtener el mensaje original, es claro que este algoritmo no es el adecuado para cifrar transacciones bancarias de billones de dólares.

Siendo la debilidad del algoritmo DES que la longitud de su llave es corta, se ha sugerido cifrar los mensajes tres veces utilizando el algoritmo, a esto se lo ha denominado triple DES, para lo cual se utilizan dos llavés K1 y K2 como sigue: se cifra el mensaje utilizando K1, al resultado se lo descifra utilizando K2, y a éste se lo cifra utilizando K1 nuevamente. Este proceso toma el nombre de EDE (Encrypt Decrypt Encrypt).

3.3.1.1.2 IDEA

El *Algoritmo Internacional de Cifrado de Datos* IDEA (International Data Encryption Algoritm) fue desarrollado en el Instituto Tecnológico Federal Suizo en 1990, también es un algoritmo de llave simétrica de bloques de 64 bits. IDEA utiliza llaves de cifrado de 128 bits, es muy similar al DES en su forma de operación, la diferencia radica en que los datos no son desordenados, por lo que su aplicación se la puede hacer por hardware o por software. Además, este software fue internacional y no tuvo el impedimento de venta en todo el planeta que tuvo DES, que por ser desarrollado en Estados Unidos se prohibe su venta fuera de ese país sin el consentimiento expreso del gobierno.

3.3.1.1.3 RC2

Ronald Rivest, desarrolló este algoritmo de bloque, en 1996 se divulgó en Usenet como mensaje anónimo. RC2 al implementarse permite llaves de 1 a 2048 bits. Tiene varias versiones posteriores como RC4 y RC5. Este último permite que la longitud de la llave, del bloque de datos y el número de pasadas de encripción sean valores que defina el usuario.

3.3.1.2 Algoritmo de llave pública

Utilizan una llave para cifrar el mensaje y otra para descifrarlo. Normalmente la llave de cifrado se conoce como llave pública (se la puede divulgar) y la que se utiliza para descifrarlo se conoce como llave privada. Cuando se desea intercambiar llaves en forma segura para iniciar una comunicación confidencial se utilizan estos algoritmos, sin embargo son demasiado lentos hasta el punto de que una encripción y desencripción con llave pública se ejecuta de diez a cien veces más lento que un algoritmo similar de llave simétrica.

La idea de estos algoritmos es que utilizando dos llaves se puede cifrar y descifrar un mensaje, estas dos llaves en principio no están relacionadas. Este tipo de algoritmos no han tenido el desarrollo de los de llave simétrica debido a que implican un desarrollo matemático grande e investigación de problemas matemáticos con propiedades específicas.

3.3.1.2.1 Algoritmo de intercambio de claves Diffie-Hellman

En 1979 en la Universidad de Stanford, Whitfield Diffie y Martin Hellman descubrieron un método para establecer una sesión segura entre dos individuos, cuando el intercambio de mensajes se realiza en un medio donde existen cientos y miles de participantes, esto se conoce como criptografía de llave pública. Este algoritmo se basa en el principio matemático de que teniendo dos números públicos P y r (raíz primitiva de P) y dos participantes con cifras A y B respectivamente, si P es suficientemente grande es muy difícil obtener A si solamente se conocen P, r y r^A , para esto P debe ser por lo menos de 500 bits. La criptografía pública es muy costosa en tiempo ya que maneja llave muy extensas. Este algoritmo, sin embargo, no tiene la posibilidad de averiguar si la persona con la cual se ha establecido la comunicación es la verdadera o simplemente en un impostor. Por esta razón Diffie-Hellman se emplea con algún tipo de sistema de identificación, para asegurarse que la persona con la que se intercambia información sea la verdadera.

3.3.1.2.2 RSA-llave pública/llave privada

Funciona utilizando un par de llaves, las cuales funcionan de manera concatenada, lo que se ha cifrado con la una, solamente puede ser descifrado con la otra. Cada usuario genera dos llaves, la una la mantiene secreta mientras que la otra la hace pública.

RSA (Rivest, Shamir y Adleman del MIT) puede utilizarse para identificación, para cifrado o ambos. Por ejemplo si lo que se desea es enviar un mensaje cifrado, lo que se hace es cifrarlo utilizando la llave pública del destinatario, si lo que se desea es identificar a una persona, el mensaje se cifrará con la llave privada del remitente. El problema surge cuando cualquiera puede enviar un mensaje privado a un destinatario específico, utilizando su llave pública. De igual modo cualquiera puede leer el mensaje enviado desde un origen específico utilizando la llave pública del remitente. Lo que se hace para llevar el trabajo de procesamiento a niveles aceptables, debido a la extensión de la llave que es de 500 bits (puede alcanzar 2000 bits), es elegir una llave de sesión aleatoria DES, triple-DES o IDEA. Utilizando técnicas RSA cifrar esa llave, así el receptor emplea su llave privada para abrir el mensaje, ve quien es el remitente y utilizando la llave pública de éste recupera la llave de sesión.

3.3.1.3 Criptosistemas híbridos

En estos sistemas la criptografía de llave pública se utiliza para intercambiar la llave de sesión, la que se utiliza como base para los algoritmos de llave simétrica. De hecho casi todos los sistemas implementados de llave pública son sistemas híbridos.

3.3.1.4 Funciones de síntesis o compendio de mensajes

Este tipo de funciones han alcanzado gran popularidad en los últimos años. Consisten en generar un patrón de bits único (objetivo de las funciones) o casi único, a partir de un mensaje, el cual no sea factible de procesamiento, se consideran como las huellas digitales de los archivos.

Son funciones de un solo sentido, es decir, que no se puede recuperar el mensaje original a partir de un compendio dado.

Si se altera un solo bit de la síntesis el resultado de la recuperación del mensaje puede ser cualquier cosa, menos el mensaje original.

Estas funciones combinan ciertas propiedades matemáticas[5]:

- Cada bit de la función de síntesis o compendio de mensajes sufre la influencia de cada bit de la entrada de la misma función
- Si se modifica cualquier bit de la entrada de la función, cada bit de salida tienen 50% de probabilidad de cambiar
- Dado un archivo de entrada y su compendio correspondiente, debe ser no factible computacionalmente encontrar otro archivo con el mismo valor de compendio

Las funciones de síntesis más utilizadas en la actualidad son las siguientes:

- *HMAC* Código de Autenticación de Mensajes por Hash. Se hace referencia a esta función en la RFC 2104, fortalece una función de síntesis haciéndola resistente a un ataque externo, aún si la función es violada.
- *MD2* Compendio de Mensajes #2. Es la función más segura desarrollada por Ronald Rivest, así mismo es la que más se demora en calcular. El compendio es de 128 bits.
- *MD5* Compendio de mensajes #5. También desarrollado por Rivest incluye técnicas para hacerlo más seguro que su predecesor MD4 (originado del MD2), del cual se descubrió que arrojaba dos síntesis iguales a partir de dos documentos diferentes. Produce un compendio de 128 bits.
- *SHA* Algoritmo Seguro de Hash. Desarrollado por la NSA para aplicarse junto con el estándar de firmas digitales DSS del NIST. Produce un compendio de 160 bits.

[5] "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed., 1999, pág. 202- 203

- *SHA-1* Revisión del SHA. Es posible que sea más seguro que SHA con las modificaciones introducidas, igualmente produce un compendio de 160 bits.

3.3.2 ATAQUES CONTRA ALGORITMOS DE ENCRIPTACIÓN Y FUNCIONES DE COMPENDIO

Para que los sistemas criptográficos sean útiles, deben ser capaces de resistir a ataques directos. La mejor forma de comprobar si un algoritmo es confiable es publicarlo y esperar que alguien le encuentre una debilidad.

3.3.2.1 Contra algoritmos simétricos

3.3.2.1.1 Ataques de búsqueda de llaves (fuerza bruta)

Los ataques de fuerza bruta consisten en probar todas las llaves posibles. No existe manera de proteger los sistemas contra este tipo de ataques, sin embargo, no son muy efectivos debido a la gran cantidad de llaves por probar. Por ejemplo para el caso del algoritmo DES de 56 bits, existen 7.213[2]895.789[1]838.340 posibles llaves, que se expresan en números hexadecimales. Si se dispone de una computadora que calcule mil millones de llaves por segundo, le tomaría aproximadamente 834 días el rastrear todas las posibles combinaciones. Por otro lado si el algoritmo es de 128 bits la cosa cambia radicalmente ya que se necesitarían 1013 años, contando con mil millones de computadoras que procesen mil millones de llaves por segundo para probar las 3.4×10^{38} posibles llaves.

3.3.2.1.2 Criptoanálisis

La longitud de las llaves no es el único factor para la seguridad de un código y no habría ningún problema en el campo del cifrado de datos, como se ha visto se utilizarían llaves de 128 bits y la criptografía desaparecería. Los ataques de fuerza bruta son rara vez necesarios para acceder al contenido de un mensaje cifrado, en muchas ocasiones con la ayuda de las matemáticas y una buena computadora se puede descifrar un mensaje sin conocer siquiera el algoritmo de encriptación.

Los ataques más comunes de criptoanálisis son:

- *Ataque de texto llano conocido*: se debe contar con el texto llano y el texto cifrado, para poder encontrar la llave de cifrado y posiblemente el algoritmo para poder descifrar otros mensajes.
- *Ataque de texto llano elegido*: el atacante incita a cifrar textos conocidos para poder analizarlos y obtener la llave de cifrado.
- *Criptoanálisis diferencial*: el ataque se produce sobre textos cifrados con ligeras diferencias, procediendo como en el caso anterior.
- *Análisis diferencial de fallas*: este ataque se efectúa sobre el hardware de cifrado. Se expone al equipo a factores ambientales de tal suerte que cometa errores en el momento de encriptar o desencriptar la información, estas fallas se estudian y a partir de ellas se puede conocer la llave e incluso el algoritmo.

3.3.2.1.3 Ataques basados en el sistema

La otra forma es atacar al sistema de cifrado sin atacar al algoritmo en sí. Para que la criptografía funcione correctamente, no solamente se debe contar con un algoritmo poderoso, sino también contar con un sistema robusto que evite ataques.

3.3.2.2 Contra algoritmos de llaves públicas

3.3.2.2.1 Ataques de factorización

Son los más comunes, el objetivo es derivar la llave secreta a partir de la pública. Para el caso de RSA la fortaleza radica en la dificultad que se tenga para factorizar números grandes.

3.3.2.2.2 Ataques de algorítmicos

Son los más comunes, el objetivo es derivar la llave secreta a partir de una debilidad fundamental en el principio matemático en el que se basa.

3.3.2.3 Contra funciones de compendio

El primero de los ataques contra las funciones de compendio es encontrar dos mensajes que tengan las misma síntesis. El segundo es teniendo un mensaje, encontrar otro que tenga la misma síntesis. Claro está que en

ambos casos los mensajes deben ser en el mismo idioma, completamente legibles para las personas, e incluso estar hechos en el mismo procesador de palabras.

3.3.3 FIRMAS DIGITALES

Cuando se recibe un mensaje, se desea conocer que la fuente del mismo es verdadera y que la información no se ha alterado, se requieren de firmas digitales. Para ello se debe recurrir a las funciones de compendio de mensajes, las más utilizadas son MD5 y SHA (Secure Hash Algorithm). Lo que hacen estas funciones es procesar un mensaje y obtener una síntesis de longitud fija así MD5 devuelve síntesis de 128 bits y SHA de 160 bits.

Específicamente la firma digital funciona así:

- Se envía el texto original claramente definido
- Seguidamente se envía la síntesis del mensaje cifrado con la llave privada del autor
- El receptor calcula la síntesis del mensaje
- Descifra el mensaje utilizando la llave pública del autor
- Compara los dos mensajes: el original y el descifrado, si coinciden entonces el mensaje será auténtico

Con este se consigue la *no-repudiación.*

DSS (Digital Signature Standard) es el estándar de firmas digitales, fue desarrollado por la NSA (National Security Agency) adoptado como estándar de procesamiento de información federal (FIPS, Federal Information Processing Standard) por el Instituto Nacional de Estándares y Tecnología (NIST). DSS se basa en el DSA (algoritmo de firmas digitales). El estándar especifica que DSS solamente se utilizará para firmas digitales con llaves de 512 a 1024 bits, aunque DSA permite también realizar encriptación.

3.3.4 LIMITACIONES DE LA CRIPTOGRAFÍA

Cuando se escucha que alguna empresa promociona un *servidor web seguro,* en realidad lo que tiene en su poder es un *servidor web con características criptográficas.* Todas las transaciones de Negocio Electrónico realizadas por redes de comunicaciones sean éstas públicas o privadas, si

se necesita que sean seguras, deberán utilizar a la criptografía. Se debe entender que la criptografía no soluciona todos los problemas de seguridad de los datos de una organización, se debe tener en cuenta que el cifrado de datos nada puede hacer ante los siguientes casos[6]:

- La criptografía no puede proteger los documentos no cifrados
- La criptografía no puede proteger contra robo de llaves de cifrado
- La criptografía no puede proteger contra ataques de negación de servicio
- La criptografía no puede proteger contra el registro de un mensaje ni contra el hecho de que el mensaje haya sido enviado
- La criptografía no puede proteger contra un programa de encriptación con trampas
- La criptografía no puede proteger contra un traidor o un error

Queda claro que si bien es cierto la criptografía es un elemento fundamental en la seguridad de la información no es el único.

3.3.5 SISTEMAS DE ENCRIPTACIÓN ACTUALES

Para transacciones segura a través de Internet y a través de sistemas de comunicaciones privados, se han desarrollado muchos algoritmos y sistemas criptográficos.

Existen dos corrientes o tendencias en sistemas criptográficos: los utilizados para cifrar correo electrónico y los sistemas criptográficos que proporcionan confidencialidad, integridad, autenticación y no repudio, dentro de redes de información.

3.3.5.1 PGP

PGP (Pretty Good Privacy) es considerada de una confidencialidad excelente. Es un programa que se utiliza para enviar y recibir correo electrónico firmado digitalmente, así como también mensajes cifrados. La *privacía bastante segura* Se gestiona mediante tecnología RSA de llave pública, pudiendo el usuario elegir longitudes de llaves que van desde 500

[6] "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra Ed , 1999, pág 210-211

a 2000 bits, además, maneja la llave simétrica para los mensajes secretos con IDEA de 128 bits y el algoritmo de síntesis MD5.

PGP ofrece confidencialidad mediante el algoritmo IDEA, integridad mediante funciones hash MD5, autenticación mediante uso de llaves públicas y no repudio mediante firmas digitales.

PGP calcula las llaves de encriptación mediante un compendio de mensajes, permitiendo que los usuarios puedan introducir frases de acceso.

PGP se está generalizando en el ambiente de Internet tanto para verificar la integridad el mensaje como para identificar al emisor y se basa en una red de confianza en donde los individuos puede firmar determinadas llaves basándose en el conocimiento de otras personas. Claro está, que ésta no es una base para proporcionar llaves seguras a escala mundial.

3.3.5.2 S/MIME

MIME (Multipurpose Internet Mail Extensions) es el estándar de *extensiones multipropósito de correo de Internet* el cual envía archivos binarios. S/MIME es la extensión del estándar para proporcionar seguridad en el correo firmándolo electrónicamente. La confidencialidad se ofrece a través de algoritmos de encriptación especificados por el usuario. La integridad mediante las funciones hash, también son definidas por el usuario. La autenticación se la obtienen mediante certificados de llave pública X.5909 v3. La no-repudiación se la consigue utilizando mensajes firmados digitalmente.

3.3.5.3 SSL

El *nivel de conexiones seguras* SSL (Secure Socket Layer) es un protocolo de cifrado que asegura canales de dos vías sobre TCP/IP, se lo puede utilizar en cualquier servicio basado en TCP/IP.

Cuando se escribe un URL y se desea activar el protocolo SSL lo que se debe escribir en lugar de *http:* es *https:*.

Los algoritmos y funciones de confidencialidad e integridad de SSL son definidas por el usuario. La no-repudiación se consigue con firmas digitales cifradas.

El protocolo SSL está compuesto por dos capas. La capa más baja está encima del protocolo de nivel 4 (del modelo OSI) y es SSL Record Protocol, utilizado para encapsular los diferentes protocolos de nivel superior. Una vez encapsulado, SSL Handshake Protocol permite al servidor y al cliente autentificarse uno a otro y negociar el algoritmo de encriptación y las llaves antes de que los protocolos superiores transmitan o reciban los primeros bytes de la información.

Debido a la importancia de este protocolo y su estrecha relación con TCP/IP y con el Negocio Electrónico, será analizado más detalladamente en la sección 3.6.

3.3.5.4 PCT

PCT (Private Communications Technology), es similar a SSL y fue desarrollado por Microsoft. La *tecnología de comunicaciones privadas* se basa en SSL 2.0, corrigiendo algunos defectos que éste tenía, para luego formar parte de SSL 3.0.

3.3.5.5 S-HTTP

Es un protocolo que firma digitalmente toda la información que usa el protocolo de transferencia de hipertexto. Este es un protocolo poco utilizado y lo más probable es que muera.

3.3.5.6 SET y CyberCash

El protocolo para *transacciones electrónicas seguras* SET (Secure Electronic Transactions) está diseñado para enviar números de tarjetas de crédito por Internet.

SET tiene tres partes una billetera electrónica que está en la computadora del usuario, un servidor que se ejecuta en el sitio del vendedor y un servicio de pagos que se ejecuta en el banco del vendedor.

Al igual que SET, CyberCash en un protocolo para pagos electrónicos y de hecho SET fue diseñado tomando algunos parámetros de CyberCash.

Desde el punto de vista de Negocio Electrónico, estos dos protocolos son de gran importancia por lo que se analizarán con mayor detalle en la sección 3.10 de éste capítulo.

Cybercash o *ciberefectivo* se basa en una tecnología de llave pública, lo que permite utilizar las tarjetas de crédito en la red Internet. La opción para manejar menores cantidades de dinero con este esquema se la conoce como *Cybercoin.* Estos servicios se pueden equiparar al que presta una tarjeta de crédito.

Cuando se ejecuta este software por primera vez se crea una combinación de llaves pública y privada, así como también se crean bitácoras de transacciones y números de tarjetas de crédito. Todo esto se guarda en el disco dentro del disco duro en forma encriptada con el uso de una frase de acceso. Esta información permitirá colocar dinero de la tarjeta de crédito o de una cuenta corriente, en una cuenta de Cybercash utilizando la *transferencia automática de fondos* ACH (Automated Clearing House). Si el dinero que se transfiere desde una cuenta corriente, la transacción se puede reversar, pero si provienen de una tarjeta, el dinero debe ser gastado.

3.3.5.7 DNSSEC

Este estándar de *seguridad del sistema de nombres de dominio* (Domain Name Security) fue diseñado para crear una infraestructura de llaves públicas sobre el DNS. A cada nombre del DNS se le asigna una llave, con esto se puede conseguir una actualización segura de los DNS desde los servidores.

3.3.5.8 IPSEC e IPv6

La confidencialidad de este protocolo es de principio a fin, funciona con la versión estándar de IP, es decir, la que está en uso actualmente IPv4, la versión de IP de próxima generación ya incluirá IPSEC. La única característica que proporciona este protocolo es confidencialidad y se lo usa para crear túneles cifrados para VPN (Virtual Private Networks) a través de Internet o simplemente cifra información entre computadoras. La utilidad de IPSec va más allá de las VPN, utilizando un registro central de *intercambio de claves de Internet,* IKE (Internet Key Exchange), dos máquinas en el Internet pueden comunicarse utilizando cifrado y autentificación.

IPSec es similar en cuanto a servicios con SSL, pero los servicios de IPSec se orienta a redes, por lo tanto es transparente para las aplicaciones. La transparencia para las aplicaciones se produce ya que ellas no necesitan ningún conocimiento sobre este protocolo para poder usarlo. Por tener estas opciones IPSec es muy complejo.

Este protocolo funciona en cualquiera de lo siguientes casos:

- Host a host
- Host a red
- Red a red

IPSec se basa en dos protocolos:

- AH (Authentication Header) que es la *cabecera de autenticación,* asegura partes de la cabecera IP del paquete como las direcciones de origen y destino, no proporciona confidencialidad.
- ESP (Encapsulated Security Payload) que es el *cargo de seguridad encapsulado* el que puede proveer confidencialidad, autenticación, integridad y no-repudiación, a los datos, es decir, a todo lo que sigue después de la cabecera.

