

REPUBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

“IAEN”

FACULTAD DE GERENCIA EMPRESARIAL

**ANÁLISIS DE LOS FACTORES QUE OBLIGAN A
PROTEGER LOS DATOS EN LOS NEGOCIOS
REALIZADOS A TRAVÉS DEL COMERCIO
ELECTRÓNICO – CASO ECUADOR**

**Tesis presentada como requisito para optar al Título de
Master en Gerencia Empresarial**

**AUTORIA: Ing. HUGO MARCELO DALGO PROAÑO
DIRECTORA: Eco. GUADALUPE VIDAL LEÓN**

QUITO JULIO 2007

Agradecimiento

A todos quienes conforman el Instituto de Altos Estudios Nacionales “IAEN”, en especial a cada uno de los docentes, por su incondicional apoyo y esfuerzo de formar profesionales.

Marcelo

Dedicatoria

DANNY, El arma racional es la sabiduría, estudia, persevera y alcanza tus objetivos bajo el más absoluto silencio; la palabra imposible no tiene significado.

Marcelo

ÍNDICE GENERAL

Introducción	1
Planteamiento del problema	3
Marco teórico	6
Hipótesis	7

CAPITULO I Marco teórico de la protección de datos

1.1 Preceptos jurídicos	8
1.2 Protección de datos en relación con el marco jurídico ecuatoriano ...	9
1.2.1 Constitución Política del Ecuador	9
1.2.2 Ley de Propiedad Intelectual	12
1.2.3 Código de Comercio – Contratos	14
1.2.4 Ley Orgánica de Defensa del Consumidor	19
1.2.5 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	20
1.2.6 Resolución de CONATEL 584-23-CONATEL-2003	23
1.3 Derechos y responsabilidades	24
1.3.1 Intervenientes	28
1.3.2 Entidades de certificación de información	29
1.3.3 Firma electrónica	31
1.4 Protección de los datos	34

CAPITULO II Comercio Electrónico

2.1	Clases de comercio electrónico	36
2.1.1	Comercio electrónico tradicional	37
2.1.2	Comercio electrónico directo	39
2.1.3	Comercio electrónico indirecto	40
2.1.4	Comercio electrónico internacional	41
2.2	Presencia de la organización en el comercio electrónico	44
2.2.1	Recursos electrónicos	46
2.2.2	La competencia	51
2.2.3	El cliente	54
2.2.4	Canal de distribución	55
2.2.4.1	Flexibilidad y rapidez de cambio	56
2.2.4.2	El coste	56
2.2.4.3	Posibilidad de control del canal de distribución	57
2.2.5	Datos estadísticos en el Ecuador	58
2.3	Visión comercial en Internet	71
2.4	Los medios de pago	76
2.5	Tributación	82

CAPITULO III Protección de datos y seguridad

3.1	Barreras de protección	86
3.2	Seguridad del ciberespacio	92
3.3	Firma electrónica	98
3.3.1	Criptografía	100

3.4	Certificación de información	107
3.5	Confidencialidad y reserva	113

CAPITULO IV Propuesta, conclusiones y recomendaciones

4.1.-	Propuesta	117
4.1.1	Elementos Indispensables para la creación de una empresa virtual o inserción de la empresa en el comercio electrónico	118
4.1.2	Elementos Indispensables del comercio electrónico desde el punto de vista del cliente	128
4.1.3	Barreras de protección	135
4.1.4	Aspectos jurídicos y legales	139
4.2	Conclusiones	144
4.3	Recomendaciones	150
	Glosario de términos	154
	Bibliografía	157

INTRODUCCION

El desarrollo del comercio electrónico impulsado a través de las denominadas nuevas tecnologías de información y comunicación como Internet, ha mejorado y facilitado la forma de satisfacer las necesidades del ser humano, a la vez ha creado una serie de factores que ocasionan la pérdida de la intimidad personal y violación de los derechos fundamentales de las personas.

El comercio electrónico, toma parte de un mercado en el cual se ven involucrados en las transacciones proveedores y consumidores que pueden satisfacer sus necesidades electrónicamente y se desenvuelven en un medio de operaciones que puede ir desde el contacto electrónico entre el proveedor inicial hasta el consumidor final. Sin embargo, este desarrollo tecnológico, presentado a nivel mundial, obliga a replantear algunos de los procedimientos del comercio tradicional, surgiendo nuevos problemas e incluso agudizando algunos de los ya existentes como es la protección de datos en los negocios realizados a través del comercio electrónico; en calidad de personas naturales, instituciones de derecho público y privado, el estado también se debe proteger el patrimonio y las inversiones realizadas con reglas y normas claras, tecnología y procedimientos que permitan generar confianza entre los usuarios.

El presente trabajo, tiene como objetivo analizar los factores que obligan a proteger los datos en los negocios realizados a través del comercio electrónico y plantear una propuesta que permite minimizar los fraudes informáticos.

El primer capítulo comprende el marco jurídico ecuatoriano en el que se desenvuelve la protección de los datos de las personas, así: la Constitución

Política del Ecuador en lo que se refiere a los derechos y garantías de las personas; la Ley de Propiedad Intelectual a los derechos de autor; el Código de Comercio a la modalidad de contratación; la Ley Orgánica de Defensa del Consumidor en lo referente a los derechos de consumidor y la publicidad; la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos como aporte al desarrollo y regulación de la actividad electrónica, las Regulaciones que para el caso ha emitido el CONATEL y los derechos y responsabilidades de las personas que intervienen en una negociación.

El segundo capítulo corresponde a la negociación a través del comercio electrónico, la forma como se clasifica, la presencia de la organización en cuanto a recursos, canales de distribución, clientes y competencia, se realiza un análisis de los datos estadísticos en el Ecuador y su evolución, la visión comercial esperada en Internet y sus medios de pago utilizados.

El capítulo tercero, permite establecer las formas técnicas de protección de datos y seguridad, las barreras de protección que se pueden utilizar, la vulnerabilidad que genera el ciberespacio, la garantía que brinda la firma electrónica y la criptografía al momento de enviar información; los beneficios de la certificación de información y la confidencialidad y reserva que deben mantener los mensajes de datos.

El capítulo cuarto contiene la propuesta, basada en principios y factores administrativos, técnicos y jurídicos que permiten dar seguridad al proceso transaccional, a manera de ensayo se incluye la creación de una empresa virtual o inserción de las empresa en el comercio electrónico, se establecen las pautas que desde el punto de vista del cliente se debe considerar para seguridad de la información, se obtienen las conclusiones de la investigación y se recomienda la incorporación de varias normas jurídicas que permitan garantizar aún más la seguridad de los datos.

PLANTEAMIENTO DEL PROBLEMA

El Ecuador no está ajeno al desarrollo e integración de las denominadas nuevas tecnologías de la información, instituciones públicas y privadas están creando páginas de información en Internet y promoviendo por este medio la actividad comercial de productos, por lo que en los últimos tiempos el crecimiento comercial por la Web es importante.

De esta realidad, surge la necesidad de regular la actividad denominada comercio electrónico, que en un concepto mas general se refiere a toda transacción civil, comercial o financiera contractual o no que se efectúa a través del intercambio de mensajes de datos por la red de Internet, manifestado en los conceptos de e-commerce e e-business.

Las transacciones electrónicas¹ son actos de comercio a los que se someten dos o más personas para el cumplimiento de una obligación, entendiéndose por personas capaces para contratar a todas aquellas que la ley determina como tales, con capacidad jurídica y capacidad de obrar, con la suficiente confianza para poner en manos de personas que únicamente se conoce a través de una computadora, mas no como normalmente se acostumbra hacer las transacciones en los diferentes tipos de contratos, convenios, negocios o cualquier clase de acto de comercio, donde primero se conoce a la persona con quien se va a contratar y posteriormente se realiza la negociación; cosa que no ocurre en el Comercio Electrónico, por dar un ejemplo, se ingresa a

¹ Contratación electrónica: Se distinguen los contratos celebrados en medios electrónicos y aquellos que utilizan los medios electrónicos para su perfeccionamiento. También están los diferentes tipos de contratos que usualmente se están elaborando para asegurar los negocios electrónicos. Barzallo José Luis, Ficha de procedimiento. Derecho informático.

una página Web en Internet, se revisa que es lo que se quiere negociar y simplemente lo adquiere, por una parte simplifica y ahorra al usuario una serie de inconvenientes, facilitando enormemente los actos de comercio, pero por otro lado corre el riesgo de buscarse problemas por el mismo hecho de no existir ningún compromiso al no conocer directamente a la persona con quien se está contratando y obtener un producto distinto al que se pretendía adquirir, o simplemente de ser interceptada su información y ser utilizada en forma fraudulenta.²

En éste tipo de comercio, normalmente intervienen dos partes: el emisor y el destinatario, sin embargo, por las formalidades que necesariamente tiene la contratación electrónica, existe la intervención de otras personas como los ISP o proveedores del servicio y correo normal o courier; en caso de incumplimiento o de existir cualquier tipo de fraude, se provocaría un conflicto legal que deberá resolverse ante los jueces competentes; pero, tratándose de empresas extranjeras, se generaría un conflicto mucho mayor y a niveles internacionales³.

Existiendo la voluntad de realizar un determinado acto de comercio electrónico, el usuario tiene que someterse a las condiciones preestablecidas por el destinatario y confiar en la buena fe de aquellas personas.

Para entender los problemas que se pueden generar por las negociaciones realizadas a través del Comercio Electrónico, el usuario es el principal protagonista sin el cual, no se podría bajo ningún concepto llevar a cabo este tipo de transacciones. Existe otros factores como: Protección y privacidad del

² Hacer negocios por Internet, se dice que es un acto de fe porque debe creer en la entidad de las personas que le ofertan productos y servicios además de que lo que le ofertan por la red es lo que realmente va a recibir.

³ Depende de las leyes de cada país en relación al e-commerce, ya que es muy difícil legislar transacciones que no tienen límites geográficos y se hace por medios telemáticos.

libre flujo de la información, protección del interés público y privado, seguridad de los datos, ética y moral de las personas, entidades certificadoras de información y legislación clara y vigente que no necesariamente permite proteger la información de las personas que realizan transacciones electrónicas; estos factores son los que se propone analizar y confrontar con la presente investigación.

MARCO TEORICO

El comercio electrónico en nuestro país es una nueva forma de hacer negocios, para proteger la realización y concreción de estos negocios se ha creado la: “Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos, y su Reglamento”⁴, se ha encargado al CONATEL, Consejo Nacional de Telecomunicaciones la regulación del comercio electrónico, para lo cual se ha expedido el “Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para Prestar Servicios de Certificación de Información y Servicios Relacionados”⁵, de ello lo mas importante es la protección de la información y de las personas que intervienen en estos negocios con el fin de obtener un beneficio; puesto que puede acarrear una serie de consecuencias en el ámbito legal, comercial y personal, en concordancia con lo que establece la Constitución Política del Ecuador en el Art. 23 numeral 8, sobre el derecho a la honra, a la buena reputación y a la intimidad personal.

Este tema se relaciona con la Ley de Propiedad Intelectual en lo referente a la Información electrónica y la Ley de Defensa del Consumidor en lo pertinente a la protección contractual; en lo que se refiere al Derecho Comparado encontramos entre otras legislaciones latinoamericanas, la protección de los datos personales, asentados en archivos, registros, bancos de datos u otros medios electrónicos que garantizan la intimidad de las personas⁶.

⁴ Publicados en el Registro Oficial No. 67 suplemento 557 del 17 de abril del 2002.

⁵ Resolución 584-23-CONACEL-2003.

⁶ Para ello se utiliza “El Derecho Informático, es una herramienta indispensable para el desarrollo uniforme de las transacciones electrónicas por la seguridad que otorga a los negocios en la red. Es la ciencia del derecho que estudia los fenómenos que ocurren en el mundo digital para desarrollar nuevas formas de incorporar los actos y hechos en la normativa jurídica nacional e internacional.” Barzallo José Luis. Ficha de concepto, Derecho Informático.

HIPOTESIS

Encontrándonos en el siglo 21, aceptando el proceso de globalización al que nos encontramos expuestos, en donde el avance de la tecnología se ha desarrollado enormemente, facilitando el convivir de las personas y la humanidad, nace la posibilidad de hacer negocios, y transmitir información a través de medios electrónicos, para dar facilidades a las personas, también puede conllevar a una serie de problemas en los ámbitos comerciales, económicos y legales, por lo que se hace necesario salvaguardar la integridad de la información en beneficio del usuario, sea este emisor, proveedor de servicio electrónico o destinatario.

Un marco jurídico acorde a la protección de datos, permitirá que las transacciones electrónicas y el comercio electrónico se desarrollen en el Ecuador.

Con reglas y procedimientos claros en relación a las obligaciones y responsabilidades que tiene cada uno de los intervinientes en una relación de comercio por vía electrónica se puede fomentar el desarrollo electrónico comercial.

El insertar los principios de integridad, autenticidad y confidencialidad en las transacciones de comercio electrónico, permitirá aumentar la confianza en el servicio.

La conformación de procedimientos, controles y seguridades permitirá satisfacer los niveles de seguridad que los usuarios necesitan.

CAPITULO I

1.- MARCO TEÓRICO DE LA PROTECCIÓN DE DATOS

1.1.- PRECEPTOS JURÍDICOS

Desde el punto de vista jurídico, es necesario considerar los siguientes principios que los mensajes de datos, información de archivos o negocios electrónicos deben contener y asegurar que proviene de la persona que se dice que lo envía; que no ha sido alterado o interceptado en el camino; que el emisor no podrá negar su envío ni el destinatario su recepción; y, en su caso, garantizar su confidencialidad. La satisfacción de estos preceptos jurídicos se consigue con la aplicación de determinadas soluciones técnicas, que aportan los siguientes principios:

“Seguridad.- *La autenticación: que asegura la identidad del remitente del mensaje y permite asegurar que un mensaje procede de quien dice que lo envía.*

Integridad.- *El mensaje recibido por una de las partes, debe ser idéntico al enviado por la otra. Dicho en otras palabras no debe haber alteración de la información enviada, en su recorrido por la red, que sean accidentales o intencionales.*

El no rechazo o no repudio en origen y en destino.- *Ninguna de las personas puede negar haber enviado o recibido los mensajes correspondientes. De esta forma, si se cierra un trato a través de la red y una de las partes no cumple con lo pactado, la otra podría efectuar las acciones legales correspondientes. Los mensajes deben tener la misma validez que si estuviesen escritos en papel y firmados, y*

Confidencialidad.- Los mensajes enviados solo podrán ser leídos por el destinatario. Esto significa que ninguna persona en la red puede interferir e interpretar dichos mensajes.”⁷

Cuando se construye un sistema, estos principios deben formar parte de él, y se los debe aplicar de forma combinada, esto permite garantizar la integridad de la información.

1.2.- PROTECCIÓN DE DATOS EN RELACIÓN CON EL MARCO JURÍDICO ECUATORIANO

EL marco Jurídico que regula la protección de datos en todo el Estado Ecuatoriano, está establecido en: La Constitución Política del Ecuador y las siguientes Leyes Especiales: Ley de Propiedad Intelectual; Ley de Defensa y Protección del Consumidor, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento; Reglamento del CONATEL y el Código Penal en lo que se refiere a las sanciones.

1.2.1.- CONSTITUCIÓN POLÍTICA DEL ECUADOR

La Constitución Política del Ecuador reconoce como función primordial del Estado Ecuatoriano el asegurar la vigencia de los derechos fundamentales del hombre y considera como el más alto deber del Estado la exigibilidad y el respeto de los derechos humanos que garantiza la constitución.

En estas garantías se encuentra contenida una principalísima como es la intimidad personal, cuyo texto lo describe el artículo 23, numeral 8:

⁷ MARTÍNEZ Nadal Apolonia “Comercio Electrónico, Firma Digital y Autoridades de Certificación” Pág. 32 2003 Madrid

“Art. 23.- Sin perjuicio de otros derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas lo siguientes:

...num. 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La Ley protegerá al hombre. La imagen y la voz de la persona.”⁸

Protección de datos personales como objeto tutelar del derecho a la intimidad, privacidad o autodeterminación informática.

El avance tecnológico ha originando una alta inmersión del Internet en la vida de las personas, ocasiona una serie de nuevas situaciones que podrían crear una cierta vulnerabilidad de sus derechos de las personas o pérdida de algunas libertades que tienen que ser precauteladas por el Derecho Informático, como por ejemplo: El tomar decisiones que afecten en forma negativa a las personas sin que ellas tengan conocimiento del porque se resuelve de esa manera, actuando con negligencia, sin actualizar, borrar o complementar los datos registrados; utilizando los datos de las personas para proyectar al futuro y saber cuales podrían ser sus relaciones y comportamientos, elaborando un perfil de los individuos con la interconexión de los ficheros que permita un control de sus actividades.

Tal es el caso que se ha creado el Derecho Informático que permite a los ciudadanos proteger la información de su intimidad personal. Todos tenemos derecho a que la información personal que contengan los bancos de datos sean reservados, fidedignos, accesibles y que únicamente cumplan su fin; de lo contrario invadirían la vida privada alterando los derechos de igualdad ante la sociedad.

⁸ Constitución Política del Ecuador 1998

En el capítulo de las garantías de los derechos de la Constitución Política del Estado, sección segunda se encuentra tipificado el principio del Habeas Data como garantía constitucional, el Art. 94 dice:

“Toda persona tendrá derecho acceder a los documentos, bancos de datos e informes que sobre si misma, o sobre sus bienes, consten en entidades públicas o privadas, como conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización”⁹

“Doctrinariamente el Hábeas Data protege a la integridad moral de las personas, frente a informaciones referidas a su personalidad, donde prima la intimidad y la privacidad y su entorno familiar.

Si es verdad que el Hábeas Data, nació con el desarrollo tecnológico del mundo contemporáneo, gracias a ese avance "los mensajes de Datos" han requerido especial tipificación, pues muchos países han adoptado regímenes jurídicos propios, autónomos con leyes especiales sobre el tema, generando infraestructura física, personal especializada y procedimientos con instancias administrativas para atender las necesidades del usuario.”¹⁰

Por naturaleza el Hábeas Data es una garantía que protege varios derechos, tales como, la honra, la buena reputación, la intimidad y también el derecho a la información. Así como la actualización rectificación eliminación o anulación de datos, para que dicha información equivocada no circule, no afecte su intimidad ni ocasione daño moral.

“El Hábeas Data no es una acción procesal civil es una garantía constitucional con objetivos muy claros que busca que el accionante sepa:

- *Por que motivos legales el poseedor de la información llego a ser tenedor de la misma.*
- *Desde cuando tiene la información.*

⁹ Constitución Política del Ecuador 1998

¹⁰ <http://ecuador.derecho.org/> marzo 17 del 2006

- *Que uso ha dado a esa información y que hará con ella en el futuro.*
- *Conocer a que personas naturales o jurídicas el poseedor de la información le hizo llegar dicha información*
- *Por que motivo o con que propósito y la fecha en la que circuló la información.*
- *Que tecnología usa para almacenar la información.*
- *Qué seguridades conoce el tenedor de la información para precautelar que la misma no sea usada indebidamente.*

El Hábeas Data no puede ser usado en la obtención de información propia del sigilo profesional tampoco puede usarse como un medio que pueda obstruir la acción de la Justicia, no puede usarse el Habeas Data como medio de liquidar obligaciones civiles bancarias, comerciales, crediticias, etc. No puede ser un medio de prueba de existencia o no de tales obligaciones. Para probar éstas, el Código de Procedimiento Civil le franquea la posibilidad de juicio de exhibición, que sí es un medio de prueba”¹¹

1.2.2.- LEY DE PROPIEDAD INTELECTUAL

“Son derechos que corresponden por ley al autor de una creación desde el momento en que toma una forma en cualquier tipo de soporte tangible (papel, en el caso de una obra literaria o de una partitura) o intangible (por ejemplo, ondas hercianas, para las obras de televisión o soporte magnético, en el caso de una grabación informática y similares). La idea para un cuento, la receta culinaria que una familia se transmite de generación en generación, una canción que se silba por la calle, no son obras protegidas por la ley. Pero una vez que son escritas, grabadas o representadas en público, las leyes reguladoras del copyright, los diseños o las patentes reclaman la protección de los derechos de sus autores, como titulares de la propiedad intelectual.”¹²

El sistema de copyright descansa en este principio de la propiedad intelectual, al proveer un mecanismo de compra y venta de derechos, cesiones, etc., y el control de su uso dentro y fuera del país por convenios internacionales.

¹¹ <http://publicaciones.derecho.org/redi/> Marzo 17 del 2006

¹² Biblioteca de Consulta Microsoft® Encarta® 2003

La propiedad intelectual cubre todo trabajo original literario, dramático, artístico, musical, científico, con independencia de que su calidad sea buena o mala: todo producto de la inteligencia humana está protegido. Además de que existen leyes nacionales, también hay un gran número de acuerdos internacionales para la protección de las obras. Los más importantes de todos ellos son el Convenio de Berna y la Convención Universal del Copyright de 1952. Otros convenios importantes son los de París y Ginebra.¹³

Se debe mencionar que la Ley de Comercio de Electrónico, Firmas Electrónicas y Mensajes de Datos, establece que se someterá a la Ley de propiedad Intelectual que en su Art. 26.- dice:

“También constituyen violación a los derechos establecidos en este Libro cualquiera de los siguientes actos:

Remover o alterar, sin la autorización correspondiente, información electrónica sobre el régimen de derechos; y,

Distribuir, importar o comunicar al público el original o copias de la obra sabiendo que la información electrónica sobre el régimen de derechos ha sido removida o alterada sin autorización.

Se entenderá por información electrónica aquella incluida en las copias de las obras, o que aparecen en relación con una comunicación al público de una obra, que identifica la obra, el autor, los titulares de cualquier derecho de autor o conexo, o la información acerca de los términos y condiciones de la utilización de la obra, así como número y códigos que representan dicha información”¹⁴.

Los mayores problemas que presenta el sistema de propiedad intelectual son los que hacen referencia a la protección de las publicaciones electrónicas (copias de cintas de música o de vídeo), así como las fotocopias de una obra

¹³ El artículo 9 del Convenio de Berna establece que "los autores de obras literarias y artísticas protegidas por el presente Convenio gozarán del derecho exclusivo de autorizar la reproducción de sus obras por cualquier procedimiento y bajo cualquier forma.

¹⁴ Ley de Propiedad Intelectual R.O 266 de 1998

escrita, el control de las copias presenta enormes dificultades, y no siempre debe enfrentarse a la cuestión de copias privadas, sino de un mercado de gran magnitud de copias piratas o ilegales. Lo mismo cabe decir de los programas de software, que pueden ser copiados en menos de un segundo, a todo ello hay que añadir los problemas derivados de la puesta en práctica del sistema Internet, el uso lícito de las copias en el mundo académico, por ejemplo, no puede justificar un estado de cosas en que al autor no le compense llevar a cabo un trabajo creador si su producto puede ser reproducido con facilidad y sin que ello le suponga remuneración alguna.

Existe alguna excepción al carácter universal que rige los convenios del copyright en China, la propiedad intelectual no pertenece al creador de la obra original, sino a la colectividad.

1.2.3.- CÓDIGO DE COMERCIO – CONTRATOS

“El contrato se puede definir como un acto por el cual una parte se obliga para con otra a dar, hacer, o no hacer alguna cosa. En concordancia con lo dispuesto por la norma civil, se entiende por contratación electrónica a todo acuerdo de voluntades (...acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa...) que se haya realizado a través o con utilización de algún elemento electrónico.”¹⁵

Es necesario mencionar lo que establece el Código de Comercio en lo referente a su ámbito, la definición de comerciante y quienes pueden realizar estos actos:

“Art. 1.- Ámbito.- El Código de Comercio rige las obligaciones de los comerciantes en sus operaciones mercantiles, y los actos y contratos del comercio, aunque sean ejecutados por no comerciantes.

¹⁵ YANEZ Pablo Introducción al Estudio del Derecho Informático Pag. 192 Gráficas SOS 1999 Quito

Art. 2.- Comerciantes.- Son comerciantes los que, teniendo capacidad para contratar, hacen del comercio su profesión habitual.

Son actos del comercio: la compra, venta o permuta de cosas, muebles o inmuebles, comisión o mandato mercantil, el transporte de mercaderías o personas que ejerzan el comercio, los seguros, depósitos de mercaderías, las letras de cambio, pagares o remesas de dinero, las operaciones bancarias, correduría, de bolsa, los fletes, prestamos entre otros.

Las personas que pueden realizar actos de comercio de acuerdo al Código de Comercio son:

Art. 6.- Capacidad para contratar.- Toda persona que, según las disposiciones del Código Civil, tiene capacidad para contratar, la tiene igual para ejercer el comercio.

Art. 7.- Incapacidades Especiales.- Sin embargo de lo dispuesto en el artículo anterior, no pueden comerciar:

- *Las corporaciones eclesiásticas, los religiosos y los clérigos;*
- *Los funcionarios públicos a quienes esta prohibido de ejercer el comercio por el Art. 266 del Código Penal, salvo las excepciones establecidas en el mismo artículo*
- *Los quebrados que no hayan obtenido rehabilitación”¹⁶*

Contratos

Es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer una cosa. Los actos de comercio puede realizar toda persona legalmente capaz, sean estos contratos de las formas existentes o como para el caso que interesa, mediante procesos electrónicos, como en el Internet o cualquiera de las formas de comunicación.

¹⁶ Código de Comercio Ecuador R.O –S-1202 1960

Los contratos por medios electrónicos, deben gozar del mismo compromiso y constituirse en obligación para las partes como cualquiera de las formas de contratación existentes.

Se debe destacar dos tipos de contratos de comercio electrónico:

Comercio electrónico de bienes y/o servicios entregados de forma electrónica

“En esta categoría se incluyen aquellos bienes y/o servicios que pueden ser digitalizados, manipulados, transferidos, enviados y almacenados vía magnética, utilizando medios telemáticos.

A continuación se definirá una serie de bienes y/o servicios que se pueden brindar bajo esta modalidad de contratación electrónica:

- *Contratos de venta de software: consisten en la venta de archivos ejecutables para descargar software disponible en la página Web del oferente*
- *Contratos de licencia de uso de software: consisten en la venta de licencias para el uso de software comprado tangiblemente, o descargado de la página Web del oferente*
- *Contratos de leasing sobre el software: consisten en el alquiler de archivos ejecutables para utilizar software disponible en la página Web del oferente*
- *Contratos de licencia de uso de bases de datos: consisten en el acceso a las bases de datos disponibles en línea para los compradores, o en la venta de las mismas vía descargas de los archivos de la página Web del oferente*
- *Contratos de almacenaje de bases de datos: consisten en el almacenamiento digital de diferente información en los servidores del oferente*¹⁷

La compra de un archivo digital que no involucre el pago directamente al momento de aceptar la oferta, no deberá ser considerada como un acto de

¹⁷ olman@orimola.com San José, Costa Rica mayo 2005

comercio electrónico, sino como un acto de comercio de bienes electrónicos transados de manera convencional por su particularidad del pago.

Comercio electrónico de bienes y/o servicios entregados por medios no electrónicos

“Bajo esta modalidad, se incluyen todas las transacciones negociadas en una página Web que no impliquen la transferencia de la propiedad de los bienes y/o servicios de forma electrónica, es decir, la negociación de bienes tangibles, siempre y cuando dicha negociación se sujete a los parámetros de oferta y aceptación electrónica, incluyendo dentro de esta última, el pago.

Dentro de las transacciones de bienes y/o servicios entregados por medios no electrónicos podemos citar los siguientes:

- *Venta de discos compactos de música y películas*
- *Venta de libros, revistas y periódicos*
- *Venta de computadoras y accesorios afines*
- *Venta de tiquetes aéreos*
- *Venta de juguetes*
- *Venta de ropa*
- *Venta de comida enlatada*
- *Venta de bebidas*
- *Venta de servicios de traducción de documentos*
- *Venta de servicios de correduría aduanal*
- *Venta de servicios de pagos de impuestos*
- *Venta de servicios de correduría bursátil*
- *Venta de servicios de pago de servicios públicos*
- *Venta de servicios publicitarios”¹⁸*

La lista podría ser infinita, dependiendo de la evolución y desarrollo de las diferentes herramientas informáticas que van permitiendo día a día la inclusión y automatización de una mayor cantidad de procesos de venta de bienes y servicios.

¹⁸ Idid.

La contratación electrónica EDI

El intercambio electrónico de datos (Electronic Data Interchange) es una de las primeras manifestaciones de comercio electrónico a través de medios telemáticos.

