# SEGURIDAD DEL COMERCIO ELECTRÓNICO EN COLOMBIA DESDE UNA PERSPECTIVA JURÍDICA

**Fernando Arcesio Bolaños Ordóñez**

**John Edinson Martínez García**

**Directores**

Mg. Alejandro Hernández

Ing. Siler Amador Donado

Universidad del Cauca

Facultad de Derecho, Ciencias Políticas y Sociales

Facultad de Ingeniería Electrónica y Telecomunicaciones

Popayán, 2003

**Nota de Aceptación**

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Popayán 27 de Agosto de 2003

**A Dios,**
**a mis Padres y Hermanos**
**que siempre han sido mi motivación,**
**a mis amigos de Cali y compañeros**
**de la Universidad**

**John E**

**A Dios,**
**A mi Madre y a mi Padre,**
**a mi Universidad del Cauca**
**porque juntos me dieron la oportunidad**
**de realizarme como profesional**
**y como persona**

**Fernando**

## AGRADECIMIENTOS

La realización de este trabajo de grado fue posible gracias a la intervención de varias personas a las cuales queremos darles nuestros mas sinceros agradecimientos:

A los profesores Siler Amador Donado y Alejandro Hernández, nuestros directores de Trabajo de grado, quienes nos brindaron sus conocimientos, apoyo y amistad.

A nuestros profesores de la Facultad de Derecho e Ingeniería Electrónica que nos solucionaron dudas y generaron otras en pro de un mejor trabajo.

A nuestros compañeros y amigos de la sala de trabajo 340 quienes nos brindaron su amistad y entusiasmo en las largas jornadas.

El agradecimiento final hacia nuestra querida Alma Mater por acogernos a lo largo de estos años.

## CONTENIDO

## LISTA DE GRAFICAS

***Para que el comercio Electrónico se afiance, además de consagrar normas que protejan la seguridad jurídica se deben adoptar medidas de seguridad en los ambientes informáticos*.**

# INTRODUCCIÓN

El comercio ha evolucionado a lo largo de la historia apropiándose de los avances e inventos humanos para ser cada vez más efectivo y veloz, su último paso en ese continuo avanzar es el comercio electrónico. Esta innovadora forma de hacer negocios ha creado nuevos conflictos sobre su seguridad y confiabilidad, pues las vulnerabilidades de las tecnologías y la falta de regulación legal sobre el tema permiten que se incurra en conductas antisociales que perjudiquen a los usuarios. A raíz de la implementación de la Internet y su continuo afianzamiento entre las poblaciones del mundo, se hace necesario el planteamiento de soluciones tecnológicas que permitan brindar mayor seguridad y confianza en el comercio electrónico, así como también se hace necesario la creación y unificación internacional de una regulación legal de las conductas humanas que se realizan a través de la utilización de medios tecnológicos.

Lo que se plantea en el presente trabajo es un análisis sobre la seguridad jurídica y tecnológica del comercio que se realiza a través de Internet. Se plantearán soluciones a problemas que se han presentado en la aplicación del comercio electrónico y se darán opiniones y puntos de vista de los autores de este documento. Por lo novedoso y poco difundido del tema del comercio electrónico no existe una base jurisprudencial ni doctrinal que permitan dar respuestas a algunos interrogantes sobre la seguridad del comercio electrónico, lo mismo ocurre desde el punto de vista tecnológico.

La presente monografía de grado es realizada de forma multidisciplinaria entre las facultades de Derecho y de Ingeniería Electrónica, pretendiendo encontrar en la unión de los conocimientos jurídicos y tecnológicos un mejor análisis y planteamiento de soluciones sobre el tema central. Con respecto a la multidisciplinariedad, es un avance dentro de las formas de desarrollar una monografía de grado, pues cada vez mas los campos del saber se hacen más específicos pretendiendo una mayor profundidad del conocimiento, lo que hace necesaria la unión de campos del saber si se quiere que una investigación sea al mismo tiempo amplia y profunda. Se concluye que se deben implementar las tesis multidisciplinarias entre las facultades de nuestra Alma Mater.

Uno de los desafíos de la presente monografía es que, por estar dirigida tanto a los conocedores de la ciencia del derecho como a los conocedores de la ingeniería electrónica, el documento final debe ser de fácil entendimiento para ambos campos del saber, evitando en lo posible el exceso de palabras técnicas y explicando paso a paso los diferentes conceptos de cada campo del saber. Es por lo anterior que se incluye un glosario jurídico-tecnológico que permita al lector una mayor comprensión del documento. Por lo anterior se ruega a los lectores de este documento receptibilidad hacia los conceptos ajenos a su campo del saber.

Se pretende también con la presente monografía sentar un precedente doctrinal sobre la seguridad del comercio electrónico que pueda servir de consulta a futuros estudiosos del tema y de argumentación en litigios, así como para el planteamiento de futuras soluciones tecnológicas.