3.3.5.9 Kerberos

Desarrollado por el MIT, se basa en códigos simétricos, el servidor Kerberos encripta los mensajes que envía a cada usuario, debiendo agregarse el soporte de Kerberos a cada programa que se desee utilizar. Sin embargo, es un sistema poco amigable para su administración debido a que cada sitio necesita de un servidor Kerberos y si uno de ellos es violado se necesitan cambiar las claves de acceso de todos los usuarios del sistema completo.

3.3.5.10 SHH

SSH (Secure Shell) que es el *intérprete de comandos seguro*, proporciona operaciones seguras para Telnet y FTP.

La tabla 3.3 resume todos los sistemas de criptografía citados anteriormente[7].

[7] SEGURIDAD Y COMERCIO EN EL WEB", S Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed., 1999, pág 218-219

SISTEMA	¿Qué Es?	Algoritmos	Proporciona
PGP	Aplicación para encriptar correo electrónico	IDEA, RSA, MD5	Confidencialidad, Autenticación, Integridad, No-repudiación
S/MIME	Formato para encriptar correo electrónico	Especificado por el usuario	Confidencialidad, Autenticación, Integridad, No-repudiación
SSL	Protocolo para encriptar transmisiones TCP/IP	RSA, RCZ, RC4, MD5, otros	Confidencialidad, Autenticación, Integridad, No-repudiación
PCT	Protocolo para encriptar transmisiones TCP/IP	RSA, MD5, RCZ, RC4, otros	Confidencialidad, Autenticación, Integridad, No-repudiación
S-HTTP	Protocolo para encriptar peticiones y respuestas HTTP	RSA, DES, otros	Confidencialidad, Autenticación, Integridad, No-repudiación, Sin embargo es obsoleto
SET y CyberCash	Protocolos para envío de instrucciones de pago seguras a través de Internet	RSA, MD5, RC2	Confidencialidad de tarjetas de crédito, Autenticación del cliente y proveedor, Integridad de todo el mensaje, No-repudiación de las transacciones

Tabla 3.3 Comparación de sistemas de encriptación disponibles en la actualidad

SISTEMA	Qué Es?	Algoritmos	Proporciona
DNSSEC	Sistema de seguridad del sistema de nombres de dominio	RSA, MD5	Autenticación, Integridad
IPSEC e IPv6	Protocolo de bajo nivel para encriptar paquetes IP	Diffie-Hellman, otros	Confidencialidad (opcional) Autenticación, Integridad
Kerberos	Servicio de seguridad de red para asegurar aplicaciones de más alto nivel	DES	Confidencialidad, Autenticación
SHH	Terminal remota encriptada	RSA, Difie-Helman, DES, TripleDES,otros	Confidencialidad, Autenticación

Tabla 3.3 Comparación de sistemas de encriptación disponibles en la actualidad (continuación)

3.4 IDENTIFICACIÓN Y PRIVACÍA

Debido al crecimiento de las redes de datos, en número y en conexiones, es necesario saber con certeza con quien se tienen relaciones de negocios, de esta manera no se revelará la información confidencial a personal u organizaciones no autorizadas.

3.4.1 IDENTIFICACIÓN

La verificación de la identidad de un usuario u operador de un sistema es el punto primordial de la seguridad, en la vida cotidiana las tres formas de probar la identidad[8] son: con algo que se *tiene*, se *sabe*, o se *es*. De aquí que la identificación dentro de las redes se complique, ya que lo único de lo que se dispone es de flujos de bits.

Los tres tipos de identificación más usados son:

[8] "LAN TIMES GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J. Hsu, McGraw Hill, 1ra Ed., 1998, pág. 219

3.4.1.1 Identificación mediante posesión

Se basa en algo que el usuario *tiene*, se trata de una identificación electrónica, normalmente son dispositivos portátiles que generan contraseñas las cuales se comparan con otras generadas en una computadora, el inconveniente es el elevado costo. En el futuro la identificación por posesión será llevada al campo de las tarjetas inteligentes. Los inconvenientes de este tipo de dispositivos, como las tarjetas, son:

- El dispositivo no prueba realmente que el usuario sea quien dice ser.
- Si un usuario pierde el dispositivo, pierde también su posibilidad de acceso.
- Algunos dispositivos pueden ser falsificados con facilidad.

En realidad este sistema identifica al dispositivo más bien que al usuario.

3.4.1.2 Identificación mediante características intrínsecas

Se basa en la anatomía humana, es decir, en algo que se *es*. La identificación biométrica para el caso de las LAN en muy costosa. La tecnología apunta hacia el hecho de que las cámaras que vienen instaladas en las computadoras sean capaces de reconocer los patrones anatómicos y biológicos de sus usuarios.

Esta técnica puede ser muy confiable, sin embargo, los problemas que presenta son:

- El parámetro de identificación debe ser almacenado con anterioridad en una computadora.
- El costo del equipo que mide las formas biométricas de los usuarios.
- La protección de equipo de medición contra ataques y fraudes.

3.4.1.3 Identificación mediante el conocimiento

La otra alternativa y la más usada se basa en algo que se *sabe*, normalmente una contraseña. Sin embargo, este método es poco fiable dentro de una LAN, ya que si alguna persona descubre o rastrea una contraseña y la captura, la red estará totalmente abierta. Los problemas más comunes con respecto al uso de las claves son:

- La clave debe estar guardada en la computadora del usuario para poder ser comprobada.
- La clave puede ser interceptada en el momento que se está siendo enviada al servidor.
- El olvido de las claves de acceso por parte de los usuarios.
- Las claves elegidas por las personas usualmente son predecibles.
- Las personas revelan sus claves a otros.

3.4.2 PRIVACÍA

La privacía es un elemento muy importante cuando de comunicaciones y comercio se trata, normalmente un usuario que ha detectado que su privacía ha sido violada, no recuperará la confianza y no hará más transacciones en ese lugar.

La privacía puede ser violada desde varios puntos: bitácoras de acceso, ligas de referencia y los *cokies* (rastreo de un usuario a través de varias peticiones HTTP).

3.5 PRINCIPIOS Y POLÍTICAS DE SEGURIDAD PARA REDES

3.5.1 PRINCIPIOS DE SEGURIDAD

El caso de estudio del presente trabajo se centra en redes privadas de comunicaciones, denominadas *extranets*, debido a este particular, las nociones de seguridad aplicables a los modelos tradicionales no son suficientes para proteger las datos en estas redes. Por una parte las LAN son locales, las extranets, no, pudiendo abarcar países enteros o incluso pueden llegar a ser mundiales. Sin embargo, las consideraciones de seguridad que se han aplicado a los entornos de mainframes o de redes completamente abiertas, se deben adoptar para la protección de extranets, las que son una realidad cada vez más difundida.

"El objetivo de la seguridad en una extranet es otorgar solo a las personas indicadas el tipo correcto de acceso a los recursos de la intranet." "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág. 309.

El primer punto para poder dar seguridad a extranets es contar con un adecuado plan de seguridad, el mismo que debe contar con lo siguientes aspectos:

- Adaptar planes conocidos a las nuevas fronteras de comunicación. No necesariamente decentralizar la red, implica decentralizar la seguridad.
- Controlar los acceso a los archivos, las medidas que se aplican a las LAN pueden ser útiles.
- Se debe especificar prioridades con respecto a áreas de mayor pérdida.
- Las auditorías del sistema ayudan a encontrar comportamientos anómalos.
- La encriptación es una herramienta que debe estar presente en toda la extranet, pero su uso no debe ser abusado.
- Procurar que las medidas de seguridad sean lo más sencillas para su uso, lo que facilitará que las personas efectivamente las utilicen.

Debido que la extranets son redes que unen a varias empresas, la seguridad es más complicada, por esta razón los empleados de toda la EBC deben tener por lo menos la conciencia de lo que significaría poner en peligro la seguridad de su empresa o de las otras dentro de la comunidad. Lo ideal es que una empresa de la comunidad sea la encargada de manejar toda la seguridad computacional del grupo, así se podría garantizar una homogeneidad en los planes y políticas básicas, esto no implica de ninguna manera que esa empresa tenga acceso a la información y a los archivos del resto.

Se debe emplear una categorización[9] en cuanto a los usuarios de la red, de la siguiente manera:

- El supervisor de la red, debe tener acceso a todas las funciones, incluyendo el sistema de seguridad.
- Los usuarios administrativos, siendo un grupo pequeño, deben tener los derechos de acceso justos para mantener y dar soporte a la extranet.
- Los usuarios de confianza deben tener el acceso para usar la información importante.

[9] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág. 285-286

- Los usuarios vulnerables, cuyo acceso no va más allá de sus responsabilidades.

Los sistemas de comunicaciones y de cómputo deben ser capaces de avisar las anomalías en referencia a intentos de acceso no válidos, normalmente esta actividad se registra en las bitácoras de la red.

El NIST (National Institute for Standards and Technology) ha expuesto los requisitos mínimos necesarios para la seguridad en sistemas multiusuario. Cabe indicar que éstos no son únicos para la extranets. Las funciones principales son:

- Identificación y autenticación
- Control de acceso
- Responsabilidad
- Rastros de auditoría
- Reutilización de los objetos
- Precisión
- Confiable
- Intercambio de datos

Otro problema con las extranets es que el acceso remoto hace que la información sea vulnerable.

3.5.2 POLÍTICAS DE SEGURIDAD

En cuanto a las políticas de seguridad no existe ninguna receta. Cada organización debe determinar la mejor política ya que los negocios son diferentes, tienen diferentes formas de comunicación, diferentes necesidades de almacenamiento, en suma los negocios con vistas al intercambio electrónico cambian rápidamente, lo que presupone que las políticas de seguridad y en general todas las políticas de la organización deben ser flexibles.

Los ataques a computadoras son tan graves que la Yankee Group, empresa consultora del ramo, indica que la pérdida total financiera por estos delitos es cercana a los 5 mil millones de dólares, incluidos pérdidas de productividad, confianza y ventaja competitiva. Adicionalmente otros tipos de

pérdida, que también influyen en la suma de cantidades como la anterior son:

- Interrupción del servicio, cuando el ataque provoca una para en los procesadores de datos y de comunicaciones.
- Interceptación de datos importantes de la empresa o robo de información de un servidor.
- El cambio de datos con la consecuente presentación fraudulenta de información.

Al evaluar las políticas y los planes de seguridad debe hacérselo observando qué tipo de negocio se piensa realizar, por ejemplo: las necesidades de seguridad que requiere una transacción bancaria o con tarjeta de crédito, no serán las mismas que cuando una organización necesita exponer en un catálogo virtual los productos disponibles a sus clientes.

Dentro de las políticas de seguridad se deben tener en cuenta algunos factores[10]:

- Como interactúan los usuarios internos y externos
- Implementación de la arquitectura y topología de la red corporativa
- Implementación de controles al interior de la organización
- Las políticas de seguridad no deben ser coercitivas
- Establecimiento de acuerdos con los participantes de la comunidad que tengan acceso a la extranet
- Se debe asegurar que todos los socios tengan políticas de seguridad similares a las de la organización y que sus redes estén protegidas adecuadamente
- Las políticas deben contener herramientas actuales y disponibles en el mercado
- Se debe tener un medio de aviso y reporte de intentos de ingreso fallidos
- La información importante debe ser manejada adecuadamente y en lo posible lejos del Internet
- La seguridad de ser la adecuada para cada tipo de usuario

[10] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág. 315-319

- Se debe tener como respaldo un plan de contingencia ya que el mejor plan de seguridad puede llegar a fallar y producir pérdidas

Los elementos que conformarán la política de seguridad y que, además, toman en cuenta los factores antes mencionados son:

- Seguridad física: consolas centrales, cuarto de servidores
- Firewalls y control de acceso
- Controles personalizados
- Mecanismos de contraseña
- Encriptación y privacidad
- Autenticación en integridad
- Usar herramientas de *hacker* para beneficio de la organización

3.6 CAPA DE CONEXIONES SEGURAS

Como se ha indicado en el punto 3.3.5.3, SSL es la *capa de conexiones seguras* (Secure Sockets Layer).

La idea de este protocolo es enviar información segura en aplicaciones web, pero también se lo puede utilizar para aplicaciones fuera de las del web, como por ejemplo Telnet. Debido a que la criptografía cambia frecuentemente, este protocolo debe ser y de hecho es extensible y adaptivo. A partir de éste se está creando otro protocolo, el TSL (Transport Layer Security). Este *protocolo de seguridad de la capa transporte* se basa en la última versión del SSL.

SSL se ubica entre el protocolo TCP/IP nativo (capa transporte) y la capa de aplicación y está compuesto por dos capas. La capa más baja está encima del protocolo de nivel 4 (OSI) y es SSL *Record Protocol*, utilizado para encapsular los diferentes protocolos de nivel superior. Una vez encapsulado, SSL *Handshake Protocol* (capa más alta) permite al servidor y al cliente autentificarse uno a otro y negociar el algoritmo de encriptación y las llaves antes de que los protocolos superiores transmitan o reciban los primeros bytes de la información.

SSL agrega algunas características a las iniciales del TCP/IP que son enviar información libre de errores entre dos puntos, sean máquinas o procesos. Las características añadidas al flujo de información de TCP/IP son[11]:

- Autenticación y no-repudiación del servidor mediante firmas digitales
- Autenticación y no-repudiación del cliente mediante firmas digitales
- Confidencialidad de los datos mediante encriptación
- Integridad de los datos mediante códigos de autenticación de mensajes

3.6.1 CARACTERÍSTICAS DE SSL VERSION 3

3.6.1.1 Separación de responsabilidades

Los algoritmos para cifrado, autenticación e integridad utilizados por SSL tienen llaves independientes, mediante esta característica se pueden utilizar llaves más largas para determinadas funciones, esto tiene que ver con reglamentas federales dentro de los Estados Unidos de Norteamérica (los aspectos legales será analizados en la sección 3.11).

SSL permite conexiones no encriptadas pero autenticadas y protegidas, especialmente contra cambios que se pueda producir en la transmisión.

3.6.1.2 Eficiencia

Como se ha visto en secciones anteriores el cifrado de llave pública es un proceso demorado, por lo que SSL mantiene *secretos maestros* para cada conexión, lo que permite que cuando se inicia la comunicación, ésta se hace segura desde el inicio, sin necesidad de realizar el proceso de llaves públicas.

3.6.1.3 Autenticación con base en certificados

La autenticación de clientes y de servidores es una función de SSL, esto se realiza mediante certificados digitales y firmas digitales.

Para los certificados SSLv3 utiliza el protocolo X.509v3 (que será analizado en la sección 3.9), sin embargo, es posible utilizar cualquier estándar que se vaya creando y probando. La autenticación es opcional de SSL, pese a que las certificaciones de servidores son obligatorios en la actualidad.

[11] "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed , 1999, pág 234

3.6.1.4 Agnóstico en cuanto a protocolos

SSL se diseñó para correr sobre TCP/IP, sin embargo, puede hacer sobre cualquier protocolo confiable orientado a la conexión, como X.25, por ejemplo. No corre sobre protocolos no confiables no orientados a conexión como UDP. Las palabras claves para los protocolos TCP/IP que usan SSL son:

- *https* para HTTP protegido con SSL
- *ssmtp* para envío de correo protegido con SSL
- *snews* para grupos de noticias protegidos con SSL
- *spop3* recepción de correo protegido con SSL

3.6.1.5 Protección contra ataques de hombre en el camino y de reproducción

Un ataque de hombre en el camino consiste en que un individuo intercepta la comunicación entre dos puntos, haciendo creer a ambos que están hablando con quien desea, por ejemplo: cuando una persona necesita comunicarse con un servidor, existe otra persona que hace creer a la primera que efectivamente se está comunicando con el servidor; y hace creer al servidor que la solicitud está siendo enviada por la primera persona y no por el interceptor. SSL protege contra este tipo de ataques mediante certificados digitales, haciendo conocer al usuario el nombre validado del sitio al cual se conecta.

El ataque de reproducción consiste en que un individuo intercepta una solicitud de un tercero hacia un servidor, la copia y luego la ejecuta un sinnúmero de veces, por ejemplo: cuando una persona hace una operación de pago desde su cuenta, el atacante puede repetir esta operación y realizar varios pagos desde la cuenta de la otra persona. SSL utiliza el mismo proceso anterior, con la variante de que ahora el sitio es el que verificará la validez del cliente o usuario que hace una petición al servidor.

3.6.1.6 Soporte de compresión

Al encriptar los datos éstos no pueden comprimirse debido a que el buen cifrado elimina las repeticiones y autosimilitudes, es decir, que si los datos una vez cifrados son susceptibles de comprimirse, la encripción no es

buena. SSL permite que los datos del usuario sean comprimidos antes de que sean encriptados.

3.6.1.7 Compatibilidad retrospectiva

La posibilidad de manejar conexiones de la versión anterior de SSL sin obligar al usuario a realizar reconexiones es una característica favorable de SSL.

3.6.2 FUNCIONAMIENTO DE SSL

La ubicación de SSL entre la capa de transporte y la de aplicación lo hace un protocolo muy flexible.

El cifrado de datos que proporciona SSL es de llave simétrica pudiendo elegirse algoritmos DES, tripleDES, RC2, RC4 o IDEA, clave de sesión se cifra mediante algoritmos de llave pública como RSA. Esta clave de sesión es utilizada para cifrar los datos que viajen entre el servidor y la estación, la clave de sesión es distinta para cada transacción, lo que asegura que si un atacante logró capturar la clave de una transacción, ésta no le sirve para descifrar la siguiente. Los algoritmos más utilizados para compendio son SHA y MD5.

Esta característica de SSL de elegir entre tantos algoritmos le otorga una flexibilidad criptográfica muy grande.

Al iniciar una sesión con SSL el servidor y el cliente intercambian mensajes para negociar la mejor alternativa de seguridad, para lo cual se tienen las siguientes fases[12]:

- *La fase Hola*: usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación. El navegador le informa al servidor los algoritmos que posee. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.
- *La fase de autenticación*: en la que el servidor envía al navegador su certificado X.509v3 que contiene su clave pública y solicita a su vez al

[12] http://www.eitig.com/redes/trabajos/ssl.html

cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).

- *La fase de creación de clave de sesión*: en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la de sesión para cifrar los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la pública del servidor que extrajo de su certificado en la fase de autenticación. Posteriormente, ambos generarán idénticas claves de sesión a partir de la maestra generada por el navegador.
- *La fase Fin*: en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

Una vez que se tiene la sesión SSL abierta, el protocolo proporciona un canal seguro para las comunicaciones entre el servidor web y el navegador, a través del cual se intercambiará cifrada la información.

3.6.3 ESTANDAR TSL[13]

TLS 1.0 basa su estructura en SSLv3, las diferencias entre los dos protocolos no son sustanciales.

Los dos protocolos han sido diseñados para proporcionar privacidad e integridad de los datos entre aplicaciones.

TLS tienen dos capas, al igual que SSL: record protocol y handshake protocol.

Mientras el Record Protocol, para ambos casos, se dedica a codificar y decodificar los mensajes que se trasmiten y reciben, el HandShake Protocol consiste de un conjunto de subprotocolos que se usan para permitir a las partes de la comunicación estar de acuerdo respecto de parámetros de seguridad, autenticación y condiciones de informes de error.

[13] http://www.eitig.com/redes/trabajos/tls1.html ; http://www.eitig.com/redes/trabajos/tls2.html

A continuación se describen con más detalle cada una de las capas de TLS, cuya explicación se aplica sin mayores diferencias para sus respectivos en SSL.

El Record Protocol

Se encuentra a un nivel más bajo sobre un protocolo de transporte fiable (por ejemplo: TCP), proporcionando una conexión segura y privada. Usa criptografía simétrica para la encriptación de los datos (por ejemplo: DES, RC4, etc.), pero puede utilizarse sin la encriptación. El transporte del mensaje usa un mensaje de chequeo de integridad que utiliza un *código de autenticación de mensaje* MAC (Message Authentication Code) con clave, usando funciones de hash seguras como SHA y MD5, pero puede operar sin usarla. Este protocolo se usa para el encapsulamiento de varios protocolos de más alto nivel: HandShake Protocol y el protocolo de la aplicación. Fundamentalmente se encarga de tomar los mensajes a ser transmitidos, fragmenta los datos en bloques manejables, opcionalmente comprime los datos, aplica una MAC, encripta y transmite el resultado. El dato recibido es descifrado, verificado, descomprimido y reensamblado, entregándose a los clientes en niveles más altos. Este proceso se lleva a cabo mediante el uso de cuatro estados posibles de conexión: el estado de lectura actual, el estado de escritura actual, el estado pendiente de lectura y el estado pendiente de escritura.