Comprende el intercambio de información comercial entre computadoras conectadas entre sí bajo una misma red, es decir, una Intranet o red privada. Las partes contratantes se ponen de acuerdo de forma previa para transmitir formatos estandarizados de compra, aceptación, envíos, y otros, relacionados con transacciones de compra venta.

En cuanto a la modalidad de contratación, la práctica es la de contratos con cláusulas predisuestas.

En Internet, esta modalidad de contratación recibe la denominación de Click-wrap agreements, puesto que la exteriorización de la voluntad se manifiesta mediante un click del mouse.

En lo referente a la responsabilidad jurídica de las partes en la relación contractual:

Debe atenderse a:

- Normativas sobre protección del consumidor
- Normas sobre contratación
- Forma de los actos jurídicos

En la práctica, los requisitos mencionados anteriormente son muy difíciles de probar, aún con legislaciones que receptan la instrumentación digital de los actos jurídicos.

1.2.4.- LEY ORGANICA DE DEFENSA DEL CONSUMIDOR.

La Ley de Defensa del Consumidor que por falta de publicidad y conocimiento de los usuarios no es aplicada en un 100% en nuestro país, contiene normas jurídicas que protegen las transacciones comerciales entre otras.

En el Art. 4.- Derechos del Consumidor.- se establece:

“Son derechos fundamentales del consumidor, a más de los establecidos en la Constitución Política de la República, tratados o convenios internacionales, legislación interna, principios generales del derecho y costumbre mercantil.

En los incisos que a continuación se detalla:

2. Derecho a que proveedores públicos y privados oferten bienes y servicios competitivos, de óptima calidad, y a elegirlos con libertad;

4. Derecho a la información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo los riesgos que pudieren prestar;

6. Derecho a la protección contra la publicidad engañosa o abusiva, los métodos comerciales coercitivos o desleales”¹⁹

De igual forma el Art. 6 de la misma Ley.- Publicidad Prohibida; manifiesta:

¹⁹ Ley de Defensa del Consumidor Registro Oficial No. 520 de septiembre 12 de 1990

“Quedan prohibidas todas las formas de publicidad engañosa o abusiva, o que induzcan a error en la elección del bien o servicio que puedan afectar los intereses y derechos del consumidor.

Infracciones Publicitarias.- Comete infracción a esta Ley el proveedor que a través de cualquier tipo de mensaje induce al error o engaño en especial cuando se refiere a:

1. País de origen, comercial o de otra índole del bien ofrecido o sobre el lugar de prestación del servicio pactado o la tecnología empleada.”²⁰

1.2.5.- LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

Para la utilización de este servicio de redes electrónicas incluido el Internet fue necesario la creación de una Ley que los regule, norme y controle todos los actos y contratos de carácter civil y mercantil que se realicen a través de estas redes; y que el Estado cuente con herramientas jurídicas que permitan el uso de los servicios electrónicos, incluido el comercio electrónico brindando mayor facilidad a las negociaciones internacionales.

El Honorable Congreso Nacional, considerando que:

“El uso de sistemas de información y de redes electrónicas, incluida la Internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado;

Es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos;

²⁰ Idid.

Se debe generalizar la utilización de servicios de redes de información e Internet, de modo que estos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura;

A través del servicio de redes electrónicas, incluida la Internet, se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia;

Es indispensable que el estado ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez mas compleja red de los negocios internacionales.²¹

Bajo estos considerándose se creó la Ley de Comercio Electrónico, firmas electrónicas y Mensajes de Datos, que entró en vigencia en el año 2002²².

Considero que la ley tipifica dos aspectos generales muy importantes, el primero, que se refiere al objeto de la ley, que abarca la regulación de seis temas que aportan al desarrollo y regulación de la actividad del comercio electrónico:

- Mensaje de datos,
- Firma electrónica,
- Servicios de certificación,
- Contratación electrónica y telemática,
- Prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico; y,
- Protección a los usuarios de estos sistemas.

²¹ Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos R.O. 67 Suplemento 557-2002

²² Ibid., Registro Oficial N° 557 Suplemento del 17 de Abril de 2002.

Y, el segundo, el agregado al Código Penal del Capítulo relativo a las Infracciones Informáticas, que para concepto de la Ley, se consideran Infracciones Informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, entre estas están:

- La divulgación o la utilización fraudulenta de la información protegida,
- Obtención y utilización no autorizada de información,
- Destrucción de documentos, títulos, programas, datos, base de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica.
- Falsificación electrónica,
- Daños informáticos
- Apropiación ilícita; y,
- El que violare el derecho a la intimidad.

Sin duda el desarrollo tecnológico registrado en las últimas décadas, ha obligado y dado origen la creación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Ley especial y específica que debe estar relacionada y en concordancia con la Constitución Política de la Republica, para proteger los derechos de las personas; en este contexto, el Art. 9 del referido cuerpo legal manifiesta:

“Protección de datos.- para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean

necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo²³

1.2.6.- RESOLUCIÓN DE CONATEL 584-23-CONATEL-2003

El CONATEL (Consejo Nacional de Telecomunicaciones) es el Organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas en el Ecuador; por tanto, expide el Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para Prestar Servicios de Certificación de Información y Servicios Relacionados; el objeto es establecer las normas y procedimientos aplicables a la prestación de servicios de certificación de información, emisión de firmas electrónicas y certificados de firma electrónica, registro de datos y sellado de tiempo y la operación de una infraestructura de clave pública en Ecuador, así como los deberes y derechos de los prestadores de estos servicios y de sus usuarios.

Lamentablemente desde la publicación de la Ley y este Reglamento en el año 2003, ninguna empresa ha sido calificada ni autorizada como proveedora de estos servicios en el país.

La falta de entidades de certificación de información y servicios relacionados, constituyen un obstáculo para alcanzar el desarrollo del comercio electrónico en nuestro país.

²³ Ibid., Registro Oficial N° 557 Suplemento del 17 de Abril de 2002.

1.3.- DERECHOS Y RESPONSABILIDADES

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, en el Art. 5.- dice:

“Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.”²⁴

Esta Ley ni su Reglamento no hacen referencia a sanciones, sino únicamente a lo que dispone el Código Penal como norma sancionadora por lo que no se cumple el principio de confidencialidad ni reserva de la información para su propietario y peor aún los derechos de privacidad e intimidad garantizados por la Constitución Política de la República.

La Protección de datos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

“El Código Penal anterior no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de la persona o para violar, acceder y descubrir sus secretos.

En el Ecuador el Régimen de Protección de Datos esta ligado al derecho fundamental de la Intimidad que lo tipifica la Constitución Política. La

²⁴ Ibid., Registro Oficial N° 557 Suplemento del 17 de Abril de 2002.

*nueva Ley aclara algunos aspectos de concepto y objeto del Mensaje de Datos y su protección vinculada a la intimidad y privacidad.*²⁵

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el capítulo de los derechos de los usuarios o consumidores de servicios electrónicos establece en los artículos:

“Art. 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

“Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

- *El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,*

²⁵ ACURIO Del Pino Santiago sacurio@larreategui-fabara.com.ec extraído marzo 2006

- *El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:*
 - 1 *Derecho u opción de recibir la información en papel o por medios no electrónicos;*
 - 2 *Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;*
 - 3 *Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,*
 - 4 *Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.*

Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la Internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o Servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo²⁶

Conforme a lo previsto en el Artículo 50 del referido cuerpo legal la Ley de Defensa del Consumidor en relación a los Derechos y Obligaciones de los Consumidores, dice:

“Art 4.- Derechos del Consumidor.- Son derechos fundamentales del consumidor, a más de los establecidos en la Constitución Política de la República, tratados o convenios internacionales, legislación interna, principios generales del derecho y costumbre mercantil, los siguientes:

- 1. Derecho a la protección de la vida, salud y seguridad en el consumo de bienes y servicios, así como a la satisfacción de las necesidades fundamentales y el acceso a los servicios básicos;*
- 2. Derecho a que proveedores públicos y privados oferten bienes y servicios competitivos, de óptima calidad, y a elegirlos con libertad;*
- 3. Derecho a recibir servicios básicos de óptima calidad;*
- 4. Derecho a la información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo los riesgos que pudieren prestar;*
- 5. Derecho a un trato transparente, equitativo y no discriminatorio o abusivo por parte de los proveedores de bienes o servicios, especialmente en lo referido a las condiciones óptimas de calidad, cantidad, precio, peso y medida;*
- 6. Derecho a la protección contra la publicidad engañosa o abusiva, los métodos comerciales coercitivos o desleales;*
- 7. Derecho a la educación del consumidor, orientada al fomento del consumo responsable y a la difusión adecuada de sus derechos;*
- 8. Derecho a la reparación e indemnización por daños y perjuicios, por deficiencias y mala calidad de bienes y servicios;*

²⁶ Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos R.O. 67 Suplemento 557-2002

9. *Derecho a recibir el auspicio del Estado para la constitución de asociaciones de consumidores y usuarios, cuyo criterio será consultado al momento de elaborar o reformar una norma jurídica o disposición que afecte al consumidor;*
10. *Derecho a acceder a mecanismos efectivos para la tutela administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a la adecuada prevención, sanción y oportuna reparación de los mismos;*
11. *Derecho a seguir las acciones administrativas y/o judiciales que correspondan; y,*
12. *Derecho a que en las empresas o establecimientos se mantenga un libro de reclamos que estará a disposición del consumidor, en el que se podrá anotar el reclamo correspondiente, lo cual será debidamente reglamentado.*

Art. 5.- Obligaciones del Consumidor.- Son obligaciones de los consumidores:

1. *Opinar y ejercer el consumo racional y responsable de bienes y servicios;*
2. *Preocuparse de no afectar el ambiente mediante el consumo de bienes o servicios que puedan resultar peligrosos en ese sentido;*
3. *Evitar cualquier riesgo que pueda afectar su salud y vida, así como la de los demás, por el consumo de bienes o servicios lícitos; y,*
4. *Informarse responsablemente de las condiciones de uso de los bienes y servicios a consumirse.²⁷*

1.3.1.- INTERVENIENTES

En el Comercio Electrónico, como en la protección de los datos intervienen tres tipos de personas: Emisor, Proveedor del servicio electrónico y destinatario.

Emisor.- Es la persona que origina un mensaje de datos, cuando el mensaje de datos ingrese en un sistema de información o red electrónica se considera emitida la información por el emisor.

²⁷ Ley de Defensa del Consumidor Registro Oficial No. 520 de septiembre 12 de 1990

Proveedor del servicio electrónico.- Es la empresa que se encarga de recibir la información a través de mensaje de datos, que deberá ser almacenada para luego enviar a los que requieran de dicha información.

En el mundo cibernético, la oficina postal es un servidor de correo, es decir, una máquina que proporciona el servicio de correo electrónico a los usuarios.

El sistema es tan simple que quizá por eso hoy el correo electrónico es el medio de comunicación por excelencia dentro de las empresas, ya que en algunos casos, evita hacer llamadas telefónicas de larga distancia o el envío de faxes.

Ahora, una vez hecha la analogía con el servicio postal, se da cuenta que el sistema real no difiere mucho, es probable que recibido varios correos electrónicos; se puede ver y enviar, se necesita un programa que haga la función de cliente, el cual puede ser un programa cargado en la computadora o utilizar un servicio de correo gratuito como Hotmail, yahoo, etc.

Destinatario.- Es la persona a quien va dirigido el mensaje de datos, se entenderá que lo pertenece cuando el mensaje de datos ingresa a un sistema de información electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos.

1.3.2.- ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su capítulo III, habla sobre las entidades de certificación de información, textualmente dice:

“Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros²⁸.

A más de estos artículos se establecen las obligaciones y responsabilidades que tienen las empresas en la prestación de servicios; la terminación contractual y notificación de cesación de actividades; pero sin duda nos interesa analizar la protección de los datos por parte de las entidades de certificación de información citado en el Art. 32 de la Ley.

Las empresas certificadoras deberán adoptar medidas para evitar la falsificación de certificados, almacenar toda la información por un periodo considerable, (mínimo de 10 años), especialmente a efectos de prueba en procedimientos judiciales. El almacenamiento podrá ser realizado por medios electrónicos. Deberá, garantizar la integridad, intimidad y confidencialidad de la información y proteger la información frente a terceros.

²⁸ Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos R.O. 67 Suplemento 557-2002

1.3.3.- FIRMA ELECTRÓNICA

“Es una manera de representación y confirmación de la identidad de un de sujeto en el medio electrónico en donde el titular aprueba y reconoce la información contenida en el mensaje de datos.”²⁹

“El tránsito del comercio tradicional al comercio electrónico nos introduce en un ambiente en el que la firma no sólo se hace prácticamente imposible sino que conspira contra la automatización de las actuaciones”³⁰.

Ello es más claro aún en el nuevo contexto del comercio electrónico abierto basado en Internet, ya que mientras el tráfico se realizó entre empresarios a través de redes cerradas, la utilización de éstas implicó que los participantes pactaran previamente en soporte papel cómo se estructurarían las operaciones entre ellos. Por consiguiente, ambas partes disponían de una prueba de sus relaciones análoga a la emergente de negocios plasmados sobre papel.

“En cambio, la actual contratación de bienes y servicios a través de redes informáticas y telemáticas facilita relaciones ocasionales entre las partes, sin necesidad de contactos previos. Ello apareja múltiples ventajas pero también encarta un conjunto de riesgos e incertidumbres ya que cualquier tercero puede "pinchar" la red e interceptar el tráfico electrónico que fluye a través de ella”³¹

²⁹ Ibid., Registro Oficial N° 557 Suplemento del 17 de Abril de 2002

³⁰ ALEGRÍA Héctor "Nuevas fronteras de la documentación, la forma y la prueba de las relaciones comerciales", Vol. 1, Pág. 94, Buenos Aires, 1997

³¹ LLANEZA González Paloma - Internet y comunicaciones digitales Bosch, Pág. 295 2004 Madrid,

Que garantiza la Firma Electrónica

- Autenticación de las partes (son quienes dicen ser)
- Garantiza la integridad del documento (la totalidad del documento es verídica, y se mantendrá íntegra)
- Garantiza que los firmantes no pueden repudiarlo (no podrán negar su existencia y validez legal)

Se establece dos tipos de Firmas Electrónicas:

- **Firma electrónica.-** Autentifica la identidad de la persona, es como "mostrar" la cédula de identidad, para que se confirme quien es.
- **Firma electrónica Avanzada.-** Autentifica la identidad, pero además permite llevar a cabo transacciones comerciales avanzadas y contratos, es como ir a la Notaria donde se presenta la cédula pero además se confirma ante el Notario la legalidad de la transacción o relación

La diferenciación entre ambas clases de firmas está hecha en función de la protección legal que ellas producen.

Los efectos jurídicos que ella produce son consecuencia de ser un medio apto al que se le atribuye la cualidad de contener la voluntad de la persona.

Firma digital.- Una firma electrónica es la firma digital, entendida como aquella que se crea usando un sistema de criptografía asimétrica o de clave pública.

“Básicamente una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. Aparentemente estos se consiguen con los criterios de autenticidad e integridad anteriormente citados, pero estos no son

suficientes si se pretende equiparar a la firma manuscrita que además tiene las propiedades de ser barata, fácil de producir, fácil de reconocer tanto por el propietario como por otros e imposible de rechazar por el propietario.

Para ello existen 2 métodos de firma digital:

“Firma digital con árbitro.- *Dos usuarios con desconfianza mutua confían en un tercero. Se utilizan criptosistemas de clave única (una sola clave para cifrar y descifrar). El emisor y el receptor tienen sus propias claves por lo que es el árbitro el encargado de recibir el mensaje del emisor descriptarlo con la clave del emisor. De esta forma el emisor y el receptor no necesitan compartir claves.*

Firma digital ordinaria.- *En la cual el usuario firmante envía directamente la firma al destinatario, y este debe poder comprobar la validez de la firma sin necesidad de un árbitro. A este método pertenecen los sistemas de firmas actuales que se basan en criptosistemas de clave pública”³².*

Requisitos.- La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos manifiesta:

“Art.15 Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

- a) Ser individual y estar vinculada exclusivamente a su titular;*
- b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;*
- c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.*

³² MARTINEZ Nadal Apolonia - "La ley de firma electrónica" cit., Pág. 37 y sigtes. 2003 Madrid

d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,

e) Que la firma sea controlada por la persona a quien pertenece.”³³

1.4.- PROTECCIÓN DE LOS DATOS

El Art. 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, habla sobre la protección de los datos, referidos en el punto 1.2.5.- del presente trabajo, además, el Art. 32 del mismo cuerpo legal establece:

El Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta Ley.”³⁴

Lamentablemente el Reglamento General de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, no aclara, ni desarrolla este tema tan importante y trascendental como es “La Protección de los Datos” y de las personas como establece la Constitución Política de la República, al hablar del Derecho a la privacidad, intimidad, y confidencialidad de los datos personales.

La información tiene sin duda un valor. De acuerdo a las ciencias económicas la información tiene un valor de uso, que puede ser utilizada como el valor marginal de producción. La información tiene el carácter de monopólico, puesto que la pertenece a esa persona por el hecho de mantener su posesión.

³³ Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos R.O. 67 Suplemento 557-2002

³⁴ Ibid. R.O. 67 Suplemento 557-2002

Es fácil demostrar que vivimos en un país donde el robo de una mesa de la sala de sesiones está más severamente penado que el robo de los secretos de la sala de sesiones, esto se da por la naturaleza del bien entre tangible e intangible y constituyen una clara evidencia de la falta de normativa respecto a la protección de datos, que por otra parte no puede asegurar la integridad de los datos y la intimidad de las personas.

Por tales razones es necesario que las normas legales, sean mas claras y explícitas, especialmente en todo lo que se refiere a la protección de los datos y de las personas.

CAPITULO II

COMERCIO ELECTRONICO

2.1.- CLASES DE COMERCIO ELECTRÓNICO

El comercio electrónico se ha convertido en los últimos años en un instrumento que amplía los negocios de las empresas, no sólo para dar a conocer su marca y productos a través de la Red, sino para que los consumidores como principales “beneficiarios” puedan hacer, de una manera más sencilla y sin costes de desplazamiento, la compra de artículos que consideren más convenientes para satisfacer sus necesidades.

Las empresas son conscientes del cambio evolutivo que la sociedad está experimentando, es por ello que son cada vez más los canales de distribución de los que disponen las mismas para hacer frente a la demanda de servicios por parte de los consumidores. Sin embargo, los consumidores no pueden dejarse llevar por la más atractiva de las técnicas para hacer uso del comercio electrónico, es decir, del establecimiento de una Página “Web” con múltiples contenidos, de múltiples animaciones, etc., éste aspecto es importante, sobre todo de cara a la competencia, imagen y marketing que todo negocio debe realizar, pero no sólo ha de atenderse a esta dimensión, sino que se ha de tener presente los derechos y obligaciones que tanto a una y otra parte le son aplicables, se refiere a derechos tan importantes para los consumidores como: el desistimiento, justificante de compra, devolución, etc., y obligaciones

impuestas a las empresas como la existencia de las condiciones generales de la contratación, protección de datos, registro, etc.

No se pretende orientar los aspectos que hacen que el comercio electrónico no se encuentre mejorando, ni tampoco de las diferentes formas de financiación que las pequeñas y medianas empresas (PYMEs) tienen para afrontar y hacer frente a este nuevo canal de información y venta, más bien es una exposición de la ausencia de una normativa unificada para la prestación de servicios por medios electrónicos, es decir, los aspectos que un consumidor debe tener en cuenta a la hora de comprar por medio de Internet, teléfonos u otros medios no tradicionales.

Algunos autores categorizan al comercio electrónico de acuerdo a la relación existente entre los diferentes participantes en:

*“Empresa - a empresa (B2B)
Empresa - a consumidor (B2C)
Consumidor - a consumidor (C2C)
Empresa - Gobierno (B2G)”³⁵*

Sin embargo para el presente estudio se pretende investigar más allá y determinar otros aspectos que amplían su clasificación como son: Tradicional, Directo, Indirecto e Internacional.

2.1.1.- COMERCIO ELECTRÓNICO TRADICIONAL

³⁵ <http://www.Wikipedia.com> abril 2006

“En el ámbito del comercio electrónico cobran una especial importancia los sistemas de resolución extrajudicial de conflictos (arbitraje, códigos de conducta e instrumentos de resolución extrajudicial de conflictos por medios electrónicos), ya que la celeridad de las transacciones y la globalización e internacionalización de las mismas no se corresponde con la lentitud de la justicia tradicional a la hora de resolver sobre los conflictos que se presentan. Sin olvidar esto, hay que decir que a la hora de hablar de comercio electrónico hay que acudir a las mismas materias que influyen en la regulación del comercio tradicional”³⁶

El comercio en Internet representa un revolucionario alejamiento de los métodos tradicionales de comercialización y puede estar lleno de peligros latentes, con todos los mitos y predicciones que rodean a Internet, es fácil entender mal el medio y cometer errores.

El desafío consiste en montar un eficaz programa de comercio electrónico que atraiga un público nuevo, grande y numeroso (mucho de este público antes era inaccesible), que satisfaga a ese público, que los convierta en clientes asiduos y asociados comerciales leales y productivos, esto involucra mucho más que generar un tráfico; abarca todos los factores que se requieren para conservar al público desde un diseño amigable para el usuario hasta una arquitectura del sitio Web que facilite la realización de las transacciones.

La innovación del comercio electrónico involucra nuevas tecnologías, nuevas formas de hacer negocios y nuevos procesos, como resultado, las compañías deben prepararse para educar a su público acerca de los beneficios y técnicas del nuevo medio, esto es particularmente cierto en el caso del comercio de empresa a empresa.

³⁶ Ley de Comercio Electrónico y Firmas Electrónicas y Mensaje de Datos R.O. 67 Suplemento 557 2002, Abril 17 .Ecuador.

Existen tres factores principales que deben tener en cuenta en la planificación de una estrategia de Internet:

- La importancia de una pronta presencia en el comercio electrónico.
- La personalización y comunidad que únicamente caracterizan las relaciones por Internet y por la “Web”.
- La des-intermediación y re-intermediación de las cadenas de distribución.

Sin embargo el comercio electrónico no va a reemplazar al comercio tradicional, pero en todo caso, el comercio tradicional puede reforzarse con comercio electrónico. Las tiendas virtuales más exitosas (Barrabés, por ejemplo) son extensiones del comercio tradicional.

2.1.2.- COMERCIO ELECTRÓNICO DIRECTO

“En el comercio electrónico directo la selección, pedido, envío y pago se realiza totalmente en línea, a través de la misma red mundial, lo cual abarata considerablemente los costos para el fabricante o distribuidor. Este tipo de Comercio Electrónico sólo puede realizarse, evidentemente, con mercancías denominadas “intangibles”, cuyo ciclo total de venta, pago y entrega puede realizarse por Internet: Videos, fotos, libros, revistas, programas de computación y música.”³⁷

³⁷ POTTS Ricardo F. (2003) Clases de Comercio Electrónico. Extraído 10 de enero del 2005
flavio@enet.cu

En este caso, el pedido, el pago y el envío de los bienes intangibles y/o servicios se producen “*on-line*” (en línea), ejemplos de esta modalidad son las transacciones vinculadas con el *software* y la música, y se lleva a cabo exclusivamente mediante un medio electrónico.

Por comercio electrónico directo se entiende todo aquel comercio en donde el proceso de compra y venta (oferta y aceptación del producto) se realiza por medio de equipos electrónicos (Internet, teléfonos móviles, PDA's, etc.), por ejemplo, la compra de un libro por Internet, el consumidor visualiza la oferta insertada en una Página “Web” y acepta la misma, pagando el precio ofertado mediante el uso de una tarjeta de crédito y descargándose el libro en su propio equipo electrónico, es decir, toda la operativa de compra-venta y pago se realiza desde la Página “Web” del vendedor y desde el equipo electrónico del comprador. Dentro de este tipo de comercio electrónico se asimilarían las ventas a distancia, pero de productos intangibles, que dan como resultados acciones tangibles como son bienes y servicios.

2.1.3.- COMERCIO ELECTRÓNICO INDIRECTO

“En el comercio electrónico indirecto la selección y pedido de las mercancías, insumos o materias primas por medios electrónicos, se envía al cliente final por los canales tradicionales, lo cual requiere una logística de apoyo en transportes e infraestructura”³⁸

38
Ibid Potts, (2003)

Consiste en adquirir bienes tangibles que necesitan luego ser enviados físicamente usando canales tradicionales de distribución.

Por Comercio electrónico indirecto se entiende todo aquel comercio en donde sólo la oferta y la solicitud de compra se realiza por medio de equipos electrónicos (*online*) y la entrega del producto y/o el pago se va a realizar en el “mundo físico” (*offline*). En concreto es lo que equivale a la modalidad de contratación recogida en la Ley de Comercio Minorista³⁹, la llamada venta a distancia, donde la transmisión de oferta y aceptación se realiza por cualquier medio de comunicación a distancia, cualesquiera que sea su naturaleza y a través de un sistema de comunicación organizado por el vendedor. El típico ejemplo es una Página “Web” donde existe una serie de productos y servicios con un precio determinado, y el consumidor escoge el que mejor se adecua a sus necesidades, pero en el que la entrega y/o pago de ese producto se realiza fuera de la Página “Web”, en un lugar físico (*offline*).

2.1.4.- COMERCIO ELECTRONICO INTERNACIONAL

“Las redes mundiales de información están transformando al mundo y acercando más a la gente a través de la innovación de las comunicaciones mundiales, posibilitando cambios en todos los ámbitos de la actividad humana, como la competitividad, el empleo y la calidad de vida de las naciones. Con las nuevas tecnologías, el tiempo y la distancia dejan de ser obstáculos, los contenidos pueden dirigirse a una audiencia masiva o a un pequeño grupo de expertos con alcance mundial o meramente local. Las redes mundiales de información, como Internet no conoce fronteras, es decir no tienen barreras geográficas.”⁴⁰

³⁹ Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico. Extraído el 18 de enero del 2006 <http://www.injef.com/php/index.php>.Madrid

⁴⁰ REDI Revista Electrónica de Derecho Informático - Número 26 (Septiembre de 2000). Extraído el 18 de enero del 2006 <http://www.premium.vlex.com/doctrina/>.

Hay diversos grados de apertura de un país y de las empresas al comercio internacional, la apertura permite la importación de productos que no pudieran ser fabricados en el interior del país; si finalmente se diera libertad total de comercio, sería lógico esperar que sólo se importasen los productos que no pudieran ser fabricados en el país o que pudieran ser fabricados en el país a un coste excesivamente alto. Pero lo que observamos en el mundo real es algo más avanzado: con mucha frecuencia se comercializa con productos que podrían ser fabricados fácilmente por el país importador (galletas, camisas, etc.) pero que resulta más ventajoso adquirirlos en el exterior.

Una de las ventajas del comercio internacional es consecuencia de las economías de escala: al aumentar la cantidad producida para satisfacer un mercado más amplio, los costes variables disminuirán. Además están las ventajas de la especialización: cuando un individuo se especializa en la realización de un trabajo concreto, adquirirá más habilidad y maestría en él, que los que lo realizan de forma eventual; esa argumentación, válida para un trabajador individual, también es válida para una empresa y para un país.

Los argumentos de carácter económico a favor de un sistema de comercio abierto son muy sencillos y se fundan en gran medida en el sentido común comercial, pero en la realidad la experiencia adquirida en materia de comercio mundial y crecimiento económico, desde la segunda guerra mundial, los aranceles aplicables a los productos industriales han bajado vertiginosamente.

“Durante los primeros decenios posteriores a la guerra, el crecimiento económico mundial tuvo una media de aproximadamente el 5% anual, y esta elevada tasa se debió en parte a la reducción de las barreras arancelarias. El comercio mundial creció a un ritmo aún más rápido, con una media de alrededor del 8% en el mismo período.”⁴¹

⁴¹ <http://www.monografias.com/trabajos6/meti.shtml>. extraído abril 2006

Los datos demuestran que existe una relación estadística indudable entre un comercio más libre y el crecimiento económico. La teoría económica señala convincentes razones para esta relación. Todos los países, incluidos los más pobres, tienen activos -humanos, industriales, naturales y financieros- que pueden emplear para producir bienes y servicios para sus mercados internos o para competir en el exterior. La economía nos enseña que podemos beneficiarnos cuando esas mercancías y servicios se comercializan. Dicho simplemente, el principio de la "ventaja comparativa" significa que los países prosperan, en primer lugar, aprovechando sus activos para concentrarse en lo que pueden producir mejor, y después intercambiando estos productos por los productos que otros países producen mejor.