Se abarcará el análisis de la seguridad del comercio electrónico desde tres ramas del derecho que son: el derecho comercial, el derecho penal y el derecho comparado. Se analizará lo concerniente con el derecho comercial por tratarse lógicamente de una forma de hacer comercio que se apropia de muchas figuras jurídicas de esta rama del derecho como por ejemplo los títulos valores. Con el derecho penal es imprescindible su análisis pues muchas de las conductas que se realizan a través de la utilización de Internet y específicamente del comercio electrónico se constituyen como delitos, y finalmente con el derecho comparado porque el carácter globalizado de la Internet le han restado eficacia a las legislaciones de cada Estado haciendo necesaria la unificación internacional de legislaciones para obtener una mayor seguridad jurídica de comercio electrónico. Además, el documento plantea un análisis del estado actual de la seguridad de los sitios web colombianos empezando con los conceptos generales que intervienen en la seguridad para luego entrar a analizar las vulnerabilidades, ataques y efectos informáticos de los sitios Web para posteriormente hacer un análisis de casos de ataques informáticos con soluciones jurídicas.

Con esta breve introducción del tema y la forma de desarrollo del presente documento se empieza el análisis de la seguridad del comercio electrónico.

# CAPITULO I
# ANÁLISIS DE LA SEGURIDAD DEL COMERCIO ELECTRONICO

Internet ha sido comparada como una nueva invención de la imprenta de Gutemberg, como una nueva revolución industrial, que por sus efectos y alcances en todos los campos de acción del hombre ha modificado en un corto tiempo costumbres y métodos que estaban muy arraigados, como comprobación de esto basta con analizar como la Internet ha desplazado las administraciones postales, los faxes; ha variado la industria telefónica, la música, la pedagogía, la forma de hacer política y lo que será objeto de nuestro estudio ha modificado también la forma de hacer negocios. Estamos siendo partícipes de una nueva revolución, *La Revolución Digital.*

Como todo fenómeno cultural que implica necesariamente un desarrollo de conductas humanas debe entrar en acción el Derecho, como mecanismo regulador de esas conductas para impedir abusos y mantener el equilibrio social. Como suele ocurrir, primero surge el fenómeno y posteriormente el derecho entra a regularlo, ese es el desafío del legislativo y de los juristas, intentar avanzar al mismo paso que avanzan los fenómenos tecnológicos y culturales intentando dar solución a los conflictos que estos generan. Un ejemplo de esto es lo que está ocurriendo con el derecho médico. Los juristas se introdujeron en un campo que hasta hace muy poco era sagrado y totalmente ajeno a la ciencia jurídica y entraron a establecer responsabilidades legales a los médicos acerca de sus actos.

En el campo de la informática no podía ser diferente, ya que como se dijo anteriormente las nuevas tecnologías originadas en Internet han creado y modificado conductas que a su vez han generado nuevos conflictos de intereses que el Derecho debe entrar a regular para buscarles una solución. Es así como ahora se habla del Derecho Informático.

## 1. EL DERECHO INFORMÁTICO

El derecho Informático genera algunos interrogantes que merecen un detallado análisis. Se plantean entonces los siguientes interrogantes:

- ¿Qué es el Derecho informático?
- ¿Pertenece el Derecho informático al derecho público o al Derecho Privado?
- ¿Qué es Internet?
- ¿Qué clases de conflictos intenta resolver el Derecho Informático?
- ¿Se desvirtúa el factor territorial de la aplicación de la Ley debido al alcance mundial de la Internet. ?
- ¿Se debe contemplar el derecho informático en el contenido programático de los estudiantes de derecho, ingeniería electrónica y sistemas?

Estas son preguntas claves para poder crear una base de conocimientos y poder edificar posteriormente conceptos derivados del Comercio electrónico, eje central de este estudio.

Es difícil entrar a decir que se puede entender exactamente por derecho informático, pues la palabra “informático” puede ser objeto de dos interpretaciones:

Una primera, en la que se toma a la información por si sola. En la jurisprudencia de la Corte Constitucional se toma la palabra Informático refiriéndose a la información por si sola y la relaciona con derechos constitucionales como el derecho a la intimidad a la privacidad o con el derecho a la libertad periodística, sin hacer la más mínima referencia a la utilización de algún tipo de tecnología.

Una segunda interpretación es la que toma la información asociándola a la utilización de tecnologías, como podría ser Internet. Esto se ve por ejemplo en el Código Penal (Art. 195) en el que se toma la palabra “informático” para referirse a la utilización de tecnologías a través de computadores.

El punto común es que tanto la primera interpretación como la segunda tienen como objeto esencial la utilización y transformación de la información, por lo que se plantea entonces tomar la primera interpretación como el género y la segunda interpretación como la especie, puesto que en la información transmitida a través de Internet también se deben garantizar derechos constitucionales como el derecho a la intimidad, a la libertad

periodística y a la inviolabilidad de comunicaciones privadas que son los derechos que se tutelan en la primera hipótesis.

En este documento se hará énfasis en el concepto que hace referencia a la utilización de tecnologías, para poder centrarse en el tema a desarrollar que es el de la seguridad del comercio electrónico.

En Colombia existe una carencia de regulación legal y jurisprudencial, hasta el punto que hasta octubre de 2002 no existía ningún sindicado por delitos cometidos a través de Internet[1] y los únicos proyectos de ley respecto al Derecho Informático se refieren a derechos de autor y no al comercio electrónico, tal es el caso del proyecto de ley sobre software libre presentado por el congresista Gustavo Petro Urrego.