El Handshake Protocol

Este protocolo involucra el uso del Record Protocol de TLS para intercambiar una serie de mensajes entre un servidor TLS-enabled y un cliente TLS-enabled al comienzo de una conexión TLS. Este intercambio de mensajes se diseñó para permitir las siguientes acciones:

- La autenticación del servidor por parte del cliente.
- Permitir que el cliente y el servidor seleccionen los algoritmos criptográficos que ambos puedan soportar.
- La autenticación opcional del cliente por parte del servidor.

- Usar técnicas de encriptación de clave pública para generar secretos compartidos.
- Establecer una conexión TLS encriptada.

Varias operaciones en el Record Protocol de TLS y el Handshake Protocol requieren el uso de un MAC con clave. Intentar falsificar el MAC es imposible sin conocer el secreto. La construcción que usa el protocolo para estas operaciones es conocida como HMAC. TLS lo usa en el Handshake Protocol con dos algoritmos de hash diferentes: MD5 y SHA.

Para encriptar los datos, el Record Protocol utiliza alguno de los siguientes algoritmos de criptografia simétrica: RC4, DES, IDEA.

Para realizar el intercambio de claves, el Record Protocol utiliza los siguientes algoritmos: RSA, Diffie-Hellman.

3.6.4 DESVENTAJAS DE SSL

La confidencialidad de los datos mediante SSL se la tienen solamente cuando están en el canal de comunicaciones, es decir, que si se envían datos importantes (números de tarjetas de crédito, seguridad social, etc.), SSL asegura, mientras viajan desde el navegador hasta el servidor, que no serán interceptados o modificados. Una vez en el servidor, el destino de los datos escapa al alcance del protocolo, esto toma mucha importancia debido a que SSL no garantiza la identidad del servidor. Este caso por ejemplo sería cuando el servidor seguro, al cual se está conectando un cliente esté suplantando la identidad de otro servidor conocido, aquí se hace muy importante la comprobación del certificado del sitio, y de esta manera no conectarse a sitios piratas.

Otro inconveniente del uso de SSL es que la velocidad de transmisión se degrada. El desempeño se ve mermado como resultado de la encriptación y desencriptación de llave pública requeridas para iniciar la sesión. Se han registrado degradaciones de desempeño que alcanzan hasta un 50%, comparándola con enviar la misma información sin utilizar SSL, sin embargo, como SSL tienen la posibilidad de guardar secretos maestros, este inconveniente se presenta solamente la primera vez que se acceda a un sitio seguro.

3.7 SEGURIDAD Y TCP/IP[14]

La tecnología IP permite mediante el uso de protocolos túnel realizar conexiones desde unas redes a otras por medio de Internet, sin tener que gastar en tecnología WAN ni conexiones privadas punto a punto, además, éste es el método utilizado por IP para los accesos remotos.

Las conexiones vía dialup no son más seguras que Internet, la diferencia radica en que la probabilidad de interceptar las comunicaciones en el sistema telefónico son reducidas (para el común de los mortales). Esto se debe principalmente al diseño, que incluye la ubicación del equipo y la falta de accesibilidad a los componentes implicados.

Sin embargo, en Internet, resulta más fácil interceptar los datos debido a que se conocen los componentes y el acceso a los componentes de la red sin que sea una dificultad la distancia. De este modo si un usuario desea beneficiarse de la posibilidad de utilización de los túneles en medio del Internet, debe disponer e implementar tecnologías que lo protegen contra este tipo de riesgos.

La Seguridad IP (IPSec) proporciona un modelo para proteger los datos en el momento en que se transmiten a través de una red. Es la primera ocasión en la que el protocolo IP es modificado con el objetivo de brindar seguridad. IPSec proporciona autenticación, integridad y, opcionalmente, confidencialidad. IPSec no se encarga de la información cuando ésta se encuentra almacenada, sino que proporciona seguridad desde que el equipo emisor transmite la información, hasta que el receptor la toma y la decodifica. IPSec al igual que el resto de protocolos de seguridad, basa su funcionamiento en llaves de cifrado y se puede utilizar para proteger equipos, sitios, dominios, comunicaciones de aplicaciones, usuarios de acceso telefónico y comunicaciones de extranet. Con la aplicación de IPSec la seguridad no es asunto de las aplicaciones, es decir, no importa que las aplicaciones estén o no preparadas y que sean o no seguras, este protocolo pone la seguridad al nivel de red, por lo que para las aplicaciones es transparente si trabajan o no con canales seguros. Los datagramas IP se

[14] http://www.microsoft.com/latam/technet/articulos/200011/art03/default.asp

protegen sin tener en cuenta la aplicación que inicialmente generó el tráfico. En otras palabras, las aplicaciones no son compatibles con IPSec. Las reglas de seguridad las define el administrador sin tener en cuenta qué aplicación se ejecuta.

3.7.1 FUNCIONAMIENTO DE IPSEC

La seguridad proporcionada por IPSec, es al nivel de datagramas IP de extremo a extremo. Los dispositivos existentes entre el origen y el destino no necesitan conocer el cifrado, las llaves y todos los aspectos de la seguridad, para saber cómo enrutar los datagramas, esto quiere decir que el canal de transmisión puede o no puede ser seguro y que solamente los host que se comunican necesitan saber acerca de IPSec.

IPSec funciona identificando el tráfico que necesita ser protegido y, a continuación, aplicando el nivel definido de seguridad. El tráfico que reúne ciertos criterios, como la dirección IP de origen o el nombre de host será protegida eligiendo el nivel adecuado de seguridad basado en esos criterios de identificación.

Utilizando IPSec, los datos se pueden proteger entre hosts, enrutadores de red, o servidores de seguridad específicos, o entre hosts y enrutadores o servidores de seguridad. Utilizando algoritmos de autenticación y de cifrado estándar en la industria, IPSec aprovecha las tecnologías existentes y ofrece un método completo para proteger el tráfico de la red.

Como ya se mencionó en secciones anteriores, los protocolos que intervienen el IPSec son el *encabezado de autenticación* (AH) que garantiza la integridad de los datos, proporciona no-repudiación y autentifica al host; y la *carga de seguridad de encapsulación* (ESP), que además de la funcionalidad de AH incluye de forma opcional la confidencialidad de los datos. Es importante tener en cuenta que ni AH ni ESP proporcionan los algoritmos criptográficos reales para implementar las características especificadas anteriormente, pero en cambio AH y ESP aprovechan la existencia de algoritmos criptográficos y de autenticación.

Los protocolos de IPSec se pueden utilizar en dos modos distintos, denominados modo de transporte y modo de túnel. El funcionamiento de AH y ESP no cambia como consecuencia del modo de operación.

El modo de transporte se usa para proteger paquetes donde el extremo de las comunicaciones es también el extremo criptográfico.

En el modo de túnel, el extremo criptográfico es una puerta de enlace de seguridad que proporciona seguridad en nombre de otra red. En este caso, el paquete IPSec se autentifica, se comprueba y posiblemente se descifra antes de reenviarse al extremo de las comunicaciones. El modo de túnel podría usarse en un escenario para crear una VPN de enrutador a enrutador.

Los párrafos siguientes fueron obtenidos de la dirección de Internet:

http://www.openbsd.org/faq/es/faq13.html.

"En el modo transporte un host es el que genera los paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (TCP, UDP), antes de que la cabecera IP sea añadida al paquete. En otras palabras, un AH añadido al paquete cubrirá el resumen criptográfico de la cabecera TCP y algunos campos de la cabecera IP extremo-a-extremo, y una cabecera ESP cubrirá el cifrado de la cabecera TCP y los datos, pero no la cabecera IP extremo-a-extremo.

Un ejemplo de un paquete AH en modo transporte es:

IPhdr AH TCPhdr datos

El modo túnel se usa cuando la cabecera IP extremo-a-extremo ya ha sido adjuntada al paquete, y uno de los extremos de la conexión segura es solamente una pasarela. En este modo, las cabeceras AH y ESP se usan para cubrir todo el paquete, incluida la cabecera extremo-a-extremo, y se añade una nueva cabecera IP al paquete que cubre sólo el salto al otro extremo de la conexión segura (aunque eso puedan ser varios saltos de distancia).

Un ejemplo de un paquete AH en modo túnel es:

Debido a que una cabecera ESP no puede autenticar la cabecera IP exterior, es útil combinar una cabecera AH y una ESP para obtener lo siguiente:

A esto se le llama «Adyacencia de Transporte».

La versión del túnel sería algo así:

"

"Es importante tener en cuenta que aunque IPSec en el modo de túnel puede usarse sólo para que sea compatible con el acceso remoto, el trabajo hacia una VPN a través de IPSec pura todavía está en curso. Los problemas más significativos actualmente son la interoperabilidad con las implementaciones de proveedores diferentes y la incapacidad para enviar por túnel el tráfico de multidifusión y de difusión. El último obstaculiza la habilidad de crear conexiones VPN de enrutador a enrutador utilizando el modo de túnel de IPSec. Por ahora, la solución es usar L2TP/IPSec para la creación de túneles para las conexiones de acceso remoto."[15]

3.7.2 VPN

Las VPN o redes privadas virtuales permiten la comunicación entre dos host utilizando redes públicas de telecomunicaciones como por ejemplo Internet. Para el usuario es como utilizar una conexión dedicada punto a punto.

La transmisión de datos se logra encapsulando la información en paquetes que permitan el intercambio de información, así una vez que el servidor VPN reciba el encapsulado desecha el encabezado y reenvía la información dentro de la red local y privada.

La red pública proporciona la plataforma para que se realice el intercambio de información, pero el verdadero establecimiento de las redes privadas

[15] http://www.micosoft.com/latam/technet/articulos/200011/art03/default.asp

virtuales debe ser controlado por varios protocolo túnel, como por ejemplo: el *protocolo de túnel punto a punto* PPTP (Point to Point Tunneling Protocol), el protocolo de túnel de nivel 2 L2TP (Level 2 Tunneling Protocol). La tabla 3.4 compara los protocolos mencionados hasta aquí.

Características admitidas	PPTP	L2TP/IPSec
Autenticación de usuario con contraseñas	Sí	Sí
Autenticación de usuario con tarjeta inteligente o token	Sí, con EAP[16]	Sí, con EAP
Autenticación del host	No, sólo usuario	Sí, con una infraestructura PKI[17] que utilice certificados x.509
Traducción de direcciones de red (NAT) posible	Sí	Actualmente no
Sin protocolo IP	Sí	Sí
Dirección IP interna para el cliente de túnel	Sí	Sí
Difusión IP, multidifusión	Sí	Sí
Método de cifrado	El Cifrado punto a punto de Microsoft (MPPE) proporciona cifrado de 40 bits o 128 bits	DES de 40 bits, DES de 56 bits y 3DES que utilice cifrado de 128 bits

Tabla 3.4 Comparación de protocolos para VPN

3.8 CORTAFUEGOS O FIREWALLS

Los cortafuegos o *firewalls* son equipos electrónicos o equipos electrónicos más software, que están conectados a dos redes diferentes, con la finalidad de dejar pasar información con ciertos criterios de selección.

[16] EAP significa *Protocolo de Autenticación Extensible*, y permite la negociación entre el cliente y el servidor de acceso remoto en relación con el método de autenticación que se debe utilizar. Los ejemplos serían extensiones para dispositivos biométricos, tarjetas de identificación

[17] Infraestructura de clave (llave) pública (Public Key Infraestructure)

Hoy en día lo más usual es colocar a la entrada un ruteador y este conectado a una computadora con sistema operativo UNÍX o LINUX, los que presentan ventajas en cuanto a la seguridad dentro de las redes de información

Al ejercer un control sobre la información que cursa entre dos redes los firewalls ayudan a mejorar la seguridad de la información.

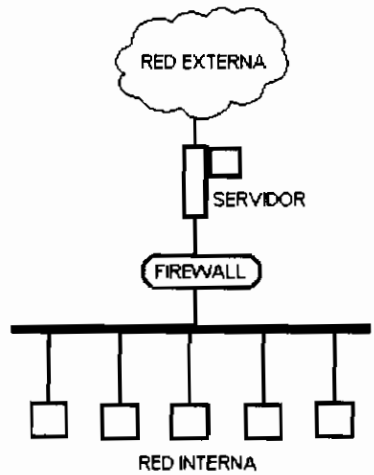
"No es fácil construir firewalls correctamente. Además, a menudo las organizaciones olvidan la seguridad interna una vez instalado el firewall. De ahí que muchos de ellos solo den la ilusión de mejorar la seguridad aunque, en realidad, algunas organizaciones pueden estar menos seguras después de su instalación.", "Seguridad y Comercio en el Web", S. Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed., 1999, pág. 7.

La idea del firewall para el caso de las extranets en aislar a la red interna, intranet, de los intentos de acceso no autorizados, y mantener los datos lejos de los espías y atacantes, bloqueando conexiones no deseadas. De esa manera los firewall son una parte muy importante de los planes y de las políticas de seguridad de las organizaciones.

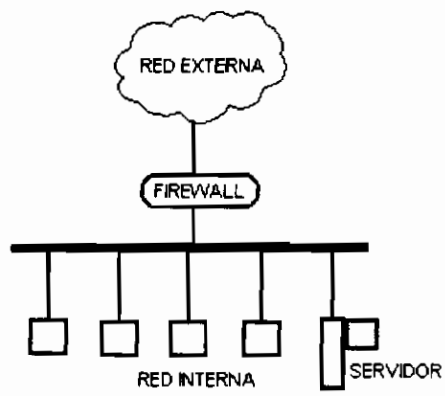
La correcta colocación del firewall respecto al servidor de la organización, que en Negocio Electrónico es necesariamente un servidor web, puede significar la diferencia entre el éxito o el fracaso de la seguridad.

La figura 3.2 indica la posición del firewall, respecto al servidor web, en tres casos diferentes:

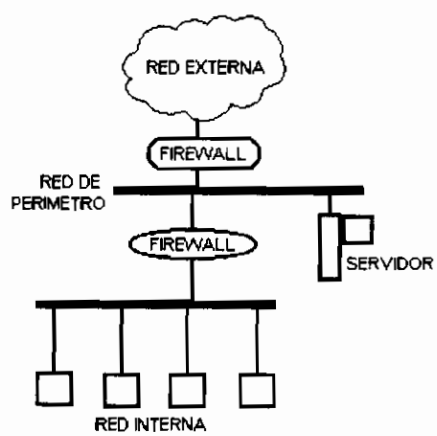
a) Servidor web fuera del firewall, esta técnica otorga seguridad al la red ya que si el servidor es víctima de un ataque, éste no podrá ingresar a la red, sin embargo el servidor no participará de la protección.
b) Servidor web dentro del firewall, para esta técnica se debe configurar el firewall para que permita transacciones TCP/IP entre el servidor y el mundo externo, sin embrago, una vez que el atacante ha violado las seguridades, tendrá acceso a toda la red.
c) Servidor web entre un firewall interno y el externo, ésta es la mejor opción ya que el servidor está protegido contra ataques externos e internos, su desventaja es el costo que puede llegar a tener, tanto monetario como de administración.



a)



b)



c)

Figura 3.2 Técnicas de ubicación de firewall

Los firewalls, para que resguarden efectivamente la información y bloquee los accesos no autorizados de forma correcta, deben ofrecer las siguientes características[18]:

- *Control de acceso flexible*: las reglas de admisión o rechazo de paquetes, visitantes e información en general, deben ser completamente parametrizables por los administradores.
- *Facilidad de uso*: la administración de los firewalls, es una gran responsabilidad. Es necesario un firewall que facilite su configuración y facilite vigilar los parámetros elegidos así como su administración.
- *Respuesta al error*: la información oportuna de los intentos de acceso no válidos y la identificación del origen es una cualidad importante que deben tener los firewalls.

También los firewall se utilizan cuando en la misma organización existen redes LAN de los diferentes departamentos, y una vez más se protege contra ataques internos, separando (protegiendo) esas redes entre sí con el uso de firewalls y pasarelas. En el caso de la extranets, las organizaciones de la comunidad requieren que solamente sus socios de negocios que sean autorizados tengan acceso, solamente a la información autorizada.

Normalmente los puntos que se deben tener en cuenta cuando se decide instalar un firewall dentro de una EBC son:

- Cuáles servicios se deben proporcionar y cuáles se debe bloquear, es decir, que uso se le va a dar a la conexión con la otra red.
- Se necesita toda la red interconectada, esto dependerá del punto anterior, en función de los servicios que desee brindar.
- Si el requerimiento es un ambiente de trabajo más amplio, probablemente la solución será crear una red en medio de las dos organizaciones, la cual estará protegida por dos firewalls, una de cara a cada empresa.

Cabe mencionar que el uso de cortafuegos reduce la velocidad de transmisión entre las redes debido al procesamiento que debe realizar para la seguridad, es decir, más seguridad, menor desempeño.

[18] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág. 347.

Entre los más comunes se tiene[19]:

- **Filtros de paquetes:** el firewall examina cada paquete (IP) que ingresa, compara las direcciones y servicios de origen y destino con una lista previamente definida (de ahí que los clientes deben tener direcciones IP fijas). Este es el control más sencillo de administrar y lógicamente de vulnerar. Este firewall se lo debe colocar a la entrada al sitio, lo que causará un efecto disuasivo, más que de protección completa.

- **Compuertas de aplicación:** la idea de este firewall es restringir la información a una aplicación específica, utilizando un código específico en lugar de uno general como el anterior. Estos son considerados más seguros ya que el usuario da los parámetros para que el software filtre la información de una aplicación específica. Los proxi como tal conforman este tipo de compuertas. Este tipo de firewalls debe usarse cuando se trata del acceso de lo empleados de la organización al Internet.

- **Compuertas a nivel de circuitos:** la compuertas a nivel de circuito conectan un puerto externo TCP/IP a un destino interno, por ejemplo una impresora de red. Funcionan como filtros inteligentes que pueden distinguir una sesión TCP o UDP válidas. No identifican la aplicación que se está utilizando.

- **Asuntos de estado:** la *técnica global de múltiples niveles* SMKT (Stateful MultiLayer Technique) es un procedimiento que examina el estado de un paquete comparándolo con políticas de seguridad que la organización ha definido y con un historial de recepciones anteriores. SMLT se aplica en los niveles más bajos de la pila protocolos de red de *Interconexión de Software Abierto* que filtra la transmisión antes de que se establezca una conexión con el sistema operativo.

[19] "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000, pág. 345 - 346

3.9 NEGOCIO ELECTRÓNICO CON SEGURIDAD

Cuando se trata de Negocio Electrónico, sea por Internet o en redes privadas, la seguridad es un aspecto sumamente importante, así se deben definir las políticas y tener los medios tecnológicos necesarios para que cada una de las transacciones sea fiable.

Los párrafos siguientes han sido extraídos del libro "LAN TIMES: GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J. Hsu, McGraw Hill, 1ra. Ed., 1998, página 243 y describen transacciones fiables para Negocio Electrónico.

"Se realiza el cifrado con una combinación de RSA y técnicas de llave secretas. En primer lugar, las llaves públicas de unas pocas autoridades de certificación seleccionadas se integran en el visualizador. Si un negocio desea disponer de un acceso fiable para los usuarios, primero debe obtener un certificado electrónico de alguna de estas autoridades. Cuando así lo hace recibe un par de llaves RSA, cuya llave pública está firmada digitalmente por la autoridad de certificación.

En el ámbito personal, cuando se desea conectar al servidor Web de una compañía, en primer lugar, el navegador responde enviando su certificado, que puede verificarse fácilmente a partir de la firma de la autoridad de certificación integridad en el visualizador. Esta identificación confirma que la comunicación no se está realizando con una empresa falsa que se está haciendo pasar por alguna otra.