La actividad productiva de una economía de mercado, conformada por los sectores primario y secundario, se encarga de la producción y transformación de bienes para el consumo final e intermedio; sin embargo, se hace cada vez más importante en cualquier sistema económico que se vean bien complementados con el sector terciario que brinda servicios como: comercio, transporte y comunicaciones. Se encarga de impulsar a los sectores productivos a la vez que es impulsado por ellos.

La esencia económica del sector servicios en general no es la producción de algo físico sino de intangibles que hacen posible que el aparato productivo siga funcionando. Otra de las funciones importantes del sector terciario es la relación y síntesis de la información de oferta y demanda que ayude a la formación de precios y mantenimiento de un modelo de mercado con competencia perfecta.

“Se entiende por comercio internacional, dentro de sus múltiples acepciones, aquella operación pactada entre dos sujetos situados en distintos territorios políticos mediante la cual un bien o servicio se traslada de la esfera de dominio de un sujeto hacia la esfera de dominio de otro sujeto. La operación más importante del comercio internacional es la compraventa internacional de mercaderías donde el bien se traslada cruzando fronteras, previo paso por aduanas. El Derecho del Comercio Internacional es la disciplina o rama del derecho que tiene por objeto las transacciones internacionales” ⁴²

Para las personas domiciliadas física y virtualmente en un país, las transacciones electrónicas pueden ser internas o internacionales, dependiendo de la dirección del ofertante y del tipo de la mercadería sujeta a transacción, se imagina la compra de software a través de Internet y la compra un cuadro de una galería ubicada en Nueva York,

En el primer caso se está ante una operación netamente virtual donde la celebración del contrato y la ejecución, es decir, el envío del bien es a través de procedimientos informáticos, obviamente muchos autores lo calificarían como un caso típico de comercio electrónico directo.

En el segundo supuesto está ante una contratación electrónica que involucra una ejecución física de la misma, es decir, la obra de arte tendrá que ser embalada y enviada por un medio de transporte, quizás aéreo y declarada ante las aduanas de origen y de destino. Entonces, en este segundo supuesto 'la operación es propia del comercio electrónico indirecto.

Tanto el comercio electrónico directo como el indirecto pueden constituirse en comercio electrónico internacional, dependiendo del bien si es tangible o intangible.

⁴² REDI Revista Electrónica de Derecho Informático - Número 26 (2004, Septiembre)

Finalmente se pretende precisar que el envío de bienes intangibles a través de la red no es como el envío de mercadería a través del courier o similar. Técnicamente el software se envía al espacio y es el comprador quien lo recupera desde el mismo.

2.2.- PRESENCIA DE LA ORGANIZACIÓN EN EL COMERCIO ELECTRÓNICO

La competencia ha alcanzado un nivel de intensidad no conocida en prácticamente todos los sectores industriales. La mera supervivencia, sin considerar el éxito, requiere que las organizaciones logren un nivel de efectividad sin precedentes. Los nuevos factores que sobre los negocios influyen son:

Reducir el ciclo de desarrollo de productos.- el tiempo de diseño y desarrollo se está convirtiendo en un factor significativo respecto de la habilidad para lograr participación de mercado, rentabilidad y supervivencia.

Reducir costos.- La necesidad de controlar costos, con el correspondiente deseo de mejorar la productividad, continúa siendo un objetivo permanente, con especial énfasis en los trabajadores calificados.

Incrementar la calidad y el servicio al cliente.- A medida que la competencia crece, el incremento en las expectativas de los consumidores respecto al tipo de respuesta que reciben de parte de las empresas, y está comenzando a cambiar la cultura y los procesos de muchas industrias.

Incrementar la respuesta del mercado.- La única constante es el cambio. La necesidad y habilidad de responder a los cambios del mercado continúa al punto de requerir adoptar nuevas tecnologías para reaccionar rápidamente.

Nuevos modelos de negocios.- El cambio continuo está presionando a muchas corporaciones a adoptar nuevos modelos de negocios, a desarrollar productos y trabajar en conjunto.

A pesar de que cada factor de los antes mencionados requiere sus propias estrategias, el enlace común a todas ellas es la necesidad de extender las comunicaciones dentro de la organización, entre socios comerciales y dentro del mercado. La adopción de tecnología Internet internamente, para crear una Intranet puede ser una contribución a cada una de esos factores críticos.

A más de estos nuevos factores es necesario destacar el servicio de post venta que brinda al cliente un servicio complementario y constituye un gran negocio para la empresa, dando valor agregado a los bienes y manteniendo al cliente en el tiempo.

Internet esta cambiando fundamental y rápidamente la manera de conducir los negocios, el ingreso al comercio electrónico le da a una compañía experiencia, lo que apareja una importante ventaja competitiva; además, le da prioridad a la marca y cumple con las expectativas de los clientes y asociados comerciales de hoy.

La utilización del Internet como medio publicitario hace que las empresas estén más cerca del cliente y en el caso de productos o servicios intangibles, puede servir de canal de distribución y como medio de cobro.

2.2.1.- RECURSOS ELECTRÓNICOS

Toda empresa que pretende incursionar en el comercio electrónico debe invertir y proveerse de recursos electrónicos capaz de conseguir una ventana al mundo, en donde se pueda realizar *bechmarking* y conocer los aspectos cambiantes del mercado de una manera más ágil para reaccionar a la competencia; el objetivo es mas amplio y pretende que el mundo conozca a través de esta ventana la empresa y los productos, para ello es necesario contar con tecnología que permita lograr la eficiencia.

Internet

Los principales componentes tecnológicos de Internet son:

- Protocolo de comunicaciones: La habilidad de conectar y comunicar redes y dispositivos de escritorio individuales.
- Intercambio Electrónico de Datos (*EDI-Electronic Data Interchange*)
- Transferencia de archivos: La habilidad de transferir archivos entre ubicaciones punto a punto
- Correo Electrónico (*E-mail o Electronic Mail*): La habilidad de proveer comunicaciones entre individuos y grupos.
- Navegación de *Web*: La habilidad de proveer acceso a la información bajo el modelo uno a muchos, a pedido.
- Emulación de terminal: La habilidad de acceder a aplicaciones existentes.

- Interfaces de usuario: La habilidad de canalizar la creciente complejidad técnica al escritorio de una manera transparente e intuitiva.
- Aplicaciones de Voz: Buzones, Servidores
- Diseño y Fabricación por Computadora (CAD/CAM)
- Multimedia
- Tableros Electrónicos de Publicidad
- Videoconferencia
- La tecnología Internet provee el medio para comunicar la información hacia los departamentos y los individuos. Poderosos motores de búsqueda permiten a las personas encontrar a grupos o individuos que tienen las respuestas a las preguntas que surgen durante el trabajo cotidiano.

Intranet

Aquellas empresas que adoptaron las Intranets, las han utilizado en alguna de las siguientes formas:

- Publicación de documentos corporativos: Ésta es un área donde significativos recortes de costos pueden ser obtenidos, así como mejoras en el tiempo y precisión de las comunicaciones a través de toda la organización.
- Acceso a directorios mediante búsquedas: Las Intranets permiten acceder rápidamente a agendas de direcciones globales y otros servicios de directorios similares.

- Páginas de individuos, de departamentos: Así como la cultura dentro de las organizaciones cambian al punto que cada departamento se orienta hacia sus propios objetivos.
- Aplicaciones de grupo: La tecnología Intranet puede ser utilizada para complementar o como alternativa de aplicaciones de grupo, Todo depende de la escala, costo y tiempo
- Distribución de software: Los administradores internos pueden utilizar Internet para entregar software y actualizaciones de software a pedido, a través de la red corporativa.
- Correo: Aunque el correo electrónico ha sido considerada la aplicación más utilizada, en muchas ocasiones su uso ha sido limitado o complicado en exceso, con el desarrollo de productos de correo a través de la Intranet que añaden a los mensajes documentos, video y sonido, el correo ha recibido un nuevo impulso y se posiciona como la herramienta estándar para la comunicación interna.

Con la aparición de la tecnología *Web*, nuevas y más apropiadas herramientas están disponibles para comunicaciones de uno a muchos.

- Interfase de usuario: La tecnología Intranet está evolucionando tan rápidamente que las herramientas disponibles, en particular el HTML, pueden ser utilizados para cambiar dramáticamente la manera que interactuar con los sistemas, estos permiten mayor flexibilidad en el diseño y el uso de las aplicaciones, así como un entorno unificado para acceder a los recursos de la organización. Haciendo esto, no sólo se crean interfaces que los usuarios pueden utilizar y apreciar, sino que también se elimina el exceso de funcionalidad y acceso a elementos que los usuarios específicos no necesitan.

Internet versus Intranet.

A lo largo de la evolución de Internet, una serie de aplicaciones han sido creadas para satisfacer las necesidades de cada área, dentro de cada área, la supervivencia del más apto ha generado muchas aplicaciones que se convirtieron en estándares de la industria; por ejemplo, el protocolo estándar para transferencia de archivos FTP, la tecnología de *Mosaic* para navegación de la *Web*, el estándar *MIME* para la distribución transparente de formatos de archivo, la sintaxis del HTML como lenguaje de la *Web*, etc.

Hay muchas razones por las cuales las tecnologías de Internet han tenido semejante impacto sobre las aplicaciones de las redes de las organizaciones:

- Comunicaciones universales: Cualquier individuo y/o departamento puede interactuar con otro individuo o departamento, o aún con socios comerciales y también con su mercado.
- Desempeño: Sobre una red con alto ancho de banda, la habilidad para manipular archivos de audio y video incrementa el nivel de eficiencia de la comunicación.
- Confiabilidad: La tecnología Internet está probada: es altamente robusta y confiable.
- Costo: Comparado con sistemas propietarios, los costos de la tecnología Internet es sorprendentemente bajo.
- Estándares: La adopción de protocolos estándar y APIs tales como MIME, Windows Sockets, TCP/IP, FTP y HTML otorgan una serie de herramientas que permiten construir, reestructurar y extender redes para satisfacer las cambiantes necesidades de las empresas, y permiten

intercomunicaciones basadas en estándares entre entidades externas y potenciales clientes.

La distinción clave entre Internet e Intranet es más semántica que basada en la tecnología: ambas utilizan las mismas herramientas y técnicas, protocolos y productos, sin embargo hay algunas diferencias entre ellos:

- Primero, mucha información corporativa no es para acceso público. Remuneraciones, planes comerciales y proyecciones de venta son ejemplos de información que las empresas no quieren publicar en Internet, y necesitan proteger cuidadosamente, como lo han venido haciendo con bases de datos.
- Segundo, muchas Intranets comienzan con proyectos pilotos para testear las tecnologías y entender los niveles de habilidad que ellas requieren, ellas rápidamente crecen a sistemas de información de tiempo completo que se adaptan a la cultura y métodos de la organización.

Por último, muchas organizaciones quieren que sus Intranets privadas tengan el mismo nivel de servicio que sus antiguas redes, y esto sólo es posible cuando la red está bajo completo control corporativo de principio a fin.

Entonces Internet no compite con Intranets., para ponerlo en contexto, Internet continúa definiendo las tecnologías disponibles para comunicación externa, mientras que las Intranets son la aplicación de esas tecnologías dentro de la organización y centradas en las redes corporativas.

Como se puede observar los recursos de Internet e intranet no representan costos elevados para las empresas sin embargo el servicio que presta a la organización es bastante representativo, sin lugar a duda existen otros

medios tecnológicos que hacen posible este mejoramiento que sin dejar de mencionarlos no representan información relevante para este estudio como son:

- Computadores
- Fax
- Teléfonos
- Bandas de comunicación
- Software y
- Otros Recursos

2.2.2.- LA COMPETENCIA

Dando un salto sobre la competencia la experiencia temprana es esencial para ganar y mantener una ventaja competitiva en el campo on-line. Las interacciones de los clientes en Internet difieren de las interacciones comerciales tradicionales, la publicidad y promoción electrónica, por ejemplo, están más personalizadas, customizadas y dirigidas a ciertos targets, la entrega de servicio y soporte basados en la *Web* debe estructurarse de forma diferente para guiar a los clientes a través de las actividades de autoservicio.

Las compañías no pueden aprender cómo dirigir eficazmente los negocios on-line simplemente observando lo que están haciendo sus competidores, tienen que “mojarse los pies” y aprender de sus propias experiencias.

Es típico que quienes ingresan tardíamente no puedan aprender suficientemente rápido como para lidiar con quienes ingresaron temprano, como resultado deben estar permanentemente relegados al rol de seguidores en vez de líderes y/o contratar personal técnico con suficiente conocimiento sobre la materia lo cual implica desembolso de recursos económicos.

Es esencial que las compañías vayan más allá de la imitación a fin de encontrar nuevos modelos de valor y nuevas formas de hacer negocios, ser más rápidos y más económicos puede ayudar, pero el verdadero éxito probablemente requerirá cambiar las reglas para llevar un nuevo tipo de valor a la oferta de productos o servicios de una compañía.

Amazon.com, por ejemplo, ha acumulado abundante experiencia en la realización de negocios on-line, como los competidores observan e imitan, Amazon.com continuamente añade, adapta y refina sus servicios y procesos basándose en su experiencia de expansión en la venta de libros por la *Web*; la temprana presencia de la compañía en la *Web*, junto a su aplicación de las características únicas ofrecidas por Internet a su modelo de negocio, le han permitido a Amazon.com mantener exitosamente una ventaja competitiva.

Otro ejemplo es Microsoft Expedia siendo Microsoft un líder experimentado en el mercado de la tecnología, la compañía no tenía experiencia en la industria de viajes, sin embargo Microsoft advirtió la oportunidad de ganar una importante participación de mercado en una industria completamente diferente y nueva: los servicios de viajes on-line, la estrategia aplicada por Microsoft ha permitido que ingrese a un nuevo negocio mediante la diversificación del negocio en pequeñas empresas.

Tradicionalmente, las compañías han usado la imprenta, la radio y la televisión para potenciar y expandir la identidad de la marca, un proceso que exige persistencia y una considerable cantidad de dinero y tiempo.

Internet es un medio en el que pueden crearse marcas nuevas y poderosas casi de la noche a la mañana siendo una oportunidad para las empresas en razón de que sus costos de tiempo y dinero son bajos.

Estas nuevas marcas rápidamente pueden hacerle sombra a las marcas que están bien establecidas en otros medios. En apenas dos años, Amazon.com surgió de la nada y se convirtió en el vendedor de libros líder de Internet, barriendo con nombres muy conocidos como *Barnes & Noble*.

Amazon.com usó una nueva metodología que es la Palabra de *Web* (que sirve como expresión equivalente de la *Web*); para establecer la marca más poderosa de Internet para la compra de libros. La naturaleza fundamental de Internet alimentó un rápido crecimiento al permitirle a la gente hablar de la marca por medio de foros, chats on-line y otros medios, para dar prioridad a sus marcas, las compañías deben establecer a sus marcas en el ciberespacio lo más rápido posible.

El nivel creciente de las expectativas por parte de los clientes y de los asociados comerciales presiona a las compañías para que actúen inmediatamente, dos años atrás, la gente esperaba que una compañía tuviera un sitio *Web* que ofreciera simplemente información a nivel de folletería acerca de la compañía y sus productos.

Actualmente, la gente espera poder dirigir los negocios con una compañía mediante su sitio *Web*, para un consumidor, tales negocios pueden incluir investigación competitiva, compra de productos, o recibir servicios y apoyo; las expectativas para un distribuidor o un asociado comercial pueden ir desde los pedidos de propuestas, la automatización de las ventas (pedido de sometimiento de propuestas, seguimiento de la contabilidad), sistemas de apoyo a los intermediarios, sitios para remates y procesamiento de reclamos por garantías, la presión para brindar entrega a estos públicos aumenta exponencialmente a medida que los competidores comienzan a entregar creativamente bienes y servicios a través de Internet, es decir que ya no constituyen solamente un medio de información.

2.2.3.- EL CLIENTE

Inicialmente, la gente responde a las nuevas tecnologías copiando lo que ya hacen en los nuevos medios, los primeros programas de TV, por ejemplo, se parecían a obras teatrales, de manera análoga, los primeros sitios de Internet se parecían a las revistas y a los folletos sobre productos; con el tiempo, la gente comienza a comprender el poder y las características únicas del nuevo medio, y aprenden a usar ese medio en beneficio propio. Internet no es la excepción, la personalización y la comunidad son dos de las principales características distintivas de Internet que debe comprender una compañía para desarrollar un plan de negocios mediante comercio electrónico.

Los diarios, radio, televisión y otros medios basados en la difusión son una oferta de una sola vía y no ofrecen ninguna interacción con sus públicos, en cambio, Internet proporciona una vía para obtener información del cliente y retroalimentarla directa e inmediatamente, las compañías pueden usar esa información para crear experiencias individualizadas para sus públicos, esta capacidad de dirigir un marketing personalizado, de uno a uno, es el sueño de la gente que hace marketing hecho realidad.

Además, Internet ha fomentado el desarrollo de miles de comunidades on-line basadas en intereses, incluyendo un amplio conjunto de grupos de noticias y salas de chateo, las compañías pueden potenciar las comunidades existentes o incluso desarrollar sus propias comunidades para establecer nuevas formas de interactuar con los clientes y los asociados, las interacciones personalizadas de estas comunidades permiten incrementar el valor de la experiencia con los clientes y asociados; por ejemplo, los sistemas de servicio al cliente creados en base a chateos, grupos de discusión y video conferencias crean comunidades

en las que los clientes pueden interactuar con la compañía y también con los asociados de la compañía y con los otros clientes de estos asociados.

La tendencia consiste en que las preferencias y expectativas de los clientes están cambiando.

Actualmente, muchos clientes prefieren realizar las compras on-line por la conveniencia, alcance y amplia disponibilidad de información, de productos y servicios, las compañías que no desarrollen una presencia en Internet perderán la oportunidad de ganar nuevos clientes y pueden perder muchos de los clientes existentes.

Además, empresas tecnológicamente agresivas pueden insistir en que los proveedores, distribuidores y otros asociados comerciales conduzcan todo el negocio junto a ellas vía Internet; el ahorro en los costos y la eficiencia ofrecida por Internet son razones de peso para que estas empresas eventualmente insistan en que todos los asociados realicen las transacciones de esta forma a fin de permanecer competitivas.

2.2.4.- CANAL DE DISTRIBUCIÓN

Dentro de Internet, el gran fenómeno de los últimos años es definitivamente la explosión de servicios de información multimedia, basados en el sistema www (*World Wide "Web"*) o más conocido simplemente como "*Web*".

La *Web* www se constituye como un verdadero canal de distribución, caracterizándose principalmente por la no hegemonía o control del mismo por ninguna empresa, además es de bajo coste y de impacto ilimitado, a su vez

permite una distribución rápida de los productos de información, y por último el coste de cambio de precios o productos comercializados es bajo, permitiendo así una rotación de productos bastante rápida.

2.2.4.1.- FLEXIBILIDAD Y RAPIDEZ DE CAMBIO

Otra característica interesante del *www* es que la información expuesta puede ser cambiada muy rápidamente, y que por tanto puede llegar a los clientes y a los compradores inmediatamente, esta característica será especialmente importante para aquellos sectores en los que la competencia esta basada en grandes campañas publicitarias que apoyan nuevos productos con un ciclo de vida muy corto.

El cambio rápido de producto, adecuándose así al mercado, no sólo permite obtener una ventaja competitiva puntual sino que también la mantiene.

2.2.4.2.- EL COSTE

La distribución de bienes dirigida al gran público a través del *www* recuerda mucho a la venta por catálogo, llegando incluso a tener ciertos parecidos, ya que ninguno de los dos necesitan: tiendas con escaparates, personal, stocks, etc., sino que la mercancía es servida directamente desde un almacén.

Los dos ofrecen información detallada sobre los bienes que el cliente podría comprar, uno en su catálogo y el otro por medio de una página *Web* que puede incluir una fotografía del artículo.

No obstante también sería necesario mencionar las diferencias entre un catálogo y una página *Web*:

a). Un pedido se origina cuando el lector del catálogo encuentra algo que le interesa, en el otro caso el comprador puede encontrar en el *www* una foto del objeto deseado que puede llegar a ser idéntica a la del catálogo. La diferencia estriba en que es más fácil ojear un catálogo impreso que uno que ésta en el *www*.

b). El vendedor por catálogo sólo tiene acceso a las personas que tienen su catálogo, mientras que en la red otros clientes potenciales desconocidos pueden acceder a él.

Pero también existen semejanzas como cuando los dos sistemas son compatibles, el vendedor por catálogo puede publicarlo en el *www* y utilizar a misma estructura que ya tenía montada para recibir pedidos, enviarlos, etc. lo interesante de ambos sistemas es que son canales de distribución de bajo coste, la inversión a realizar para acceder al *www* es pequeña, no es necesario tener servidor propio ya que terceras partes venden este servicio al por menor a un precio asequible; por otro lado, en el caso de que se maneje mucha información y que esta a su vez cambie a menudo, la compra de un servidor y su conexión a la red se amortizarían rápidamente.

2.2.4.3.- POSIBILIDAD DE CONTROL DEL CANAL DE DISTRIBUCION

Al no tratarse de un canal controlado es un punto de entrada para nuevas empresas, como canal de distribución normal no es controlable, a no ser que las empresas del sector consigan centrar la atención de los clientes en unas

páginas determinadas (un mercado virtual) del cual las empresas ajenas serían excluidas.

Una de las características principales de un canal de distribución es que debe llegar al cliente potencial, el interés del www como canal depende de que los clientes potenciales (o reales) estén conectados, actualmente sólo clientes potenciales de sectores muy específicos están conectados en suficiente número. universidades, bancos, hardware, software de microinformática... etc. es por tanto, en este momento un canal limitado en el número de clientes que acceden a él y en los sectores que pueden estar interesados en acceder buscando los clientes ya conectados.

Sin embargo es necesario interesar a los clientes potenciales en su uso, y de esta forma ofrecerles algo que les atraiga lo suficiente como para que den el salto y se conecten, de esta forma es necesario crear el mercado, el cual depende en buena parte del sector.

El sector que controla los canales de distribución existentes puede muy bien no estar interesado en crear un nuevo canal de distribución que no domina, ya que de esta forma lo estaría abriendo a nuevos competidores, por otro lado miembros de un sector en el que los canales de distribución sean muchos y busquen nuevas formas de competir (sin importarles por tanto la entrada de nuevos competidores) pueden acercarse al www como forma alternativa de distribución.

Por último no hay que olvidar que el acceso a un canal de distribución, sólo es uno de los factores que pueden impedir el acceso al mercado de nuevos competidores, además de esto los candidatos deberían pasar por encima del "coste de cambio" y otros factores que dificultan la entrada.

2.2.5.- DATOS ESTADÍSTICOS EN EL ECUADOR

En Ecuador no se han realizado estudios sobre personas o empresas que realicen comercio electrónico, esto da una clara muestra de la importancia que tiene el tema ante las autoridades y sus entidades responsables de regular el comercio electrónico; sin embargo, a continuación se consideran varios datos de encuestas, entrevistas y publicaciones realizadas por entes privados sobre el tema:

Sitios ecuatorianos de éxito en Internet

Una entrevista realizada en el año 2004 por la empresa Globalización y Gestión ON-LINE, permite determinar el poco avance que nuestro país a tenido sobre este tema en ese año.

“¿Qué porcentaje de ecuatorianos acceden a Internet y cuántos de ellos realizan compras a través de la Red?”

R: Existen aproximadamente 50.000 cuentas de Internet en Ecuador con más de 200.000 usuarios. Un 10 por ciento ha realizado compras a través de Internet y lo piensan hacer en el futuro.

P: ¿Cuál es el perfil del internauta ecuatoriano?

R: Generalmente el internauta ecuatoriano usa Internet con fines comerciales y empresariales, pero no con fines de compra en su mayor porcentaje. Los empresarios y profesionales entre los 20 y 45 años son los principales navegantes y compradores.

P: ¿Cuáles son los principales servicios y/o productos que adquiere el internauta ecuatoriano?

R: El comercio local está restringido a artículos como discos compactos, libros y electrodomésticos para el hogar. Las compras internacionales están disponibles para quienes poseen tarjetas de crédito internacional (un porcentaje mínimo de internautas ecuatorianos) y que disponen de medios para importar lo que adquieren en el exterior a costos razonables.

P: ¿Qué porcentaje de empresas está presente en la red y cuántas de ellas ofrecen la posibilidad de poder adquirir productos a través de la Red?

R: Existen aproximadamente 600 sitios de Internet locales y la mayoría de ellos se encuentran alojados en el exterior, principalmente en Estados Unidos. Un 25 por ciento de ellos tienen capacidad de vender productos en la red, especialmente hacia el exterior o servicios como turismo.

P: ¿Considera que una empresa debe estar presente en Internet para tener éxito?

R: Creo que es una oportunidad valiosa e importante para reforzar el éxito ya obtenido o para sustentar una política de crecimiento sana e internacional. Las pequeñas y medianas empresas (PYMEs), tienen una oportunidad para estar en nuevos mercados pero deben emplear estas herramientas principalmente para mejorar su posición y competitividad y luego para comercializar en el mercado internacional.

El empresario debe prepararse más para enfrentar con éxito el desafío de nuevos mercados más que para estar en Internet simplemente. Esto es mas comercio que electrónica.”⁴³

Encuesta para conocer la incidencia de las transacciones virtuales en Ecuador

⁴³Globalización y Gestión ON-LINE.(2004). <http://www.Monografias.com>

El universo.com realizó una encuesta telefónica entre 166 personas para conocer la incidencia del comercio electrónico a nivel de país.

“1.- ¿Ha realizado alguna compra por Internet?”

<i>SI</i>	<i>94</i>	<i>57%</i>
<i>NO</i>	<i>72</i>	<i>43%</i>
<i>Total</i>	<i>166</i>	<i>100%</i>

Del grupo entrevistado, un 57% ha realizado compras utilizando Internet, y el 43% no lo ha realizado

2.- ¿Qué compró?

<i>Acc. vehículos</i>	<i>4</i>	<i>4%</i>
<i>Películas</i>	<i>5</i>	<i>5%</i>
<i>Ropa</i>	<i>5</i>	<i>5%</i>
<i>Art. Hogar</i>	<i>6</i>	<i>6%</i>
<i>Libros</i>	<i>8</i>	<i>9%</i>
<i>Computación</i>	<i>15</i>	<i>16%</i>
<i>Cd's</i>	<i>16</i>	<i>17%</i>
<i>Otros</i>	<i>35</i>	<i>37%</i>
<i>Total</i>	<i>94</i>	<i>100%</i>

Un 57% ha realizado compras utilizando Internet, de éstos, el 17% ha comprado discos compactos, un 16% ha adquirido accesorios de computación y un 9% ha comprado libros, frente a un mayoritario 37% que ha adquirido bienes diferentes a los mencionados y a artículos del hogar, ropa, películas y accesorios de vehículos.

3.- ¿Cuál fue la forma de pago?

<i>T/Crédito</i>	82	87%
<i>Transferencia</i>	4	4%
<i>Envío dinero</i>	7	7%
<i>Otras</i>	1	1%
<i>Total</i>	94	100%

En un 87% las compras se efectuaron con tarjetas de crédito, frente a un 7% que lo hizo enviando el dinero y un 4% que realizó una transferencia monetaria.

4.- Compró en sitios Web...

<i>Nacional</i>	12	13%
<i>Internacional</i>	82	87%
<i>Total</i>	94	100%

Una gran mayoría 87% ha comprado en sitios internacionales frente a un mínimo 13% que realizó la transacción en Webs nacionales.

5.- *¿Con qué frecuencia ha comprado?*

<i>Una vez</i>	<i>43</i>	<i>46%</i>
<i>2 y 5 veces</i>	<i>42</i>	<i>45%</i>
<i>Más 5 veces</i>	<i>9</i>	<i>10%</i>
<i>Total</i>	<i>94</i>	<i>100%</i>

Los usuarios de la red han realizado una única compra en un 46%, de 2 a 5 veces un 45% y más de 5 veces apenas un 10%.

6.- *¿Cuál fue su grado de satisfacción?*

<i>Bueno</i>	<i>87</i>	<i>84%</i>
<i>Regular</i>	<i>7</i>	<i>7%</i>
<i>Malo</i>	<i>0</i>	<i>9%</i>
<i>Total</i>	<i>94</i>	<i>100%</i>

En una abrumadora mayoría, el 84% cataloga como buena la transacción virtual, frente a un 7% que la considera regular y un 9% que se queja del servicio.⁴⁴

Entrevistas

“El comercio electrónico cambia sustancialmente la forma de negociar porque hay que innovar ya que la competencia está a un click de distancia.