Según algunos autores jurídicos, se ubica al Derecho Informático dentro del Derecho Público, ya que es el Estado el encargado de garantizar la protección de derechos de los asociados que se vean amenazados por la aplicación de las nuevas tecnologías, como pueden ser el derecho a la privacidad, a la propiedad intelectual y algunas conductas que recaen en el campo penal. Al vulnerar bienes jurídicos protegidos por nuestra legislación penal como el Pánico Económico, y el acceso abusivo a un sistema económico consagrado en el Artículo 195 del Código Penal. En síntesis se puede decir que es el Estado el encargado de la promulgación de normas reguladoras para el uso de las nuevas tecnologías. Sin embargo el Derecho Informático también interactúa con el Derecho Privado, sobretodo tratándose del comercio electrónico donde lo que prima es la expresión de la voluntad de las partes en el momento de realizar negociaciones a través de Internet, la idea de libertad contractual pertenece eminentemente al campo del derecho privado.

Se asume una tesis ecléctica concluyendo que el Derecho Informático abarca tanto el campo del derecho privado como del derecho público. Tratándose del Comercio electrónico es indudable que como toda actividad mercantil se ubica dentro del derecho privado donde el Estado no interfiere como parte activa sino que es el encargado de velar

[1] Periódico Ámbito Jurídico de octubre de 2002. Separata especial " Seguridad del comercio electrónico"

por la correcta aplicación de la normatividad y tutelar los derechos que se puedan ver vulnerados por la mala aplicación de la informática.

Si es indudable la existencia y regulación jurídica que tiene el derecho informático este siempre debe propender por la unificación supranacional pues no es correcto concebir a cada Estado de manera independiente, como islas, con legislaciones cerradas frente a los otros Estados, sino que cada vez se hace más necesaria la unificación de normatividades, dado que la Internet no tiene fronteras estatales sino que es de cobertura mundial. Es por eso que la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) elaboró una ley modelo del Comercio Electrónico para que cada Estado la introdujera como una ley dentro de cada legislación interna y lograr en cierta forma la unificación internacional de la legislación en materia de Comercio Electrónico, en Colombia el texto de la ley modelo de la CNUDMI se introdujo en la ley 527 / 99. Con lo anterior es claro que los conflictos jurídicos relacionados con Internet desvirtúan el factor territorial de aplicación de la ley ya que una de las partes en conflicto o el posible infractor de una ley penal puede estar en el computador contiguo como puede estar al otro lado del mundo.

**Relación del derecho informático con otras ramas del Derecho.**

El Derecho Informático como todas las ramas del Derecho se interrelaciona con las demás formando parte de todo el sistema jurídico. Se verá a continuación la interrelación del Derecho Informático con las demás ramas.

***Con el Derecho Constitucional:*** Toma el derecho constitucional una amplia concepción del derecho informático abarcando toda clase de comunicación así esta no sea transmitida o almacenada a través de la utilización de tecnologías. La Constitución Política consagra el derecho a la información como un derecho fundamental y lo tutela a través del derecho de petición del artículo 26, el cual se puede explicar brevemente como la posibilidad que tiene todo ciudadano de elevar peticiones respetuosas ante cualquier autoridad para obtener información correcta y concreta sobre cualquier asunto. También protege la Constitución Política el derecho a la información en el artículo 20 referente a la libertad de opinión, prensa e información, y en el artículo 73 al consagrar la libertad e independencia de la actividad periodística.

***Con el Derecho Internacional:*** Como se decía anteriormente, es fundamental que existan normatividades internacionales que unifiquen las legislaciones internas para saltar los obstáculos presentados en los litigios del derecho informático debidos a la globalización de la Internet. Es por esta razón que se creó dentro de la Organización de Naciones Unidas la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), que cumple funciones de entidad supranacional en pro del comercio internacional.

***Con el Derecho Penal:*** El Código Penal, Ley 599 de 2000 establece tipos penales que tipifican conductas realizadas a través de nuevas tecnologías. Mas adelante se dará una detallada explicación del Derecho Penal con el Derecho Informático.

***Con el Derecho Civil:*** Hay interrelación en la celebración de negocios jurídicos como compraventas y permutas civiles, actos relacionados con la propiedad intelectual (derechos de autor) realizados a través de la utilización de un medio tecnológico, el más común seria el de Internet.

***Con el Derecho Comercial:*** En actividades como el comercio electrónico y los títulos valores electrónicos, compraventa comercial, suministros, propiedad industrial y transacciones bancarias.

***Con el Derecho Fiscal:*** A través de la implementación de facturas electrónicas y declaraciones tributarias a través de Internet, además de la facultad que tienen las personas jurídicas de organizar el registro de actividades comerciales en cintas magnetofónicas.

Se acaba de ver como el derecho informático justifica su existencia en el estudio y la consiguiente regulación de toda clase de ingerencia entre el derecho y las nuevas tecnologías en áreas como las telecomunicaciones, la propiedad intelectual, la teoría general de los contratos, el derecho penal, las garantías de los derechos fundamentales como el derecho a la privacidad y el derecho al habeas data. Todo lo anterior tiene como objeto “la información” la cual se debe proteger por tratarse de un bien jurídico.

**Utilización de la Internet.**

Todo lo relacionado con el Derecho Informático utiliza el mismo canal de comunicación de Internet, la cual deja de percibir a los computadores como máquinas aisladas para permitir la interacción de estos y lógicamente el intercambio de toda clase de información.

Internet es una red de computadores que permite la comunicación de manera global. Es por eso que al referirnos a Internet lo hacemos con el artículo "la" pues nos estamos refiriendo a una red. La noción más simple es la de una red de redes, como una telaraña de redes de telecomunicaciones, servidores, y computadores personales.