Una vez verificado que realmente la comunicación se realiza con la compañía elegida para realizar el negocio, se pasa a un intercambio de llaves parecido al de Diffie-Hellman con el objeto de establecer una llave de sesión secreta que se utilizará durante el resto de la conversación con el servidor. Llegados a este instante, el usuario debería sentirse seguro para solicitar la mercancía y suministrar el número de su tarjeta de crédito sabiendo que la conversación que está manteniendo con el servidor en el otro extremo es confidencial. Este protocolo se denomina *capa de conectores seguros* SSL (Secure Socket Layer)."

La figura 3.3 indica el grado de seguridad que debe existir cuando se trata de Negocio Electrónico, comparándola con otros tipos de intercambio de información electrónica.

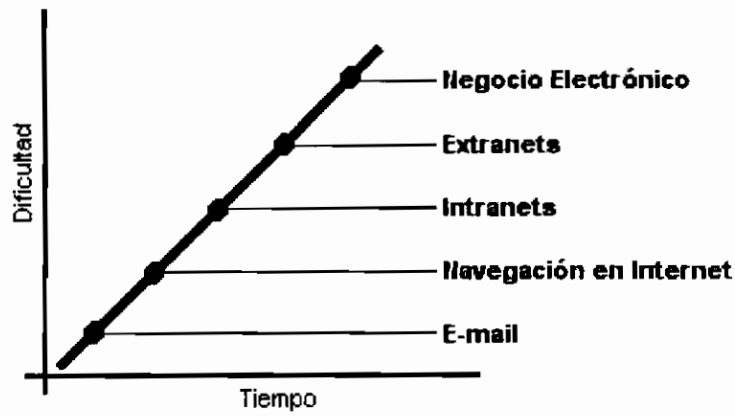


Figura 3.3 Complejidad en la seguridad del Negocio Electrónico[20]

Siempre surge la pregunta acerca de todo lo seguro que es comprar en línea. Se dice que no es más peligroso comprar por Internet y dar el número de tarjeta de crédito, que comprar por teléfono o por correo. Los riesgos son similares ya que la información entregada no se puede impedir que sea utilizada con otros fines.

Cuando se compra software el peligro consiste en recibir un virus o un tipo de código malicioso. Igualmente que los bancos atraen a ladrones convencionales, sitios de gran éxito en el Internet ataren a piratas cibernéticos y ladrones digitales. Lo que se persigue es reducir los riesgos de ataque a un sitio dedicado al Negocio Electrónico. Como se ha visto en secciones anteriores, la forma preventiva más efectiva que se tiene a disposición es la criptografía, así que cuando una organización esté pensando en implementar el comercio electrónico, debe necesariamente hacer una implementación paralela de sistemas de cifrado y de planes y políticas que le permitan tener sus datos seguros e íntegros.

[20] http://ute.edu.ec/~mjativa/ce/main.html

3.10 CERTIFICADOS Y PAGOS DIGITALES

3.10.1 CERTIFICADOS DIGITALES

Los *certificados electrónicos* son documentos digitales que sirven para asegurar la veracidad de las llaves del cifrado, pertenecientes al propietario del certificado ó de la entidad, con la que se realiza la firma digital de documentos, los que puedan proporcionar las más absolutas garantías de seguridad respecto a autenticación, confidencialidad, integridad y no-repudiación.

Los certificados digitales tienen como objetivos: identificar un usuario, servidor o empresa, permitiendo el cifrado de las comunicaciones y la firma de un documento electrónicamente.

Existen varios tipos de certificados según el protocolo de comunicaciones y la aplicación que se esté utilizando:

- Certificado personal: documento de identificación de un usuario de Internet para navegar, comprar, enviar y recibir correo, firmar documentos electrónicos, etc. de forma segura.
- Certificado de servidor: permite asegurar toda comunicación entre un navegador y un servidor web.
- Certificado para VPNs: permite la comunicación segura, entre las empresas y sus empleados, clientes y proveedores, mediante la creación de redes privadas virtuales en el entorno abierto de Internet.
- Certificado Servidor WAP: permite asegurar toda comunicación entre un terminal móvil y un servidor WAP (Wireless Access Protocol).
- Certificado para firmar código: permite a una empresa firmar su software y distribuirlo de forma segura.

Los certificados digitales aseguran que la información que se intercambia se encuentra cifrada, por lo que si se captura, los atacantes solamente encontrarán caracteres sin significado, por lo que se tienen que hacer uso de las llaves públicas y privadas correctas, para acceder a la información.

Un certificado electrónico contiene una llave pública, y una firma digital. La firma digital de un certificado es su identidad electrónica, previamente autentificada y registrada por la Autoridad de Registro, que es quien asegura al destinatario del mensaje que éste proviene efectivamente de usted y que no ha sido falsificado ni manipulado

Para su correcto funcionamiento, los certificados contienen, además, la siguiente información[21]:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país. Todos ellos conforman el DN (Distinguished Name) del usuario.
- Otro identificador de quién asegura su validez, que será una *Autoridad de Certificación*.
- Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.
- Los navegadores actuales gestionan y almacenan las llaves públicas de los certificados que permiten al emisor de mensajes firmarlos y cifrarlos utilizando las llaves públicas de los destinatarios.

Para garantizar la seguridad en una transacción es necesario utilizar por lo menos dos tipos de certificados, uno para comunicaciones seguras, por ejemplo X.509 y otro para transacciones económicas como por ejemplo

[21] http://www.penta3.com/infoPKI/certificado.htm

SET. El primero será analizado más adelante en esta misma sección, SET se lo analizará en el punto 3.10.2.

A continuación se ejemplifica la manera de obtener un certificado digital. Se supone la existencia de dos usuarios A y B. El usuario A, tanto para cifrar un mensaje como para verificar una firma de un texto de B, necesita disponer de la clave pública de éste. La forma que tiene de obtener esa clave pública es conseguir el certificado electrónico de B. A, disponiendo del certificado de B y la clave pública de la Autoridad de Certificación que asegura la validez del mismo, puede obtener de forma segura la clave pública sin temor a que ésta no pertenezca a B.

Para obtener el certificado de B, A puede acceder al directorio de certificados y preguntar por éste para descargarlo y utilizarlo.

Otra forma de obtener el certificado es que A haya recibido algún mensaje de B, que lleve dentro el certificado.

Los certificados digitales tienen muchas aplicaciones, a continuación se enumeran algunas:

- Dentro de las organizaciones, instituciones, para certificar personas, aplicaciones (corporativas, cliente/servidor, locales).
- Infraestructuras de tecnologías de información para garantizar elementos de comunicaciones (pasarelas, HUBs, líneas de transmisión).
- Protección de los derechos de propiedad intelectual en medios como discos compactos, libros electrónicos y bases de datos.
- Servicios (tarjetas de crédito, TV por cable o satélite y WebTV).
  - Los servicios de certificación cruzada y autorizaciones.
  - La compulsa y notaría electrónica privada de documentos, productos y servicios.
  - La homologación de productos para servicios de tercera parte confiable.
  - Consultoría para implantación de Autoridades de Registro (RA) o de Autoridades de Certificación (CA).

A continuación se analiza el estándar X.509v3, que es el más popular para certificados de llaves públicas y es una recomendación de la Unión Internacional de Telecomunicaciones, Sector de Telecomunicaciones, la ITU-T (International Telecommunication Union – Telecommunication Standarization Sector). La figura 3.4 indica la estructura que tiene un certificado X.509. Los certificados X.509 pueden ser de navegador y de servidor. Los de navegadores pueden ser emitidos para particulares o profesionales. Permiten intercambiar información entre usuarios de una forma segura. Es la mejor forma de autenticar los datos en Intranets/Extranets e e-mail.

Versión
Número de serie
Algoritmo identificador:
- Algoritmo
- Parámetros

Emisor
Período de validez
- No antes de
- No después de

Materia
Materia de llave pública
- Algoritmo
- Parámetros
- Llave pública

Firma

Figura 3.4 Estructura esquemática del certificado X.509 típico[22]

La Autoridad de Certificación[23], CA (Certification Autority), es quien firma digitalmente los certificados, asegurando la integridad del mismo y certificando la relación existente entre la clave pública contenida y la

[22] "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra Ed , 1999, pág 117.
[23] http://www.penta3.com/infoPKI/ca.htm

identidad del propietario. La firma de la CA es la que garantiza la validez de los certificados.

La confianza de los usuarios en esta CA es fundamental para el buen funcionamiento del servicio. La seguridad física de la CA se supone que ha de ser muy fuerte, en particular en lo que respecta a la protección de la clave privada que utiliza para firmar sus emisiones, si este secreto se viera comprometido, toda la infraestructura de llave pública (PKI) se viene abajo.

Las autoridades de certificación pueden realizar las siguientes tareas:

- Emisión de los certificados que haya validado antes la RA.
- Revocación de los certificados que ya no sean válidos. Un certificado puede ser revocado por que los datos han dejado de ser válidos, la clave privada ha sido comprometida o el certificado ha dejado de tener validez dentro del contexto para el que había sido emitido.
- Renovar un certificado.
- Publicar certificados en el directorio de repositorio de certificados.

3.10.2 PAGOS DIGITALES

Los pagos digitales son una forma de intercambiar dinero, sin que se encuentre presente ningún objeto tangible. El pago electrónico es una forma de crédito que en su más general definición expresa la confianza en la habilidad y deseo de una persona de pagar en un momento futuro bienes o servicios que se le entregan en este momento. Siendo la confianza un aspecto que se debe fundamentar en una buena reputación y un sistema confiables de llevar las cuentas. El dinero electrónico se viene utilizando desde los años 60 mediante la transferencia de fondos, otra forma de dinero digital se presenta cuando la gente no necesariamente debe ir a una oficina bancaria para sacar dinero de su cuenta, sino que basta acercarse a una máquina de cajero automático ATM (Automatic Teller Machine). Además, las tarjetas de crédito han existido de una forma u otra durante casi 80 años

Las tarjetas de crédito son hoy por hoy la forma de pago más común en el Negocio Electrónico por lo que muchos sistemas se han apoyado en ellas para realizar sus transacciones y los nuevos sistemas que surgen a diario no

han buscado sustituirlo. Es así como una transacción mediante tarjeta de crédito puede involucrar hasta cinco participantes:

- El comprador
- El vendedor
- El banco del comprador, que es el emisor de la tarjeta
- El banco del vendedor
- La red interbancaria

Las fases de establecimiento de un pago electrónico son: la suscripción (cuando el cliente establece una relación con el sistema de pagos), la compra, y el ajuste (compensación entre las cuentas de los participantes).

Indistintamente si se trata de una transacción electrónica o no, una compra con pago mediante tarjeta de crédito tiene los siguientes pasos[24]:

- El vendedor entrega su tarjeta de crédito al vendedor
- El vendedor pide autorización a su banco
- La red interbancaria envía un menaje del banco del vendedor al banco del comprador, pidiendo autorización
- El banco del comprador envía una respuesta al banco del vendedor mediante la red interbancaria (el banco del vendedor puede también detener parte de la línea de crédito del comprador, quedando pendiente del cierre de la transacción)
- El banco del vendedor notifica el comerciante que el cargo ha sido aprobado
- El vendedor llena la orden del comprador
- En algún momento posterior, el vendedor presenta cierta cantidad de cargos a su banco
- El banco del vendedor envía cada solicitud de pago al banco del cliente mediante la red interbancaria
- El banco del cliente debe la cuenta del cliente y coloca el dinero (tal vez deduciendo un cargo de servicio) en una cuenta de pagos interbancaria

[24] "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed., 1999, pág. 316.

- El banco del vendedor hace un crédito a la cuenta del comerciante y retira una suma similar de dinero de la cuenta de pagos interbancaria.

Las tarjetas de crédito en el Negocio Electrónico utilizan tres técnicas principales:

- Pagos *offline,* cuando el comprador escoge el producto y luego llama al comerciante para decirle su número de tarjeta, siendo éste un sistema no menos peligroso que comprar por teléfono.
- Pago *online con encripción,* el número de tarjeta se envía mediante una red de telecomunicaciones en forma cifrada.
- Pago *online sin encriptación* el comprador envía su número de tarjeta sin encripción el momento de realizar la compra.

Los sistemas de pagos basados en Negocio Electrónico no solamente se circunscriben a la popular tarjeta de crédito. Otros sistemas tienen algunas ventajas, como son: costo reducido de transacción, anonimato y mayor mercado. Entre los sistemas de pagos están[25]:

- Anónimos
- Privados
- Identificatorios

Los sistemas de cifrado son muy importantes para realizar transacciones e pago, los más utilizados son CyberCash y SET. Los certificados SET, permiten realizar transacciones económicas de comercio electrónico mediante tarjeta de crédito de forma segura con las máximas garantías para todas las partes intervinientes. Los certificados pueden ser de: titulares (cardholder), para los usuarios o tenedores de las tarjetas, comerciantes (merchant) y de pasarelas de pago (payment gateway). Estos certificados se obtienen a través de las entidades financieras. El protocolo SET está diseñado para cifrar ciertos mensajes relacionados con pagos.

[25] "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed., 1999, pág. 322.

Las metas de SET son: permitir que la transacción sea confidencial, autentificar a los participantes de la transacción, dar integridad a las instrucciones de pago derivadas de la transacción comercial, y autenticar las identidades de los intervinientes. Debido a que existe información confidencial que interesa a ciertos participantes, SET incluye una estructura criptográfica conocida como *firma dual* que se muestra en la figura 3.5.

Encriptación con la llave del comerciante	Mensaje del cliente al comerciante	**Mensaje del cliente al banco**	Encriptación con la llave del banco
	C1 Compendio	**C2 Compendio**	
	Firma dual del cliente		
	C3 = compendio (C1 + C2)		

Tabla 3.5 Solicitud SET con firma dual

La firma dual permite tanto al comerciante como al banco leer y validar su firma, sin tener que descifrar la parte que del otro. La seguridad del protocolo se basa fundamentalmente en un sistema estricto de certificación (norma X509) y en que cada uno de los agentes conoce exclusivamente la información que le concierne y que le es estrictamente necesaria para poder realizar la compra, la venta o la transacción. Así el comerciante no llegará a saber cual es el número de tarjeta de crédito del comprador, ni la pasarela de pago cuales son los productos comprados por el consumidor. SET, por construcción, obliga a que todos los agentes que intervienen en el proceso de comercio electrónico estén debidamente certificados por una autoridad de confianza.

3.11 LEYES Y NEGOCIO ELECTRONICO

El Negocio Electrónico al ser una actividad relativamente nueva, sobretodo en el Ecuador, debe ajustarse a las necesidades cambiantes del mercado, por lo que la legislación es este sentido debe ser lo suficientemente flexible, para el cambio y el seguimiento de las tecnologías. No flexible en el sentido de ser

débil en cuando a sus artículos y su aplicación, como es obvio robo y atraco deben ser penados por la ley.

Otro punto importante a ser incluido en la ley es aquel en el cual se protege a los consumidores y a los comerciantes, respecto a sutilezas en cuanto a entrega de productos, contrato de trabajo a distancia, satisfacción del usuario.

Existe una proyecto de ley para Negocio Electrónico en el Ecuador, en esta sección se tratará de analizarlo y emitir ciertos criterios, enmarcándolo en la realidad mundial.

El *Proyecto de Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos* del Ecuador se basa principalmente en el cifrado de datos lo que permitiría tener autenticidad, integridad, confidencialidad y no-repudiación de los datos que cursen por los sistemas de Negocio Electrónico que se implanten. Esta ley ha sido aprobada a la fecha, en primera instancia por el Congreso Nacional, lo que no significa que esté en vigencia aún.

El proyecto de ley inicia con conceptos que sustentan los aspectos técnicos del Negocio Electrónico sin ser éstos del todo claros y sin abarcar algunos tópicos como por ejemplo pagos digitales.

Queda claramente estipulado que los datos deben estar disponibles para consultas en el futuro. Para ello deben ser almacenados en formatos estándares los mismos que el futuro puedan demostrar su origen, destino, fechas y horas de emisión y recepción, no deben existir cambios a la información almacenada, salvo que el formato de lectura en el futuro, así lo requiera, siempre y cuando se puedan comprobar las características anotadas. Todos los servicios que se desprendan de esta actividad, pueden ser tercerizados, siempre y cuando la empresa que brinde estos servicios sea homologada por las instancias legales pertinentes y por los organismos de control que estén en vigencia.

Además, el presente proyecto de ley hace referencia a la propiedad intelectual de la información e indica que la ley de Propiedad Intelectual será aplicada para los casos de delitos y fraudes que se lleven a cabo con los datos.

Cuando se tratan temas de seguridad y autenticación se hace referencia a la firma electrónica y se menciona que tendrá igual valor penal y judicial que un

documento en papel, como pruebas en los juicios cuando sea necesario. Indica, además, que las firmas digitales estarán compuestas por la firma electrónica, un adecuado algoritmo de encriptación y las respectivas infraestructuras de llaves públicas o privadas.

Se deben crear *órganos de control* y *entidades de certificación* para la administración de las llaves y de las empresas que se dediquen a la actividad electrónica, para lo que se utilizarán estándares e internacionales. Realmente esto implica que se deben crear otros organismos estatales que controlen y administren esta actividad en el país, con los problemas de dominio público ya que las entidades gubernamentales no son del todo eficientes y tienden a volverse entes completamente burocráticos, lo que entorpecería el desarrollo del Negocio Electrónico en el Ecuador.

Los contratos enviados en forma electrónica tendrían el mismo valor que los que se firman y aceptan en papel y su incumplimiento sería motivo de litigios en cortes de justicia. Esto trae a colación otro problema, la Función Judicial ecuatoriana, no está lista para poder hacer frente a la nueva tecnología, cuando en sus juzgados no se cuenta con la infraestructura informática necesaria. Otro aspecto que retrasaría la implantación de la *justicia electrónica*, por llamarla de algún modo es que la fuente de corrupción de la justicia se vería seriamente afectada, debido a que todos los archivos de juicios, contratos y pruebas se llevarían con controles informáticos que son más difíciles de violar.

Por último el proyecto de ley no contempla absolutamente nada de pagos electrónicos, lo que se hace más crítico cuando se entiende que el Negocio Electrónico es una actividad a nivel mundial y que en otros países se cuentan con sistemas de pagos electrónicos, otro factor importante a ser tomando en cuenta cuando se trate los pagos es que éstos no caigan en manos de los típicos estafadores que hacen negocio con el dinero ajeno.

El Consejo Nacional de Telecomunicaciones (CONATEL) autorizará, registrará y regulará a los organismos de certificación. Todas las políticas que rigan a las autoridades de certificación las emitirá la Secretearía de Nacional de Telecomunicaciones (SENATEL). El control de operación será ejercido por la Superintendencia de Telecomunicaciones (SUPTEL).

Con la participación de estos organismos ahora se cuenta con sanciones tanto escritas como económicas, que se encuentran codificadas en la ley.

Como conclusión a este breve análisis del proyecto de ley, está claro que todavía falta mucho por caminar en este sentido en el Ecuador, incluso falta reglamentar adecuadamente la ley, cuando ésta sea aprobada en segunda instancia por el Congreso Nacional, es decir, que todavía se debe esperar a que los organismos que regulan y ejercen el control sobre las actividades de las empresas en el Ecuador reglamenten la parte pertinente de esta ley (ejemplo: SRI, Aduanas, Cámaras de Comercio, etc.). Se debe procurar que proyectos como éstos sean discutidos por gente que conoce la materia, no solamente por políticos, invitar a expertos extranjeros para intercambiar experiencias al nivel de país. Asimismo, es compromiso de las universidades dar al país el elemento humano necesario para que se pueda contar con infraestructuras sólidas de desarrollo, por ejemplo formar personal técnico orientado a la administración de sitios de Negocio Electrónico, formar abogados con conocimientos en telecomunicaciones e informática. En general orientar la cultura de la población para que se familiarice con el entorno tecnológico que vive el mundo entero y no llegar a ser como en muchos otros aspectos, una porción de tierra aislada del mundo, una isla tecnológica.