"Hay que recordar que los modelos de negocios aparecen y perecen a diario", aseguran Freddy Rodríguez Flores, presidente de la Comisión de Conectividad y Carlos Vera Quintana, director de la Agenda de Conectividad.

Lastimosamente en el país no hay estadísticas que avalen el uso del comercio electrónico a nivel interno o internacional.

Vera Quintana afirma que en la red es posible realizar todo tipo de transacciones. El grado de desarrollo o de uso depende del mercado e interés de cada país. En Ecuador, la red es más informativa aunque ahora también se realizan compras, reservas de hoteles y se interactúa incluso con el Gobierno a nivel nacional.

Desde el Ecuador para el exterior hay más uso por las facilidades de los sitios internacionales que permiten estas transacciones.

Las transacciones son diversas, desde compras simples a elección, modelos de subastas, modelos de subastas inversas (tengo cierta cantidad de dinero para un pasaje por ejemplo), etc.

Vera y Rodríguez se manifiestan plenamente convencidos del éxito de las transacciones virtuales. Son completamente seguras, creen los entrevistados. Muchos sitios incluso ofrecen seguro de devolución de

⁴⁴ <http://www.eluniverso.com/especiales/comercioelectronico/encuestacomercioelectronico.asp>
Extraído el 26 de marzo del 2006

dinero en caso de fraude por usar la red, pues están seguros de que es poco probable que esto ocurra.

Siempre hay que trabajar con sitios que aseguren la transacción y eso se logra con servidores seguros y certificados digitales.

Las empresas ecuatorianas no necesitan estar inscritas en ningún organismo para negociar.

"La Ley de Comercio Electrónico claramente establece que para hacer negocios en red no se requiere ningún requisito adicional a los exigidos para las transacciones fuera de línea. Es decir si una persona fabrica camisas y cumple con la ley para poder hacerlo legalmente, si las quiere vender en Internet no tiene que establecer requisitos mayores a los que no sean relacionados con seguridad del sitio y temas de protección al consumidor", asegura el director de la Agenda de Conectividad.

Lo que necesita cualquier empresario ecuatoriano para ejecutar negocios electrónicos es tener un sitio de la empresa o de un supermercado que lo aloje, por ejemplo, dice Vera Quintana.

En este aspecto, el Banco Central debe jugar un rol más relevante para que los costos de tecnología se repartan entre los diversos actores en cuanto a los sistemas como medios electrónicos de pago"⁴⁵

Aplicaciones en comercio y educación hay más desarrollo

El portal Internet World Stats en la revista LIDERES del día lunes 20 de marzo del 2006, presenta un estudio sobre Aplicaciones en comercio y educación y dice:

".... Desde el 2003, www.todo1.com lanzó al mercado una pasarela de pagos que permite hacer compras virtuales. En la actualidad la plataforma cuenta con 55 establecimientos como usuarios activos.

⁴⁵ <http://www.eluniverso.com/especiales/comercioelectronico/internetydesarrolloempresarial.asp> Extraído el 26 de marzo del 2006

Según Hely Gudiño gerente general de todo1.com, un 45 % es comercio electrónico, en ofertas de servicios varios y un 10% se usa en pagos de servicios universitarios.

Al cierre del 2005, el sistema registro 23,859 transacciones, que en conjunto movieron 8,3 millones de dólares. En sólo en lo que va del 2006, se han contabilizado 7000 transacciones y movimientos por 5,2 millones de dólares. Por el momento la plataforma acepta exclusivamente pagos con Visa y Dinners. Pese a que el último paso del proceso aún es manual (entrega de la factura física), según Gudiño, no es obstáculo. “Aunque no hay empresas certificadas en Ecuador para validar firmas y facturas electrónicas las empresas no se hacen problema”....⁴⁶.

Los cibernautas se multiplican en Ecuador pese a las limitaciones

Albertina Navas publica de igual forma en la revista LIDERES del día lunes 20 de marzo del 2006 la siguiente información:

“Ecuador está cada vez más conectado, muchos se sorprenderán y no se explicarán cómo, pese a la “deplorable infraestructura disponible en telecomunicaciones”, la baja penetración de PC respecto de la media regional o los costosos de servicios de conectividad. Tienen razón, todo ello es válido y demostrable. Sin embargo, igualmente innegable es que Internet crece en el país a un ritmo exponencial.

En ocho años (1998 – 2006), el número de usuarios creció más de 130 veces, de 4064 a 547513, según la superintendencia de telecomunicaciones (SUPTTEL) el 2002 fue el primer año que registró seis cifras (100663) y, a partir de entonces, el mayor incremento tuvo lugar entre el cierre del 2004 y el cierre del 2005, cuando el total de usuarios aumento 16%, de 191903 a 514020. Y sólo el primer mes del 2006, se sumaron más de 33000 nuevos usuarios.

Estas son cifras oficiales. No obstante, hay diversidad de criterios sobre su precisión puesto que el universo de usuarios no pasa de ser un

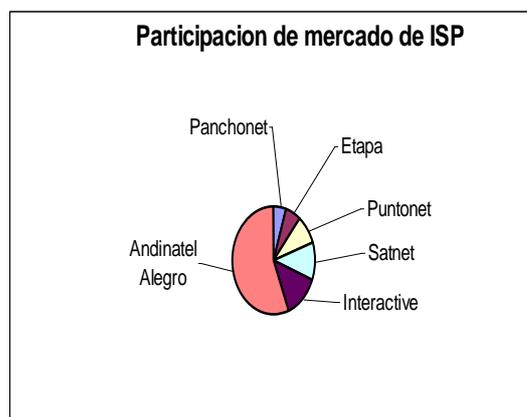
⁴⁶ REVISTA LIDERES, lunes 20 de marzo del 2006 pag. 7

estimado (número de cuentas por un factor), más no un conteo uno por uno. Por ello, no siempre los números coinciden.

Por ejemplo, el reporte 2005 de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo registró en el 2004 a 624579 usuarios en Ecuador. Esto es 21% superior al número registrado ese año por el organismo ecuatoriano de control de telecomunicaciones....⁴⁷

EL CIBERESPACIO CAUTIVA AL ECUATORIANO

El universo de usuarios actualizado a enero 2006	
Cuentas Dial Up totales	106603
Usuarios Dial Up totales	426412
Cuentas Dedicadas totales	31976
Usuarios Dedicados totales	121101
Cuentas totales	138579
Usuarios totales	547513



Fuente: Revista Lideres 20 de marzo del 2006

Reportes de prensa

El cyberdelito se gesta 'casa adentro'

"Fue después de sufrir dos ataques que José Luis Barzallo, abogado decidió especializarse en el área del delito informático.

En la primera ocasión, un ciudadano ruso le robó su nombre de dominio. Cuando regresaba a Ecuador, luego de cursar sus estudios de posgrado

⁴⁷ REVISTA LIDERES, lunes 20 de marzo del 2006 pag. 6

en España, este abogado realizó una transacción por Internet y en lugar de que su cuenta registrara el valor de 500 dólares, el sistema agregó un cero más. “Demostré el error a la empresa involucrada en la transacción y me reembolsaron el dinero.” El especialista advierte que los delitos informáticos más comunes son los relacionados con el fraude electrónico.

En términos técnicos se lo conoce como phishing (la duplicación de una página Web para hacer creer al usuario que se encuentra en la página original).

Barzallo dijo que gracias a la Ley de Comercio Electrónico se introdujeron reformas al Código Penal, referidas a los delitos informáticos. Eso significa que en esta Ley existe la figura del delito por medios informáticos.

Explica que a la Fiscalía han llegado algunos casos por delitos informáticos, ligados sobre todo, con fraudes bancarios.

Santiago Acurio, abogado y especialista en el tema, afirma que desde el 2003 hasta la fecha, el 90% de los ataques informáticos se gestan dentro de las mismas empresas.

A estas personas se las conoce como “insiders” y, con frecuencia, son empleados descontentos. Acurio lo llama “delito de carácter ocupacional”.

Dice que quienes vulneran la seguridad son empleados de las compañías que denuncian el ataque. Acurio y Barzallo participaron en la cita infoSecurity, organizada por la compañía Impsat.

Dicen que aunque la tecnología avanza más rápido que las leyes, hay aportes significativos en Ecuador con relación a las infracciones informáticas.

Acurio advierte que en el artículo 2 de la Ley de Comercio Electrónico ya se incorporan las amenazas e injurias por medios informáticos, se puede procesar una injuria, porque esta Ley da validez jurídica a los mensajes de datos (equivalencia funcional). La injuria precisa, sigue siendo injuria, aunque se hayan utilizado medios electrónicos para difundirla, en este campo del delito informático hay aspectos que resultan aún difíciles de abordar, como es el caso de las evidencias digitales, a las que se refirió Barzallo. El especialista advierte que las pruebas y elementos que quedan de todo movimiento informático son fundamentales en un caso

de fraude electrónico, él se refiere a discos duros, memorias flash o portátiles u otro tipo de recursos donde se almacena información sustancial para comprobar un ataque.

Sin embargo, no es fácil obtener esta información y más aún si la persona que ejecuta el fraude utilizó una computadora de un cybercafé donde no llevan ningún registro de los usuarios.

“Si no tengo el rastro de cómo se cometió el fraude, el robo, el engaño, no puedo llegar a esa persona”. Aunque es difícil determinar quien fue el responsable, los especialistas pueden seguir el rastro de los correos porque viajan de un servidor a otro.

El riesgo de no hallar al responsable aumenta con la proliferación de las redes inalámbricas. Si un usuario ingresa, por medio de una red Wi-fi, en el centro histórico para realizar un ataque, es más difícil saber quién lo hizo. “Mientras más abierta es una red más difícil es identificar a quienes ejecutan los ataques”.⁴⁸

Navegación segura.- En la red hay guías para usuarios desprevenidos

“Desde que la Internet se convirtió en un campo minado, con la aparición de los fraudes electrónicos y otras amenazas, la palabra protección ha cobrado más vigencia.

Una muestra del interés que suscita la seguridad son los esfuerzos que aparecen en la misma Internet por publicar guías para una navegación segura.

Aunque muchos informáticos subestiman su validez, pueden salvar a más de un cibernauta.

Estas guías no actúan como escudos “antiataques”, pero ayudan, sobre todo, si el usuario no ha protegido su PC con una contraseña, abre cualquier archivo con un título sugestivo y acostumbra enviar mensajes en cadena. Estas guías no están dirigidas a expertos informáticos y por eso son más valiosas.

⁴⁸ El Comercio, Tecnología cuaderno 2 Pag. 14 , 19 de noviembre del 2006.

¿Qué saben los cibernautas no especializados de “firewalls” (cortafuegos), de criptografía de datos, de “protección del perímetro? Los usuarios de hogar no necesitan especializarse en seguridad para evitar ser atacados.

Solo requieren conocer algunos trucos básicos y hacia allá apunta la Agencia de Protección de Datos que publica, con cierta frecuencia, nuevas guías de seguridad. Navegar en páginas seguras, que ofrezcan ciertas garantías, es una herramienta tan eficaz como lo puede ser un cortafuegos. No hay que invertir grandes sumas de dinero para que un usuario se sienta menos vulnerable cuando éste se conecta a diario con Internet.

No hay que subestimar estos consejos de navegación que por más obvios que sean ayudan a recorrer con más cautela esa red donde más de un usuario puede robar datos para luego efectuar transacciones comerciales.”⁴⁹

Con el scam no hay trabajo seguro

“Seguridad.- Mediante correos y chats, los cyber delincuentes ofrecen un empleo inexistente.

Las estafas en línea.- Una vez que los cyber delincuentes consiguen las claves o cuentas bancarias del usuario, ejecutan transferencias de fondos sin el consentimiento de los titulares de las cuentas.

Quienes muerden el anzuelo pueden convertirse también en cómplices de esta actividad ilícita, porque muchos delincuentes utilizan sus cuentas para lavar dinero, por ejemplo.

El sistema de estafa en la red se denomina scam, que a través de correos electrónicos, Chat o anuncios difundidos en la Web. se ofrecen trabajos fáciles desde el propio domicilio con jugosos beneficios. Según Francisco Hallo Master en Ciencias de la Computación, estas formas crecieron en número cuando apareció la Internet y quienes están detrás de estos fraudes tienen el propósito de robar datos personales. Otro de los métodos es informar al usuario mediante correo electrónico que ha sido premiado por una lotería, aunque éste ni siquiera haya participado, luego solicita al destinatario un desembolso de dinero para hacer frente a algún costo causado por algún trámite importante.

⁴⁹ El Comercio, Tecnología cuaderno 2 Pag. 14 , 19 de noviembre del 2006.

En Ecuador hay algunos casos de estafa de personas que por conseguir empleo enviaron dinero para poder obtenerlo, otros cyberdelincuentes buscan lavar dinero. El scam ha cobrado mayor fuerza en Estados Unidos y España ⁵⁰.

El delito informático, una plaga global

“El país no está libre de la cyberdelincuencia y por eso ya existe un proyecto para conformar una unidad de delitos informáticos. Tres expertos hablaron del tema.

De acuerdo con la consultora Gartner, cada año se pierden, por robos de identidad y estafas en línea, más de 50.000 millones de dólares en el mundo, lo más preocupante es que cada vez es más difícil localizar a los cyberdelincuentes, quienes dirigen sus actividades a través de varias computadoras, situadas en varias partes del mundo.

Está claro que el cyberdelito está orientado a aprovechar las vulnerabilidades de los equipos, sistemas y redes computacionales.

Ecuador no está libre de esta amenaza y por esta razón Santiago Acurio, especialista en delitos informáticos e informática forense, propuso la creación de la unidad de delitos informáticos del Ministerio Público UDIMP; tiene como misión, investigar, perseguir y prevenir todo lo relacionado con la llamada criminalidad informática en todos sus ámbitos. Acurio, sostiene que en Ecuador se han registrado algunos procesos legales por fraude informático, sólo en el año 2005 hubo 10 casos. Esta organización estará encargada, según lo planteado de investigar amenazas, injurias calumnias por correo electrónico, fraudes, mensajes SMS, Webs, pornografía infantil, phishing, propagación de virus, extracción de información, conductas ilícitas, entre otras.

En Ecuador, no existe un organismo especializado en estos delitos, como existe en otros países como EEUU, donde el FBI cuenta con el Computer Cime UNIT. Incluso en España, la Guardia Civil tiene un departamento especializado en esta clase de infracciones, El tema resulta bastante preocupante, más aun cuando este tipo de delitos permanecen sin castigo.

⁵⁰ El Comercio, Tecnología cuaderno 2 Pag. 14 , 18 de febrero del 2007

En este proyecto presentado a la Fiscalía, también está incluida la creación de un sistema de información de delitos informáticos que permitirá al Ministerio Público obtener información sobre su forma de combate y prevención. Un estudio publicado en el Manual de las Naciones Unidas para el control de los delitos informáticos señala que el 90% de esos ilícitos realizados por computadora, fue ejecutado por empleados de la propia empresa.”⁵¹

Los datos estadísticos, las entrevistas, los comentarios expresados por expertos en el tema, y las publicaciones de los diarios presentados, sustentan el estudio del tema propuesto y la necesidad de tomar acciones que permitan proteger la información del estado, las empresas y los usuarios en general.

2.3.- VISIÓN COMERCIAL EN INTERNET

“Se pronostica que el comercio electrónico por Internet se desarrollará a una tasa creciente en los próximos años, con ventas en línea ponderadas en trillones de dólares, muchas empresas han establecido importantes sitios Web y están utilizando este nuevo canal de ventas este informe sintetiza los conceptos fundamentales del comercio electrónico, cubriendo la venta por catálogo on-line y compra on-line.”⁵²

La mayoría de las empresas con presencia en Internet tienen sitios institucionales, el objetivo de este tipo de sitios es complementar actividades tradicionales de Marketing, tales como brindar información adicional, y promocionar la compañía.

Un sitio de comercio electrónico es distinto, el objetivo es cerrar la operación electrónicamente con el pago (y en algunos casos la entrega) realizados por

⁵¹ El Comercio, Tecnología cuaderno 2 Pag. 15 , 3 de diciembre del 2006

⁵² REVISTA LIDERES, lunes 20 de marzo del 2006 pag. 3

Internet, este tipo de sitios incluye información detallada de los productos, fundamentalmente porque los visitantes apoyarán su decisión de compra en función de la información obtenida y de la percepción que el sitio *Web* les haya generado respecto a la confiabilidad y solvencia de la empresa.

Ese tipo de sitio *Web* tiene generalmente cuatro secciones:

- Información institucional: Esta sección intenta atraer a los clientes y generar un clima de confianza en la empresa.
- Catálogo: Información detallada sobre los productos, sus beneficios y precios.
- Carro de compras donde el cliente selecciona los productos que requiere.
- Procesamiento de órdenes: Esta sección incluye un método para especificar y configurar la orden.

Los sistemas más avanzados pueden incluir sistemas de seguimiento de la orden.

Los sitios de comercio electrónico pueden encontrarse solos o formar parte de un sitio de venta mayor, comúnmente denominados "shopping mall", presentan una apariencia estandarizada, en donde muchas empresas tienen presencia en un único *Web site* (sitio *Web*) a través del cual los visitantes pueden acceder a información de distintas empresas.

Un emprendimiento de comercio electrónico no es simplemente construir un catálogo con posibilidad de comercio electrónico. "Ponerlo en Internet y visitarán" nunca ha sido un enfoque que ha funcionado en Internet. El sitio debe ser promocionado tanto en Internet como en medios de comunicación tradicionales. Otras alternativas efectivas son:

- Negociar links con otros sitios *Web*.
- Promoción y Marketing tradicionales.
- Publicitar en motores de búsquedas y otros sitios de alto tráfico.
- Programas de referencia de visitantes, por los cuales los sitios que refieren visitantes obtienen una comisión por ventas.
- Una vez que el sitio está construido y el dominio registrado se puede investigar otras formas de promocionar su negocio, tales como ofertas especiales y los programas de referencia de visitantes, ellos pueden ser monitoreados en su comportamiento dentro del sitio y las ofertas personalizadas según sus propios intereses.

El comercio electrónico no es igual al marketing directo, el error de igualar el número de usuarios de Internet con un mailing de esa cantidad de piezas distribuidas, si hay 2 millones de potenciales compradores en Internet, un “*Web site*” no es comparable con un mailing a 2 millones de personas, sólo una parte de ellos encontrarán su sitio y lo navegarán exhaustivamente.

No obstante, habrá gran cantidad de visitantes interesados en sus productos y servicios, y debe estar preparado para recibirlos.

Los responsables de las acciones de marketing directo a menudo tienen problemas para trabajar con catálogos on-line, el hecho es que si alguien visita un sitio y decide no realizar una compra, entonces ése es el final de la relación, si alguien recibe un catálogo por correo y decide no comprar, la empresa o comercio puede enviar nuevamente el catálogo, realizar un seguimiento telefónico o articular otras acciones posteriores. Las personas encargadas de llevar a cabo acciones de marketing directo suelen lamentar esta falta de control de la situación.

En realidad, ellos deben aprender las nuevas herramientas que Internet provee para lograr los objetivos perseguidos con esas acciones, tales como las

newsletters, el Opt-in, e-mail, los sistemas de suscripción de visitantes y otras. Internet es un medio apto para realizar acciones de marketing directo, luego de entender la lógica de la relación entre la empresa, su “*Web site*” y los clientes, y las herramientas disponibles.

La venta por Internet no es venta *retail*, y no es marketing directo, tiene sus propias características, que van evolucionando a medida que la tecnología se desarrolla, se conoce más sobre negocios en Internet y su tecnología, se encuentran nuevas formas para desarrollar los negocios, las cuales son únicas para este medio.

Aunque se buscan maneras de desarrollar relaciones uno a uno utilizando Internet, esto debe hacerse cuidadosamente, puede ser capaz de verificar la frecuencia de visitas de un visitante, pero esa persona puede no saber que está siendo seguido en sus movimientos. Intente mantener archivos de las preferencias de sus visitantes, a través de los cuales podrá presentarles ofertas especiales de acuerdo con sus intereses, pero no olvide que es preferible hacerlo con su consentimiento. Internet permite a los hombres de marketing alcanzar un objetivo siempre soñado, el cual es lograr la personalización masiva.

Este juego de palabras aparentemente contradictorias, encierra la posibilidad de realizar ofertas comerciales masivamente, pero cada una de ellas personalizadas de acuerdo con las preferencias del cliente, con ello se logra una máxima compatibilidad entre las necesidades de los visitantes y los satisfactores de necesidades que la empresa puede proveer, evitando la navegación redundante en páginas que contienen información y productos no deseados por los visitantes.

Este nuevo mundo requiere nuevas actitudes y nuevas habilidades de marketing.

No exijamos a Internet una cualidad que no presenta ningún medio ni canal de ventas, pero cuando es apropiado, puede ofrecer un canal de bajo costo con un punto de venta virtualmente en cada país del mundo.

La clave para obtener un buen sitio de comercio electrónico es proveer un ambiente que facilite a los clientes navegar a través del catálogo de productos y eventualmente realizar una compra.

El consumidor al navegar en Internet debe estar en condiciones de encontrar el producto que necesita sin recorrer infinitos niveles de índices o menús, el visitante debería poder llegar a los productos que ellos necesitan con unos pocos clicks. 80% de los visitantes de sitios mirarán las páginas a la que arriban al sitio y aquella por la que se van. Ha sido estimado que se pierden el 20% de los visitantes cada vez que se les pide que sigan un link a otra página, una buena lógica de navegación es esencial.

La información debe ser detallada una vez que el cliente ha ubicado el producto de interés, facilite imágenes y diagramas para ayudarlos a entender que se le está ofreciendo.

Cuando el catálogo es pequeño (menos de 5 ítems), un simple formulario puede hacer la toma del pedido. Sin embargo, en sitios más grandes, los consumidores incluirán productos dentro de una canasta de compras electrónica durante la navegación. En algún momento el consumidor puede controlar el contenido de la canasta, el costo de los productos y demás detalles de la compra. Esto le facilita al consumidor la selección de productos mientras visita el sitio.

Cuando la sesión de búsqueda de productos está completa, el cliente clickea sobre un link que lo lleva hacia el área de confirmación de la orden de compra.

En este momento, se le muestra al consumidor el listado de los productos que ha seleccionado, el costo total, los gastos de envío, impuestos, etc. el consumidor puede ingresar instrucciones de envío, su nombre, dirección y demás datos necesarios para cerrar la transacción.

En general, le son ofrecidos al consumidor un conjunto de opciones de pago, la más habitual es utilizar tarjetas de crédito, en esta etapa del proceso el sistema debería haber pasado a un modo de navegación segura. La tecnología normalmente utilizada es el SSL (*Secure Socket Layer*). Esto significa que todas las comunicaciones con el servidor son encriptadas en una forma que posibles intrusos no puedan (sin una dificultad desproporcionada) robar información importante, estos temas serán discutidos en el siguiente capítulo, pero es importante para la confianza del cliente que el sitio opere en modo seguro tan pronto como información de tarjetas de crédito sea requerida.

El cliente será visualmente advertido por el "Web" *browser* que está en un modo seguro: una llave azul y una línea azul en *Netscape Communicator* y un candado cerrado en Microsoft Explorer, advierten del paso a un modo de navegación segura.

Esta tecnología es ampliamente utilizada y entendida por los usuarios de Internet. La mayoría de la bibliografía sobre Internet enfatiza la necesidad que los clientes entreguen su información confidencial en una sesión segura, por lo cual es esencial tener este aspecto en cuenta a la hora de encarar la construcción de un sitio de comercio electrónico.

2.4.- LOS MEDIOS DE PAGO

El método de pago más popular es la tarjeta de crédito, y claramente, esta alternativa requiere que el pago sea seguro, sin embargo, es posible encontrar sitios que aceptan pagos con tarjeta sin proveer de seguridad extra en la transacción.

Los sitios que aceptan información de tarjetas de crédito sin seguridad extra están tomando el riesgo de posibilidad de fraudes, no hay razón por la cual las empresas no puedan ofrecer un catálogo de productos funcional, con un mecanismo de pago seguro apropiado, esto puede ser realizado a costos reducidos.

a) **Pago con tarjeta de crédito.-Procesamiento de la transacción en línea a través de un Gateway Internacional.**

Para el procesamiento en línea de una compra realizada con tarjeta de crédito, es necesario acceder a un servicio conocido con el nombre de *Gateway* de pago o **procesamiento de transacciones**. Los *Gateways* de pago toman la información de pago provista por el cliente al momento de realizar su compra por Internet, y la validan, autorizando la operación con vistas a su perfeccionamiento comercial; se ocupan de corroborar la existencia de la tarjeta de crédito, su aptitud para ser utilizada como medio de pago para la transacción y generan el crédito por la venta realizada.

Lamentablemente en Latino América, las empresas emisoras de tarjetas de crédito ni los bancos proveen servicios de *gateway* de pago, por lo cual la validación en tiempo real se debe realizar en *gateways* internacionales.

Si bien es cierto que las tarjetas nacionales no pueden ser procesadas, también lo es el hecho que este tipo de tarjetas conforma un porcentaje marginal del total de tarjetas emitidas por las empresas líderes del sector.

Los *gateways* internacionales exigen distintos requisitos para la prestación del servicio, en su mayoría, exigen la apertura de una cuenta denominada "*Merchant Account*". Esta cuenta permite al titular de un comercio aceptar transacciones con tarjetas de crédito (el cargo a la tarjeta de crédito y el depósito a la cuenta bancaria del beneficiario) en el caso de que un comerciante requiera procesar tarjetas de crédito en tiempo real por Internet debe abrir una "*Internet Enabled Merchant Account*", que permite procesar transacciones en tiempo real.

Es necesario sumar un alto puntaje para obtener una *Merchant Account*, cada servicio de provisión de procesamiento tiene su propio criterio de evaluación, por lo cual es recomendable visitar a varios proveedores para encontrar aquel que ofrece la apertura de cuenta con menor tasa de descuento sobre cada operación.

La apertura de una *Merchant Account* exige la preexistencia de un emplazamiento comercial y el correspondiente registro ante los organismos impositivos y de fiscalización, eso significa el establecimiento de una sociedad en el exterior -los principales servicios de "*Gateway*" (puerta de entrada) se prestan en Estados Unidos-, el registro de la sociedad ante los organismos de fiscalización impositiva del país donde se registra la sociedad.

Afortunadamente, existen servicios que prescinden de la apertura de una *Merchant Account*, lo cual simplifica enormemente el acceso al servicio de procesamiento de pagos con tarjeta de crédito, en este caso, se realiza una fiscalización más rigurosa, pero se exime al comerciante de los requisitos anteriormente mencionados.

Esta última alternativa es ideal para los sitios de comercio electrónico, por dos razones:

1. Facilita enormemente el acceso al procesamiento de tarjetas en tiempo real, puesto que no se requieren gestiones ante múltiples organismos públicos y privados sino sólo ante el proveedor de servicios.
2. Permite disponer de los fondos en la institución bancaria que se designe, en cualquier lugar del mundo.

b) Pago con tarjeta de crédito.- Procesamiento de la transacción fuera de línea.

Una alternativa al servicio de *gateway* de pago es procesar fuera de línea el pago con tarjeta de crédito.

En este caso, el visitante ingresa sus datos de tarjeta de crédito en el browser de Web, y el sistema los dirige hacia su empresa, donde debe ser procesado manualmente.

La operación es similar a la venta telefónica: se le envía a las empresas que extienden las tarjetas de crédito (VISA, *Mastercard*) un resumen de transacciones pendientes de autorización por fax, y luego de obtenerse la autorización se procede al envío de los productos y su facturación.

Para aquellas empresas que poseen un sistema electrónico de captura de datos, pueden procesar sus transacciones originadas en Internet a través de él, obteniendo ahorro de tiempo y procesos administrativos.

El procesamiento para el pago con tarjeta de crédito es el siguiente:

Autorización.- El comerciante debe obtener una autorización para él realizar un cargo.

La autorización significa que la tarjeta no ha sido reportada como robada, y que tiene crédito suficiente para afrontar la operación, el resultado es la reducción temporaria del límite de compra de la tarjeta del comprador por un monto igual al de la compra.

Hay dos formas en que se puede obtener la autorización:

Manual.- El comerciante obtiene la información correspondiente a la transacción del servidor de Web, el comerciante requiere luego autorización utilizando un método común, como por ejemplo una terminal "P.O.S" (máquina de autorización en un establecimiento comercial)

Automático.- El software del servidor se comunica directamente con la compañía que procesa las tarjetas de crédito y acuerda la autorización en tiempo real.

Claramente, el sistema automático es preferible, pero es más complejo, por que requiere que la información de la tarjeta de crédito viaje a través de la red en forma segura.