**Características de Internet**

Las características principales de Internet según la doctrina jurídica son:

**1. La conectividad:** es decir que cualquier punto o nodo se puede comunicar con otro punto de la red.

**2. La multiplicidad:** Cada uno de los nodos tiene multiplicidad de dimensiones y de formas de transmisión.

**3. Metamorfosis**: La red esta en continuo cambio y crecimiento.

**4. La movilidad de Centros:** No existe un punto central fijo sino una posibilidad múltiple de acceso y transición de la comunicación.

**5. Ruptura:** Si algún tramo de la red es interrumpido esto no afecta el resto de la red, pues Internet esta soportada en parte sobre la red telefónica pública conmutada. Por ejemplo si un ISP es bloqueado y no puede ofrecer servicio, los usuarios cuyo servicio es proveído por otro ISP podrán continuar en Internet.

**6. La convergencia de tecnologías:** No se puede concebir a la Internet como una máquina autosuficiente e independiente, sino que para lograr su cabal funcionamiento requiere de las telecomunicaciones tal es el caso de una línea telefónica, también requerirá de un computador y de toda la ciencia del software. Lo interesante entonces es la interacción de todas estas tecnologías que conforman y desarrollan la Internet..

Según todas las descripciones y comentarios sobre el Derecho Informático este se debe tomar en cuenta como una cátedra dentro de la formación de profesionales de Ingeniería y Derecho, esto con la finalidad de presentar propuestas de soluciones más completas a los conflictos generados a raíz de este.

## 1.1 EL DERECHO INFORMÁTICO Y EL DERECHO COMERCIAL

### 1.1.1 EL COMERCIO ELECTRÓNICO

De manera somera se puede decir que el Comercio Electrónico es todo intercambio de bienes y servicio con fines lucrativos, que se realiza valiéndose de la Informática al utilizar canales de comunicación como Internet.

En Colombia fue expedida por el Congreso de la República la ley 527 de 1999 que regula el uso y acceso de los mensajes de datos, el comercio electrónico, las firmas digitales y las entidades de certificación. Estos cuatro elementos que se acaban de mencionar serán objeto de análisis en este capítulo.

La Ley 527 de 1999 se puede decir que es una fiel copia de la ley modelo del comercio electrónico elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), lo que hizo el Congreso Colombiano fue transcribirla y adicionarle unos artículos referentes al Contrato de Transporte, tema este que no se desarrolla en la Ley Modelo y que se analizará en el anexo D.

No es válida la apreciación de restarle importancia a la Ley 527 / 99 argumentando que es una copia de la legislación extranjera que no es aplicable materialmente en nuestro Estado. Por el contrario lo que se pretendía al elaborar una ley modelo por parte de las Naciones Unidas era que todos los Estados la incluyeran dentro de su legislación interna para facilitar su aplicación a nivel internacional esto por el carácter globalizado del comercio electrónico a través de Internet. Es así como en el Artículo 3 de la Ley 527 / 99 dice: "*Interpretación: En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe. Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ellas, serán dirimidas de conformidad con los principios generales en que ellas se inspiran*". (Subrayado fuera del texto)

La ley 527 / 99 fue el producto de un proceso en el que participaron los sectores público y privado que tuvieron asiento en la comisión redactora de la que también formaron parte

los ministros de justicia y del derecho, transporte, desarrollo económico y comercio exterior, es de tener en cuenta que el ministerio de comunicaciones no tuvo participación en la elaboración de la Ley.

Continuando con el análisis del comercio electrónico se han determinado dos clasificaciones generales:

**a. Comercio electrónico directo:** Es cuando la entrega del bien se realiza a través de la red, se entiende entonces que los bienes que ofrece el vendedor son intangibles, como lo seria información que puede viajar en forma de un mensaje de datos.

**b. El Comercio electrónico indirecto:** La entrega del bien se realiza por medios tradicionales como el correo o el trasporte de mercancías.

Otra forma de clasificación del comercio electrónico es:

**a. Comercio electrónico completo**: Es la relación de comercio electrónico en el cual el pago se realiza a través de medios electrónicos utilizando pasarelas de pago, como las que soportan entidades como Visa y Mastercard.

**b. Comercio electrónico incompleto:** Es aquel en el que el pago se realiza utilizando medios tradicionales, como contra-entrega o consignación en cuentas bancarias.

El comercio directo e indirecto hacen referencia a la entrega del bien, mientras que el completo e incompleto se refieren a la forma de pago, por lo que se puede entonces dar interacciones entre estas clasificaciones. Por ejemplo: comercio electrónico directo y completo: que se da cuando compro un programa de computador, lo descargo de Internet y pago con tarjeta virtual utilizando la pasarela de pagos.

Respecto al recibo que garantice el pago del precio en el comercio electrónico completo, se puede enviar un mensaje de datos digitalmente firmado que pueda servir de factura, además se crea en la pasarela de pagos un registro de la transacción.

Estas clasificaciones modifican *sin desvirtuar la esencia* los conceptos clásicos del derecho civil sobre el negocio jurídico como lo seria la compraventa o la permuta.

El comercio electrónico directo desvirtúa el artículo 1929 del Código Civil que regula el lugar de pago del precio, surgen dudas sobre el momento de perfeccionarse la Tradición consagrada en el artículo 740 del Código Civil. también surge la pregunta de cuál será el valor probatorio del contrato de compraventa y donde queda registrada la voluntad de las partes que es la que perfecciona el contrato, son preguntas estas que quedan abiertas por no existir suficientes bases legales y doctrinales que les permitan dar respuesta.