CAPÍTULO 4

Estudio de Redes Privadas para Negocio y Transacciones Electrónicas Seguras

4.1 INTRODUCCIÓN

"El mercado ecuatoriano tiene capacidad para entrar al B2B y al B2C; en este último lo veo más complicado porque a la gente todavía le gusta ir a las tiendas y examinar los productos; además, no se han dado los pasos previos como la compra por catálogo." Mario Jaramillo, gerente internacional de ADEXUS.[1]

La competencia que enfrenta a empresas ecuatorianas contra emporios gigantescos *punto com* (en el Internet) que adicionalmente, tienen asociaciones con impresionantes empresas dedicadas a la logística, debe ser el punto de partida para diseñar nuevas estrategias. Estas deben llevar a las empresas nacionales a incursionar en la *nueva economía,* como se ha denominado al fenómeno del Negocio Electrónico, con nuevas variantes, las que pongan a prueba toda la capacidad innovadora de nuestra gente.

La interactividad del negocio transaccional y el dinamismo de la nueva economía deben ser la base para el crecimiento de las empresas dentro de la era digital en el Ecuador.

El Negocio Electrónico no es solamente establecer una empresa que publique una página Web en el Internet, sino en el sentido más amplio del concepto, es usar la información electrónica para mejorar el funcionamiento de la empresa, crear valor y establecer nuevas relaciones entre negocios, clientes y proveedores.[2]

Dentro del Negocio Electrónico existen tres puntos clave, a la hora de implementarlo:

---

[1] "COMPUTERWORLD" Ecuador. No 77. Año 03. Pág,10

[2] Esta definición es la utilizada por la Pricewaterhouse-Coopers, para el e-business.

- Debe ser el primero en implementar cierto tipo de comercio electrónico
- La implementación debe se lo más rápida que las circunstancias lo permitan
- El proceso no debe para por ningún motivo, hasta que llegue a su fin

La tendencia que deberían tener las empresas nacionales en Negocio Electrónico es el negocio empresa a empresa (B2B, Business to Business), debido a la penetración muy baja, casi nula que tiene el Internet en los hogares del Ecuador y en general, en los de la región. Esto hace difícil que se pueda desarrollar, por lo menos a mediano plazo, el negocio empresa a consumidor (B2C, Business to Consumer). Por otra parte el negocio empresa administración y el negocio consumidor administración no tienen un desarrollo y una implementación cercana, debido a que en este país no existe una legislación clara sobre Negocio Electrónico y no se ha visto la intención real de parte del gobierno nacional por impulsar esta industria. Sin embargo, como se demostrará más adelante combinaciones de los diferentes tipos de categorías de comercio electrónico, pueden ser las salidas dentro del mercado ecuatoriano.

"Según todos los analistas, las transacciones B2B online serán el motor de los e-negocios." Francisco J. Pachano, consultor de Pricewaterhouse-Coopers.[3]

Todos los criterios emitidos en los capítulos anteriores servirán de base para el presente, brindando un marco de referencia y ciertos lineamientos para convertir una empresa tradicional, en Negocio Electrónico, dentro del ámbito ecuatoriano.

El caso de una empresa local que desea incursionar en el Negocio Electrónico será el eje del presente capítulo, emitiendo los criterios de cambios y de diseño, según sea el caso, para poder implantar la nueva economía en una empresa tradicional, cuyas características se describirán en las secciones posteriores. Sin embargo, se tratará de ser lo más general posible para que este estudio sirva como base para otras empresas que

[3] "COMPUTERWORLD" Ecuador. No. 77. Año 03 Pág,15.

deseen implantar Negocio Electrónico, como es lógico suponer, cada caso será único, pero los criterios emitidos, pueden muy bien aplicarse a diferentes empresas, con ligeras modificaciones, cuyas pautas se encuentran en los capítulos precedentes.

4.2 CASO DE ESTUDIO

El caso de estudio se centra en una empresa ecuatoriana tradicional, que ha operado por más de 20 años ofreciendo soluciones tecnológicas. Su campo de acción local se ha circunscrito a las instituciones financieras, grandes empresas y corporaciones transnacionales de varios frentes, como son industrias alimenticias, industrias licoreras y corporaciones hoteleras.

Esta compañía tiene dos divisiones que comercializan diferentes tipos de productos: la una diseña y vende sistemas de seguridad electrónica y la otra se dedica al desarrollo y venta de software aplicacional de tipo documental y transaccional. Las dos divisiones se encuentran apoyadas por una unidad administrativo/financiera y por una unidad de mercadeo. La jerarquía que se maneja es vertical, se cuenta con una mesa de accionistas, la gerencia, la subgerencia, las gerencias de división y de unidades de apoyo, y los empleados que conforma cada una de ellas.

El sistema de archivos está orientado principalmente a guardar cronológicamente documentos en papel para su posterior consulta, con los problemas evidentes que esto ocasiona, como por ejemplo gran cantidad de espacio físico y tiempo que se necesita para administrar un archivo físico y, la dificultad para encontrar tal o cual documento.

La empresa cuenta con una red LAN mediante la cual se comparten directorios en un servidor de archivos y se tiene un sistema de mensajería electrónica que se utiliza para intercambiar información entre los empleados, cuyo servidor se encuentra en la misma máquina del servidor de archivos. Además, se cuenta con un enlace dedicado hacia un proveedor de servicios de Internet, ISP (del inglés *Internet Service Provider*).

Con este esquema, la empresa ha integrado sistemas uniendo los productos, los servicios y el personal de las dos divisiones, manteniendo un sistema de atención a clientes y de relación con sus proveedores basado en el contacto

personal, atención de llamadas telefónicas, enviando y recibiendo faxes o bien haciendo uso del correo electrónico de Internet. Además, esta empresa ha sido administradora nacional de la mayor y más segura red bancaria del mundo, lo que ha permitido formar profesionales que tienen conocimiento en seguridad de sitios de procesamiento de datos y administración de los mismos.

Con la ayuda de la tabla 1.3 del capítulo 1 sección 1.11 *Sistema de Negocio Electrónico*, se resume la descripción del caso de estudio.

	CASO DE ESTUDIO
Prioridades organizacionales	La empresa cuenta con dos divisiones de negocios independientes
Prioridades del mercado	Cuenta con nichos de mercados específicos para cada división.
Definición de liderazgo	Trata de mantener hegemonía en cierto tipo de negocios y productos, manteniendo la competencia con otras empresas similares.
Relación con los mercados y las compañías no básicas del espacio en blanco	Centrarse en un tipo de producto o servicio dentro del mercado definido sin innovar.
Método para la selección y segmentación del cliente, desarrollo del mercado, inversiones en proceso y tecnología, relaciones organizacionales, grupos de interés externo y financiación, y relaciones con el gobierno.	Orientada a clientes específicos a lo que se ofrecen productos o servicios específicos.
Política de operación financiera	Cada unidad se trata como centro de costos y debe generar utilidades.
Tipos de recursos que se consideran básicos para formular la estrategia.	Los recursos disponibles se encuentran dentro de la organización bajo el mando de los responsables de cada una de las divisiones y unidades de apoyo.

Tabla 4.1 Definición del caso de estudio.

	CASO DE ESTUDIO
Grado de control asumido por los gerentes	Gerencia controla todos las actividades de las divisiones y de las unidades de apoyo.
Campo de acción de las actividades	Las actividades se circunscriben a los mercados de cada una de las divisiones.
Promoción, marcas y relaciones públicas.	Imagen y promoción tradicionales orientadas a los productos, servicios y a la imagen de la empresa.

Tabla 4.1 Definición del caso de estudio (continuación).

4.3 TRASFORMACIÓN HACIA NEGOCIO ELECTRÓNICO

4.3.1 APROXIMACIÓN A LA ECONOMIA DIGITAL

La tabla 4.2 describe las recomendaciones generales para poder iniciar la transformación, de la empresa que es el caso de estudio, hacia la economía digital.

	TRANSFORMACION A LA ECONOMÍA DIGITAL
Prioridades organizacionales	Crear nuevos sistemas de negocios, orientados a comunidades con grupos de colaboración, en donde el trabajo sea complementario.
Prioridades del mercado	Establecer nuevos mercados para el trabajo colaborativo, basándose en estudios de mercado serios.
Definición de liderazgo	Liderar alianzas con competidores y generar oportunidades de negocios para la alianza.
Relación con los mercados y las compañías no básicas del espacio en blanco	Crear nuevos productos y servicios no existentes, basándose en las alianzas con los competidores.

Tabla 4.2 Recomendaciones generales para iniciar la transición.

	TRANSFORMACION A LA ECONOMÍA DIGITAL
Método para la selección y segmentación del cliente, desarrollo del mercado, inversiones en proceso y tecnología, relaciones organizacionales, grupos de interés externo y financiación, y relaciones con el gobierno.	Integración basándose en las oportunidades del mercado y fundamentándose en el sistema formado con los demás participantes.
Política de operación financiera	Optimización del rendimiento total, partiendo de las alianzas, inyectando capital de unos grupos de colaboración a otros, cuando el caso lo requiera.
Tipos de recursos que se consideran básicos para formular la estrategia.	Hacer uso de los recursos que proporcionan los participantes en la alianza y que estén en posibilidad de dirigir el mercado.
Grado de control asumido por los gerentes	Influencia indirecta sobre las actividades de los grupos de colaboración.
Campo de acción de las actividades	Cada grupo colaborativo atendiendo y desarrollándose en diferentes mercados.
Promoción, marcas y relaciones públicas.	Orientada a sacar provecho de los contribuyentes dentro de la alianza para poder recibir realimentación de los clientes.

Tabla 4.2 Recomendaciones generales para iniciar la transición (continuación).

4.3.2 DISEÑO GENERAL

La figura 4.1 indica el proceso y los elementos estructurales de la organización, que intervienen en el diseño de un Negocio Electrónico, así como también las relaciones que tienen entre si. Con la figura 4.1 y las ideas expresadas en el capítulo 1 *Negocio Electrónico: Definiciones y principios* se puede establecer las pautas para iniciar la implantación del Negocio Electrónico en la empresa que es el caso de estudio. Puntualmente el diseño se basa en los puntos 1.15 *Diseño de un Negocio Electrónico* y en el punto 1.16 *Análisis en detalle* del capítulo 1.

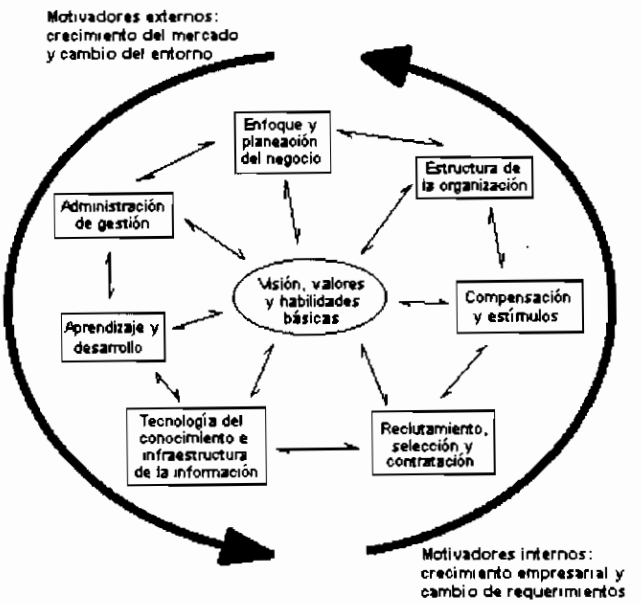


Figura 4.1 Elementos sistemáticos estructurales[4]

4.3.3 ORIENTACIÓN HACIA EL NEGOCIO ELECTRÓNICO

Debido a la crisis vivida desde finales de 1998 hasta el 2001, que ha comprendido la caída de los bancos, el cierre de varias empresas transnacionales, la agudización de los problemas políticos, sociales y morales, y en general la compresión del mercado local, acompañada por otros factores que han golpeado a toda la región, esta empresa se ha visto obligada a buscar otros mercados. El procurar "inventarse" nuevas formas de supervivencia y el haber sido administradores en el Ecuador de la red más importante y más segura a escala mundial dentro del ámbito financiero, han puesto a esta empresa en las puertas de una transformación necesaria e inevitable: la economía digital, el Negocio Electrónico.

Debido a la mínima penetración del Internet en el ámbito nacional y la poca credibilidad de la economía nacional alrededor del mundo, la empresa ha considerado que el diseñar una comunidad virtual de comercio electrónico EBC del tipo de *Alianza* (sección 1.14, punto 1.14.1 *Tipos de EBC*) que es la mejor opción hoy por hoy, siendo le empresa caso de estudio la que liderará la EBC. Para ello se tiene previsto utilizar redes privadas de

[4] "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economia Digital", Don Tapscott, McGraw Hill, 1ra. Ed.,1999, pág. 103.

telecomunicaciones de alta seguridad, para el desarrollo del Negocio Electrónico.

La decisión gerencial ha sido no incursionar directamente el la categoría de B2C, por las razones expuestas arriba. Sin embargo de la tabla 4.1 se ve la necesidad de que toda la empresa como bloque debe asumir el comercio electrónico, y basarse en los mismos esquemas de atención a clientes y logística principalmente. Esto se da ya que toda la organización se encuentra bajo una misma visión, mismos valores y habilidades básicas. Esto hace que se deban replantear las estrategias, la visión y la misión basándose en el Negocio Electrónico, apoyando por la constante actualización tecnológica que permita que la empresa de estudio siga siendo innovadora y pionera en contribuciones tecnológicas.

La preparación académica adecuada del personal debe ser una exigencia primordial. La preparación ligada estrechamente a un adecuado plan de entrenamiento y actualización, permitirá que todo el personal genere conocimiento, tomando como base la información disponible. El entrenamiento debe ser básicamente en asuntos liados estrechamente el Negocio Electrónico como por ejemplo: comercio electrónico, logística, manejo del conocimiento, help desk, procedimientos de seguridad. Toda esta estructura de aprendizaje debe ir acompañada por un eficiente sistema de información dentro de la intranet de la organización, el cual debe disponer de toda la tecnología, estándares y protocolos de web, para su mejor aprovechamiento y su fácil difusión.

La ubicación de esta empresa dentro de la comunidad ha sido definida como el líder dentro espacio de valor. Por otra parte la empresa se encargará de llevar a cabo, con todas las seguridades tecnológicamente y financieramente aceptables, las transacciones, su almacenamiento, registro y en definitiva la administración de todo el espacio de valor generado en la EBC de alianza, que es la que se ha decidido implementar. Por añadidura la atención a clientes será también responsabilidad de la empresa bajo estudio.

Las alianzas estratégicas son el punto de partida para la organización adecuada de la estructura interna de la empresa. Tomando en cuenta que la jerarquía se pierde un poco y da paso a la colaboración.

4.4 SERVICIO AL CLIENTE

Este punto se lo ha tratado de manera aislada debido a la importancia que tiene el trato con clientes dentro de la economía digital. En este punto se indican las pautas generales para el diseño de un eficiente servicio de help desk orientado a empresas que incursionan en el Negocio Electrónico, como es el caso de estudio del presente trabajo.

El principal factor que se toma en cuenta el momento de diseñar un sistema de atención al cliente, es la relación costo/efectividad. "Los problemas del día a día, los constantes cambios tecnológicos, la carencia de información de gestión y la necesidad de mantener personal suficientemente experimentado y formado, se traduce en una enorme dificultad para gestionar los costos." INEA Internet. Sin embargo, un Negocio Electrónico que no disponga de un adecuado help desk no podrá hacer frente al mercado. Para poder dedicarse adecuadamente al comercio electrónico las empresas deben contratar los servicios de terceros, es decir, contar con el outsourcing de este tema. Cabe destacar que dentro del help desk se encuentra la logística de: entrega de mercadería, garantías de productos; por lo que esta actividad de igual manera debe encargarse al outsourcing.

Los beneficios que la organización debe esperar al interior cuando se contrata un servicio de help desk con otra empresa son[7]:

- Centro de atención único para cualquier tipo de problema
- Mejora de servicio a sus usuarios finales
- Reducción de tiempo de resolución de incidentes
- Mayor disponibilidad de sus sistemas
- Valoración productiva de problemas
- Generación de informes detallados para todas las incidencias reportadas
- Reducción de costos administrativos y recursos necesarios

[7] http://www enciclonet.com.ar/productos_y_servicios/helpdesk.htm

- Flexibilidad para el acceso a nuevos requerimientos tecnológicos
- Visibilidad para identificar actividades que pudieran constituir fácilmente áreas de mejora

Por otra parte se debe tener muy en cuenta la óptica de los clientes sobre el tipo de servicio que desean recibir. Es así como todos los clientes de empresas de comercio electrónico tienen las siguientes prioridades[8]:

- Seguridad adecuada de parte de los proveedores de host externos
- Prontas soluciones que permitan una rápida integración al mercado
- Comprensión de las necesidades comerciales específicas de la industria
- Capacidad de integración con los sistemas hereditarios
- Capacidad de crear soluciones acordes con el nuevo diseño de los procesos corporativos

Para realizar el análisis costo/efectividad, y tener los argumentos para tomar la decisión de que la atención a clientes debe hacerse dentro de la organización y no contratar los servicios de terceros, debe tomar muy en cuenta los siguientes aspectos:

- Disponer de las aplicaciones y de las herramientas necesarias
- Seleccionar el personal más apto para desempeñar esa función
- Disponer de analistas calificados en cada una de las áreas de trabajo del Negocio Electrónico
- Definir los horarios de atención a los clientes dependiendo del tipo de negocio que se desarrolle
- Asumir la responsabilidad de manera única sobre cada llamada de los clientes, es decir, que los analistas que reciben la llamada deberán hacer el seguimiento del incidente y de no poder solucionarlo, la empresa debe contar con la infraestructura que permita pasar la llamada a un nivel superior de especialistas
- Contar con un sistema de gestión para poder registrar las llamadas, el especialista que la atenderá, las acciones emprendidas para resolverlas;

[8] http://www br.ibm.com/e-business/espanol/ebusiness/e commerce/services.html

esta información debe ser constantemente revisada para poder incluso anticiparse a los problemas comunes

- Laboratorio de atención a clientes que debe contar con todos los medios de hardware y software dónde se reproduzcan las configuraciones de los clientes y así aislar los problemas que se produzcan

Contar con un sistema de informes y estadísticas para mantener informados a los clientes de las actividades desarrolladas, también un sistema de encuestas y así obtener la realimentación para alcanzar la mayor efectividad y eficiencia en el servicio

4.5 DESCRIPCIÓN DE SERVICIOS

Una vez definidos los puntos de transición de la empresa tradicional al Negocio Electrónico se deben definir los servicios transnacionales y servicios de valor agregado que se pondrán a disposición de los clientes.

El objetivo de esta empresa es llegar a ser el primer ASP (Application Service Provider) del Ecuador, es decir, el primer *proveedor de servicios de aplicaciones* del país. Juntamente con alianzas con los principales ISP (Internet Service Provider) del país, para poder brindar servicios de valor agregado a los clientes de estos últimos y a los clientes antiguos de la empresa. Así como también crear nuevos servicios con los que se interactúe con otras instituciones.

Para poder describir adecuadamente los servicios, en primer lugar se debe elegir el tipo de EBC con el que se va a trabajar. Como se ha mencionado en el capítulo 1, sección 1.14, punto 1.14.1 *Tipos de EBC,* para este caso se ha escogido a la EBC tipo *Alianza* (figura 1.8 EBC de Alianza), con ésta se estructurará la extranet de alta seguridad con la cual se pretende hacer Negocio Electrónico en el Ecuador.

Para el caso de estudio los Productores se convierten en *Proveedores* de cualquier bien o servicio que exista en el mercado ecuatoriano, como: electrodomésticos, computadoras, equipos de audio y video, automóviles, insumos de oficina, insumos agrícolas, alimentos, consultorías de cualquier tipo, bolsa de turismo, bolsa de educación, etc. Completando la figura, se han escogido como Proconsumidores a las instituciones y entidades financieras,

como: cooperativas, mutualistas y bancos. La razón es muy sencilla, las entidades financieras aglutinan a muchas personas, las cuales son sujetas de crédito por las primeras, lo que produce que los bienes y servicios existentes gracias a los proveedores, resultan atractivos a los clientes de las entidades financieras. La figura 4.2 ilustra como queda el modelo de Negocio Electrónico para el caso de estudio.