Captura.- La etapa final consiste en el débito de la tarjeta de crédito, esto puede ocurrir al mismo tiempo que la autorización, siempre que el comerciante se comprometa a la entrega de las mercaderías dentro de un plazo de tiempo

preestablecido, caso contrario la captura se realiza cuando los productos son enviados.

c) Sistemas propietarios de pago:

Fueron desarrollados antes que la tecnología de servidor seguro estuviese ampliamente disponible. Operan de distintos modos.

Cybercash.- usa una billetera electrónica para guardar los datos de tarjeta de crédito y transmitirlos con seguridad utilizando su propio *software* de encriptamiento.

First virtual.- Usa un sistema de mensajes de "*e-mail*" (correo electrónico) para confirmar la venta, el problema con este sistema es que requieren que el usuario haga algo para configurarlas, o bien instalar *software* especial o registrarse en la organización con la cual se realiza las transacciones.

Cheques electrónicos.- Son utilizados principalmente en Estados Unidos.

Ordenes de compra.- Para transacciones entre empresas, esta modalidad es apropiada y ampliamente utilizada.

d) Otros métodos de pago.

Hay un número de alternativas al pago con tarjeta de crédito, que deberían estar disponibles en un sitio de comercio electrónico.

Pago por Fax.- El visitante navega el “Web site” y elige los productos que desea adquirir, cuando decide comprarlos, el sistema le requiere sus datos personales (no se incluye información del medio de pago) y a continuación genera un reporte en pantalla con toda la información relativa a la compra, en ese momento se le pide al comprador que imprima la información pantalla, escriba sobre la impresión los datos de su medio de pago y luego la envíe por fax a las oficinas de su empresa, donde se procederá al procesamiento interno tal como fue descrito en el punto anterior, es un método realizable y razonablemente seguro.

Venta telefónica.- El visitante navega el “Web”site y elige los productos que desea adquirir, cuando decide comprarlos, el sistema pide sus datos personales y su número de teléfono, esta información junto con el listado de productos ha adquirir es enviado al personal de su empresa, que procede a tomar contacto telefónico, obtener los datos de la tarjeta de crédito por vía telefónica y cerrar la transacción, esta alternativa permite completar la compra sin necesidad de enviar información financiera a través de Internet.

El proceso se completa enviando a las empresas que extienden las tarjetas de crédito (*VISA, Mastercard*) un resumen de transacciones pendientes de autorización por fax, y luego de obtenerse la autorización se procede al envío de los productos y su facturación.

Para aquellas empresas que poseen un sistema electrónico de captura de datos, pueden procesar sus transacciones originadas en Internet a través de él, obteniendo ahorros de tiempo y procesos administrativos.

Pago contra entrega.- En esta alternativa, el visitante navega el “Web site” y elige los productos que desea adquirir, cuando decide comprarlos, el sistema le requiere sus datos personales, los cuales son remitidos a las oficinas de su empresa junto con la información específica de la compra, la cual permitirá

hacer la verificación previa al envío de los bienes, el cobro se efectúa en el momento de la entrega de los bienes.

Micropagos.- Mientras que las tarjetas de crédito son particularmente útiles para compras de monto significativo, ellas no son eficientes para compras de poco monto (\$10 o menos). Hay sistemas en desarrollo que operan como un monedero electrónico, el cual puede ser recargado utilizando mecanismos de pago tradicionales, el monedero puede ser vaciado sin formalidades mediante la realización de pequeños pagos.

First Virtual.- (FV) es un sistema de pagos operado por *First USA* y EDS, basado en el mantenimiento de cuentas virtuales de clientes que se liquidan periódicamente contra tarjetas de crédito.

2.5.- TRIBUTACIÓN

Las autoridades deben prever que el comercio electrónico no socave la capacidad del Gobierno para recaudar los ingresos públicos vía tributación. asimismo, los principios de tributación que rigen a los gobiernos en relación con el comercio tradicional deberían adecuarse para su aplicación a esta nueva vía de comercialización.

“La relación existente entre la jurisdicción tributaria y el comercio electrónico no es tan sencilla como se puede imaginar, dado que el término "comercio electrónico" reúne transacciones muy diversas, tanto en sus contenidos como en los sujetos intervinientes, incluso en la forma de su ejecución, pues la transacción puede concluirse y realizarse a

través de la propia Web on line o por medio de otros medios off line (fuera de línea).”⁵³

La tributación en el caso del comercio electrónico ecuatoriano, se puede decir que no se ha desarrollado, pero para ello se establece los siguientes puntos de referencia como los más importantes:

Ausencia de control del usuario.- Por las características propias del ciberespacio se dificulta el anclaje físico, por esta razón es muy difícil la localización física del usuario.

Imposibilidad de localización de la actividad.- Por la misma razón, es muy difícil la detección de las actividades que realiza, sumado a ello, gran cantidad de “ISP” (proveedores de servicio electrónico), los que no tiene ningún control sobre la información que pasa por sus servidores

Carencia de medios para identificar al usuario.- Por lo general una dirección de *e-mail* o un nombre de dominio sólo indican quién es el responsable tecnológico y no puede vincularse con la computadora o el usuario correspondiente

Criterios de imposición.- Las actividades comerciales en Internet provocan un serio cuestionamiento de los criterios de imposición, tanto del impuesto a la renta como del impuesto al valor agregado, surge así el problema de determinar la jurisdicción con potestad para gravar las transacciones que se realiza por Internet

⁵³ Yáñez Pablo. (2000) .Introducción al estudio del Derecho Informático 2000

Jurisdicción competente.- Internacionalmente los criterios de imposición están basados en los principios de residencia, fuente y nacionalidad, lo que permite que cada Estado ejerza su potestad

Principio de la residencia.- La mayoría de los Estados ejercen su potestad sobre las rentas obtenidas por los individuos o empresas establecidas permanentemente en su territorio, en términos de residencia

Principio de la fuente.- Otros países se enrojan en el principio de la fuente, es decir que se tienen en cuenta el lugar en donde se produce la renta sin importar otros aspectos

Principio de la nacionalidad.- Por último, algunos países establecen su criterio de imposición en relación al carácter legal de la empresa o individuo con el Estado, es decir, su nacionalidad.

“En el ámbito internacional se dan transacciones entre personas de países con legislaciones que entran en colisión por ello, muchos países optan por el principio de la fuente o se amparan en los tratados internacionales.

Uno de los principales obstáculos para el comercio electrónico son las normas sobre celebración y ejecución de los contratos, las disposiciones convencionales no funcionan adecuadamente en entornos digitales.”⁵⁴

Las cláusulas predispuestas no siempre cuentan con redacciones claras, cuando las transacciones se realizan enteramente online pueden ocultarse las transacciones al momento de ser registradas, al menos que el consumidor exija su factura y existe un cruce de información por la Institución en cargada de controlar los Impuestos Sistema de Rentas Internas Ecuatoriano (SRI).

• ⁵⁴ PEREZ de Ayala José Luis. *Explicación de la técnica de los Impuestos*. 3era ed. Editoriales de Derecho Reunidas, S.A., 2004. Madrid

Es necesario que este tema sea analizado por las autoridades correspondientes, sin embargo y para efecto de la seguridad de los usuarios del comercio electrónico, se requiere que exista tanto para el cliente como para el vendedor el respaldo de ingreso y egreso económico de la transacción realizada, de esta forma se puede evitar fraudes fiscales y desconocimiento de las transacciones en caso de litigio también se deberá observar los convenios Internacionales y los aspectos citados anteriormente.

CAPITULO III

PROTECCION DE DATOS Y SEGURIDAD

3.1.- BARRERAS DE PROTECCION

Estas palabras provienen de la industria del automóvil. En los automóviles modernos, existe una barrera entre el motor y el habitáculo de los pasajeros que evita la extensión de un incendio hacia zonas vulnerables.

En la industria informática, una barrera de protección lleva a cabo una función similar separando componentes vulnerables, se sitúa entre la red y el servidor de la Internet, o entre el servidor de la red y las estaciones de trabajo (barrera Intranet), está compuesta por software (sistemas) y hardware (equipos), subrayemos que la primera barrera de protección para Internet apareció en 1986 y que fue desarrollada por Digital Equipment

Una barrera de protección resulta de la combinación de hardware y software, y actúa como una guardia electrónica, la multinacional Amazon de conocido renombre posee un servidor Web con mucho tráfico, así como una red que es central a sus operaciones, su sistema esta compuesto por varios servidores que de esta forma comprueban qué y quién está intentando entrar y salir de la red, tomando nota de cada conexión y, hallando el punto de origen.

Este es un ejemplo extremo de una barrera de protección, no obstante, demuestra el tipo de seguridad que puede llegar a construirse alrededor de un sistema, cuando una empresa depende de ello, de seguridad y confianza.

Una barrera de protección hace mucho más que proteger simplemente la red de posibles intrusos, puede además proporcionar también información vital sobre la actividad del sistema, entre sus prestaciones tenemos:

- Controlar el acceso a los sistemas de las redes privadas.
- Poner la gestión de la seguridad en manos de unos pocos.
- Aumentar el nivel de privacidad ocultando las direcciones de los usuarios individuales de la red.
- Realizar un seguimiento del tráfico por razones de auditoria, de envío de factura, y por seguridad
- Informar de sucesos sospechosos.
- Trabajar con comprobadores de virus e Intranet, así como con la Internet.

Principales limitaciones de las barreras de protección:

- Es muy celosamente protectora, impidiendo el acceso a algunos servicios deseables para la empresa.
- No previene problemas en el interior de la red.
- Provoca cuellos de botella debido a un alto volumen de tráfico o utilizando programas anti-virus.
- Si existe un punto que falle entre las barreras de protección, nada podrá entrar ni salir.

Todas las barreras ofrecen un nivel de protección considerable contra posibles intrusiones de piratas informáticos, sin embargo nadie puede garantizar un 100% de seguridad, esto depende mucho del software y hardware utilizado.

Debe realizarse un seguimiento de las barreras de protección, comprobándose los históricos de los ordenadores y llevando a cabo modificaciones en la línea con las recomendaciones de los fabricantes. Una barrera de protección necesita personal con experiencia para poder ser bien gestionada.

Por sí solas las barreras de protección no pueden detener virus que puedan haber incrustado en mensajes de correo electrónico, pero existe productos (software) en el mercado que pueden comprobar la existencia de virus en los mensajes que entran.

Pese a ello, si la puerta de entrada maneja un gran número de mensajes de correo electrónico, se crearán retrasos inaceptables como consecuencia de la exhaustiva comprobación de virus, como sucede con todos los temas de seguridad, la decisión siempre resultará de un compromiso entre el coste, el riesgo y las necesidades empresariales.

Las barreras de protección son rutinas que se incorporan al software del computador, que permiten facilitar la información y garantizar la integridad de la misma; si bien no al 100%, se puede tener un alto grado de confiabilidad, dependiendo de la eficiencia y lógicamente que se refleje en sus costos.

En el Boletín del Criptomomición N.51⁵⁵ Se publicó una encuesta sobre las barreras al comercio electrónico, la misma que tenía como objetivo analizar cuáles eran los mayores factores que actúan de freno a la expansión de la actividad comercial en Internet.

⁵⁵ ITAA (Information Technology Association of America) y Ernst & Young, 09/06/1999

“De acuerdo con los resultados obtenidos, la barrera más importante es, la falta de confianza (señalada por el 62% de los encuestados), esta desconfianza hacia las nuevas tecnologías se articula en torno a tres temores fundamentales:

La privacidad (60%), los usuarios finales sienten amenazada en la medida en que desconocen hasta qué punto los datos personales que suministran a un servidor de comercio electrónico serán tratados de forma confidencial. ¿Quién le asegura al comprador que sus datos no se almacenarán a la ligera, siendo accesibles fácilmente por un hacker o un empleado desleal? ¿Cómo saber que no se revenden a terceros?

La autenticación (56%), que inquieta a los usuarios, quienes dudan de si la persona con la que se comunican es verdaderamente quien dice ser, cuando se entra en los locales físicos del Corte Inglés de la ciudad de New York uno se siente seguro de que no hay trampa; sin embargo, dada la relativa facilidad de falsificar una página Web e incluso un sitio Web completo, ¿cómo asegurarse de que se está comprando en el Corte Inglés virtual y no en una imitación fiel?

La seguridad global (56%), preocupa a los usuarios, pues temen que la tecnología no sea suficientemente eficiente para protegerles frente a ataques y apropiaciones indebidas de información confidencial, especialmente en lo que respecta a los medios de pago. Es interesante el hecho de que de toda la actividad de compra, lo que más sigue preocupando es la operación de pago, es decir, el momento en el que el comprador se enfrenta a la ventana donde ha introducido su número de tarjeta de crédito y duda a la hora de pulsar el botón de enviar ¿me timarán?, ¿seré víctima de un fraude?, se pregunta el usuario en el último momento.”⁵⁶

Estos temores, tienen su fundamento real y su solución no resulta trivial; en el primer caso, la tecnología, y en concreto la criptografía, ofrecen las herramientas necesarias para la protección férrea de la información almacenada en las bases de datos corporativas, información como listas de

⁵⁶ ALVAREZ, Marañón Gonzalo. Barreras al Comercio Electrónico Instituto de Seguridad de Internet 2001-2003 extraído el 23 /03/2006 de ITAA (Information Technology Association of America) y Ernst & Young, 09/06/1999 <http://www.instisec.com/publico/verarticulo.asp/?id=47>

clientes, sus datos personales y de pago, listas de pedidos, etc.; existen muchas técnicas de control de acceso que hábilmente implantadas garantizan el acceso a la información confidencial exclusivamente a aquellos usuarios autorizados para ello, se han producido incidentes de servidores de comercio que almacenaron esta clase de información sensible, en ficheros accesibles vía Web por cualquier navegante, por lo tanto, aunque la tecnología provee de medios aptos, depende en última instancia del comerciante, el nivel de compromiso que adopte respecto a la seguridad de los datos que conserva en sus ficheros y su política de control de acceso.

Este es un temor presente y sin fácil respuesta. La tecnología nada tiene que decir si un comerciante decide vender su información a terceros, la delgada línea que protege la privacidad del usuario está constituida en este caso por la integridad moral del comerciante, en estas circunstancias, es mejor asegurarse antes con quién se va a comercializar.

En el segundo caso, la solución inmediata que ofrece la criptografía viene de la mano de los certificados digitales, la tecnología de certificación está suficientemente madura como para autenticar adecuadamente a las partes involucradas en una transacción; la más comúnmente utilizada es SSL⁵⁷ y a pesar de la limitación criptográfica de claves débiles de 40 bits, a la hora de autenticar a las partes, principalmente al servidor, SSL funciona satisfactoriamente, otro asunto es si asegura o no la confidencialidad, cuestión más que dudosa, si se tiene en cuenta que una clave de 40 bits se rompe en cuestión de horas, con lo que los datos por ella protegidos quedan al descubierto rápidamente; otras tecnologías emergentes, como SET⁵⁸, ofrece mayor confianza en este campo y da solución al primer problema de la privacidad. SET permite autenticar a las partes involucradas en la transacción

⁵⁷ SSL.- Secure Sockets Layer

⁵⁸ SET.- Secure Electronic Transaction

de manera completamente segura, sin restricciones criptográficas debidas a absurdas leyes de exportación, su mecanismo de firma dual garantiza además que el comerciante no conozca los datos de pago (número de tarjeta de crédito), eliminando así la posibilidad de fraude por su parte. SET garantiza así que: el comerciante cobre por la venta y que el comprador no sea estafado por el comerciante ni por un hacker.

En cuanto al tercer temor, nuevamente la criptografía moderna y los productos de seguridad proporcionan las soluciones a los problemas; otra cuestión es: ¿incorporan los servidores de comercio todas las medidas necesarias para asegurar las transacciones con el usuario? en otras palabras, la tecnología está sobre el tapete y ofrece solución tecnológica a los retos que se le presentan a la seguridad en el comercio electrónico, pero ¿se usa correctamente? o ¿simplemente no se usa?

Por lo que parece, las verdaderas barreras al comercio electrónico no son tanto tecnológicas como humanas, una vez más, el eslabón más débil de la cadena es de índole personal, no tecnológicos.

Los proveedores de los servicios de Internet ofrecen entre sus paquetes promocionales este tipo de barreras; encaminados principalmente a filtrar información como son pornografía, pasquines span y programas con virus, entre otros.

Las barreras de protección, también nos permiten proteger nuestros servicios y sistemas de los llamados “Comisión de Delitos por Medios Informáticos”, así tenemos lo ocurrido en Instituto de Seguridad Social (IESS), el Banco de Pichincha, a quienes los han obligado a rediseñar sus sistemas e incluir nuevos controles de carácter técnico o llamados barreras de protección, que por falta de seguridad sufrieron serios problemas principalmente de carácter financiero y

que por falta de auditorias no lograron determinar responsables; las dos Instituciones citadas han conseguido incluir en sus sistemas barreras de protección propias como en el caso del IESS, donde fue necesario rediseñar los módulos de ingresos de usuarios y administradores y otorgar nuevas claves a sus usuarios; de igual forma en el Banco de Pichincha donde se incluyó el sistema e-key Max Security⁵⁹, esto ha permitido mejorar los niveles de confianza para realizar transacciones financieras y comercio electrónico.

El Ecuador cuenta entre la tecnología importada con software y hardware de diferentes tipos de barreras de protección, sus cometidos son esencialmente los mismos: detienen cada llamada, la vetan y la dejan pasar sólo si cumple con requisitos preestablecidos, pero como sucede con todo, según se pague, así será la calidad del producto; entre los que encontramos en el mercado podemos citar los siguientes:

Firewall.- Componente diseñado para prevenir accesos desautorizados a una red, actúan como un puente de seguridad entre las redes internas y externas.

IDS e IPS.- Censor de intrusos, toman acciones de prevención (IDS Intrusion Detection System), (IPS Intrusion Prevention System).

Antivirus.- Protección de software.

Filtros URL.- Permite filtrar la información antes de ingresar a la red.

Spyware.- Software pirata.

⁵⁹ E-Key Max Security.- Llave de máxima seguridad

Software de Encriptación.- Permite encriptar la información Ej. Formato HTTPS⁶⁰.

3.2.- SEGURIDAD DEL CIBERESPACIO

Existen numerosas barreras para la aceptación generalizada del comercio electrónico en el mundo de hoy, muchas de las grandes ventajas como transacciones en la banca y las compras en el ciberespacio representan también obstáculos potenciales que son necesarias superar.

En primer lugar, el reciente aumento del uso de la Red de Internet ha dirigido la atención del mundo entero a un problema crucial, la privacidad, hasta el momento, no ha existido una protección real que garantice que los mensajes que se envía o recibe no sean interceptados, leídos o incluso alterados por algún desconocido, ya que nadie en realidad dirige o controla la red de Internet.

En segundo lugar, en el mundo del ciberespacio el potencial para que exista el fraude y la estafa es mucho mayor, la capacidad de tener acceso a información las 24 horas del día, desde cualquier lugar del mundo, es para muchos un beneficio que brinda la red Internet, sin embargo, esto plantea algunos inconvenientes prácticos como los llamados phising (pinchazos) entre otros.

El espectacular despliegue que se está produciendo en Internet en los últimos años, permite pensar en prometedoras expectativas de utilización como vehículo de comercio, ya que el acceso de millones de usuarios en todo el mundo hace de la red el mejor mercado global en el que se pueda comerciar; piense simplemente en la posibilidad de ofrecer un producto o servicio que sea

⁶⁰ HTTPS.- Formato de página encriptada

comprado en los cinco continentes, los beneficios serían muy grandes en comparación con otros sectores de área limitada, lo único necesario e imprescindible sería un buen servicio de pos-venta (transporte capaz de llegar a donde el cliente quiera, servicio de mantenimiento, apoyo, etc.) y una gran seguridad en el medio del pago.

Por tanto la capacidad de ejecutar transacciones comerciales de compra-venta debe llevar asociada la capacidad de ejecutar los pagos correspondientes. Internet introduce en el escenario clásico de la ejecución de pagos la novedad de la distancia física e incluso cultural y legal entre las partes, ello introduce también posibilidades de fraude, engaño o simplemente errores y malentendidos, simultáneamente el nivel tecnológico al que acceden compradores y vendedores es tal, que parece natural exigir una mejor calidad en el servicio, antes que una degradación por intensificación de los problemas tradicionales.

Uno de los mecanismos clásicos de defensa contra transacciones comerciales fraudulentas ha consistido en la incapacidad de las partes para ejecutar enormes volúmenes de micro-transacciones, o se ejecuta una transacción de gran volumen, que automáticamente levanta todas las alarmas y cautelas, o el tiempo necesario para ejecutar multitud de pequeñas transacciones permite su tranquila detección y seguimiento.

El Internet ofrece acceso hiper - diversificado, una aldea global de compradores y vendedores, en ella se puede hablar de economías de escala capaces de rentabilizar una fuerte inversión con bajos costes por la vía del uso masivo, esto implica la necesidad de mecanismos ampliamente aceptados y fácilmente accesibles, esta amplia difusión de las técnicas, supone su exposición a malhechores cuyo beneficio obtenible del abuso de los mecanismos de pago, puede ser tan grande que es necesario realizar fuertes inversiones buscando resquicios de seguridad que puedan garantizar las

operaciones de los usuarios de la red, inversiones que prometen una alta rentabilidad pese a su elevado riesgo.

Todo sistema de pago que se precie deberá reunir las siguientes propiedades:

a) Confidencialidad: característica esencial para cualquier transacción económica en la que su conocimiento se limite a las partes intervinientes. Si hay un cliente, un comercio y un banco involucrados en la transacción, es conveniente que nadie a excepción de los tres supiera nada, el banco no conociera el detalle del pedido, el comercio no conociera los datos de la cuenta del cliente y el cliente no conociera los datos de la cuenta del comercio.

b) Anonimato: El papel moneda no tiene nombre, ni apellidos; pero las transacciones sobre redes telemáticas tienen una fuerte tendencia a dejar rastro. Limitar el anonimato del comprador puede suponer una fuerte restricción que inhiba adquisiciones, el anonimato esta compuesto de dos componentes: uno el inmediato, de que no se sepa que se adquiere tal cosa y otro a medio plazo como es el que no se pueda identificar patrones de compra, es decir el comportamiento de los usuarios respecto a sus transacciones cotidianas.

c) Integridad: Es la incapacidad de terceras partes para modificar el contenido de un intercambio de datos, sean los detalles de un pedido, el monto de un pago, la identificación de una cuenta bancaria, etc. Se trata de un mecanismo básico frente a fraudes introducidos por terceras partes o por las mismas partes que ven el imposible cumplimiento del negocio.

d) Autenticación del remitente: Salvo que el pago se haga con un valor indiscutible (por ejemplo en efectivo) en todos los demás casos el pagador debe identificarse claramente, de forma que sea posible pedir cuentas si el pago no llega a materializarse.

e) Autenticación del receptor: Igualmente, los compradores deben conocer la identidad del vendedor, salvo que el producto o servicio se libere en el mismo instante en que se hace la transacción.

f) Irrenunciabilidad (es decir no repudiable): La autenticación debe ir asociada a una cierta permanencia temporal que impida que una de las partes decline su responsabilidad. Aquí generalmente aparece un tercero que da fe de la identidad y de los deseos de una o de ambas partes a tal fecha, se trata del notario electrónico o podría una tercera persona realizar dicha tarea de dar fe pública de que los mensajes de datos son auténticos y que tanto el cobrador como el vendedor son quienes dicen ser.

Con todas estas características habría que diseñar escenarios comerciales coherentes capaces al menos de reproducir la mayor parte de ellas sino todas, pues para que el comercio electrónico se desarrolle más en Internet depende en gran parte de que exista confianza en las transacciones electrónicas por parte tanto del vendedor como del cliente.

De esta forma se tiene como uno de los pilares básicos del comercio electrónico la seguridad. Los usuarios de las tecnologías de la Información y Comunicación (TIC), deben: saber que su información está protegida, poder verificar a quién realmente la están transmitiendo, saber quién la está recibiendo, y que no haya sufrido modificaciones no autorizadas.

Las nuevas tecnologías que hacen posible la sociedad de la información tienen un denominador común: La información es tratada digitalmente, esto es, codificada en sistema binario (unos y ceros), el fax, el correo electrónico, el vídeo, la televisión, la telefonía móvil, el intercambio electrónico de documentos (EDI), la transferencia electrónica de fondos (EFT), las tarjetas inteligentes, el teletrabajo, la telemedicina etc., todo ello funciona con la información codificada en bits y transmitidos a través de cable, fibra óptica, radios por telefonía móvil,

retransmitidos por nodos terrestres o por satélites y almacenados en medios magnéticos u ópticos.

Sin embargo los bits tienen una gran vulnerabilidad, son accesibles fácilmente, la codificación en bits no aporta ningún impedimento para el conocimiento de la información que representan, no son seguros y no tiene personalidad, todos son iguales. La modificación, sustitución, borrado o destrucción de cualquiera de ellos puede modificar total o parcialmente, el origen, el destino, o el contenido de la información que representan, de esta forma para evitar o protegerse de los errores que pudiera provocar el canal de comunicaciones por donde transitan los bits, se emplean las técnicas de detección y corrección de errores, dichas técnicas son estándares de las telecomunicaciones digitales, perfectamente conocidas e implementadas por los fabricantes, operadores y usuarios de las "TIC's".

Para dar mayor confianza al comercio electrónico se han desarrollado los certificados digitales, que son aquellos que representan el punto más importante en las transacciones electrónicas seguras, éstos brindan una forma conveniente y fácil de asegurar que los participantes en una transacción comercial electrónica puedan confiar el uno en el otro, esta confianza se establece a través de un tercero, por ejemplo Visa, suministrará certificados digitales a las instituciones financieras emisoras de tarjetas, y cada institución, a su vez, ofrecerá un certificado digital al tarjeta habiente, el proceso será similar en el caso de los comercios.

El estándar "SET" (Secure Electronic Transaction), se perfila como una respuesta a todas estas consideraciones. SET hace que las compras a través de la Red Internet sean tan convenientes y seguras como al usar su tarjeta de crédito en un centro comercial local.

En el momento en que se efectúa la transacción, el software que cumple las normas de SET de cada entidad participante en la transacción, verifica y confirma la identidad del comerciante y del tarjeta habiente antes de que se intercambie ningún tipo de información, esta confirmación se realiza revisando los certificados digitales emitidos por una tercera parte autorizada y confiable.

Los certificados digitales en pocas palabras, garantizan que dos computadoras que se comunican entre sí puedan efectuar transacciones de comercio electrónico con éxito, la base de esta tecnología reside en los códigos secretos; aunque podría parecer algo que sólo ocurre en una novela de espionaje, lo cierto es que el comercio electrónico se apoyará firmemente en la criptografía, es decir, en el arte de utilizar los códigos secretos.

El Ecuador, no cuenta con instituciones o empresas que pueda ofrecer este servicio, no hay un tercero que nos permita realizar una transacción segura y es una de las causas por las cuales el comercio electrónico no se ha desarrollado a la velocidad que se esperaba; la criptografía para nuestros desarrolladores de software es desconocido, de igual forma, no hay empresa en el país dedicada al desarrollo de estos sistemas; pero si existe en el mercado software importado que permite encriptar la información; como ejemplo de esto tenemos: SecureDoc (software de encriptación) y la empresa proveedora o distribuidora es Win Magic, otro es Safeboot sin representación en el país pero de procedencia americana; son software de encriptación comercializados por el número de archivos a encriptar o el número de usuarios a utilizar estos sistemas.

3.3.- FIRMA ELECTRÓNICA

La firma electrónica o digital es un conjunto de datos electrónicos que identifican a una persona en concreto, suele unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se tratara, de esta forma el receptor del mensaje está seguro de quién ha sido el emisor.

La firma electrónica puede utilizarse en el sector privado o público, para contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo, la compra de un libro o un compacto por Internet) y entre empresas (por ejemplo, realizar un pedido a un distribuidor) o incluso entre los mismos consumidores finales (por ejemplo, venta de una raqueta de segunda mano, una colección de monedas etc.).

También sirve para realizar actuaciones con y entre la Administración, es decir, sirve tanto para las relaciones entre el usuario y los entes públicos (por ejemplo, la solicitud de prestaciones a la seguridad social o incluso la presentación de la declaración de la renta por Internet).

Funcionamiento de la firma electrónica

La firma electrónica funciona mediante la encriptación o cifrado de los datos que la componen, de forma que si no se tiene la clave, el documento se convierte en ilegible.