Lo que se pretende mostrar es como, si a diario surgen litigios sobre el contrato de compraventa que atestan los juzgados civiles y aquellos que conocen de controversias comerciales, surgirán más conflictos al realizar negocios de compraventa a través de la Internet teniendo en cuenta que no hay interacción directa de las partes, pese a esto deberán aplicarse igualmente conceptos del derecho como las acciones y obligaciones propias de los negocios jurídicos. El inconveniente surgiría cuando choquen dos legislaciones internas de derecho privado por encontrarse las partes en diferentes Estados, en caso de que esto ocurra, la solución más adecuada es la de acudir a un tribunal arbitral internacional que dirima el conflicto, pero por los altos costos que representa el acudir a un arbitro se hace de muy difícil acceso a los casos cotidianos de choques de legislaciones internas, tema que se ampliara al final del capítulo IV.

Otra clasificación del Comercio Electrónico según los agentes económicos que intervienen en los negocios son:

**Comercio electrónico negocio a negocio (B2B):** Es el intercambio de servicios y bienes entre dos o más empresas, ya sea de forma directa o indirecta como podía ser la negociación de información o de maquinaria respectivamente, esto implicaría que cada empresa constituiría un e-business entendido este como una categoría de Internet, como también lo serian e-government y e-commerce.

**Comercio Electrónico de Empresa a consumidor (B2C):** Permite el suministro de bienes y servicios a los consumidores.

**Comercio electrónico entre consumidores (C2C):** Es la interacción de consumidores a través de intermediarios que realizan martillos y remates que tienen unos claros reglamentos prefijados que buscan darle seguridad jurídica a la realización de la transacción. Un ejemplo de esto es Deremate.com. quien no actúa como parte del negocio jurídico sino que facilita el acercamiento de las partes dando la posibilidad de ofrecer productos y de comprarlos.

¿Se puede entonces según nuestra legislación catalogar como comerciante a Deremate.com y empresas similares?

La respuesta se empieza a encontrar en el artículo 10 del Código de comercio que dice *"Son comerciantes las personas que profesionalmente se ocupan en alguna de las actividades que la ley considera mercantiles"*. La palabra *"profesionalmente"* se debe entender según reiterada jurisprudencia como "habitualmente". El mismo Código en el artículo 20 numeral 7 consagra como mercantiles las operaciones de martillo y finalmente el artículo 13 dice que se presume que una persona ejerce el comercio cuando tiene un establecimiento de comercio abierto al publico, en el caso de estas empresas si existe un establecimiento de comercio que la doctrina los denomina establecimientos de comercio virtuales que se ampliara más adelante. En conclusión de la simple lectura de los tres artículos acabados de citar se deduce que entidades como Deremate[2] y demás empresas que ofrecen bienes ajenos al público si pueden ser catalogados según nuestra legislación como comerciantes. Existe de forma similar el sitio web ventadegaraje.com que tiene sus instalaciones físicas en la ciudad de Popayán pero que su dominio no fue obtenido a través de la Universidad de los Andes, que es la entidad encargada de registrar los dominios en Colombia, este sitio es un establecimiento de comercio virtual según nuestra legislación y deberá cumplir con las obligaciones legales de los establecimientos de comercio tradicionales[3].

[2] http://colombia.deremate.com

[3] Respecto de las obligaciones tributarias de los sitios web que no tienen dominio colombiano se elevo un derecho de petición al administrador del dominio ".co", que es Uniandes cuya respuesta da sustento a lo planteado en el documento. El texto del derecho de petición se encuentra en el Anexo L.

### 1.1.2 LOS MENSAJES DE DATOS

Estos son definidos por la misma ley 527/99 en su Artículo 2 que dice: *"se entenderá por mensajes de datos la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".*

El intercambio electrónico de datos (EDI) lo define la misma ley como: "*La transmisión electrónica de datos de una computadora a otra que está estructurada bajo normas técnicas convenidas al efecto*", las normas técnicas pueden ser los protocolos de telecomunicaciones definidos por la ISO[4].

Es un concepto muy amplio el que presenta la ley sobre mensaje de datos lo que permitirá aun utilizando el riguroso método exegético ubicar jurídicamente muchos elementos de la informática.

Lo importante de la ley de comercio electrónico en Colombia sobre mensaje de datos es que se ha previsto que cuando la ley requiere que la información conste por escrito, ese requisito queda satisfecho con un mensaje de datos, si la información que este contiene es accesible para su posterior consulta. Al igual que los documentos físicos se puede presentar falsificaciones de los mensajes de datos, es estos casos existe jurídicamente la posibilidad de tacharlos de falsos y entrar a demostrar a través de un perito informático la veracidad del mensaje de datos.

### 1.1.3 LA FIRMA ELECTRONICA

La información que viaja a través de redes de información se encuentra en gran medida amenazada por la inseguridad que le produce el mismo entorno tecnológico. Se presentan inseguridades como ataques con virus, sabotajes, bloqueos de canales de información y robos de información con las consecuencias económicas que estos ataques generan.