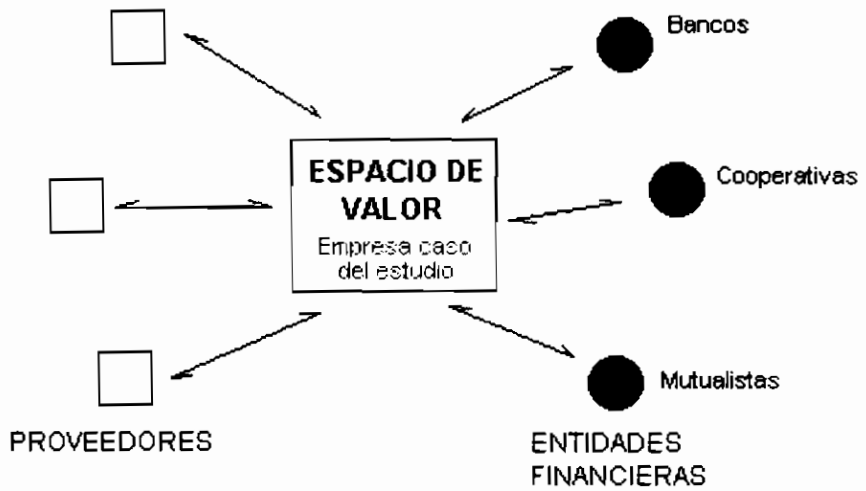


Figura 4.2 Negocio Electrónico de la empresa caso de estudio

Con este principios de trabajo, y esta estrategia de mercado se crea una nueva categoría de Negocio Electrónico que la denominaremos B2B2C (business to business to consumer), siendo los primeros los proveedores, los segundos las entidades financieras y los *consumers* los socios y clientes de las entidades financieras. Este modelo o categoría ha surgido por la dificultad encontrada en el mercado nacional para el desarrollo del Negocio Electrónico, y se cree que es el modelo que cubre las necesidades del mercado local.

Debido a la falta de penetración de Internet y de tecnología de punta en los hogares ecuatorianos las entidades financieras hacen de facilitadoras de tecnología. La tecnología, el procesamiento y el manejo de las relaciones dentro del Negocio Electrónico se realiza en el centro de procesamiento que es la empresa que se estudia, es decir, en el espacio de valor creado.

De este modelo se pueden derivar infinidad de servicios, los mismos que tengan que ver con cualquier ámbito de negocios entre empresas, entre empresas y entidades financieras (que tengan clientes o socios), entre entidades financieras y cualquiera de ellos con sus socios estratégicos y aliados de negocios. Los servicios pueden ser contratados directamente por los interesados o también pueden ser revendidos como servicios de terceros por empresas grandes, por ejemplo ISP.

Esto es en grandes rasgos las características principales de un ASP, donde el negocio no consiste en ser una tubería de datos, sino agregar valor a las transacciones electrónicas. Las aplicaciones que corren en este sitio no son solo cliente/servidor para web, sino toda una infraestructura de *aplicaciones Internet*. No se debe confundir el término de aplicaciones Internet a programas desarrollados exclusivamente para la Red, sino más bien son aplicaciones que utilizan los estándares y protocolos que se utilizan en el Internet.

Del esquema de la figura 4.2, los servicios transaccionales disponibles pueden ser:

- Compra y venta de bienes y servicios
- Giros bancarios desde el exterior con acreditación a cuentas nacionales
- Compensación electrónica entre compradores y vendedores
- Compensación electrónica entre bancos con imágenes de cheques girados
- Administración centralizada de compras
- Bolsa de turismo
- SAN (Storage Area Network), backup corporativo, respaldo de información en grandes volúmenes
- Manejo de exportaciones
- Manejo de cadenas de distribuidores
- Help desk corporativo
- Call center
- Manejo del rol de pagos
- Contabilidad

Cada uno de los servicios mencionados en la lista puede ser particular y ser manejado como proyecto exclusivo para un cliente en particular, llegando a tener incluso su propio servidor dedicado, sus líneas de comunicaciones independientes y su propio sistema de cifrado de datos.

El espacio de valor se crea mediante un tratamiento completamente confiable de la información. Para ello se está utilizando la tecnología de punta para cada una de las áreas involucradas en cada transacción, de esta forma se crea una extranet de alta seguridad, como consecuencia de la experiencia de haber manejado por más de una década la red bancaria mundial con mayor seguridad del mundo.

Las aplicaciones, es decir, el software que se tenga dentro del ASP, debe ser capaz de:

- Generar informes personalizados hacia los compradores o vendedores
- Imprimir los máximos niveles de seguridad, tanto en la intranet, como en la extranet
- Brindar el servicio web a todos los participantes de la comunidad
- Permitir que la interacción de los clientes no necesite en principio, software específico ni complicado, sino más bien un navegador
- Las aplicaciones particulares deben ser *web enable* igualmente pero como es lógico suponer, si se llegara a una particularización grande, el cliente puede llegar a necesitar software específico

4.6 PLANTEAMIENTOS TÉCNICOS PARA EL ASP

Se debe analizar el ASP desde varios puntos de vista, como son:

- Desde el punto de vista de los clientes, el ASP debe garantizar dos aspectos principales:
  - Ofrecer la conectividad hacia su sitio de procesamiento, para poder utilizar todos los servicios disponibles. Cabe mencionar que los canales de comunicaciones desde el cliente hasta el centro de procesamiento del ASP son responsabilidad del cliente. La responsabilidad del ASP es disponer de los medios de acceso, asignados o elegidos por el cliente, siempre disponibles. Ruteadores, servidor de acceso remoto, equipos receptores de enlaces dedicados,

central telefónica, todo en perfecto funcionamiento. No es negocio del ASP las líneas de comunicaciones hacia el centro de procesamiento.
  - Servicios transaccionales contratados siempre disponibles dentro del horario convenido de uso de los mismos.
- Desde el punto de vista del proveedor de servicios, la visión es más compleja ya que se tienen mayor cantidad de variables que manejar, por ejemplo el hecho de que un ASP puede usar los servicios de un ISP y al mismo tiempo dar servicios transaccionales a los clientes del ISP. Los principales puntos a tener en cuenta son:
  - Diseño de la red interna del ASP
  - Canal de conexión al ISP
  - Canales de acceso para sus clientes
  - Planificación de los servicios que se prestarán según lo detallado en la sección 4.5 *Descripción de Servicios* del presente capítulo
  - Mecanismos de seguridad

Por otra parte el ASP debe prestar especial atención a conservar la disponibilidad de sus servicios al ciento por ciento.

El ASP debe tener las siguientes características técnicas para su buen desempeño:

4.6.1 DISPOSITIVOS DE RED

Toda red de computadoras dispone de dispositivos físicos que permiten la interconexión entre máquinas y evidentemente el intercambio de información. No interesa de que tamaño sean las redes, los dispositivos básicos son:

- Los hubs o concentradores, son usados para conectar múltiples usuarios a un dispositivo físico, el cual es conectado a la red. Los hubs o concentradores realizan la misma labor de los repetidores regenerando las señales que pasan a través de ellos, y operan en la capa física del modelo OSI (OSI capa 1). A diferencia de un repetidor que tiene pocas puertas (2 en general), un hub repite las señales por varias puertas (de 5 a 24 puertas). Debido a que operan en la capa física, donde en general

no se considera direccionamiento, no poseen facultades para establecer dominios.

- El bridge es empleado para separar lógicamente segmentos dentro de la misma red, y operan en la capa de datos del modelo OSI (OSI capa 2). Una de las principales funciones de un bridge es poder realizar la traducción de paquetes de tecnologías de capa 2 (por ejemplo: en una puerta ethernet y en la otra token ring).
- El switch es similar al bridge, pero usualmente tiene más puertas. El switch provee un único segmento de red por cada puerta (esto se conoce como microsegmentación) siendo capaz de separar dominios de colisión. De este modo los errores producidos por colisiones de paquetes en un segmento no son transmitidos a los otros. Hoy en día los diseñadores de redes están reemplazando los hubs por switches de manera de incrementar las prestaciones y ancho de banda de una red, conservando las instalaciones de alambrado existentes. Al igual que los bridges, los switches operan en la capa de datos del modelo OSI (OSI capa 2).
- Los routers son equipos diseñados para interconectar redes en el ámbito de la capa de red del modelo OSI (OSI capa 3). Dentro de sus capacidades está la de separar dominios de broadcast, lo que permite realizar un mejor empleo del ancho de banda en una red de gran extensión, de modo que los mensajes de difusión colectiva en una red sólo afectan a la red que los origina, sin utilizar los recursos de las redes vecinas. Los routers encaminan el tráfico de acuerdo al contenido del campo de direccionamiento de los paquetes de capa 3. Los routers son dependientes del protocolo.

Las técnicas de diseño e implementación de las redes actuales utilizan routers y switches para la gestión del tráfico, puesto que además de presentar un mejor desempeño, ofrecen mecanismos de crecimiento más flexible y escalable. Las redes internas se construían utilizando bridges y hubs.

La intranet de la empresa del caso de estudio está formada por una red Ethernet con 25 estaciones de trabajo, en las cuales se deben distribuir

todos los grupos de colaboración que forman la organización. Esta red se encuentra conectada a la extranet el ASP, mediante un computador que hace las veces de ruteador por software (un *gateway*), que cuenta con un firewall incorporado que brinda la seguridad a la intranet y sirve como límite dentro de la extranet, separando la red de la organización de la red del ASP que conforma la EBC.

El diseño de la red interna del ASP, no la extranet, sino el sitio donde se llevarán a cabo las transacciones se recomienda utilizar un modelo jerárquico de capas, lo que permitirá administrar la red desde el punto de vista de unidades independientes, replicables e independientes, aislando los problemas o fallas con mayor facilidad. La figura 4.3 indica un modelo jerárquico sugerido por Cisco Systems.

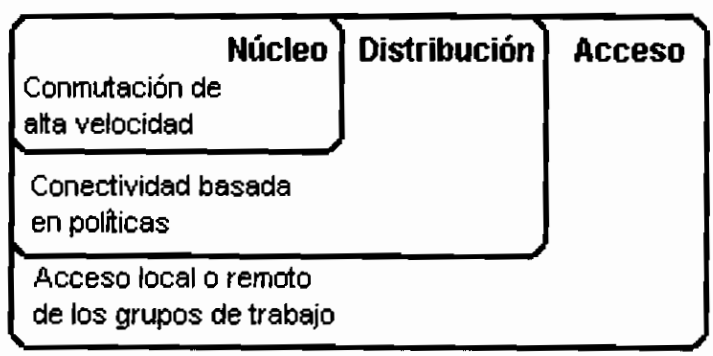


Figura 4.3 Modelo jerárquico de redes para diseño[9]

La figura 4.4 indica el diseño de la de la red dentro del centro de procesamiento del ASP, donde se muestra claramente las tres capas del modelo jerárquico.

[9] http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm

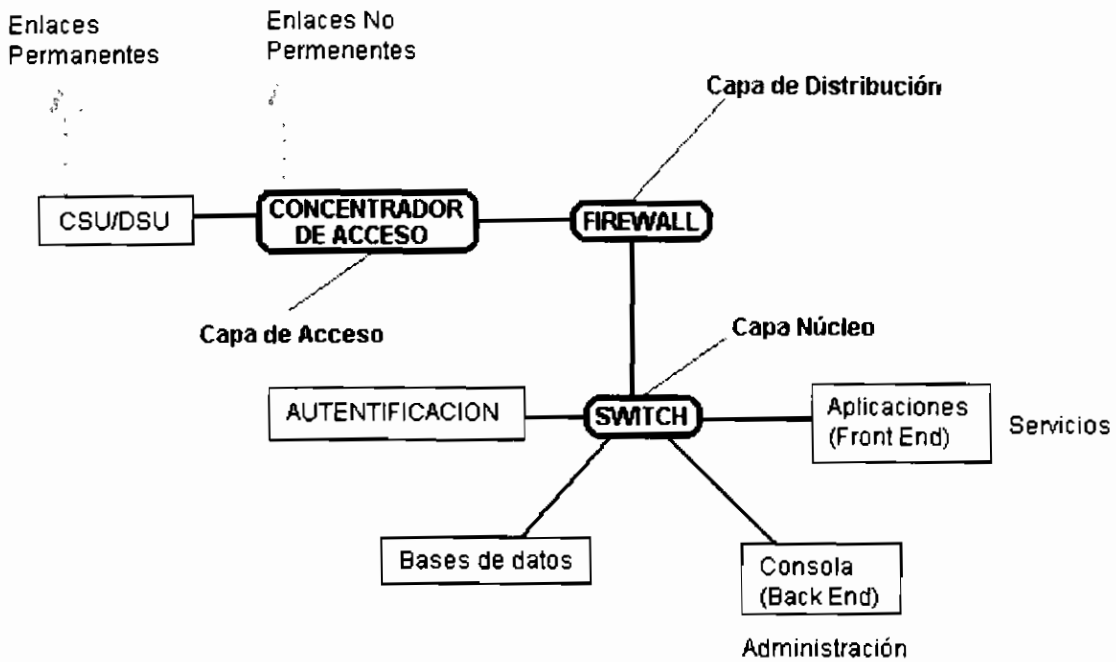


Figura 4.4 Estructura Interna del ASP

4.6.2 SOFTWARE

Para la conexión, los clientes deben disponer del software necesario esto es: Windows 9x, Mac OS y Linux, entre otros, incluyen un conjunto de aplicaciones necesarias para establecer su conexión y además de navegadores como Internet Explorer de Microsoft o Navigator de Nestcape, que incluyen los protocolos IP necesarios para la comunicación. Ambos navegadores implementan HTML (web), NNTP (noticias), FTP (transferencia de archivos) y SMTP/POP3 (correo). En este punto los usuarios están conectados, y pueden obtener más programas. Como se puede observar no es software *raro* ni tampoco específico de cada cliente.

Dentro del software se encuentran todos los paquetes de cifrado de datos, es decir la infraestructura de llaves que se indicó en el capítulo 3 del presente trabajo.

4.6.3 CANALES DE COMUNICACIONES Y CIFRADO

Por la naturaleza de este ASP, el número de clientes que manejará no sobrepasará los 1000. todos los canales de comunicaciones deben disponer del protocolo IPSec que se analizó en el capítulo 3 punto 3.7 *Seguridad y TCP/IP*.

La infraestructura de comunicaciones básica con la que debe contar el ASP es la siguiente (capa de acceso figura 4.4):

- Canal de acceso ASP a ISP
- Canal de acceso cliente a ASP
- Canal de acceso ASP a medio de pago

4.6.3.1 Canal de acceso ASP a ISP

Este canal de comunicaciones debe estar disponible para:

- Mantener la comunicación con empresas que se encuentran fuera del país y con las cuales se ha llegado a acuerdos previos para formar la EBC
- Brindar servicios corporativos de valor agregado a los clientes del ISP
- Brindar acceso al Internet al personal de la empresa

Dentro de las posibilidades del negocio no se recomienda tener un canal a un ISP, sino más bien asociarse con algunos de ellos, para de esta manera ampliar el espectro de clientes a los cuales se les ofrezcan servicios de valor agregado.

Dependiendo de los clientes, los servicios y el grado de eficiencia que se desea se pueden contratar canales X.25, ATM, Frame Relay. Los más recomendados para estos casos son las líneas xDSL, ya que proveen servicios de alta velocidad con un bajo costo. Toda la información relativa se encuentra en el capítulo 2 del presente trabajo. Todos los enlaces deben ser protegidos con protocolos SSL (capítulo 3 punto 3.6 *Capa de Conexiones Seguras*)

En el caso de que la EBC se ha formado con empresas del extranjero, se debe aumentar un servidor en el centro de procesamiento, el mismo que maneje protocolos de túnel para de esta manera formar una red privada

virtual (como se describe en el capítulo 2 punto 2.6.7 *Redes Privadas Virtuales*). Si se desea añadir mayor seguridad se puede implementar protocolos de cifrado como SSL.

En la figura 4.4 este canal estaría formando parte de los especificados como *enlaces permanentes* que se encuentran conectados al CSU/DSU (Chanell Service Unit/Data Service Unit) que son las unidades de servicio de canal y de datos, respectivamente.

4.6.3.2 Canal de acceso cliente a ASP

Este enlace puede ser dedicado (permanente) o no dedicado (no permanente). En cualquiera de los dos casos se deberán utilizar los protocolos de autenticación más adecuados para las necesidades de los usuarios, se recomienda SSL, por las bondades presentadas en el capítulo 3 del presente trabajo.

4.6.3.2.1 Canal de acceso cliente a ASP permanente

De igual manera que el canal de acceso ASP a ISP, un cliente puede hacer uso de los servicios del ASP mediante una conexión dedicada con cualquiera de las tecnologías analizadas en el punto 4.6.3.1.

4.6.3.2.2 Canal de acceso cliente a ASP no permanente

En este caso el cliente debe disponer de un módem de preferencia que cumpla la recomendación V.90 de la UIT-T para el acceso remoto. Esta recomendación especifica módems de 32 - 56 kbps con capacidad de datos, fax y telefonía, además configurar en la computadora el acceso telefónico a redes con los protocolos PPP (capítulo 2 punto 2.5.6 *Protocolo Punto a Punto*), de esta manera se pude establecer una comunicación con el protocolo TCP/IP, además de requerir la contraseña encriptada.

4.6.3.3 Canal de acceso ASP a medio de pago

Este canal de comunicaciones se puede formar desde dos puntos de vista: canal directo con el medio de pagos, red privada virtual utilizando Internet.

Este medio de comunicaciones deberá ser permanente, ya que se estima que las transacciones de compensación entre participantes de la EBC puede llegar a ocurrir en cualquier momento del día, más aún si se tiene previsto estructurar la EBC con empresas del extranjero.

Cabe mencionar que éste no se trata de un canal hacia un medio de pago único, sino más bien hacia varias instituciones que pueden funcionar como medio de pagos para las transacciones que se presenten en las negociaciones electrónicas. Entre los medios de pago, se pueden tener, bancos, tarjetas de crédito, cooperativas de ahorro y crédito o financieras.

Los protocolos de cifrado, indicado en el capítulo 3 del presente trabajo, para transacciones financieras, son lo que se deben implementar dentro de los servicios que brinde el ASP. El protocolo más recomendado es SET, por las prestaciones que presenta (capítulo 3 punto 3.10.2 *Pagos Digitales*)

4.6.3.3.1 Canal directo con el medio de pago

Utilizando CSU/DSU para mantener el canal funcionando, de igual manera se pueden utilizar las tecnologías mencionadas en el punto 4.6.3.1, dependiendo de la infraestructura que tenga el o los medios de pagos con los que la empresa firme contratos.

Esta conexión se utilizaría por ejemplo para enlazar varios bancos para realizar la cámara de compensación nocturna, utilizando las imágenes de los cheques depositados en cada banco.

4.6.3.3.2 VPN utilizando Internet

Utilizando los protocolos de túnel para la formación de VPN, se pueden enlazar el servidor web del ASP con el servidor web del medio de pagos, para de esta manera formar una extranet de alta seguridad, utilizando el Internet, lo que baja los costos de implementación. Sin embargo, al tratarse del Internet se deben aumentar las seguridades y esta posibilidad debe ser muy bien estudiada y diseñada de tal manera que los riesgos que se presenten sean mínimos.

Esta conexión se utilizaría cuando por ejemplo se realiza una venta de un electrodoméstico en una cooperativa y ésta debe pagar al proveedor mediante un giro bancario al banco del segundo que posee una sitio web;

o cuando se ha realizado la compra de insumos agrícolas utilizando una tarjeta de crédito y se debe hacer el respectivo débito de la tarjeta del comprador, mediante la el sitio web del banco que maneja dicha tarjeta.

4.6.4 PROTECCIÓN DE INFORMACIÓN

4.6.4.1 Protecciones físicas

Dentro de las protecciones físicas se deben instalar:

- Sistemas contra incendios
- Sistemas de extinción de incendios
- Sistemas de acceso al sitio central de procesamiento
- Sistemas anti robo
- Sistemas de circuito cerrado de televisión

Todos estos sistemas deben ser continuamente supervisados por lo que la creación de un listo de chequeo es una práctica muy recomendable. Este chequeo se lo debe hacer de manera diaria, y mensual. Es factible incluir dentro de este listado aspectos relacionados con los equipos de comunicaciones y con el hardware.