Para ello es necesario contar con un par de claves que son: la clave privada y la clave pública, que se corresponden de forma matemática. Un ejemplo de esto es, escribir un documento y firmarlo con nuestra clave privada y lo

enviamos a nuestro receptor al cual previamente le habremos otorgado nuestra clave pública, esta clave pública es la que permite verificar la procedencia del mensaje y que verdaderamente ha sido firmada por quien lo envía, que es el único poseedor de la clave privada.

Con esta encriptación se consigue que:

- La información enviada bajo la firma electrónica sólo pueda leer la persona autorizada que posea la clave.
- Acreditar la identidad de quien firma el documento electrónicamente.

“Existen dos tipos de firma electrónica: la básica y la avanzada.

La firma electrónica básica contiene un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio documento, pero este sistema tiene algunos problemas. ¿cómo saber que los datos enviados han sido creados por la persona que lo firma o que verdaderamente lo ha firmado él y no una tercera persona haciéndose pasar por él?

Para resolver este problema se crea la firma electrónica avanzada, a la que nuestro ordenamiento atribuye plena eficacia jurídica y valor probatorio en juicio.

Permite la identificación del emisor del mensaje ya que está vinculada de manera única al que firma el documento y a los datos que incorpora, debido a que es el signatario quien únicamente posee el control exclusivo de estas claves, además de que permite saber si estos datos han sido modificados posteriormente o en su transcurso de la emisión del mensaje.

Sin duda son figuras todavía desconocidas y complicadas para el uso y entendimiento de la población, no sólo porque son tratadas desde un punto de vista excesivamente técnico, sino por la propia ambigüedad que produce la lectura de las definiciones que ofrece la regulación actual.”⁶¹

⁶¹ RUBIO V, Rodríguez Muñoz. Aspectos Legales y Técnicos de la firma Electrónica. pp. (32-33). Ed. Experiencia 2005 Madrid.

“El problema fundamental que se plantea en la firma electrónica, desde los puntos de vista jurídico y comercial se puede resumir en cuatro grandes puntos, que han sido puestos de manifiesto por numerosos expertos en las materias: AUTENTICIDAD; INTEGRIDAD; CONFIDENCIALIDAD y NO REPUDIO, que fueron tratados en la seguridad del ciberespacio”⁶².

Podemos Adicionar a los puntos indicados, la Auditabilidad como requisito indispensable que permite identificar y rastrear las operaciones realizadas por el usuario, dentro de un sistema informático; cuyo acceso se realiza mediante la presentación de certificados, especialmente cuando se incorpora el estampillado de tiempo, que añade de forma totalmente fiable la fecha y hora a las acciones realizadas por el usuario, en el Ecuador se lo conoce como sellado de tiempo que no es mas que la verificación de que los mensajes de datos lleguen en forma oportuna.

El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada entre las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL (Secure Sockets Layer). La información contenida en las firmas digitales es completamente segura y fiable, y no es posible ningún tipo de falsificación o fraude en su verificación.

3.3.1.- CRIPTOGRAFIA

“La criptografía (del griego kryptos, "ocultar", y grafos, "escribir", literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

⁶² <http://es.wikipedia.org/wiki/Criptograf%C3%ADa>, Categoría: Criptografía extraído febrero 2006

Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con el objeto de recuperar la información original en ausencia de la clave.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (sean personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía sea auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.”⁶³

La criptografía necesita de una tercera parte de confianza (una entidad de certificación que debe realizar tal asociación vinculando dos personas debidamente identificadas con un par de claves), por ello, para asociar un par de claves con un potencial firmante, una entidad de certificación emite un certificado, un registro o documento electrónico que liga una clave pública con el sujeto del certificado, y confirma que el potencial firmante identificado en el certificado tiene la correspondiente clave privada

Un mensaje puede pasar por un proceso de conversión o de encriptación, que lo transforma en código usando una "clave", es decir, un medio de traducir los signos de un mensaje a otro sistema de signos cuya lectura no tenga ningún sentido para un desconocido que los intercepte, esto se conoce como el proceso de "encriptación" de un mensaje, un ejemplo sencillo de una clave

⁶³ Obtenido de "<http://es.wikipedia.org/wiki/Criptograf%C3%ADa>" Categoría: Criptografía extraído febrero 2006

puede ser el reemplazar cada letra con la próxima letra del alfabeto, así la palabra Visa se convertiría en WJTB, para descifrar el mensaje o revertir la encriptación, el que lo recibe necesita conocer la clave secreta.

Tipos de Criptografía

Existen dos tipos de criptografía de uso común, la más antigua y simple se la conoce como criptografía de "clave sencilla o de clave secreta" y criptografía de "clave pública":

Encriptación de Clave Secreta

En este tipo de encriptación la codificación o encriptación de clave secreta resulta útil en muchos casos, aunque tiene limitaciones significativas, todas las partes deben conocerse y confiar totalmente la una en la otra, cada una de ellas debe poseer una copia de la clave, una copia que haya sido protegida y mantenida fuera del alcance de los demás.

Por sí sola, este tipo de encriptación no es suficiente para desarrollar el pleno potencial del comercio electrónico, el cual debe vincular a un número ilimitado de compradores y vendedores de todas partes del mundo; de un lado, resulta poco práctico que una gran corporación intercambie claves con miles o incluso millones de clientes o, peor todavía, con posibles clientes con los que nunca ha tratado.

La encriptación de clave pública

En este tipo de encriptación la solución a la seguridad en toda red abierta es una forma de codificación más novedosa y sofisticada, desarrollada por los matemáticos de MIT (Mathematics Institut Tecnologic) en los años setenta, y conocida como "clave pública", en este tipo de enfoque, cada participante crea dos claves o "llaves únicas".

Por ejemplo, usted dispone de su propia "clave pública", que divulga en un tipo de directorio al que el público en general tiene acceso, y dispone además de su clave o "llave privada", que mantiene en secreto.

Las dos claves funcionan conjuntamente como un curioso dúo, cualquier tipo de datos o información que una de las claves "cierre", sólo podrá abrirse con la otra, de forma que, si usted desea enviar a un amigo un mensaje que no desea que ningún intruso lea, simplemente busca la clave pública de su amigo y la utiliza para realizar la encriptación del texto, cuando él lo recibe, utiliza su clave privada para revertir la encriptación del mensaje en la pantalla de su computadora y aparece el mensaje en forma de texto normal y corriente, si un extraño interceptara este mensaje, no podría descifrarlo porque no tendría la clave privada de su amigo.

Las claves consisten en una serie de contraseñas electrónicas guardadas en las unidades de disco de las computadoras personales, o transmitidas como datos a través de las líneas telefónicas siguiendo lo especificado en los estándares de la industria; el trabajo más difícil es el complejo proceso matemático de encriptación del texto y su opuesto lo realiza la computadora, usted no tiene que preocuparse de nada más.

Además, los bancos, los comercios y otros participantes en el nuevo mundo del comercio electrónico podrán ajustar las características más importantes del software para satisfacer las necesidades específicas de sus clientes, en este tipo de software se incluirá un nivel de código que se ajuste al nuevo estándar de la industria, este nivel emplea la encriptación de clave pública para asegurar que los mensajes que contengan números de tarjetas bancarias y otro tipo de información similar se mantengan en el más estricto carácter confidencial, este código también da lugar a otra revolución en el campo de las transacciones seguras en el ciberespacio que son las firmas digitales.

Cuando usted recibe un mensaje en el ciberespacio, ¿cómo sabe que lo envió su amigo Pedro y no un delincuente que se hace pasar por él? ¿y cómo sabe un comerciante si la orden que recibió es la suya o la de alguien que se propone estafarle una buena suma de dinero? lamentablemente, el potencial para este tipo de fraude se ha hecho más evidente en las redes abiertas.

El sistema de clave pública, sin embargo, puede resolver este problema en una forma sencilla pero eficaz; digamos, por ejemplo, que estoy comunicándome con mi banco en el ciberespacio y deseo probar mi identidad, sólo tengo que guardar un mensaje con mi clave privada, entonces el banco puede "abrir" el texto con mi clave pública, tomada de mi certificado digital, lo que prueba que soy la única persona que pudo haber cifrado ese mensaje en primer lugar.

Este proceso crea lo que los criptógrafos denominan la "firma digital". Una firma digital ofrece una forma de asociar el mensaje con la entidad que lo envía, y es la forma en la que usted puede "firmar" al efectuar una compra en el ciberespacio, de esta manera, sólo usted podrá utilizar su cuenta de tarjeta de crédito en la Red Internet.

Pero, para garantizar el cumplimiento de los puntos mencionados, se plantean las siguientes alternativas:

“Sistemas de Criptografía Simétrica.- Obliga a los interlocutores a utilizar la misma clave para encriptar y desencriptar el mensaje, técnica que fue desarrollada por IBM (sistema “DES”), pero que fracasó debido a su inseguridad en cuanto al secreto y confidencialidad de dicha clave, no obstante, este sistema, ha sido el más utilizado históricamente, dependiendo de la naturaleza de la aplicación utilizada tiene cuatro variantes para su implementación: EBC (Electronic Codebook Mode), para mensajes cortos de menos de 64 bits; CBC (Cipher Block Chaining Mode), para mensajes largos; CFB (Cipher Block Feedback) para cifrar bit por bit; y el OFB (Output Feedback Mode) análogo al CFB, pero permite evitar la propagación de errores.

La práctica se ha encargado de poner de manifiesto las carencias de estos sistemas para la transmisión de información de alta seguridad.

Sistemas de Criptografía Asimétrica.- consistente en la asignación de dos claves, una pública y otra privada, asociadas a un solo interlocutor. este sistema, parece el más adecuado, para el cumplimiento de los requisitos anteriores, y es el más utilizado en la práctica, bajo la denominación RSA, que se debe a las iniciales de sus creadores (Rivest, Shamir y Adelman), y que es el contemplado en el documento de la ISO (International Standard Organisation), 7498-2, de Julio de 1988, que señala la arquitectura de seguridad para proteger las comunicaciones de los usuarios de las redes. Se puede definir como “una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario”.⁶⁴

El éxito de este sistema se debe a que garantiza la seguridad y confidencialidad de las comunicaciones telemáticas, en otras palabras, hace que el contenido del mensaje sea irreversible, único e invariable, además facilita una perfecta identificación del remitente y destinatario; esta última función se realiza a través de los llamados “terceros de confianza”, que han sido denominados por algún sector de la doctrina especializada, como “Notarios Electrónicos”, estos son:

⁶⁴ RUBIO Víctor, Aspectos Legales y Técnicos de la F. E. pp. (177-187). Ed. Experiencia. Madrid 2005

Las autoridades de certificación (CA o certification authorities): que vinculan la clave pública a la entidad registrada proporcionando un servicio de identificación, una CA es a su vez identificada por otra CA creándose una jerarquía o árbol de confianza: dos entes pueden confiar mutuamente entre sí, si existe una autoridad común que directa o transitivamente las avala.

Autoridades de registro (RA o registration authorities): que ligan entes registrados a figuras jurídicas, extendiendo la accesibilidad de las CA autoridades de fechado digital (TSA o time stamping authorities): que se vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado (resolverían el problema de la exactitud temporal de los documentos electrónicos).

Estas autoridades pueden materializarse como entes individuales, o como una colección de servicios que presta una entidad multipropósito.

El modo de funcionamiento de la firma digital electrónica basado en clave pública es el siguiente:

- Cada participante tiene un par de claves, una se usa para encriptar y la otra para desencriptar.
- Cada participante mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública).
- El emisor calcula un resumen del mensaje a firmar con una función hash, (marcado o bloque) el resumen es un conjunto de datos de pequeño tamaño que tiene la propiedad de cambiar si se modifica el mensaje.

- El emisor encripta el resumen del mensaje con una clave privada y ésta es la firma digital que se añade al mensaje original.
- El receptor, al recibir el mensaje, calcula de nuevo su resumen mediante la función hash. Además desencripta la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó, si ambos resúmenes coinciden entonces la firma es válida por lo que cumple los criterios ya vistos de autenticidad e integridad además del no repudio ya que el emisor no puede negar haber enviado el mensaje que lleva su firma.

“La diferencia entre la firma electrónica y la firma digital es que: La firma electrónica es un género, caracterizado por el soporte: todo modo de identificación de auditoría basado en medios electrónicos es firma; luego vienen las especies, que en general, se caracterizan por agregar elementos de seguridad que la sola firma electrónica no posee, las legislaciones reconocen el género de la firma electrónica y luego eligen una especie que denominan “firma electrónica avanzada” o “firma digital”, que es la que utiliza un sistema, generalmente criptográfico, que da seguridad. La gran diferencia estriba en que cuando se utiliza la firma digital se aplican presunciones iuris tantum sobre la identidad del firmante y la integridad del documento que firmó.”⁶⁵

3.4.- CERTIFICACION DE INFORMACION

Para poder tener la certeza de que la Información es segura, es necesaria una infraestructura de clave pública (PKI) para cerrar el círculo de confianza, proporcionando una asociación fehaciente del conocimiento de la clave pública a una entidad jurídica, que le permite la verificación del mensaje y su imputación a una determinada persona.

⁶⁵ GRECO, Marco Aurelio, “Internet en directo”, segunda edición, Dialéctica, San Pablo, 2000

Esto quiere decir que el certificado es un documento electrónico que contiene un conjunto de información que vincula una clave pública con una persona o entidad determinada.

Consecuentemente, el sistema de certificados de clave pública supone la participación de los siguientes sujetos:

- a) el titular del certificado;
- b) el usuario o persona que confía en el certificado, y;
- c) la entidad de certificación;

El titular del certificado, también llamado sujeto o suscriptor, es la persona o entidad incluida en el certificado, que tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado.

La relación del titular del certificado con la entidad de certificación puede ser de dos tipos, según responda a una comunidad cerrada (en que exista alguna vinculación entre la entidad certificadora y los suscriptores) o abierta (en que la entidad certificadora es independiente de los suscriptores).

El usuario del certificado es la persona que obtiene la clave pública del suscriptor a través del certificado y actúa basándose en él y en la clave pública que contiene.

Las entidades de certificación son empresas unipersonales o personales que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica deben estar debidamente autorizados por el Consejo Nacional de Telecomunicaciones, para el caso del Ecuador; sin embargo se debe indicar que estas empresas no funcionan actualmente en el país por falta de aprobación.

Es necesario disponer de empresas que tengan sistemas técnicamente confiables para prestar los servicios tanto en el uso de software como de

hardware, mantener sistemas de resguardo y respaldo de la información, utilizar herramientas de firma electrónica que estén protegidas contra la modificación de las mismas, de tal forma que no puedan realizar funciones distintas a aquellas para las que han sido diseñadas, deben utilizar productos de firma electrónica que bajo estándares internacionales garanticen la seguridad técnica y criptográfica de los procesos de certificación soportados por los productos.

“Las empresas certificadoras deberán adoptar medidas para evitar la falsificación de certificados, Almacenar toda la información por un periodo considerable, (mínimo de 10 años), especialmente a efectos de prueba en procedimientos judiciales, el almacenamiento podrá ser realizado en medios electrónicos, deberá, garantizar la integridad, intimidad y confidencialidad de la información y proteger la información frente a terceros.

Otra de las actividades que deben realizar estas empresas, es: emitir certificados en relación con las firmas digitales de personas naturales o jurídicas; emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos; emitir certificados en relación con la persona que posea un derecho u obligación con respecto a cualquier documento; ofrecer o facilitar los servicios de creación de firmas digitales certificadas; ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos y archivo y conservación de mensajes de datos.

Los Proveedores de Servicios de Certificación en el archivo, uso y manejo de datos obtenidos en función de su trabajo, deben garantizar la privacidad, protección y confidencialidad de la información y datos que manejen; brindar información únicamente con el consentimiento y voluntad de la persona relacionada con dicha información y consecuentemente la no divulgación de la información obtenida por cualquier medio, protegiendo frente a terceros

Responsabilidades de los proveedores de servicios de certificación adicional a las impuestas por la Ley, el proveedor de servicio debe ser responsable por: adoptar las medidas necesarias para determinar la identidad del titular de la firma y la exactitud de sus certificaciones; almacenar y garantizar la seguridad de las claves criptográficas de firmas electrónicas que se le solicitara expresamente; el funcionamiento entre la clave pública y privada de acuerdo con el certificado expedido; proporcionar a los titulares de firmas un medio para dar aviso de que

una firma electrónica tiene riesgo de uso indebido, en cuyo caso el titular podrá solicitar la suspensión de la firma electrónica; además deberán mantener y publicar oportunamente un listado de las firmas suspendidas, canceladas o revocadas.

En el ciclo vital del certificado, se reconoce tres aspectos principales: la generación y emisión, la distribución y la vigencia del mismo⁶⁶

Para el caso de nuestro país la regulación del CONATEL prevé estos aspectos:

En primer lugar, en cuanto a la generación emisión del certificado, cabe distinguir las siguientes fases:

- a) solicitud y registro del solicitante;
- b) comprobación de la solicitud;
- c) emisión del certificado;
- d) envío de copia al solicitante y, en su caso, aceptación por éste; y;
- e) publicación y archivo del certificado.

En segundo lugar, por lo que refiere a la distribución del certificado, ésta se verifica a través de una serie de sistemas tendientes a posibilitar la verificación de una firma digital de una parte lejana o a cifrar datos de una persona destinados a una parte lejana, mediante la comunicación de la clave pública correspondiente.

En tercer lugar, la cuestión de la vigencia del certificado se relaciona con el hecho de que el certificado, como instrumento de distribución segura de claves públicas, no puede tener una validez indefinida, sin perjuicio de la eventual

⁶⁶ MARTINEZ NADAL Apolonia (2003). "Comercio Electrónico, Firma Digital y Autoridades de Certificación" cit., Pág. 149-150 Madrid

revocación anticipada o suspensión del mismo si mediaren razones que así lo impusieren.

En los métodos asimétricos, cada entidad sólo ha de poseer un par de claves (privada y pública) independientemente del número de sistemas con los que se comunique, el único requisito que se ha de cumplir es la integridad de la clave, para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo, entonces se recurre a lo que se denominan los certificados de clave pública, que son emitidos por las entidades de confianza llamadas Autoridades Certificadoras (CAs, Certification Authorities) que garantizan que una determinada clave pública pertenece a su verdadero poseedor.

Estas entidades permiten garantizar los servicios de confidencialidad e integridad de los datos y el no repudio de origen y destino.

Una arquitectura de gestión de certificados (Public Key Infrastructure) ha de proporcionar un conjunto de mecanismos para que la autenticación de emisores y recipientes sea simple, automática y uniforme, independientemente de las políticas de certificación empleadas.

Las CAs tienen como misión la gestión de los denominados certificados (de clave pública). Un certificado está compuesto básicamente por la identidad de un usuario (subject), su clave pública, la identidad y la clave pública de la CA emisora (issuer) del certificado en cuestión, su periodo de validez y la firma digital del propio certificado, esta firma, realizada por la CA emisora, permite que aquellas entidades que deseen realizar comunicaciones con la persona poseedora del certificado, puedan comprobar que la información que éste contiene es auténtica (suponiendo que confíen en la CA emisora), una vez que los certificados han sido firmados, se pueden almacenar en servidores de directorios o transmitidos por cualquier medio (seguro o no) para que estén disponibles públicamente.

Antes de enviar un mensaje encriptado mediante un método asimétrico, el emisor ha de obtener y verificar los certificados de los receptores de dicho mensaje, la validación de un certificado se realiza verificando la firma digital en él incluida mediante el empleo de la clave pública de su signatario, que a su vez ha de ser validada usando el certificado correspondiente, y así sucesivamente hasta llegar a la raíz de la jerarquía de certificación.

“Los usuarios pueden chequear la autenticidad de las claves públicas de otros usuarios verificando la firma de la CA en el certificado usando la clave pública del CA.

En el proceso de verificación se ha de comprobar el periodo de validez de cada certificado y que ninguno de los certificados de la cadena haya sido revocado.”⁶⁷

En resumen el contenido mínimo que deben tener los Certificados de Información son:

Emisor:

- Identificación y su domicilio

Firmante:

- Personas físicas: nombre, apellido y DNI (o seudónimo)
- Personas jurídicas: denominación o razón social y CIF (en estos casos se incluirá la identificación del solicitante persona física)

Optativo:

- Cualquier otra circunstancia o atributo del firmante (en caso de que solicite que así conste)

Relaciones de representación:

- Identificación del documento público autorizante

⁶⁷ www.monografias.com.Campitelli Adrián, Rosso César Luis extraído 03 de enero del 2003

- Datos de inscripción en Registro Público correspondiente (de ser preceptiva dicha inscripción)

Técnicos:

- Expresión de que el certificado es reconocido
- Código identificativo único del certificado
- Datos de la clave pública de la firma del firmante (asociados a la clave privada bajo su control)
- Firma Electrónica avanzada del prestador que emite

Validez límites:

- Comienzo y fin del período de posible utilización
- Generales de uso (en caso de existir)
- Total del valor de las transacciones (en caso de existir)

3.5.- CONFIDENCIALIDAD Y RESERVA

“La mayoría de los mensajes enviados en las transacciones electrónicas se producen utilizando conocidas herramientas de proceso de textos, bases de datos, paquetes gráficos etc. Por lo tanto utilizan formatos muy extendidos y conocidos. La información es relativamente fácil de interceptar con conocimientos muy básicos.

De acuerdo con los recientes estudios del Computer Security Institute (CSI), el robo de datos representa una de las mayores causas de daños económicos en las empresas. Nunca los datos han sido tan accesibles y las herramientas utilizadas para evitar las diferentes medidas de protección tan sofisticadas.

Cualquier ordenador de la red puede de forma sencilla visualizar el tráfico que va por ella, recuperando datos de usuario, password...etc.

Los correos electrónicos se han convertido en una herramienta imprescindible para la realización de nuestras tareas. El correo electrónico es una herramienta muy vulnerable ya que los mensajes se envían y se almacenan en un formato de texto básico. Una simple herramienta de inspección de red puede conocer el texto enviado. Mediante el acceso a un servidor de correo un usuario con permisos

*suficientes puede conocer el contenido de los mensajes sin que el receptor o el emisor puedan conocer que se ha producido dicha acción.*⁶⁸

Renato Jijena Leiva Abogado, académico consultor de empresas, y conocido jurista Chileno y especialista en Nuevas Tecnologías, Derecho Informático, y Comercio Electrónico dice:

“Una de las muestras más cotidianas de lo que ha sido la penetración en las sociedades actuales de las nuevas tecnologías y en especial de la red Internet es el uso cada vez más masivo de los denominados "e-mails" o correos electrónicos y estos son cada vez más interactivos, personales e intuitivos, sobre todo cuando se trata de los llamados "spam".

Juristas y parlamentarios se están preguntado si en materia de correos o mensajes electrónicos enviados a través de redes abiertas como Internet cabe invocar a su respecto la garantía de la inviolabilidad de la correspondencia y de toda forma de comunicación privada que se consagra en la mayoría Constituciones Políticas de los países

Con algunos sectores del debate jurídico sobre la calidad de confidencial, reservado o privado de un correo electrónico y de las casillas que los almacenan pasa exactamente igual, es una afirmación ligera homologar con simpleza el mundo del correo normal y tradicional con el de los correos electrónicos, el correo electrónico no es -de manera alguna- un instrumento similar al de un correo normal, y la diferencia no radica sólo en que cada persona posee una casilla postal de carácter electrónica denominada “casilla electrónica”.

Entonces, para reivindicar la confidencialidad o reserva el argumento central es el de asimilar los e-mails al correo tradicional argumentando que la norma no distingue si " la correspondencia inviolable" o "la comunicación privada" se realiza específicamente de alguna forma o mediante algún soporte

⁶⁸ Idem (Pag. 174)

determinado, consecuentemente se reivindica a su respecto su inviolabilidad de manera categórica, intransable e irrenunciable, afirmándose que cualquier forma de interferencia de un correo electrónico violaría una garantía constitucional y sería constitutiva de un ilícito penal.

Se estima que es equivocado y que se requiere -previamente- una distinción elemental de cara a la naturaleza física o técnica de lo que es un correo electrónico y, en segundo lugar, en consideración a si concurre o no el elemento "encriptación".

¿Porqué todos los correos pueden ser revisados por el administrador de una red o de un servidor? ¿ Porque enviados por Internet están en una red esencialmente "abierta", técnicamente los e-mails son verdaderas tarjetas postales que cualquiera podría tomar y leer ¿y acaso podría alegarse vulnerada la inviolabilidad de la correspondencia o de una forma de comunicación privada cuando la gente del servicio de correos y el cartero toman, miran, observan y leen el contenido de una tarjeta postal soportada en cartulina?. Se piensa que no.

Hay que considerar y entender la realidad fáctica antes de aplicar principios y normas jurídicas, el análisis no puede desconocer la naturaleza y características de los correos electrónicos, que son el equivalente de las "tarjetas postales", esto es, que circulan por las redes en forma abierta y cualquier administrador de un servidor de correos puede visualizarlo sin realizar ninguna operación clandestina, de espionaje, de intrusión o de "pinchazo".

No se trata por ende, de una forma de "comunicación privada" a cuyo respecto pueda exigirse inviolabilidad por parte de un receptor involuntario o distinto del que indicó el emisor, o por parte del que contractualmente provee los equipos o sistemas de casillas de almacenamiento de correos para la comunicación, los que nada necesitan abrir, violar o "pinchar" clandestinamente.

Si un usuario quisiera agregar confidencialidad o reserva a sus correos, simplemente debe utilizar mecanismos de encriptación o codificación para hacerlo, es la conducta equivalente a cerrar el sobre que mandaremos por la oficina de correos, sólo en la medida que un tercero distinto al emisor y al receptor de un mensaje que están habilitados técnicamente para entender o conocer el contenido del documento codificado- rompa o vulnere la encriptación de un e-mail protegido técnicamente, encriptado o codificado, podría hablarse de que se ha vulnerado la garantía constitucional aludida, porque ese correo claramente constituía una correspondencia inviolable y una forma de comunicación privada, reservada o confidencial.

*La fórmula que concilia y que evita las posturas dogmáticas y alejadas de la realidad tecnológica es la de atender a un elemento también técnico que permite resguardar los contenidos privados o íntimos y que transforma a las comunicaciones, a los correos electrónicos y a la correspondencia en "efectiva y técnicamente privadas", esto es, la encriptación.*⁶⁹

Por último, la propia Ley que pretende proteger los mensajes de datos, establece estos principios.⁷⁰

⁶⁹ <http://www.ecampus.cl/Textos/derecho/jijena/1/jijena1.htm> Renato Jijena Leiva extraído el 29/03/2006

⁷⁰ La Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, en el Art. 5.- dice: “Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.”

CAPITULO IV

PROPUESTA, CONCLUSIONES Y RECOMENDACIONES

4.1.- PROPUESTA

El desarrollo del Comercio Electrónico da la oportunidad para que el mercado se desarrolle en un espacio abierto donde el intercambio comercial, de bienes y servicios, se hace a través de las autopistas de la información (Internet) con miles de interconexiones en todo el mundo.

La presente tesis esta basada en la determinación de principios y factores administrativos, técnicos y jurídicos que permitan dar seguridad al proceso

transaccional en el comercio electrónico, que tanto el cliente como el proveedor requieren; estos principios que ya fueron tratados en el capítulo I, son:

- Autenticidad
- Integridad
- Confidencialidad; y,
- No repudio.

La propuesta da énfasis al cumplimiento de estos principios, e incluye a manera de ensayo la forma como se debe crear una empresa virtual, considerando los factores administrativos, técnicos y jurídicos para dar seguridad a las transacciones realizadas a través del comercio electrónico, desde el punto de vista del vendedor como del comprador.

4.1.1.- ELEMENTOS INDISPENSABLES PARA LA CREACION DE UNA EMPRESA VIRTUAL O INSERCIÓN DE LA EMPRESA EN EL COMERCIO ELECTRONICO

Constitución de la empresa.-

La creación de una empresa virtual no escapa a las formalidades que por ley regula la Superintendencia de Compañías, como: constitución, razón social, objeto, capital social, afiliación a la cámara correspondiente, registro y control del Servicio de Rentas Internas.

Inserción en el Comercio Electrónico.-

Una vez que ha decidido ingresar al mundo del comercio electrónico, la primera decisión que se debe tomar, es cual será el motor de base de datos, Ej. Oracle, SQL, u otra base que permita trabajar con un sitio Web; también es necesario determinar el desarrollador del sistema para extraer o explotar los datos recopilados, estos pueden ser Visual Basic, JAVA, Visual Fox etc. de tal manera que permitan operar su cyber tienda. Es recomendable decidir esto antes de empezar el diseño gráfico del sitio, pues a menudo el motor determina en cierta medida la estructura tecnológica de la tienda.