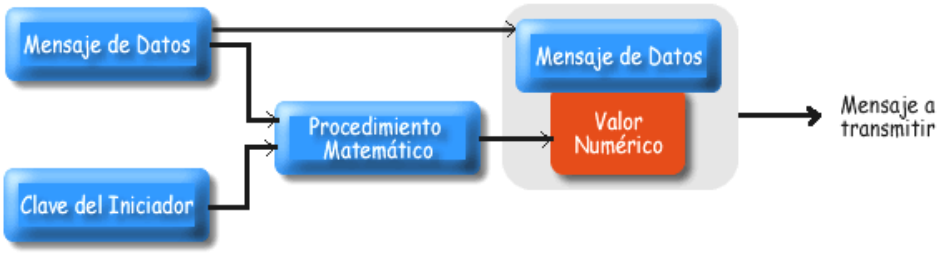
[4] ISO: International Organization for Standardization

Se utilizan para proteger la información mecanismos de seguridad informática como lo son los programas antivirus, sistemas de detección de intrusos y lo que será objeto de este análisis: las firmas electrónicas.

Lo que pretende toda firma, no solo la firma electrónica sino también la firma tradicional es identificar el autor de determinado acto jurídico o simplemente identificar a la persona que suscribe un documento. El artículo 826 del Código de Comercio define la firma como: *"La expresión del nombre del suscriptor o de alguno de los elementos que la integren o de un signo o símbolo empleado como medio de identificación*". También es función de la firma el asegurar la prueba de la existencia del contrato.

Aunque nuestra legislación no haga diferencias, de forma puramente pedagógica se ha diferenciado entre firma electrónica y firma digital. La firma electrónica es todo sistema de identificación como el utilizado por las tarjetas de crédito o una firma manuscrita reproducida por medio de un scanner. La firma digital busca lograr la identificación de una persona en redes abiertas como lo es Internet. Pero no es una firma convencional como podría serlo la firma mano-escriturada y escaneada, sino que es un algoritmo matemático, un valor alfanumérico codificado.

La ley 527/99 en el artículo 2 se encarga de definirla así: "*Se entenderá como un valor numérico que se adhiere a un menaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que ese valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transacción*". Gráficamente se puede explicar de la siguiente manera:




**Gráfica 1 Mensaje de Datos.**

La misma ley en el artículo 7 dispone que cuando en un mensaje de datos se requiera de una firma este requerimiento quedará satisfecho sí:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos
b) Sirva para indicar que el contenido cuenta con su aprobación.
c) Que el método utilizado sea confiable y apropiado.

El artículo 7 de la ley 527/99 lo que consagra es una categoría jurídica y no un tecnicismo, con esto queremos explicar que no se obtendrá un resultado igual siempre que se presente una situación de conflicto, sino que por el contrario será un juez el que en cada caso concreto haga un análisis de la tecnología empleada en la firma y logre establecer si cumple con los tres requisitos planteados por la ley.

La doctrina ha establecido tres categorías de firma electrónica que son:
Firmas basadas en:

- **Algo que usted sabe.** Tal es el caso de las contraseñas (password)
- **Algo que usted posee**. Como ocurre con los microchip y las tarjetas bancarias que funcionan con una banda magnética.
- **Algo que usted es**. Es el caso de los métodos de identificación a través de rasgos físicos (identificación biométrica) como las huellas digitales, reconocimiento de la estructura ósea del rostro, escaneo del iris del ojo o reconocimiento del timbre de la voz.

Según los requisitos de la ley 527/99 que se plantearon anteriormente estas tres categorías pueden ser catalogadas como firmas electrónicas por nuestra legislación.

La parte tercera de la ley se refiere a las firmas digitales y en el artículo 28 señala los atributos jurídicos de una firma digital, dicho artículo reza así:

***Artículo 28. Atributos jurídicos de una firma digital***.

*"Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.*

***Parágrafo****. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:*

1) *Es única a la persona que la usa.*
2) *Es susceptible de ser verificada.*
3) *Está bajo el control exclusivo de la persona que la usa.*
4) *Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.*
5) *Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional".*

Como se aprecia en la lectura de la norma, esta consagra una presunción legal que afirma que cuando un mensaje de datos lleva una firma digital *se presume* que el suscriptor del mensaje tenia la intención de firmarlo, es decir que se presume la libre expresión de la voluntad del autor del mensaje que acepta tener un vínculo con el contenido del mismo. Lógicamente al tratarse de una presunción de carácter legal se admite prueba en contrario y deberá entrar el suscriptor a demostrar que no era su firma digital o que así haya sido su firma él no había suscrito el mensaje de datos o que existió un vicio en el consentimiento y así él haya firmado el mensaje de datos no había una libre expresión de su voluntad.

EL artículo 28 de la Ley 527/ 99 que se está desglosando fue regulado por el artículo 15 del decreto 1747 de 2000. Este decreto reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las Entidades de certificación, los Certificados y las Firmas digitales. Dicho artículo crea las llamadas firmas digitales certificadas, que son firmas avaladas o respaldadas por certificados digitales emitidos por una entidad de certificación. Si la firma digital está certificada no será necesario entrar a probar los atributos del parágrafo del artículo 28 de la ley 527 / 99, esos cinco atributos a los que se ha hecho mención sirven para establecer una equivalencia entre la firma manuscrita y la firma digital, estos criterios son entonces los requisitos para la validez de la firma digital. Por el contrario, si la firma

digital no está certificada por una Entidad de Certificación el interesado deberá probar la presencia de los atributos de validez que consagra el parágrafo del artículo 28 de la ley 527/99.