El listado de chequeo debe contener los siguientes puntos:

- Verificación de la energía eléctrica que alimenta al sitio
- Chequeo de luces de emergencia
- Detectores de incendios operativos
- Detectores de movimiento operativos
- Verificación de los extintores de incendios (carga del cilindro)
- Operatividad de la central de extinción y sus respectivos tanques de gas
- Aires acondicionados operativos con sus respectivos medidores de humedad y temperatura
- Paneles de acceso operativos (mantenimiento de claves de acceso)
- Verificación del sistema de CCTV cintas de grabación y equipo grabador/reproductor
- Verificación de las líneas telefónicas de acceso al sitio

- Verificación de los equipos CSU/DSU que manejan los enlaces dedicados
- Verificación de operación de todos los servidores del sitio
- Verificación de los equipos de comunicación interna, como son los hubs, switches, ruteadores y gateways
- Verificación de los canales de comunicaciones dedicados con: los ISP, los medios de pago, los clientes

4.6.4.2 Seguridades de la información

Las seguridades de los datos tienen que ver mucho, como es lógico, con las seguridades físicas, pero también se deben tener en cuenta aspectos de respaldo de datos, almacenamiento de datos así como también elegir los equipos más adecuados para el sitio central de procesamiento. Arreglos de RAID (Redundant Array of Inexpensive [independet] Disk) que consiste en un conjunto de discos duros donde se almacena la información en forma redundante, es una de las opciones más recomendables para la seguridad de los datos, incrementando la tolerancia a los fallos debido a que se incrementa el tiempo medio entre errores y mejorando el rendimiento del sistema.

De manera similar al listado de seguridades físicas, debe existir otro que verifique el estado del software de aplicación y de base de datos que se manejan en el sitio. Los puntos principales que deben tener estos listados son:

- Verificación de que todas las aplicaciones necesarias se encuentren corriendo
- Verificación de funcionamiento de los firewalls por software (que no hayan sufrido atentados, por ejemplo que no estén haciendo procesos innecesarios de manera espontánea)
- Chequeo de listado de accesos permitidos (mantenimiento de los acceso al sitio)
- Que se encuentren levantados todos los servicios necesarios para el web, así como también todos los servicios para el correcto funcionamiento de las bases de datos

- Verificar el listado de accesos y buscar intentos de acceso no permitidos y anomalías similares
- Verificación del correcto funcionamiento de los protocolos de cifrado y de comunicaciones instalados en las máquinas que brindan el servicio

4.6.4.3 Seguridades de cifrado

Dependiendo de las necesidades de comunicación que se presenten el la implantación de la central de procesamiento, los protocolos de cifrado de datos deben irse adaptando. Se deben tomar en cuenta aspectos legales de utilización. Por ejemplo el protocolo SSL o el protocolo SET que se comercializa fuera de los Estados Unidos tiene un número de bits de encripción menor que el que se utiliza en el país del norte. Lo mismo ocurre con el software que se utilice para desarrollar el Negocio Electrónico, los fabricantes no liberan últimas versiones para Latinoamérica, por lo que no es aconsejable instalar software que no se encuentre liberado aún, ya que no se dispone del respaldo adecuado.

4.6.4.4 Seguridades contra piratas

El principal elemento que se tiene para proteger el sitio contra ataques de piratas informáticos son los firewalls, por lo que su correcta configuración y su adecuada ubicación es fundamental para evitar dolores de cabeza.

Se recomienda utilizar la configuración c) de la figura 3.2 que se encuentra en el capítulo 3 sección 3.8 *Cortafuegos o Firewalls*. Para que la seguridad sea mayor se debe utilizar firewalls con la técnica global de múltiples niveles SMKT, la cual se explica en la misma sección.

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1 CONCLUSIONES

5.1.1 REDES DE TELECOMUNICACIONES Y NEGOCIO ELECTRÓNICO

La nueva economía se fundamenta en el intercambio de información electrónica. Pero esta información es árida y no tiene sentido sino se la transforma en conocimiento, con este objetivo en mente, el intercambio de información debe ser lo más eficiente, sencillo y seguro posible, para de esta manera permitir a las personas que generen el conocimiento y se puedan llevar a cabo todo tipo de transacciones de Negocio Electrónico y se agregue valor a las mismas. Hoy por hoy, el mejor medio de comunicación entre individuos utilizando los sistemas informáticos es la computación de red. Esta es la tercera etapa dentro de la evolución de las redes de información electrónica, y toma lo mejor de las dos etapas predecesoras que son: los mainframes y el modelo cliente/servidor. Haciendo que la computación sea más manejable y también hace uso de la experiencia de los usuarios con las interfaces gráficas.

El otro aporte del Negocio Electrónico en cuanto a las tecnologías de comunicación de datos, es que al ser una aplicación nacida del Internet, los protocolos que utiliza son la familia TCP/IP, por lo que la estandarización para esta actividad se inicia por la base, es decir, por las comunicaciones.

Si se habla de las tecnologías de telecomunicaciones, se puede decir que cualquiera de ellas, que se desenvuelva correctamente con TCP/IP, es válida para transmitir datos y transacciones de Negocio Electrónico, sin hacer preferencia por ninguna actual o que se pueda presentar en el futuro. Lo que se requiere es que los sistemas de comunicaciones pongan en línea y dentro de un ambiente seguro a empleados, clientes, proveedores y en general a todos los socios comerciales de una empresa. Se ha visto que la mejor opción para realizar este objetivo son las redes privadas de

telecomunicaciones y en particular las Extranets ya que van más allá del Internet y de las Intranets. Esta característica hace que esta plataforma tecnológica permita generar un sinnúmero de aplicaciones.

Las extranets cobran mayor importancia cuando los estudios indican que la categoría de Negocio Electrónico con mayor crecimiento para los próximos años es el negocio empresa a empresa (B2B), con lo cual estar en línea con los socios comerciales es un aspecto fundamental para el desarrollo del negocio.

5.1.2 REDES PRIVADAS (EXTRANETS)

Como ya se ha explicado la mejor opción dentro de las redes privadas de comunicaciones son las Extranets. Estas hacen uso de cualquier infraestructura existente ya sean públicas (Internet) o privadas (Intranets), haciendo a las primeras seguras y confiables para el tipo de negocio y a las segundas fortaleciendo sus características de seguridad.

En cualesquiera de los dos casos, las extranets añaden valor a las redes, en el sentido de que las hacen lo suficientemente flexibles, como para adaptarse a los constantes cambios que se presentan en el mercado.

De igual manera el protocolo que utilizan es el TCP/IP, como ya se indicó, lo que permite que se desarrollen todas las aplicaciones necesarias.

El complemento para que una extranet sea tal, son los temas relacionados con la seguridad, tales como: los protocolos y las aplicaciones de cifrado de datos, y los cortafuegos o firewalls, sin estos dos elementos no se puede tener la seguridad que se persigue.

5.1.3 NEGOCIO ELECTRÓNICO Y SUS SERVICIOS

A pesar de tener toda la infraestructura de comunicaciones, las mejores computadoras y los mejores servidores, así como también el software de última versión, el Negocio Electrónico, como se ha explicado antes, se basa exclusivamente en el conocimiento y éste no puede ser generado sino por los seres humanos. Por este motivo uniendo el potencial de las personas y la funcionalidad de las redes de información y más puntualmente de las prestaciones de las extranets, los servicios que se pueden dar por medio del Negocio Electrónico son muy variados: ventas, mercadotecnia, publicación

en línea, servicio al cliente, desarrollo de productos, servicio de directorios (bases de datos), comunicación entre empleados, proyectos en grupos, servicios bancarios, etc. Solamente el potencial humano puede poner límites en cuanto a las aplicaciones que se puedan llegar a tener al conjugar las extranets con el comercio electrónico.

5.1.4 TRANSACCIONES ELECTRÓNICAS Y FLUJOS DE INFORMACIÓN

Las transacciones electrónicas y los flujos de información son el resultados del análisis previo de ciertos aspectos de la vida cotidiana, pero siempre con ojos en el futuro. Debido a este fenómeno las transacciones deben ser constantemente monitoreadas con el objetivo de corregirlas y/o adaptarlas, a los cambios que se puedan presentar. Siempre que se trabaje con información electrónica existirán flujos, los mismos que a la par de las transacciones también debe irse mejorando y optimizando.

Toda transacción en Negocio Electrónico se generará del lado del cliente, véase a éste como cliente, proveedor, empleado, o socio, es decir, que se originará una petición y evidentemente este flujo de información deberá llegar a un sitio dónde será procesada. Este proceso genera luego otro flujo, el mismo que llevará una respuesta y además las acciones que ciertos elementos dentro de la red (sean personas o máquinas), lo que deben llevar a cabo las instrucciones. Nuevamente se genera otro flujo con los resultados de las acciones, las misma que pueden ser el resultado final u otra petición. En breves rasgos, este es el flujo de información dentro de una transacción electrónica. En que lugar se lleva a cabo la petición, las respuesta, las acciones y las nuevas peticiones, desde el punto de vista de la red, es completamente independiente del buen término de una transacción.

5.1.5 NEGOCIO ELECTRÓNICO EN EL ECUADOR

Como se puede ver en el presente trabajo, el Ecuador no presta todas las facilidades para el desarrollo del Negocio Electrónico, por lo que las empresas locales deben acomodarse a las circunstancias del mercado (políticas, sociales, morales) para poder generar resultados por medio de esta actividad. En el caso de esta tesis, se ha llegado a la creación de otra categoría dentro del Negocio Electrónico, la cual se la ha denominado

B2B2C (business to business to consumer). La idea es poder llegar a la mayor cantidad de personas en el Ecuador utilizando a empresas que por actividades económicas primero aglutinen a una masa humana y segundo posean la tecnología para poder ser facilitadoras, en cuanto a los servicios que se pueden ofrecer utilizando esta actividad. Claro está que todavía falta mucho por recorrer debido a dos razones principales:

- La gente en Ecuador está todavía acostumbrada a comprar de la forma antigua (si es posible utilizar este término), es decir, viendo el bien, tocándolo y probándolo él mismo. La compra virtual, en la que solamente se pueden leer las características de un bien y en el mejor de los casos mirar su fotografía, genera cierta desconfianza al cliente, la cual desaparecerá en la siguientes generaciones.
- El gobierno no está listo todavía para tecnificar todas las áreas involucradas en el desarrollo del Negocio Electrónico. Ni siquiera se cuenta con una ley completamente aprobada y en vigencia, la que normalice esta actividad y por lo que se puede observar no está dentro de los planes a corto plazo. La justicia, los entes recaudadores de impuestos, los ministerios, en general los entes gubernamentales, no manejan la tecnología necesaria, para poder implementar a nivel nacional un programa que permita la digitalización de trámites y de esa forma contar con agilidad en todos servicios públicos, lo que implicaría implementación de un modelo de Negocio Electrónico a escala nacional.

La otra traba que se encuentra es que las personas, al oír hablar de Negocio Electrónico, asumen que se trata de un asunto muy superficial, como publicar una página web en el Internet donde vendan algo y esperar que los pedidos les lleguen. Esto no puede estar más alejado de la realidad. Negocio Electrónico es toda la reorientación de la empresa: su visión, su misión, sus políticas, sus estrategias, su servicio a clientes su logística, en fin todas las actividades que implica instalar un negocio tradicional, deben replantearse cuando de la economía digital se trata.

Necesariamente más tarde o más temprano todos estaremos inmersos en transacciones electrónicas, debido a que al ser una corriente mundial y de una gran fuerza, necesariamente deberemos aprender a vivir dentro de la economía digital.

5.2 RECOMENDACIONES

5.2.1 POR HACER

Es difícil enumerar todos los elementos que faltan para poder desarrollar esta actividad de manera adecuada, no solamente en el Ecuador sino en el ámbito mundial. La globalización es un fenómeno de gran inercia que se inició a mediados de los años 80, realmente no sabemos todo lo que implica. Por ahora se deben mejorar los sistemas de logística y de servicio a clientes para poder hacer frente a la gran ola que se acerca y de la cual será muy difícil escapar y además si no nos encontramos debidamente preparados simplemente nos hundirá sin más.

Esta actividad así como su normalización y desarrollo debe estar en manos de profesionales entendidos y no en las manos de oportunistas que solamente desean sacar provecho de la confusión que generan cuando intentan promulgar leyes confusas y sin argumentos claros.

5.2.2 FORMACIÓN PROFESIONAL

Necesariamente se deben formar profesionales orientados al Negocio Electrónico. Hasta hoy en el país se ha trabajado en base a las experiencias del extranjero, con profesionales del extranjeros, pero en ningún caso se han analizado las necesidades del mercado nacional. El B2B2C en el fruto de casi 2 años de trabajo, no es la última opción pero hoy es la que más se adpta a las necesidades del Ecuador. De la misma manera que surgió el B2B2C pueden surgir otras alternativas, siempre y cuando se cuente con profesionales que tengan las bases científicas sólidas en aspectos relacionados con:

- Telecomunicaciones
- Administración de personal
- Informática

- Manejo de proyectos
- Conocimientos financieros

Aparentemente son disciplinas dispersas, pero cuando se trata de proyectos con el Negocio Electrónico todos los ámbitos del saber humano son necesarios para el buen desenvolvimiento de esta actividad.

5.2.3 PROYECCIONES

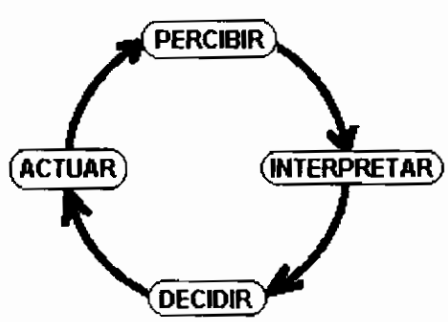
Respecto al trabajo de tesis está incompleto en cuanto a:

- Estudio de mercadeo y en base a él a la reorganización de las estrategias empresariales
- Análisis financiero que junto con un apropiada plan de negocios permita tener una mejor visión del ámbito del negocio y sus verdaderos alcances

Estos dos aspectos complementarán al análisis técnico que es el centro del presente trabajo.

Como es un tema altamente variable, es posible que algunos argumentos expresados en esta tesis no tengan validez, por lo que es necesario una constante actualización e investigación en temas relacionados con las técnicas relativas a las transacciones electrónicas y sus aplicaciones.

Siempre es necesario hacer uso del ciclo de adaptación para poder prever el futuro y poder tomar las decisiones adecuadas. El ciclo es el siguiente:



5.3 ANALISIS FODA

Para complementar las conclusiones y recomendaciones emitidas, he creído conveniente realizar un análisis de fortalezas y debilidades del presente trabajo, así como también las oportunidades y amenazas de esta actividad en el Ecuador.

5.3.1 FORTALEZAS

- La categoría de Negocio Electrónico descrita en la presente tesis es pionera dentro del territorio nacional, lo que presupone una ventaja competitiva frente a las demás empresas que desean incursionar en esta actividad
- Se han analizado todos los aspectos tecnológicos necesarios para la implantación de este modelo de negocio
- Es el primer estudio de Negocio Electrónico orientado al ámbito ecuatoriano y haciendo hincapié en la importancia de las redes privadas de telecomunicaciones, cuya expresión más amplia son las extranets

5.3.2 DEBILIDADES

- Este trabajo no cuenta la planeación de ventas, promoción y en general la planeación estratégica, que un e-business necesita, debido a que no fue planteamiento de esta tesis
- Un análisis financiero es el complemento, que junto a la planeación estratégica complementa todo el estudio para implementar un Negocio Electrónico en el Ecuador
- Debido a la amplitud del tema realmente no se puede dar una receta única para la implantación del Negocio Electrónico en el ámbito mundial y tampoco en el nacional

5.3.3 OPORTUNIDADES

- El Negocio Electrónico apunta a generar nuevas formas de realizar actividades económicas en el Ecuador
- El nuevo modelo de Negocio Electrónico se puede convertir en un producto de exportación si se toman las medidas adecuadas en el mercado internacional
- Los profesionales jóvenes, con la preparación académica necesaria, están adquiriendo la visión del nuevo entorno tecnológico en el cual se realizarán los negocios, lo que permitirá ubicar esta actividad en el entorno internacional

5.3.4 AMENAZAS

- La principal amenaza para el Negocio Electrónico, en el Ecuador, es no contar con un marco legal vigente, que normalice todos los procedimientos y demás actividades relacionadas
- El constante cambio tecnológico se convierte en una amenaza debido a que la agregación de valor a las transacciones, solamente se puede dar eficientemente, con la última tecnología probada a nivel mundial

Glosario de términos

A	
Administrador de sistemas	(System Adminitrator) Persona con autoridad y capacidades informáticas especiales, que establece los usuarios, los recursos de ordenador y las medidas de seguridad (incluyendo identificaciones y contraseñas del usuario) en un sistema de ordenador determinado.
API	(Aplication Program Interface) Interfaz que posibilita la comunicación entre programas, redes y bases de datos.
ASP	(Active Server Pages) Página activa dentro de un servidor web.
ASP	(Application Service Provider) Proveedor de aplicaciones que proporciona la infraestructura tecnológica para proveer el uso de aplicaciones y sistemas.
Autenticación	Proceso ejecutado entre un emisor y un receptor de un canal de transmisión para garantizar la integridad de los datos y la autenticidad del origen de los mismos.
Autoridad de Certificación	(CA) Es un organismo, público o privado, que garantiza la veracidad de la identidad de los participantes y orígenes en una transacción electrónica, mediante el uso de una infraestructura de claves públicas y privadas.
Autoridad de Registro	(RA) Es la entidad encargada de identificar de manera inequívoca a los usuarios para que soliciten un certificado a la CA, así como de gestionar los certificados.

B	
B2B	(Business to business) Negocios electrónicos realizados entre empresas.
B2B2C	(Busines to busines to consumer) Negocios electrónicos que llegar al consumidor a través de entidades facilitadoras de tecnología.
B2C	(Business to customer) Negocios electrónicos realizados entre empresas y consumidores.
Back-end	El mundo del comercio electrónico puede ser dividido en dos secciones distintas –el front-end y el back-end -. El front-end de un negocio de comercio electrónico, comprende todo aquello que el consumidor vé cuando visita la página : la pagina Web, el catálogo... El back-end hace referencia a la compleja infraestructura que da servicios tales como pasarelas de pagos, logísticas y atención al cliente.
BPR	(Business process reenginering) Consiste en el rediseño de los procesos de negocio, que provocan cambios drásticos en la organización.
Broker on line	(e-broker) Intermediario en un proceso de comercio electrónico que añade algún tipo de valor informacional, de seguridad o riesgo.
Browser	Navegador, visor de HTML.
Buscador	Programas que se ofrecen en ciertas páginas web, que estructuran de manera sistemática y jerárquica la información distribuida por la red.
Business Inteligence	Proceso interactivo para analizar, explorar y estructurar información. Generalmente datos referentes sobre nuestros productos, nuestros clientes y de la competencia.

C	
Carro de la compra	(Shopping Cart) Aplicación que procesa las órdenes de compra mientras los compradores navegan por la tienda virtual. Es utilizado para elegir y almacenar temporalmente los productos que compran los clientes.
Catálogo	Relación de productos y servicios que contiene información relacionada con los mismos (precio, condiciones de venta o envío, características técnicas, características de aplicación o uso, etc.).
Categorías	Agrupaciones de los productos de un catálogo que facilitan su compra.
Centro de certificación de claves	Instalación manejada por la Autoridad de Certificación, que genera y devuelve certificados, se asimila a la autoridad de certificación y muy rara vez se toma como termino independiente.
Certificado	Un certificado es un documento digital de identidad emitido por una Autoridad de Certificación que garantiza que el individuo, empresa u organización en general es quien dice ser en una transacción sobre la red. Es aplicable también a los programas software para garantizar su integridad frente a virus.
Certificados X.509	Es el protocolo que más se está extendiendo a la hora de garantizar las comunicaciones seguras entre redes de comunicación abierta como Internet, según la recomendación de la ITU-T (International Telecommunication Union-Telecommunication Standarization Sector). Su función principal es la de garantizar la identidad de los participantes en transacciones en redes abiertas, la integridad de esas comunicaciones y la privacidad y no repudio de los mensajes.