Pasos a seguir.-

Contratación del proveedor del servicio.

Los proveedores de servicios ISP⁷¹, son las empresas que facilitan la conexión hacia el ciberespacio.

El servidor es el ordenador que contiene toda la información de la página Web y se debe decidir si se quiere contar con un servicio propio o ajeno. Si la decisión es alojarlo en la empresa (hosting propio) se debe considerar la contratación de personal técnico capacitado para mantenerlo. Si se alquila el alojamiento o hosting, es importante un buen servicio técnico y acceso a la red.

⁷¹ Internet Service Provider

Sistema de comunicación.-

Esta puede ser telefónica o de banda ancha, si prevemos miles de conexiones debemos contar con un gran ancho de banda para cubrir esta necesidad y agilizar el proceso de conexión.

Contratación del dominio.-

En Internet el ámbito al que pertenece la empresa tiene una identificación o dominio⁷² tener nombre significa tener dominio. Existen dominios para todo el mundo por ejemplo: com para los comercios; .org para las organizaciones; .net para las empresas relacionadas con Internet, .edu para las universidades o centros educativos o .gov para el gobierno; claro está que debe ir acompañando al nombre de la empresa o marca del producto estrella, que es como se conocerá la página Web en el mundo y permitirá el acceso a la tienda virtual, el dominio es una de las primeras seguridades técnicas a considerar.

Diseño y construcción de la WEB.-

⁷² NIC, organismo que se encarga de regular el [registro](#) de los dominios a nivel mundial. Se encarga de indicar para que se utiliza cada dominio, quien está autorizado a registrarlo, y quien puede ser el registrador.

Para obtener un acceso fácil y rápido, hay varios puntos que se deben tener en cuenta a la hora del diseño:

- Se debe impresionar con el contenido más que con la presentación.
- Accesible para todos los navegadores y en todas sus versiones.
- La información para contactar con la empresa debe aparecer en cada página o sub-páginas (links).
- Se debe considerar si interesa ofrecer información multimedia (videos, música) o únicamente textual.
- Simplificar el proceso y definir bien las imágenes, de esta forma bajarán las páginas más rápido.
- Los títulos de cada sección deben ser lo más descriptivos posible.
- Incluir una descripción de todas las imágenes, productos o servicios que ofrezca.

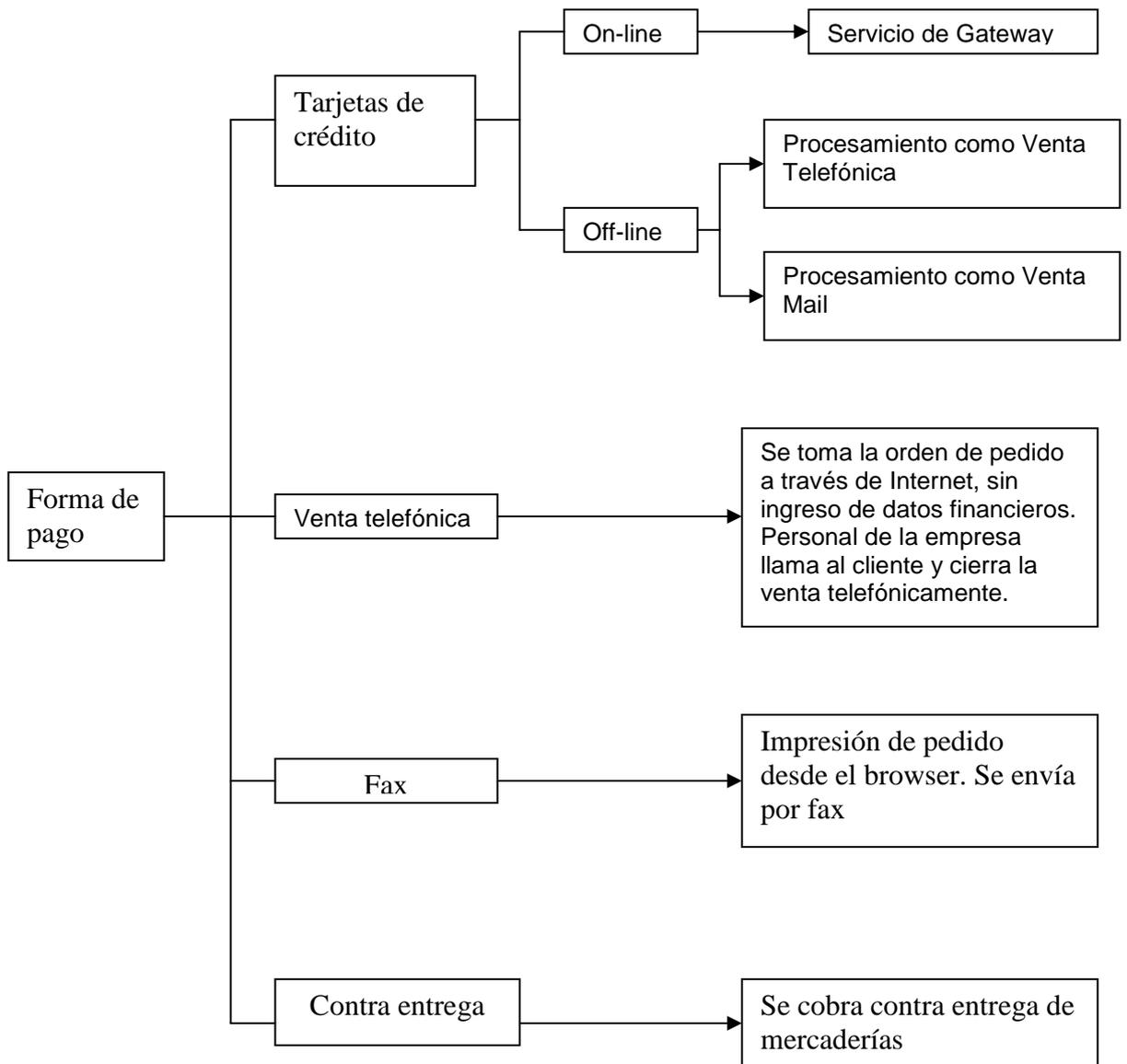
Generalmente, es conveniente requerir la intervención de un diseñador gráfico de Web, este podrá darle un aspecto atractivo al sitio, con color y estilo, esta tarea consiste usualmente en:

- Crear un espace page (espacio de página) atractivo para la tienda, con espacio para ofertas y promociones actualizables.
- Definir el modo de navegar a través del sitio, utilizando links, pero cuidando, que estos sean únicamente los indispensables.
- Diseñar los encabezados para las páginas principales y las categorías.
- Crear botones, viñetas y barras atractivas.
- Escanear y formatear las imágenes de todos los productos que sea posible. (incluir las imágenes de todos los productos?)

- Escribir la información clara y precisa de los productos, en especial lo que se refiere a costos, impuestos, y recargos por envío, correo u otros.

A más de estos aspectos y tareas descritas, es necesario considerar que, cuando el cliente ha seleccionado los productos que adquirirá, el sistema debe pasar a un modo de navegación segura. La tecnología normalmente utilizada es el SSL (Secure Socket Layer), esto significa que todas las comunicaciones con el servidor son encriptadas y se debe dar aviso al cliente de que esta realizando una transacción segura, esto proporcionará confianza a la hora de confirmar su orden de pedido o realizar el pago, y cumplirá además con los principios de seguridad requeridos y tratados en esta investigación.

Se incluirá además, las diferentes alternativas que el cliente podrá utilizar para realizar sus pagos, a continuación se presenta un esquema de estas alternativas:



En el caso de pagos con tarjetas de crédito, el sistema deberá contemplar la comunicación en línea con el emisor de la tarjeta de crédito a fin de obtener la autorización para realizar el cargo.

Será indispensable considerar la apertura de una cuenta internacional que facilite el sistema de cobros a utilizar.

Todos estos elementos pueden ser realizados mediante la programación de la página, botones activos, animaciones o incluso ambientes VRML (realidad virtual) para otorgar al sitio un aspecto vanguardista.

Certificación digital.-

Para operar con tranquilidad se requiere un sistema de seguridad en la red adecuado. En Ecuador existe la Resolución del CONATEL que permite la creación de entidades autorizadas para expender el Certificación Digital, pero lastimosamente el Consejo Nacional de Telecomunicaciones como órgano rector y de control no ha dado paso a la creación de estas empresas, pero esto no exime la posibilidad de poder contratar este servicio en el exterior. Estas empresas actúan como autoridad local de registro y certificación.

El certificado digital es un documento indispensable para:

- Identificarse frente a terceros.
- Firmar documentos electrónicamente.
- Evitar la suplantación de identidad.
- Proteger la información transmitida.
- Asegurar la irrefutabilidad de los compromisos adquiridos.

Este certificado además permite cumplir con los principios de autenticidad e integridad de las empresas y permite obtener el no repudio por los compromisos ofrecidos o adquiridos.

La creación de los fedatarios públicos electrónicos y funcionamiento de entidades certificadoras, garantizan la autenticación de los documentos y

personas a través de sus certificados y firmas digitales, siendo estos documentos probatorios y de igual valor jurídico con su desmaterialización.

Implementación.-

La implementación consiste en la configuración del programa de acuerdo a las necesidades de la empresa y diseño de la página Web, que permita ingresar la información de clientes, futuros clientes o visitantes en la base de datos de la empresa, administrar la cybertienda, definir categorías de exploración y explotación de la misma.

Hosting o Colocación de la Página.-

Para tener acceso a la página a través de Internet desde cualquier lugar del mundo, esta debe residir en algún servidor de Internet o hosting (espacio asignado por el proveedor ISP), es necesario subir la página Web al espacio asignado y la tienda virtual será dada a conocer en todo el mundo.

Para realizar comercio electrónico, se requiere que el proveedor de Internet sea capaz de soportar transacciones seguras, de modo que la información confidencial del cliente permanezca encriptada durante y después de su transmisión.

Frecuentemente, los proveedores de hosting también son diseñadores de sitios de Internet o páginas Web y proveen del dominio lo cual tiene una ventaja, solo se trabaja con una empresa para toda la etapa de implementación de la empresa virtual.

Administración de la empresa virtual.-

Si se cumple con todo lo anterior, el sitio trabajará automáticamente las 24 horas de los 365 días del año, lo que permitirá mayor flexibilidad en el trabajo de administración de la tienda virtual, básicamente éste trabajo consistirá en las siguientes actividades:

Contestar e-mails de consultas sobre artículos que no se encuentran en el catálogo, dudas sobre los pedidos, solicitudes que exigen mayor información, etc.

Procesar las órdenes de compra, realizar el despacho de productos vendidos y contratar el servicio de correo o mensajería para la entrega a domicilio.

Procesar la facturación y cobro de los productos vendidos.

Integrar los datos de clientes, nuevos clientes y potenciales clientes.

Actualizar el catálogo de productos, añadiendo nuevos y eliminando los que ya no pertenecen al catálogo, actualizando los precios, y quizás realizando promociones y ofertas.

Realizar acciones publicitarias por este mismo medio, encaminadas a mejorar las ventas, haciendo uso de la cartera de potenciales clientes que visitaron la página Web y logrando captar otros mercados.

Se recomienda que sea la empresa la que se preocupe de la administración de la tienda virtual. Pero existen casos en los cuales el diseñador puede encargarse de algunas tareas o de todas.

En cuanto a la compañía encargada del servicio de mensajería (courier), es importante considerar que, ésta cuente con cobertura en todo el mundo, si es que el producto está pensado para comercializarse de forma global, o que su servicio en el área en la cual queremos comercializar nuestro sitio, o nuestro producto sea óptimo, hay que tomar en cuenta, que el servicio de mensajería

debe poseer un rastreo electrónico de sus envíos, en caso de que se presenten problemas.

Canal de distribución – promoción.-

Si ya se tiene una excelente tienda virtual, pero no se promociona, equivale a poner una tienda física en un departamento, en el décimo piso de un edificio y no colocar ningún aviso en las ventanas o en la calle, lo que implica que sus clientes serán los familiares y amigos.

Afortunadamente, realizar la promoción en la red es muy sencillo y mucho más barato que en los medios tradicionales. Entre de las opciones más comunes, se pueden enunciar las siguientes:

- Registrar el sitio en motores de búsqueda y directorios de Internet, en especial, en los más conocidos por los usuarios, como: Google, Yahoo, Altavista, Lycos, Infoseek, Excite, Hotbot, etc.
- Realizar la promoción de acuerdo al ramo, buscando: índices, directorios, asociaciones, revistas, recursos, etc., relacionados con el ramo del negocio en los que se pueda promocionar el sitio.
- Realizar marketing mediante e-mail, actualmente existe empresas que poseen listas de e-mails de personas que solicitaron información en algún momento, sobre más de mil temas diferentes; se envía un e-mail a aquellos que solicitaron información sobre su ramo, este medio no es el conocido como Spam, ya que la información es solicitada.

- Banners; se debe diseñar un banner o anuncio atractivo y pagar para colocarlo en un sitio cuyo público es potencialmente el consumidor del producto o servicio, así cuando se realice un click sobre el anuncio irán directamente al sitio, se puede también realizar programas de intercambio de banners, con otras tiendas virtuales.
- Indudablemente, es importante también promocionar fuera de Internet, en los medios tradicionales, ya que en el país estos todavía tienen más alcance que la red de Internet; de esta forma se puede llegar a más clientes.

Navegación.-

La clave para obtener un buen sitio de comercio electrónico es proveer un ambiente que facilite a los clientes navegar a través del catálogo de productos y eventualmente realizar una compra.

El consumidor debe estar en condiciones de encontrar el producto que necesita sin recorrer infinitos niveles de índices o menús, el visitante debería poder llegar a los productos que necesita con unos pocos clicks, se entiende que 80% de los visitantes de sitios mirarán las páginas a la que arriban y aquella por la que se van.

“Ha sido estimado que se pierden el 20% de los visitantes cada vez que se les pide que sigan un link a otra página. Una buena lógica de navegación es esencial”⁷³.

La información debe ser detallada, una vez que el cliente ha ubicado el producto de interés, facilítele imágenes, diagramas e información detallada para ayudarlo a entender que se le está ofreciendo.

⁷³ <http://interactive.net.ec/comercioelectronico> Extraído el 22/03/2006

4.1.2.- ELEMENTOS INDISPENSABLES DEL COMERCIO ELECTRONICO DESDE EL PUNTO DE VISTA DEL CLIENTE

A continuación se plantea la forma de realizar comercio electrónico desde el punto de vista del cliente:

Es necesario considerar como prioritaria la seguridad de la información que se puede transmitir cuando utilizamos la red, por ello desde el primer momento se debe poner a cubierto nuestra identidad e información tomando las siguientes acciones:

- Utilice siempre la última versión de software disponible; continuamente aparecen nuevos agujeros en los programas y utilizando la última versión se corrigen los anteriores errores y fallos de seguridad.
- Borre la información comprometida, de este modo se eliminan viejos correos, cookies, los sitios Web que se han visitado en las últimas fechas, los últimos documentos que se han abierto
- Use distintas cuentas de correo para enviar correos confidenciales, se debe contratar una cuenta con un proveedor de Internet pero para los correos menos importantes puede utilizar un servidor gratuito.
- Use repetidores de correo anónimos, no hay que exponer la identidad propia inútilmente en grupos de noticias, listas de distribución, o cuando se escribe a cualquier destinatario que no conviene que conozca la verdadera identidad del usuario. Para eso están los repetidores de correo anónimos que se pueden utilizar gratuitamente.

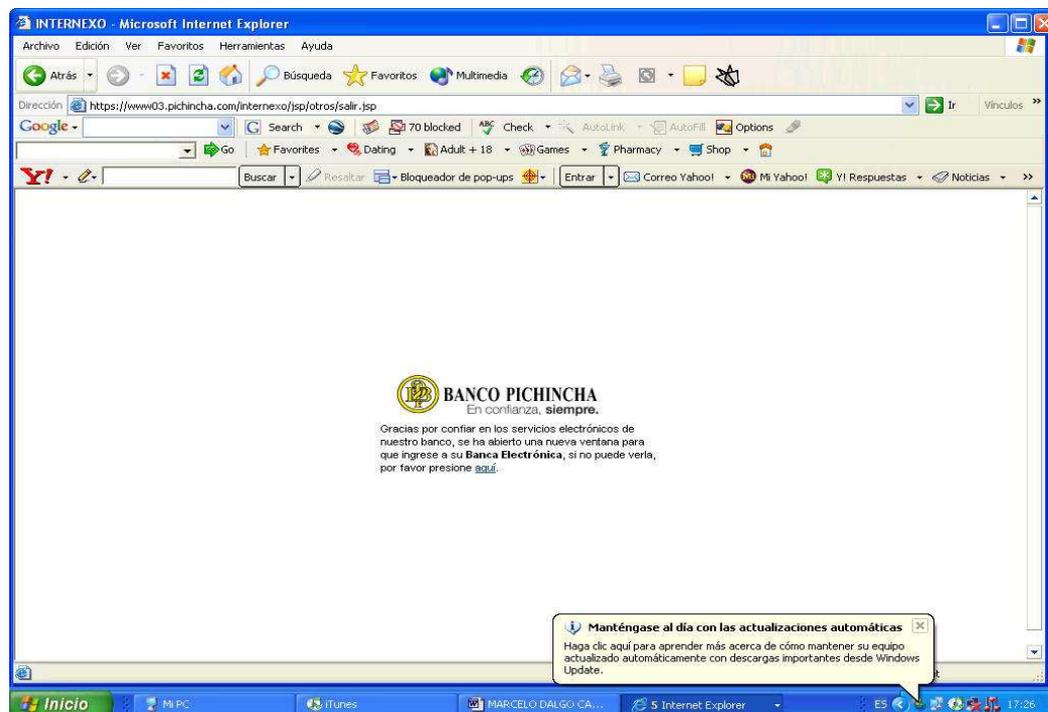
Navegue anónimamente, no es necesario dejar la dirección IP por donde se pasa, porque esto almacena demasiada información en el disco duro, para esto se puede utilizar la navegación anónima pero es necesario contar con Intranet.

- Cifre y firme los correos confidenciales, de este modo el destinatario estará seguro que nadie más lee los mensajes que le llegan, si sólo se aceptan como válidos los correos firmados no hay exposición a que nadie suplante la personalidad de otro.
- Use servidores seguros, cada vez más sitios Web ofrecen la posibilidad de navegación segura, esta debe usarse siempre que sea posible, para saber si un servidor Web es seguro, basta con comprobar el URL a la hora de ingresar la información; si la página Web empieza con `https://` en vez de `http://`, entonces el sitio posee un servidor seguro.
- Ej. : Si se requiere ingresar al Banco del Pichincha, el acceso se lo hace por la página `www.todo1.com`

En donde aparecerá el link `http://www.todo1.com/NASApp/jumpage/menu4.jsp`



Una vez que se ingresa al Banco del Pichincha por los Links indicados, la pagina cambia al modo <https://www02.pichincha.com/internexo-html> como se puede ver en la gráfica.



- No solicite el envío de correos indeseados, a veces al registrarse en un sitio, se pregunta si se desea recibir correos electrónicos, la casilla que otorga la conformidad suele estar marcada por defecto, hay que tener en cuenta esto si no se quieren recibir dichos correos.
- Borre los directorios de búsqueda, existen muchos directorios en los que puede aparecer: nombre, correo electrónico, dirección, teléfono e incluso alguno más de sus datos.
- Exprese rechazo ante el envío de correo basura, si se recibe correo basura y se puede averiguar de quién procede o al menos su proveedor de Internet, se debe escribir expresando el deseo de no recibir más publicidad.
- No revele datos personales innecesariamente, a menudo se reciben formularios que piden ciertos datos personales. Hay que rellenar sólo aquellos que sean relevantes para el servicio que se ofrece, es decir, no

contestar a cuestiones que nada tienen que ver con aquello que está solicitando el usuario.

- Consulte la política de protección de datos de quien solicita los suyos, cuando se recibe la petición de información de carácter personal, se debe buscar antes la política de privacidad que tiene quien solicita la información, de modo que sea más sencillo el exigir responsabilidades ante el incumplimiento de esta.
- Rechace respuestas de tipo comercial, ya que generalmente sirven para que se identifique al usuario que responde como un “cebo fácil” y se aumente el número de publicidad masiva que se le envía.
- Evite enviar datos confidenciales como números de cuenta, tarjetas de crédito, contraseñas, escrituras de propiedad etc. es recomendable evitar siempre que sea posible, el enviarlos a través de cualquier medio y darlos en persona y con las máximas garantías.

Desde el primer momento que se utiliza la red, se debe tomar las precauciones para evitar ser sorprendidos; si se desea realizar comercio electrónico para adquirir un producto, se puede realizar la búsqueda del producto deseado o las empresas proveedoras a través de buscadores.

Una vez identificado el sitio Web, se puede realizar la búsqueda y la exploración de los productos con el propósito de lograr obtener la mayor cantidad de información de lo que se requiere adquirir y cuales son las condiciones.

La canasta de compras.-

Los consumidores incluirán los productos a adquirir en el carro o canasta de compras electrónica durante la navegación en el sitio Web; en todo momento el

consumidor debe controlar el contenido de la canasta, el costo de los productos y demás detalles de la compra, esto le facilita al consumidor la selección de productos mientras visita el sitio.

Check out.-

Cuando la sesión de búsqueda y selección de productos está completa, el cliente clickea sobre un link que lo lleva hacia el área de confirmación de la orden de compra, en este momento, se le muestra al consumidor el listado de los productos que ha seleccionado, el costo total, los gastos de envío, impuestos, etc. el consumidor puede ingresar instrucciones de envío, su nombre, dirección y demás datos necesarios para cerrar la transacción.

En general, le son ofrecidos al consumidor un conjunto de opciones de pago, la más habitual es utilizar tarjetas de crédito, en esta etapa del proceso el sistema deberá haber pasado a un modo de navegación segura (comprobar si la página pasa del modo http:// a https://), la tecnología normalmente utilizada es el SSL⁷⁴, esto significa que todas las comunicaciones con el servidor son encriptadas para que posibles intrusos no puedan robar información importante del consumidor.

El cliente debe ser visualmente advertido por el navegador que está en un modo seguro, una llave azul o una línea azul en Netscape Communicator y un candado cerrado en Microsoft Explorer, advierten del paso a un modo de navegación segura.

Esta tecnología debe ser ampliamente utilizada y entendida por los usuarios de Internet. La mayoría de la bibliografía sobre Internet enfatiza la necesidad que los clientes entreguen su información confidencial en una sesión segura.

⁷⁴ Secure Socket Layer

Luego de haber comprobado lo anteriormente descrito, el cliente podrá entregar la información necesaria para confirmar la orden de pedido y realizar los pagos de acuerdo a las opciones presentadas y aceptadas por el consumidor.

Precio.-

El comprador debe cerciorarse de que el precio anunciado es el precio total, el mismo que debe incluir:

Descuentos y ofertas si las hubiese

Impuestos: IVA, otros.

Gastos de envío

Precio total

Pago.-

Casi todas las tiendas virtuales admiten pagos a través de tarjeta de crédito, si el comprador opta por la compra a través de tarjeta de crédito debe introducir en el formulario de pedido el número de la tarjeta de crédito y la fecha de caducidad, en la actualidad casi todos los servicios de comercio electrónico disponen de un servidor seguro que garantiza al usuario que sus datos privados entran en una zona segura y protegida, sin embargo si una empresa no dispone de un servidor seguro lo recomendable es elegir otra vía para formalizar el pago (transferencia, giros, pago contra entrega etc.).

De esta forma el cliente cumple con los principios de seguridad, autenticidad, integridad y confidencialidad de la información a la vez que garantiza el no repudio por los compromisos ofrecidos o adquiridos.

4.1.3.- BARRERAS DE PROTECCIÓN

Si bien, tanto las empresas como los clientes pueden utilizar los recursos administrativos, es necesario considerar tecnologías que permitan cubrir aun más los derechos a la intimidad e integridad de la información; esto se puede lograr utilizando recursos técnicos, conocidos como barreras de protección:

Se puede utilizar tecnología de software y hardware de diferentes tipos como barreras de protección, sus cometidos son esencialmente los mismos: detienen cada llamada, la vetan y la dejan pasar sólo si cumple con requisitos preestablecidos, pero como sucede con todo, según se pague, así será la calidad del producto; entre los que encontramos en el mercado podemos citar los siguientes:

Firewall.- Componente diseñado para prevenir accesos desautorizados a una red, actúan como un puente de seguridad entre las redes internas y externas-, su costo referencial promedio en el mercado es de 6500 dólares para 100 usuarios.

IDS e IPS.- Censor de intrusos, toman acciones de prevención (IDS Intrusion Detection System), (IPS Intrusion Prevention System); su costo promedio referencial es de 11000 dólares dependiendo de tamaño de red.

Antivirus.- Protección de software; dependiendo de su eficiencia sus costos varían.

Filtros URL.- Permite filtrar la información antes de ingresar a la red.

Spyware.- Software pirata.

Los antivirus, filtros URL y Spyware tienen un costo referencial promedio de 45 dólares por usuario.

El estándar “SET” (Secure Electronic Transaction).- Es una respuesta a las consideraciones de privacidad, verifica y confirma la identidad de los participantes.

Software de encriptación.- Permite codificar la información Ej. formato HTTPS con un costo promedio referencial de 150 dólares por usuario.

Una barrera de protección actúa como una guardia electrónica, hace mucho más que proteger simplemente la red de posibles intrusos, puede proporcionar también información vital sobre la actividad del sistema; entre sus prestaciones tenemos:

Controla el acceso a los sistemas de las redes privadas.

- Coloca la seguridad en manos de unos pocos.
- Aumenta el nivel de privacidad ocultando las direcciones de los usuarios individuales de la red.
- Realizar un seguimiento del tráfico por razones de auditoria
- Informar de sucesos sospechosos.
- Trabajar con comprobadores de virus e Intranet, así como con la Internet.

Como sucede con todos los temas de seguridad, la decisión siempre resultará de un compromiso entre el coste, el riesgo y las necesidades empresariales, mas de este tema fue descrito en el capítulo III como Barreras de Protección.

Sin embargo, se debe considerar el hecho de que muchas barreras de protección pueden hacer ineficientes los sistemas utilizados, ya que puede parecer muy celosamente o protectora, impidiendo el acceso a algunos servicios deseables para la empresa; no puede prevenir problemas en el interior de la red y además puede provocar cuellos de botella, debido a un alto volumen de tráfico o cuando se utilicen programas anti-virus, es un punto simple de fallo, si se estropea, nada podrá entrar ni salir de la red.

Otros tipos de barreras de protección son los certificados digitales, permiten dar mayor confianza al Comercio Electrónico, representan el punto más importante en las transacciones electrónicas seguras, éstos brindan una forma conveniente y fácil de asegurar que los participantes en una transacción comercial electrónica puedan confiar el uno en el otro, esta confianza se establece a través de un tercero, que suministra los certificados digitales a las empresas, y estas a su vez, ofrecerán un certificado digital al tarjeta habiente o cliente. Los certificados digitales en pocas palabras, garantizan que dos computadoras que se comunican entre sí puedan efectuar transacciones de comercio electrónico con éxito. La base de esta tecnología reside en los códigos secretos o criptografía, sin duda, esta es la forma como se debe realizar las transacciones.

La criptografía como barrera de protección garantiza el secreto en la comunicación entre dos personas u organizaciones; asegura que la información que se envía sea auténtica en doble vía; y que el remitente sea realmente quien dice ser y el remitido quien deba recibirla.

La utilización de la encriptación con clave pública es la solución a la seguridad en toda red abierta, es la forma de codificación más novedosa y sofisticada desarrollada, en este tipo de enfoque, cada participante crea dos claves o llaves únicas.

Se dispone de su propia "clave pública", que es registrada en un tipo de directorio al que el público en general tiene acceso; se dispone además de otra clave o "llave privada", que se mantiene en secreto.

El esquema de este sistema se puede resumir en los cuatro siguientes pasos:

1. A cada usuario se le entrega un número entero que funciona como su clave pública.

2. Cada usuario posee una clave privada que solo él conoce, y que es distinta para cada uno.
3. Existe un directorio de claves públicas que pueden ser conocidas.
4. El emisor envía el mensaje con la clave pública del destinatario encriptándola con su clave privada. El destinatario solo podrá abrir el mensaje con la clave pública junto con su clave privada

La encriptación y su opuesto lo realiza un software siguiendo lo especificado en los estándares de la industria, usted no tiene que preocuparse de nada más.