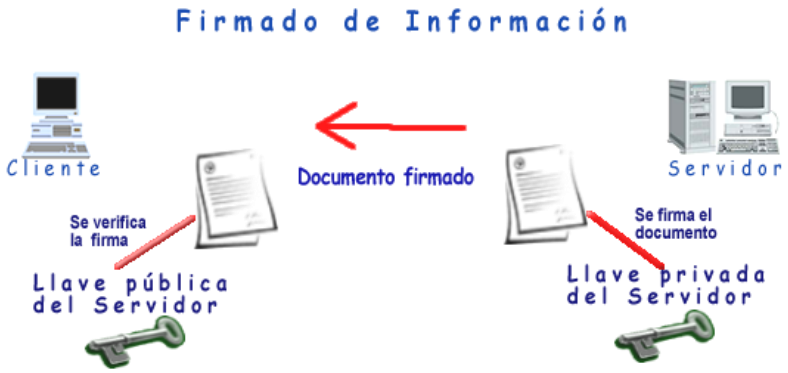
***Criptografía de llave asimétrica ( Teoría de las dos llaves)***

Se puede establecer una diferencia entre cifrado y firma de información. En lo que concierne al cifrado de información se necesita de dos llaves, una Pública de conocimiento general con la cual se puede cifrar la información que va a ser enviada a un usuario y de una llave privada que solo conoce el destinatario de la información y que permite de forma exclusiva y excluyente descifrar la información.

Se podría comparar con un casillero con dos puertas, cada una con su llave, por la puerta de un extremo alguien con una llave conocida por todos introduce un paquete y posteriormente el dueño del casillero lo abre o retira utilizando la otra puerta ubicada en el otro extremo con su llave privada.


**Gráfica 2**

En lo referente a la firma de información las dos llaves cumplen funciones diferentes al caso del cifrado. La llave Pública permite verificar la autoría de la firma mientras la llave privada permite de forma exclusiva y excluyente la realización del firmado de la información.




**Gráfica 3**

Las llaves Pública y privada son complementarias, al escribir el número secreto este se registra en una tarjeta inteligente o un programa software donde también se almacenan datos generales del firmante como el nombre, apellido, empresa, ocupación y la firma, a estos datos solo tiene acceso el firmante y no tiene acceso la empresa certificadora. Cada tarjeta o software es un verdadero procesador, es decir un computador que brindará una alta confiabilidad y mucha más seguridad jurídica que una firma manuscrita, pues la firma digital es de muy difícil falsificación o clonación.

### 1.1.4 LAS ENTIDADES DE CERTIFICACION

Son definidas por la ley 527 / 99 así "*Es aquella persona que autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transacción y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales*".

Lo que hace una entidad de certificación es dar fe de que a determinada persona corresponde determinada firma digital. Esto lo hace a través de métodos tradicionales como la presentación personal de documentos de identificación. Posteriormente se emite un Certificado Electrónico que garantiza al público que esa clave pública pertenece a la persona registrada en el certificado.

Las facultades de las Entidades de Certificación según el Artículo 30 de la Ley 527 / 99 son dos: A) emitir los Certificados Electrónicos y B) prestar el servicio de registro de la transmisión y recepción de mensajes de datos.

El decreto 1747 / 2000 en su artículo primero numerales 8 y 9 hizo una distinción entre Entidades de Certificación Abierta y Entidades de Certificación Cerrada, se hace la crítica de que dicha distinción deja muchas dudas y que no era necesaria, mas aun si se tiene en cuenta el *Principio minimista* que expresa que los Estados que adopten la Ley modelo de Comercio electrónico, no deben crear requisitos adicionales para las firmas electrónicas, y en si para todo el contenido de la ley modelo, porque si cada Estado lo hiciera se desvirtuaría el concepto de "ley modelo" que pretende la unificación internacional de la legislación del comercio electrónico.

Los numerales a los que se hace referencia expresan:

***Decreto 1747 / 00***

**Artículo 1**. "*Definiciones. Para efectos del presente decreto se entenderá por:*

*# **8. Entidad de certificación cerrada**: Entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.*

*# **9. Entidad de certificación abierta**: La que ofrece servicios propios de las entidades de certificación, tales que:*

*a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o*
*b) Recibe remuneración por éstos".*

Al respecto la Superintendencia de Industria y Comercio estableció que la razón por la que el gobierno había hecho la distinción entre entidades abiertas y cerradas era para indicar que las Entidades de Certificación cerradas no están destinadas para prestar servicios públicos[5].

[5] Concepto de la Superintendencia de Industria y Comercio número 02058647 del 31 de Julio de 2002.

Con respecto a las Entidades de Certificación ubicadas en el exterior, es muy posible que existan firmas digitales de nacionales que estén respaldadas por Entidades de Certificación que operan desde el exterior y que además no están autorizadas para operar en Colombia; la pregunta es entonces: ¿Que ocurre con la validez de las firmas digitales que están siendo respaldadas por una entidad extranjera que no este autorizada para operar conforme a nuestra legislación?. Al respecto se manifestó la Superintendencia de Industria y Comercio y dijo que dichas firmas serán validas en nuestro país porque los artículos 7 y 28 de la ley 527 que se analizan cuando se habla de firmas digitales no requieren del respaldo de un certificado digital, pues este sirve es para dar por probados los cinco atributos del artículo 28 de la ley 527 / 99 y que en los casos de estas firmas respaldadas por entidades extranjeras no autorizadas se hace necesaria la demostración de estos atributos del artículo 28 que son: que la firma digital es usada por una sola persona, que esta firma es susceptible de ser verificada, que está bajo el control exclusivo de la persona que la usa, que si se cambia el mensaje la firma queda invalida y que está conforme a la reglamentación adoptada por el gobierno nacional.