CGI	(Common gateway interface) Método estándar que permite a los documentos Web utilizar programas que están residentes en el sistema principal.
Ciberespacio	(Cyberspace) Palabra utilizada comúnmente para referirse al conjunto de sitios Web en la WWW.
Cifrado	Mecanismos y algoritmos utilizados para garantizar la confidencialidad de la información. Los sistemas de cifrado se clasifican en simétricos o asimétricos, según la clave utilizada para cifrar y descifrar sean la misma o diferente, respectivamente.
Cifrado asimétrico	1.- Algoritmo de cifra basado en una función irreversible con trampa. Este algoritmo y su inverso dependen de dos claves diferentes, denominadas pública y privada, tales que el conocimiento de una no conduce a la otra. Tanto el algoritmo como su inverso, cada uno con su clave correspondiente, puede ser empleado para cifrar, descifrándose con el contrario. 2.- Cifrado obtenido mediante técnicas criptográficas asimétricas.
Cifrado simétrico	Algoritmo de cifra basado en una función invertible, tal que tanto el algoritmo como su inverso dependen de un parámetro igual para ambos llamado clave secreta
Clave privada	En un criptosistema asimétrico, clave criptográfica de un usuario solo conocida por el mismo
Clave pública	En un criptosistema asimétrico, clave criptográfica de un usuario que se hace de público conocimiento
Clave simétrica	Clave utilizada por los sistemas de criptografía simétricos

Collaborations Platforms	(Plataformas de colaboración) Compañías que suministran herramientas y componentes online, para proyectos conjuntos entre empresas, independientemente de su localización geográfica. Otra opción es la de suministrar la plataforma a socios que pagan un canon de utilización. Proporcionan utilidades adicionales de gestión documental, flujos de trabajo, etc.
Cookie	(Espía, delator, fisgón , galletita, soplón) Fichero almacenado en el disco duro del visitante, con o sin su consentimiento explícito, que registra información sobre su navegación por el sitio entre varias visitas. Todo ello con el objetivo de reconocer al usuario para personalizar la Web, y ofrecer al Contenido, Servicios, Comercio e Información que le puede interesar. Dado que pueden ser un peligro para la intimidad de los usuarios, éstos deben saber que los navegadores permiten desactivar los "cuquis".
Cracker	(Intruso, revientasistemas, saboteador) Un cracker es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y suelen disponer de muchos medios para introducirse en un sistema.
Content Management	(Manejo de contenido). Permiten al usuario manejar todos sus datos de manera electrónica, permitiendo así reducir costos de almacenaje, incrementar seguridad, incrementar productividad, mejorar el servicio al cliente.
CRM	(Customer relationship management) Gestión de la relación con los clientes, que va desde las actividades de atraer, interesar, generar ventas y fidelizar. Estrategia tecnológica que consiste en convertir los datos de nuestros clientes en respuestas de negocio que se anticipen al comportamiento de estos.

Customización	Proceso por el cual el consumidor o visitante selecciona las preferencias del producto o servicio físico, o contenidos de información, que desea le sean suministrados.
Cybercash	Procedimiento por el cual la información de la tarjeta de crédito es pasada a una red privada usada por las instituciones financieras para autentificar y comprobar los fondos de la tarjeta de crédito.

D	
Data Mining	Es la extracción de información oculta y predecible de grandes bases de datos, es una poderosa tecnología nueva con gran potencial para ayudar a las compañías a concentrarse en la información más importante de sus Bases de Información (Data Warehouse). Las herramientas de Data Mining predicen futuras tendencias y comportamientos, permitiendo en los negocios tomar decisiones proactivas y conducidas por un conocimiento acabado de la información.
Data Warehouse	Sistema para el almacenamiento y distribución de cantidades masivas de datos.
DHML	(Dynamic HTML) Lenguaje mas avanzado que el HTML que permite la animación de las páginas web así como cierta interactividad.
Dinero electrónico o *digital*	Es el dinero del que el usuario puede disponer haciendo download desde su cuenta bancaria El "dinero" puede ser transferido desde el PC del comprador hasta el vendedor y posteriormente al banco.

E	
e-billing	(Facturación online) Proceso de cálculo, configuración y emisión de facturas utilizando medios electrónicos.

e-business	Negocios por Redes de telecomunicaciones, sean tradicionales o adaptados al nuevo medio
e-commerce	(Comercio electrónico) Proceso de comprar, venta o intercambio de productos, servicios e información utilizando redes de ordenadores. En sentido amplio cualquier forma de negocio utilizando medios electrónicos.
EDI	Electronic Data Interchange(electronic data interchange): Intercambio electrónico de documentos mercantiles. Se dice que es el precursor del comercio electronico
e-mall	(Centros comerciales online) Centros virtuales que agrupan la oferta de múltiples tiendas virtuales sectoriales con el fin de aumentar visibilidad, reducir costes y compartir sinergias.
e-Marketplace	Mercado virtual, que integra compradores (buy-side) que desean aprovisionarse, y vendedores (sell-side) que desean comercializar sus productos
e-procurement	(e-aprovisionamiento) Gestión del aprovisionamiento de materias primas y servicios básicos en los procesos de producción de una empresa., en particular compras de tipo MRO(mantenimiento, reparaciones, operaciones), que normalmente se incluyen dentro del epígrafe de compras generales y que en algunos sectores llegan a suponer casi el 40% del coste total del negocio.
ERP	Enterprise Resource Planning, Software de gestión integrada modular, usado para gestionar los procesos internos de las empresas.

	Este Software permite realizar un seguimiento de las ordenes y pedidos que se producen, las diferentes planificaciones de producción, gestión del inventario.... También dispone módulos para gestionar los recursos humanos, la distribución y las finanzas de la empresa. Debido a su alto coste, complejidad y tiempo de implantación, las empresas distribuidoras de estas aplicaciones ERP, ofrecen la posibilidad del alquiler por uso.
Espacio en Blanco	Espacio existente entre las operaciones de la empresa y los mercados existentes.
e-services	Modelo de prestación de servicios utilizando el medio electrónico.
Extranet	Fragmento de la red Internet que establece relaciones entre la empresa, sus proveedores y socios tecnológicos (partnerts). Establece características adicionales sobre Internet para garantizar la seguridad y autentificación en las transacciones e intercambio de información. Suelen utilizar plataformas de RPV (Red Privada Virtual o SVN, Secured Virtual Network) .

F	
Firewall	Un firewall (cortafuegos) es un mecanismo que permite controlar el acceso de usuarios a ciertas zonas de una red. En las Intranets, se emplean como medio de protección cuando la web interna tiene salidas hacia la externa (Internet, por ejemplo). Generalmente, los firewalls suelen interponerse entre el servidor de web (que es público y no está protegido) y la red interna (que debe ser confidencial).

	Con el uso de firewalls, se evita que los usuarios de Internet conecten a la red privada interna de la empresa. Así, estos usuarios sólo podrán acceder a una parte reducida de la Intranet, aquéllas definida como pública. El resto de la intranet sólo es accesible mediante una autorización especial Todo ello se traduce en que los usuarios de la Intranet pueden mirar hacia fuera (hacia Internet), pero nunca a la inversa.
Firma Digital	(Digital Signature) Es un mecanismo de autentificación de los participantes en una transacción electrónica basado en el uso de algoritmos y protocolos criptográficos.

G	
Gateway	Técnicamente es un hardware o software de instalación que posibilita la counicación entre dos protocolos diferentes. Por Ejemplo AOL (Aerican On-Line poesee un gateway que comunica su formato de e-mail con el formato de e-mail de Internet.
GIF	Formato intercambio de gráficos de ficheros multimedia.

H	
Hacker	(Pirata) Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término "cracker".
Hosting	Servicio mediante el cual una empresa se encarga de gestionar las páginas web de otras empresas, incluyendo el hardware, el software y las comunicaciones.

I	
ICE	(Information and Content Exchange) Protocollo desarrolado a partir del XML para el intercambio de contenidos de manera estructurada a través de la Internet.
ICP	(Internet Comerse Provider) Entidades que proveen softwares o servicios que posibilitan a las empresas construir una tienda on-line. Esta tienda puede estar albergada en la pagina web del comercio o en el servidor de la ICP.
IETF	(Internet Engineering Task Force) Organización encargada de desarrollar y aprobar nuevos protocolos de comunicaciones para Internet.
IDC	International Data Corporation
Internet	Conjunto mundial de ordenadores interconectados por un interfaz estándar de comunicaciones ordenador-ordenador denominada TCP/IP . Comúnmente se la define como la red de redes.
Intranet	Sistema de información dentro de la empresa basada en la tecnología web, por la que un usuario puede acceder a diferentes aplicaciones de la empresa. Todo se traduce en una red empresarial de maquinas conectadas a un servidor Web (o varios). Los distintos empleados podrán acceder a cualquier tipo de información publicado en un "Site" de esta web, de la misma manera que lo haría si conectase con una red global (esto es Internet). Posibilita también que el trabajador acceda a sites tanto de la red empresarial (la Intranet) como la mundial (el www, FTP...). En tal caso, la red interna de la compañía estará protegida de cualquier visitante non-grato por medio de cortafuegos o firewalls.

ISP	Operador que provee servicios de conectividad a Internet y toda la gama de servicios basados en la familia de protocolos de Internet denominada TCP/IP (acceso web, correo electrónico, resolución de nombre de dominio, red privada virtual segura, etc.)

L	
Leased lines	Conexión a través de la línea telefónica dedicada entre un sitio y otro.
Legacy System	Sistemas de legado o heredados. Sistemas y aplicaciones antiguas que normalmente no son totalmente compatibles con los sistemas operativos actuales pero que tienen información importante para la operación de la empresa.

M	
Merchant	Un merchant es cualquier individuo u organización que actúa como un vendedor en la web. Los Merchant normalmente son propietarios de la página y del catalogo on-line, al mismo tiempo que son responsables de la gestión de la relación con el cliente.
MIME	MIME es un protocolo que permite adjuntar (Attach) al correo electrónico datos binarios. Los archivos binarios (como imágenes , ficheros de sonidos, programas, etc..) contiene datos que no son únicamente texto (se entiende por texto los caracteres imprimibles).

N	
NSF	Abreviatura de National Science Fundation, organización que administro la columna vertebral de Internet en Estados Unidos hasta 1995.

Número serial de identificación	Valor entero, único de entre los emitidos por una Autoridad de Certificación, que esta asociado inequívocamente con un certificado emitido por dicha autoridad.

O	
OEDC	Organisation for Economic Cooperation and Development

P	
Pago Seguro	Forma o sistema de pago que garantiza la autenticidad, integridad y confidencialidad de las transacciones e intervinientes en un proceso de comercio electrónico.
Personalización	Proceso de adaptación masiva de productos, bienes o servicios ya sea físicos o informacionales a las preferencias y gustos inducidos del estudio del consumidor o visitante de una Web.
Pasarela de Pago	(Payment gateway) Plataforma tecnológica que realiza la intermediación segura en la transacción entre el comerciante y el banco.
Petición de comentarios	(Request for comments, RFC) Se refiere a documentos que definen los estándares que los ordenadores deben soportar para acceder y utilizar Internet. Los documentos RFC también incluyen practicas o directrices recomendadas para los usuarios de ordenadores.
PKI	Técnicamente, por PKI se conoce al conjunto de hardware, software, servicios y procedimientos necesarios para generar, manipular, almacenar y administrar certificados basados en clave pública. Esta definición tan ambigua implica una arquitectura de componentes que se distribuyen las funciones y se comunican mediante diferentes tecnologías. Para precisar

	bien cuales son estos componentes es útil enumerar las enumerar las necesidades a cubrir: Registro, Iniciación Generación de certificados Generación de claves Recuperación de claves Renovación Certificación cruzada Revocación Publicación de certificados y revocaciones. Aunque esta enumeración es larga, todo el esqueleto de una PKI se estructura en torno a tres ejes básicos y necesarios: la gestión del registro, la validación de certificados y el almacén de claves públicas. Esto es, la autoridad de registro (RA), la autoridad de certificación (CA) y el directorio de certificados.
Portal de Extranet	Portal dirigido a miembros que no pertenezcan a la empresa pero que estén relacionados con ella (clientes, proveedores, accionistas de la empresa, etc.). Proporcionan información y acceso a sus productos y servicios así como información relativa a la compañía.
Portal de Internet	Sitio de Internet o Web site en el que se ofrecen una serie de servicios al usuario. Entre los servicios con los que suele contar figuran un buscador, servicio de noticias, e-mail gratuito, chat, comunidades virtuales, etc.
Portal de Intranet	Portal dirigido a los empleados de una empresa o corporación, a la que pueden acceder para obtener información y aplicaciones de uso interno.
Portal de negocios horizontal	Portal de Internet que ofrece contenidos y servicios dirigidos al mundo de la empresa o profesional en general con un enfoque amplio.
Portal de negocios vertical	Portal de Internet que ofrece contenidos y servicios específicamente dirigidos a un sector empresarial o un colectivo de profesionales de un área concreta de la empresa.

R	
Red de Computadoras	Es un conjunto de equipos que comparten información electrónica, para lo cual utilizan medios de telecomunicaciones.
Real-time credit card processing	(Procesamiento de tarjetas de crédito en tiempo real)Autorización de la tarjeta de crédito mientras el comprador está on-line. Si se rechaza el comprador tiene la posibilidad de intentarlo con otra tarjeta de crédito

S	
Sellado en el tiempo	Significa que ligado a la transacción / intercambio de información va la Firma Digital de la fecha por parte de una Autoridad Externa. Determinando así claramente cuándo se realizó una transacción.
Servidor	Aplicación residente en un sistema de ordenador, que proporciona información a uno o mas usuarios. Un sitio Web es considerado como un servidor porque suministra la información solicitada por los exploradores de la web (por ejemplo, paginas Web y ficheros gráficos)
Servidor de Comercio	(e-Merchant) Es el programa software encargando de realizar las funciones básicas de comercio electrónico, entre las que se incluyen gestión del catálogo online, soporte para el diseño del frontal de la tienda, carrito de la compra, recepción y generación de pedidos, interfaz con sistemas de pago, interfaz con sistemas de logística, , cálculo de impuestos y costes de envío, etc.
SET	(Secured electronic transactions) Protocolo desarrollado por Visa y Mastercard para garantizar la seguridad en las transacciones electrónicas.

Smart Card	Tarjeta de plástico que incluye un microchip que puede ser recargado con dinero con cargo a la cuenta corriente del poseedor. Este tipo de tarjetas también pueden almacenar otro tipo de información
SSL	(Secured Socket Layer) Capa de connexion segura): Estandar de conexiones Internet seguras creado por Netscape que es el más ampliamente utilizado en Internet actualmente para las transacciones de comercio electrónico. A diferencia de SET, no requiere el requisito de certificados digitales para los consumidores, lo que ha favorecido su expansión.
Suite	Conjunto de aplicaciones o protocolos.
Supply Chain Management	Proceso de optimización de las entregas de bienes, servicios e información desde el suministrador hasta el cliente.

T	
Third-party Market place	Modelo por el que las compañías delegan la dirección de marketing en la Web a un tercero. Ofrecen conexiones para catálogos de productos del proveedor, así como servicios adicionales asociados a la marca, medios de pago, logística, pedidos, etc.
Tienda virtual	(e-shop, e-store, cyber-stores) Modelo de negocio de comercio electrónico que lleva a Internet el modelo de tienda tradicional utilizando las nuevas capacidades del medio.
Transferencia electrónica de Fondos	Forma de pago electrónico que transfiere una cantidad de dinero desde una cuenta bancaria a otra cuenta en el mismo o diferente banco. Se utiliza desde 1970, y actualmente es una forma de pago, que requiere protocolos de seguridad entre el proveedor del servicio, el visitante y el banco.

U	
USENET	(Users network)Es el término con el que se conoce al sistema que se encarga de gestionar el flujo de información generado por el envío, recepción, y distribución de documentos (artículos) compartido por un gran numero de redes de ordenadores y personas en todo el mundo. Es, básicamente, una de las muchas redes (o subred de redes) que componen Internet. USENET marca un conjunto de reglas para administrar los grupos de noticias newsgroup.

V	
Value chain integrator	Compañías que se especializan en la integración de distintos pasos de la cadena de valor. Dichas compañías ayudan a resolver de forma integrada distintos componentes de la cadena de valor para su negocio online. En otros casos ofrecen la externalización de distintos servicios como puede ser la logística y los medios de pagos.

W	
Workplace	Es un portal de empresa que permite a los usuarios acceder, con un navegador web, a todas las aplicaciones internas y externas, información empresarial y los servicios necesarios para que los empleados puedan desarrollar su trabajo.
World wide web (WWW)	EL world wide web es el primer servicio de información con hipertexto en la internet. Desarrollado inicialmente en la CERN de Ginebra, es uno de los sistemas mas extendidos en Internet, y permite el acceso a documentación distribuida en los distintos ordenadores.

X	
XML	eXtended Markup Language, lenguaje de marcado extensible. Similar a HTML, el 'lenguaje' de la Web. Como no mezcla contenido con presentación, es procesable automáticamente, y será el 'formato' de intercambio universal en e-Business.

Z	
Zona desmilitarizada	Es la zona que posee servicios públicos de internet en un servidor con multiples firewalls

REFERENCIAS BIBLIOGRÁFICAS

SITIOS INTERNET.

http://www.sopde.es/cajon/biblioteca/comercio/quees.html

http://www.ati.es/novatica/2000/144/josman144.html

http://ute.edu.ec/~mjativa/ce/main.html

http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html

http://www.internautas.org/documentos/pista.htm

http://www.v-1.cl/view_page_white_paper.asp?p=9

http://www.uca.edu.su/investigación/tutoriales/tcp_ip.html

http://www.canalpyme.com/redes.htm

http://www.openbsd.org/faq/es/faq13.html

http://www.eitig.com/redes/trabajos/ssl.html

http://www.telefonica-data.com.uy/esp/html/consultas/consultas.htm

http://ute.edu.ec/~mjativa/ce/main.html

http://www.eitig.com/redes/trabajos/tls1.hmtl

http://www.eitig.com/redes/trabajos/tls2.hmtl

http://www.microsoft.com/latam/technet/articulos/200011/art03/default.asp

http://www.ipsca.com/psCA/ipsCAweb.nsf/

http://www.penta3.com/infoPKI/ltroducción.htm

http://www.iec.csic.es/criptonomicon/articulos/expertos61.html

http://www.winred.com/colaboradores/colaborador28.htm

http://www.br.ibm.com/e-business/espanol/ebusiness/e.commerce/services.html

http://www.enciclonet.com.ar/productos_y_sericios/helpdesk.htm

http://www.terra.com/informatica/que-es/raid.cfm

http://www.terra.com/informatica/que-es/xdls.cfm

http://www.iies.es/teleco/publicac/publbit/bit107/quees.htm

http://www.enciclonet.com.ar/productos_y_servicios/helpdesk.htm

http://www.br.ibm.com/e-business/espanol/ebusiness/e.commerce/services.html

http://www.openbsd.org/faq/es/faq13.html.

LIBROS.

- "LA ERA DE LOS NEGOCIOS ELECTRONICOS: Cómo generar Utilidades en la Economía Digital", Don Tapscott, McGraw Hill, 1ra. Ed.,1999.
- "EXTRANETS", Richard H Baker, McGraw Hill, 1ra. Ed., 2000.
- "REDES DE COMPUTADORAS", A.S. Tanenbaum, Prentice Hall, 3ra. Ed. 1997.
- "SISTEMAS DE COMUNICACIONES ELECTRONICAS", Wayne Tomasi, Pentice Hall, 2da.Ed., 1996.
- "SEGURIDAD Y COMERCIO EN EL WEB", S. Garfinkel y G. Spafford, McGraw Hill, 1ra. Ed., 1999.
- "LAN TIMES: GUIA DE SEGURIDAD E INTEGRIDAD DE DATOS", M. Farley, T. Stearns, J. Hsu, McGraw Hill, 1ra. Ed., 1998

ARTÍCULOS.

- *Infraestructura para Comercio B2B*, ITD Latinoamérica, Volumen 6-Edicion 1-Febrero 2001.
- *Evangelizando en el E-Business*, COMPUTERWORLD Ecuador, Número 77, año 03. Del 23 de abril al 6 de mayo de 2001.
- [Cisco idg4 Basics] Cisco Systems, "Internetworking Design Basics", http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm , 06 de Enero de 2000.