Otra barrera de protección que puede ser utilizada, es la **firma electrónica o digital**, funciona como un conjunto de datos electrónicos que identifican a una persona en concreto mediante la encriptación o cifrado de los datos que la componen, para ello es necesario contar igualmente con un par de claves; la clave privada y la clave pública, se puede escribir un documento y firmarlo con la clave privada; el receptor al cual previamente se lo a otorgado la clave pública, puede verificar la procedencia del mensaje y que verdaderamente ha sido firmada por quien lo envía.

Con esta encriptación se consigue que la información enviada bajo la firma electrónica sólo pueda se leída por la persona autorizada que posea la clave y además acreditar la identidad de quien firma el documento electrónicamente.

Es necesario aclarar que los servicios de: certificados digitales, sistemas de clave pública y privada, y la firma electrónica pueden ser proporcionados por las entidades de certificación de información, lamentablemente al momento no existe en el país este tipo de empresas que proporcionen este servicio, pero se puede contratar en el exterior.

Otro aspecto a ser considerado en la propuesta es el empoderamiento que se entrega al personal responsable de los sistemas, quien debe adoptar las

medidas técnicas y administrativas descritas que resulten necesarias para garantizar la seguridad integridad y confidencialidad de la información, mantener el secreto profesional y rendir caución para su seguridad, es decir deberá ser personal de confianza ya que son los encargados de manejar datos vulnerables para la empresa.

Los servicios descritos, tanto en software y hardware pueden ser utilizados por los usuarios para minimizar el riesgo y dar mayor seguridad a las transacciones, obteniendo mayores beneficios a bajos costos de implementación.

4.1.4.- ASPECTOS JURIDICOS Y LEGALES

Por lo que parece las verdaderas barreras de protección al comercio electrónico no son tanto tecnológicas, una vez más el eslabón más débil de la cadena es de índole personal y para combatir este problema es necesario establecer reglas y procedimientos claros a través de Leyes y Reglamentos.

El Ecuador ya cuenta con una Ley y Reglamento al Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que aunque entró en vigencia a partir del año 2003, ésta Ley no es aplicada y difundida adecuadamente a más de encontrarse con algunos vacíos principalmente en lo que se refiere a la seguridad de la información.

Hay que considerar y entender que no se puede desconocer la naturaleza y características de los correos electrónicos, o información que circula por las redes en forma abierta; cualquier persona o administrador de un servidor de correo puede visualizar sin realizar ninguna operación clandestina, es decir nos

encontramos en una red de tipo abierta a la que todos podemos tener acceso y conocer la información que contiene.

No se trata de un canal de "comunicación privada" al que pueda exigirse inviolabilidad por parte de un receptor involuntario o distinto del que indicó el emisor, o por parte del que contractualmente provee los equipos o sistemas de casillas de almacenamiento de correos para la comunicación, pero tampoco estas personas pueden arbitrariamente abrir los archivos o mensajes que no les pertenece, porque estarían violando la intimidad de las personas, al margen de se encuentre los mensajes encriptados, codificados o posean las claves necesarias para su integridad, esto no se puede permitir, se debe reglamentar en el país y consecuentemente se tomará en cuenta los planteado en los convenios internacionales.

Bajo este criterio se propone que las Leyes y Reglamentos que tienen que ver con el Comercio Electrónico, incluyan los siguientes artículos que permitan garantizar la seguridad, intimidad y confidencialidad de la información:

A la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Art. Todo archivo, mensaje de datos, sean estos adjuntos que se encuentren en un sistema informático o red electrónica será de propiedad exclusiva de su autor, deberá incluir la autoría en el documento y la autorización de circulación pública o su prohibición a fin de establecer su propiedad.

Art. Las claves personales son de uso exclusivo de la persona asignada, por tanto cualquier uso o violación se considerará como hurto, robo o abuso de

confianza y será sancionado conforme se establece estos delitos en el Código Penal.

Art. Todo órgano, empresa o institución que proporcione claves de acceso o pins a los usuarios, tiene la obligación de contratar el servicio de una empresa certificadora de información.

Art. Los responsables o usuarios de bases de datos, que contengan información exclusiva de los usuarios, sean estos, claves, pines, números de tarjetas de crédito, números de cuentas corrientes o ahorros, pólizas y demás documentos, serán responsables de su custodia y por lo tanto deberán adoptar las medidas técnicas necesarias para garantizar su seguridad e inviolabilidad.

Art. Calidad de los datos.- La calidad de los datos recopilados deberán estar sujetos a:

1. Los datos personales que se recojan para efectos de su tratamiento electrónico deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad que motivó su obtención; por tanto no podrán ser utilizados para otro fin.
2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
4. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

5. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara y por lo tanto deberán contar con su consentimiento.

No será necesario el consentimiento cuando:

- Los datos se obtengan de fuentes de acceso público debidamente probadas.
- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; o, estén sujetos a lo que dispone el Artículo 2 de la Ley de Transparencia, referente al ejercicio del derecho fundamental de las personas sobre la información.

6. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros exclusivamente.

7. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

8. Las instituciones de salud públicas o privadas y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

Art. Transferencia internacional.- Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales, que no proporcionen niveles de protección adecuados. Esta prohibición no regirá

cuando se trate de: Colaboración judicial internacional; intercambio de datos de carácter médico; transferencias bancarias o bursátiles conforme la legislación que les resulte aplicable cuando: la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico; se trate de información de mercado, que no contenga datos de identidad personal, como nombres, números de identificaciones, direcciones, fechas de nacimiento, sexo etc.; la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales el Ecuador sea parte.

Al Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Art. Sanciones administrativas.- Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, se aplicara las sanciones de apercibimiento, suspensión, o multa de mil dólares (\$ 1.000.-) a diez mil dólares (\$ 10.000.-), clausura o cancelación del archivo, registro o banco de datos, garantizando el principio del debido proceso.

Al Código Penal

Art. La pena será de un mes a dos años, para quien a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales que no le corresponda; mensajes de datos o correos electrónicos que no sea el destinatario.

Con la incorporación de estos preceptos legales, tanto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: y, el Código Penal, los ciudadanos y el país estará protegido respecto a la seguridad de la información.

4.2.- CONCLUSIONES

El marco jurídico que se relaciona o esta ligado a la protección de datos en el comercio electrónico, pese a ser extenso no se puede determinar como adecuado, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, únicamente cuenta con un artículo relacionado a este propósito, el cual hace mención a la intimidad, privacidad y confidencialidad de la información en relación a lo que establece la Constitución Política del Estado en el Art. 23 numeral 8, respecto de la intimidad personal; no se prevé la forma como se garantizará estos derechos así como la práctica normal y diaria del uso de datos de terceros que se ha generalizado y que ocasiona graves daños a la intimidad de las personas o titulares de la información.

No es posible que todo un cuerpo legal que esta dedicado a regular el comercio electrónico contenga un solo artículo que se relaciona a la protección de datos,

lo que demuestra las deficiencias de nuestra legislación, referente a un punto tan delicado como es la Protección del derecho a la intimidad personal.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, así como su Reglamento, resultan insuficientes para crear el entorno de seguridad y satisfacción del cliente que se hace más común a nivel mundial y que de una u otra manera nuestro país está involucrando.

Por tratarse de un comercio abierto e inherentemente global y marcadamente virtual tiene la particularidad de ser percibido como muy inseguro

La percepción de ser muy inseguro se ve reforzada porque, generalmente, existe la carencia de un marco normativo específico o de fácil aplicación al medio.

De igual forma, el Reglamento del CONATEL que hace referencia a la acreditación, registro y regulación de entidades habilitadas para prestar servicios de certificación y servicios relacionados, no garantiza la seguridad y respeto a la intimidad de las personas y sus datos, puesto que sólo habla de los derechos y responsabilidades de las entidades de certificación y no de la protección hacia los usuarios que esta empresas deben cumplir.

El comercio electrónico es parte de un mercado donde los proveedores, consumidores, clientes, gobierno, suministradores de tecnología y quienes están involucrados en las transacciones, puedan satisfacer sus necesidades electrónicamente y se desenvuelvan en un medio de operaciones que van desde el contacto con el oferente como proveedor inicial hasta la compra venta electrónica con el consumidor final.

La aparición del comercio electrónico obliga claramente a replantearse muchas de las cuestiones del comercio tradicional, surgiendo nuevos problemas, e incluso agudizando algunos de los ya existentes. En este catálogo de problemas, se plantean cuestiones que van, desde la validez legal de las transacciones, la integridad y seguridad de los datos de las personas, la necesidad de acuerdos internacionales y leyes claras que armonicen las legislaciones sobre comercio electrónico como punto clave del desarrollo sano de esta nueva forma de hacer negocios.

No existe concordancia entre las Leyes Ecuatorianas, éstas son obsoletas como es el caso del Código de Comercio que no contempla el desarrollo tecnológico que inmerso por tanto, el panorama es confuso e inaplicable, como se puede apreciar en el primer capítulo al hablar del marco jurídico que se relaciona con el comercio electrónico

El comercio electrónico, no es más que una derivación del comercio tradicional, pues permite realizar las mismas transacciones pero apoyados por tecnología que permite mejorar principalmente la comunicación a la hora de hacer los negocios.

De la clasificación analizada, se puede mencionar principalmente dos: El comercio electrónico directo, que comercializa principalmente bienes intangibles y su proceso total es a través de las redes electrónicas y el Comercio Electrónico Indirecto, que necesita apoyarse de otros servicios como transporte de mercaderías, canales de distribución, verificación por parte de los clientes, e incluso trámites burocráticos en aduanas, impuestos, y otros.

En la actualidad, la presencia de las empresas en Internet, es fundamental, porque es el medio más rápido y de menor costo de comunicación con el cliente, esté donde esté.

La tendencia consiste en que el cliente preferirá realizar sus compras on-line por la conveniencia, alcance y amplia disponibilidad de información de productos y servicios, las empresas que no desarrollen una presencia en el llamado comercio electrónico, perderán la oportunidad de ganar nuevos clientes.

Si bien Internet funciona muy bien como canal de distribución de productos intangibles, no es el caso para otros servicios o productos físicos, sin embargo su flexibilidad y rapidez, el coste y su facilidad de control hacen que este servicio sea la mejor opción para las empresas, lógicamente con el fantasma de la inseguridad que posee tanto la empresa como el cliente.

En lo referente a las estadísticas en el Ecuador, se puede considerar como el talón de Aquiles, pues hasta el momento no se cuenta con un instrumento que permita medir como se desarrolla el comercio electrónico en nuestro país. Sin embargo de las encuestas y entrevistas realizadas se puede concluir que:

El 10% de los usuarios, realiza compras a través de Internet, es decir realiza comercio electrónico, y si decimos que aproximadamente tenemos 550.000 usuarios de Internet en el país, existen únicamente 55000 usuarios realizando este tipo de transacciones.

Otro dato importante, es que de los usuarios que realizan comercio electrónico, el 87 % de la muestra, ha realizado este tipo de transacciones en sitios internacionales, y apenas el 12% en el país, esto demuestra que las empresas nacionales, no están siendo adecuadamente promocionadas en la red, no constan o simplemente no son seguras para los usuarios.

De igual forma el 87% de los usuarios, realiza sus pagos a través de la red, con tarjeta de crédito, porque el mercado ecuatoriano no da otras opciones para hacerlo.

La tarjeta de crédito es el medio de pago más común, claro está que se la utiliza para compras denominadas mínimas, no es el caso de compras a escala o al por mayor que por seguridad, los usuarios prefieren realizarlas fuera del sistema o utilizando otros medios de pago.

En cuanto al nivel de satisfacción de los usuarios, el 84% se refiere a un nivel de satisfacción bueno, en el que se incluye seguridad, sin embargo existe un 9% que lo determina como malo, lo que hace pensar que existe, fraudes, inseguridad e incumplimiento de las obligaciones.

De los resultados obtenidos es indiscutible el subdesarrollo registrado, lo que se atribuye a la falta de: políticas y leyes claras, seguridad, confianza, conocimiento y sobre todo educación de los usuarios.

En el caso de los tributos o impuestos, se puede decir que no se ha desarrollado y es difícil pero no imposible determinar las transacciones de una empresa vía comercio electrónico; para ello es necesario considerar: la ausencia de control del usuario, la imposibilidad física de localización de la actividad, la carencia de medios para identificar al usuario, la jurisdicción, su domicilio y el tipo de transacciones que realiza; peor aún si son de carácter internacional; sólo a través de la contabilidad de las empresas se puede definir quien y en donde tributan.

La firma digital es un instrumento más que permite la adaptación a este nuevo paradigma socio-económico-cultural, que posibilita la expansión del comercio en esta nueva economía digital globalizada.

En la investigación, se ha tratado de dar una idea de los cambios importantes que ha experimentado la firma desde sus orígenes hasta nuestros días y como se debe tratar de adaptar estos cambios a la realidad social y cultural dejando la puerta abierta a otros futuros cambios y otras nuevas tecnologías que sin duda vendrán.

La firma digital con las garantías exigidas, es una alternativa para conseguir la anhelada seguridad jurídica, puede abrir un prometedor camino que deje en entredicho la eficacia real de la fe pública tradicional. Entre los objetivos de la firma digital está el conseguir una universalización de un estándar de firma electrónica, esto se establece en la llamada clave pública y privada, que permite conocer quienes están tras los computadores como canal de comunicación.

Es indiscutible que las nuevas tecnologías de la información se presentan como una oportunidad inmejorable para que los países menos desarrollados o emergentes puedan ajustar la brecha que los separa de los denominados países del primer mundo.

A pesar de que el Ecuador cuenta con tecnología de punta, que permite asegurar los sistemas y redes de posibles intrusos hackers y crackers, utilizando barreras de protección; sin embargo se puede decir que no son utilizadas correctamente o simplemente no las usan, de ahí que el problema sigue siendo de carácter formativo de las personas.

La seguridad de la información es el punto crucial en el ciberespacio, tanto compradores como vendedores dependen de esta necesidad y lógicamente al ser el desarrollo del comercio electrónico; de carácter técnico se vuelve vulnerable y sensible al comportamiento humano, sin embargo se debe anotar que el 90% de los resultados dependen de la prevención que puedan tomar, para evitar ser atacados o sorprendidos con fraudes de carácter tecnológico.

Sin duda la información se ha convertido en un factor económico más con una especial particularidad, el modelo informático está caracterizado por costos bajos con tendencias declinantes, lo que permite inferir el desarrollo de una nueva cultura técnica con utilidades financieras prometedoras. La referencia a esta tendencia mundial en la era de la globalización, que permite sostener que el comercio electrónico está produciendo una verdadera revolución en las transacciones comerciales, que afectan a un nuevo modelo en la negociación y a los sistemas de contrataciones al tiempo que significa un cambio cultural.

La confidencialidad y reserva de la información se establece en los mecanismos utilizados de encriptación, pues si bien es cierto se envía la información por la red de forma normal, esta puede ser interceptada; mientras que si agrega seguridad a través de encriptación ésta no podrá ser vulnerada.

En el capítulo III se establece varios aspectos claves como: barreras de protección, seguridad, firmas electrónicas y digitales y certificación de información; todos estos temas se basan en los principios fundamentales de la confidencialidad, la integridad, la autenticación y la irrenunciabilidad, que se resumen en la seguridad y confianza de los usuarios para realizar transacciones electrónicas.

4.3.- RECOMENDACIONES

Luego del análisis realizado se considera recomendable incorporar a la Ley y Reglamento de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y, Código Penal Ecuatoriano varios artículos citados en la propuesta, que permitan proteger a las personas y sus datos como manda la Constitución Política del Estado en su Art. 23 numeral 8.

Se debe ampliar el Reglamento del CONATEL que hace referencia a la acreditación, registro y regulación de entidades habilitadas para prestar servicios de certificación y servicios relacionados, respecto a la obligación de las entidades de certificación de información ya que a mas de proteger la integridad de la información, garantice la confidencialidad, intimidad y reserva de los datos contenidos, serán causas de suspensión de la autorización como entidad certificadora, sin perjuicio de la responsabilidad civil y penal que ocasione el hecho.

En el comercio electrónico se debe considerar los aspectos jurídicos que conforme a Derecho tiene implicaciones para los usuarios, tanto contratantes como contratados, vendedores y consumidores; estas son:

- Responsabilidad jurídica
- Protección de los consumidores
- Resolución de controversias
- Asuntos referidos a la tributación
- Jurisdicción competente y legislación aplicable

Los usuarios se deben acostumbrar a que el uso de la tecnología de la información para el comercio electrónico son los nuevos usos y costumbres que los comerciantes tienen para realizar sus transacciones, tomar como parte importante del comercio este nuevo modelo y desarrollarlo con políticas y leyes claras, que permita a los usuarios tener seguridad y confianza al momento de realizar sus operaciones, más aún cuando nos encontramos en un mundo globalizado en el que el Ecuador es parte de ello.

Se debe implementar indicadores, que permita medir la incidencia del comercio electrónico en el país, de lo analizado, se puede determinar que el comercio

electrónico está tomando fuerza, pese a la falta de seguridad existente y la desconfianza que existe en el servicio; para mejorar esto, se debe determinar los derechos y responsabilidades de cada uno de los actores.

Para el caso de las empresas, la presencia en Internet es ya parte su constitución, considerando que sus costos no son elevados y que el servicio que presta a la organización es bastante representativo; sin embargo, la responsabilidad que esto genera, obliga a tomar precauciones de tipo administrativo, jurídico y técnico.

El cliente o los usuarios, por falta de seguridad, tienden a arriesgar sus recursos al momento de realizar transacciones, por lo que se debe considerar la propuesta para alcanzar los mejores beneficios, con seguridad de que lo que está adquiriendo es en realidad lo que requiere o lo que fue ofertado.

Los proveedores del servicio, deben también ser obligados a lo que dispone la Ley en todo lo que se refiere a integridad y seguridad de los mensajes de datos, de tal forma que el servicio prestado sea óptimo y genere confianza entre los usuarios.

En lo relacionado a los medios de pago, en donde consumidores como oferentes reflexionan el hecho de concluir la transacción, debe tener las debidas precauciones para garantizar su seguridad como son barreras de entrada, certificación de información y criptología, como se refiere en la propuesta.

Cuando el Estado genere políticas de desarrollo para el comercio electrónico, éstas serán y estarán encaminadas a recaudar los ingresos públicos vía tributación con acomodo de la aplicación existente al comercio tradicional.

Es necesario incentivar a las personas sobre el uso de barreras de protección, si bien la red de Internet es totalmente abierta y no controlada por nadie, esto hace que sea vulnerable a posibles navegantes intrusos, sin que se pueda encontrar en esto un delito por no estar claramente tipificado en la Ley, ocasionando problemas de intimidad por lo que se hace indispensable que toda persona que utilice como canal de comunicación el Internet o como medio para hacer negocios, tome las debidas precauciones y utilice correctamente las barreras de protección.

El uso de software y hardware destinados a frenar los abusos informáticos permiten mantener el control del ciberespacio en lo relacionado a transmisión de datos, para ello en el capítulo III se da a conocer algunos estándares, formas y sistemas que permiten mantener el control de la seguridad de la información.

El rechazo que existe a estas nuevas tecnologías de la información no está en la electrónica, ni en las comunicaciones sino en la falta de educación y conocimiento de las personas como realidad social, para ello es necesario que el sector público y privado realice campañas educativas.

Las nuevas tecnologías de la información y las comunicaciones, unidas a otras técnicas dan fiabilidad al documento electrónico y tratan de lograr una mayor seguridad mediante el desarrollo y aprovechamiento de técnicas y procedimientos de control basados en la criptografía, esta mayor seguridad que se pretende con una adecuación normativa nos conducirán hacia la autenticación electrónica.

La creación de los fedatarios públicos electrónicos y funcionamiento de entidades certificadoras, nos llevará a garantizar la autenticación de los documentos y personas a través de sus firmas digitales que circulen a través

de las líneas de comunicación, siendo estos documentos probatorios y de igual valor jurídico con su desmaterialización.

La encriptación es un mecanismo idóneo que permite agregar confidencialidad y reserva de la información a la vez que garantiza su integridad al compararse como un sobre cerrado de tipo inviolable; que no permite conocer el contenido de los documentos, al menos que sea vulnerada su encriptación, siendo esto un violación a las garantías constitucionales que se hace referencia.

Los principios fundamentales que se han establecido en el capítulo III, como confidencialidad, integridad, autenticación e irrenunciabilidad son el propósito de todo proceso, sea este administrativo, técnico o jurídico que debe prevalecer tanto en el comercio electrónico como en todo acto realizado por las personas.

Finalmente se recomienda la aplicación de la propuesta para la creación de empresas y que estas participen del comercio electrónico, como su inserción de las ya existentes, en el caso de los usuarios tomar las medidas correctivas y propuestas para obtener los mejores beneficios y el crecimiento esperado, minimizando el riesgo respecto a la seguridad e integridad de los datos.

GLOSARIO DE TERMINOS

API.- Protocolo estándar de comunicación

B2B.- De empresa a empresa

B2C.- De empresa a consumidor

B2G.-De empresa a gobierno

Banners.- Formato publicitario

C2C.- De consumidor a consumidor

CA.- Certification authorities.- Autoridad de certificación

CAD.- Computer – Aided Design- cad.- Diseño asistido por ordenador

CAM.- Computer – Aided Manufacturing - cam.- Fabricación asistida por ordenador

CBC.- Cipher block Chiang.- Sistema de encriptación

CFB.- Cipher block feedback.- Sistema de encriptación

Check out.- Confirmación de requerimientos

Click-wrap agreements. - Contratos con cláusulas predispuestas

Copyright.- Sistema de protección de derechos

Courier.- Correo

Criptografía Asimétrica.- Escritura oculta asimétrica

Criptografía Simétrica.- Escritura oculta simétrica.

Criptografía.- (Del griego kryptos, “ocultar”, y grafos, “escribir”, literalmente “escritura oculta”

DES.- Data encryption Standard.- Algoritmo de cifrado

E mail.- Correo Electrónico

EBC.- Electronic codebook mode.- Sistema de encriptación

EDI. - Electronic Data Interchange.- Intercambio electrónico de datos

EDS.- Electronic data system.- Sistema electrónico de datos

EFT.- Transferencia electrónica de fondos

E-key Max security.- Llave de máxima seguridad

Firewall.- Controlador de comunicación.- cortafuegos

First USA.- Operador de sistemas de pago con tarjeta de crédito

FTP.- Protocolo para transferencia de archivos

FV.- First virtual.- Primer virtual

Gateway.- Puerta de entrada

Hábeas data.- Garantía que protege varios derechos, tales como, la honra, la buena reputación, la intimidad y también el derecho a la información

Hardware.- Artefacto físico de una tecnología

Hosting.- Alojamiento Web

HTML.- Hyper tex markup language.- Lenguaje de marcas ipertextuales

HTTPS.- Formato de página segura

IDS.- Intrucction detention system.- Sistema de detención de instrucciones

Intranet. - Red interna

IPS.- Instrucction prevention system.- Sistema de prevención de instrucciones

ISO.- Internacional Standard organisation.- Organización internacional de estándares

ISP.- Proveedores de servicio electrónico

Links.- Enlace entre dos paginas web

Merchant Account.- Cuenta para aceptar tarjetas de crédito

Microsoft expedia.- Sistema publicitario de viajes

Microsoft explorer.- Explorador de Microsoft

MIME.- Distribución transparente de formatos de archivos

MIT.- Matematic institut tecnologic.- Instituto de tecnología de matemáticas

Mosaic.- Tecnología para navegación

Netscape comunicator.- Navegador Web

Newsletter.- Boletín informativo

OFB.- Output feedback mode.- Sistema de encriptación

Offline.- Fuera de línea

On-line.- En línea

Opt-in E-mail.- Registro para recibir ofertas y promociones por correo

PDA .- Equipo electrónico

Pinchar.- En la red, interceptar tráfico electrónico

PKI.- Public key infrastructure.- Infraestructura de clave pública

POS.- Máquina de autorización en un establecimiento comercial

PYMEs.- Pequeñas y medianas empresas

RA.- Registration authorities.- Autoridad de registro

RSA.- Algoritmo asimétrico cifrado en bloques

Securedoc.- Software de encriptación

SET.- Secure electronic transaction.- Transacción Electrónica segura

Software.- Programas y sistemas informáticos

Spam.- Correo electrónico no solicitado

Spyware.- Software pirata

SSL.- Secure Socket Layer.- Comunicación encriptada

TCP/IP.- Protocolo de comunicación

TIC.- Tecnologías de la información y comunicación

TSA.- Time stamping authorities.- Autoridad de fechado digital

URL.- Uniform resource locator.- Localizador uniforme de recurso

VRML.- Virtual reality modeling language.- Lenguaje para modelado de realidad virtual

Web site. - Sitio web

Web.- Visualizador de Texto, imágenes o contenidos multimedia

Windows sockets.- Especificación técnica que define como el software de red de windows debe acceder a los servicios de red

BIBLIOGRAFIA

1. ACURIO Del Pino Santiago sacurio@larreategui-fabara.com.ec
2. ALEGRÍA Héctor "Nuevas fronteras de la documentación, la forma y la prueba de las relaciones comerciales", (Buenos Aires, 1997), Vol. 1.
3. ALVAREZ, Marañón Gonzalo. Barreras al Comercio Electrónico Instituto de Seguridad de Internet 2001-2003
4. GRECO, Marco Aurelio, "Internet en directo", segunda edición, Dialéctica, San Pablo, 2000
5. LLANEZA González Paloma - Internet y comunicaciones digitales Bosch, 2004 Madrid,
6. MARTÍNEZ Nadal Apolonia – "Comercio Electrónico, firma digital y autoridades de certificación Madrid 2003
7. PAEZ Rivadeneira Juan José Revista Judicial Quito 2003
8. PEREZ De Ayala, José Luis. Explicación de la técnica de los Impuestos. 3era ed. Madrid: 2004.
9. POTTS Ricardo F. (2003) Clases de Comercio Electrónico enero del 2005 flavio@enet.cu
10. RAMOS Suárez Fernando.(2000). Departamento de Comercio Electrónico. Anguiano & Asociados.
11. RUBIO V, Rodríguez C. Muñoz R. Aspectos Legales y Técnicos de la firma Electrónica. Madrid Ed. Experiencia. Madrid 2005
12. YANEZ Pablo Introducción al estudio del Derecho Informático Gráficas SOS 1999 Quito
13. Constitución Política del Ecuador 1998
14. Ley de Propiedad Intelectual R.O 266 de 1998
15. Ley de Defensa del Consumidor Registro Oficial No. 520 de sept 12 de 1990
16. Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos R.O. 67 Suplemento 557-2002
17. Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico 2006
18. Código de Comercio Ecuador R.O –S-1202 1960
19. Globalización y Gestión ON-LINE.(2004). <http://www.Monografias.com>
20. Biblioteca de Consulta Microsoft® Encarta® 2003

21. REDI Revista Electrónica de Derecho Informático - Número 26 (Sept. de 2000)
22. REVISTA LIDERES, lunes 20 de marzo del 2006
23. El Comercio, Tecnología cuaderno 2
24. olman@orimola.com San José, Costa Rica
25. <http://www.ecampus.cl/Textos/derecho/jijena/1/jijena1.htm> Renato Jijena Leiva
26. <http://es.wikipedia.org/wiki/Criptograf%C3%ADa> Categoría: Criptografía
27. <http://ecuador.derecho.org/>
28. <http://publicaciones.derecho.org/redi/>
29. <http://www.Wikipedia.com>
30. <http://www.injef.com/php/index.php>.Madrid
31. <http://www.premium.vlex.com/doctrina/>.
32. <http://www.monografias.com/trabajos6/meti.shtml>.
33. <http://www.eluniverso.com/especiales/comercioelectronico/encuestacomercioelectronico.asp>
34. <http://www.eluniverso.com/especiales/comercioelectronico/internetydesarrolloempresarial.asp>
35. <http://interactive.net.ec/comercioelectronico> 2006
36. <http://es.wikipedia.org/wiki/Criptograf%C3%ADa>", Categoría: Criptografía febrero 2006
37. www.instisec.com/publico/verarticulo.asp?id=47 Publicado en Boletín del Criptonomicón #51
38. www.monografias.com.Campitelli Adrián, Rosso César Luis enero del 2003

AUTORIZACIÓN DE PUBLICACIÓN

Autorizo a la Facultad de Gerencia Empresarial del Instituto de Altos Estudios Nacionales la publicación de esta Tesis, de su Bibliografía y anexos, como artículo de la Revista o como artículo para ser utilizado en revistas, documentos o como fuente de investigación.

Quito, junio del 2007

HUGO MARCELO DALGO PROAÑO