Es importante decir que existen dudas en torno a la asunción del riesgo ante una falla o error en las telecomunicaciones, se podría pensar con justa razón que dado el carácter profesional de la prestación de estos servicios la responsabilidad debería ser objetiva, sin embargo las empresas que prestan estos servicios no admiten la *Responsabilidad Objetiva* porque lógicamente podrían verse afectadas económicamente, lo que ocurre en la práctica es que adoptan una *Responsabilidad Subjetiva* donde se analiza cada caso concreto para determinar la posible responsabilidad por parte de la Entidad de Certificación y entrar así a resarcir el daño a través de una indemnización pecuniaria.

Cabe anotar que la Corte Constitucional en la sentencia C - 662 / 2000 dijo: "*Ni el comercio electrónico ni la actividad de las entidades de certificación son un servicio público, pues las partes no se encuentran en la obligación ni en la necesidad de solicitar los servicios de una entidad de certificación para la celebración de un negocio jurídico. Por el tipo de relaciones que regula, se trata de un asunto de la órbita del Derecho Privado que, por supuesto, precisa de un control estatal, que estará a cargo de la Superintendencia de Industria y Comercio, que vigila a las entidades de certificación desde el punto de vista técnico y operativo".*

La Superintendencia de Industria y Comercio estableció como plazo perentorio el treinta y uno de enero de 2003 para poder solicitar la autorización ante esta entidad para operar como Entidad de Certificación, lo anterior según la circular 19 que prorrogó el plazo establecido en la circular única.

A mayo de 2003 las entidades de certificación que se encuentran autorizadas por la Superintendencia de Industria y Comercio son: Aeronáutica Civil, Instituto Colombiano de Codificación y Automatización Comercial, Banco de la República y Certicamara S.A., esta ultima es la única Entidad Certificadora abierta[6].

La función de las Entidades de Certificación es fácilmente confundible con la actividad notarial, pues la función notarial consiste en dar fe de los actos de los particulares logrando la autenticidad de los negocios jurídicos y así poderlos constituir en prueba. Con base en esta similitud entre las Entidades de Certificación y las Notarias se demandó en *Acción de Inconstitucionalidad* la integridad del texto de la ley 527 / 99 que resolvió la Corte Constitucional en sentencia C 662 de julio 8 de 2000 cuyo magistrado ponente fue el entonces magistrado Fabio Morón Díaz.

La trasgresión constitucional que argumenta la parte demandante es que sé esta vulnerando los artículos 131, 152 y 153 de la Constitución Política.

La trasgresión del artículo 131 de la Constitución Política en criterio de la parte actora, se produce, en cuanto las normas acusadas crean unas entidades de certificación las que, de conformidad con la misma Ley 527 de 1999, están facultadas para emitir certificados en relación con las firmas digitales de las personas y para ofrecer los servicios de registro y estampado cronológico, la de certificación de la transmisión y recepción de mensajes de datos, así como cualquier otra de autenticación de firmas relativas a las comunicaciones basadas en firmas digitales, a emitir certificados en relación con la veracidad de firmas digitales de personas naturales o jurídicas y, en fin, a realizar actos que son propios de la *función fedal*, la que, según el entendimiento que da a la norma constitucional antes citada, es del soporte exclusivo de los Notarios, únicos depositarios de la fe pública.

[6] http://www.certicamara.com, http://www.aerocivil.gov.co, http://www.iaccolombia.org, http://www.banrep.gov.co.

La Corte argumentó que “Los cargos de la demanda resultan infundados porque las entidades de certificación no prestan un servicio público y menos dan fe pública. Las entidades de certificación no son notarías electrónicas, pues no sustituyen ni prestan los mismos servicios” .

Las Entidades de Certificación prestan una función eminentemente técnica que propende por la seguridad en los mensajes de datos.

Tampoco es fundado argumentar que los servicios públicos solo pueden ser prestados por entidades oficiales, esto seria contradictorio de los fines de nuestro Estado social de derecho consagrados en el Artículo segundo de la Constitución Política. Actualmente se ve como la prestación de los servicios públicos principalmente el de telefonía son prestados por entes privados.

En el caso hipotético de que las Entidades de Certificación dieran fe publica, esto tampoco seria un impedimento para que esta función fuera asignada a un ente privado, pues la ley no consagra dicha limitación, tal es el caso de las notarias que cumplen una función pública sin ser entes oficiales sino que son personas naturales que pertenecen al Derecho Privado.

### 1.1.5 LA RESPONSABILIDAD DE LOS ACTOS EN INTERNET

Como todo acto de la persona humana que debe estar regido por normas jurídicas para evitar abusos y violaciones, los actos en Internet tienen unas consecuencias legales que generan una responsabilidad, responsabilidad que finalmente se transformará en sanciones patrimoniales o en sanciones personales ya sea que se esté hablando de responsabilidad civil o responsabilidad penal respectivamente.

Se había planteado anteriormente como el Derecho Informático pretende proteger la Información como un bien jurídico. En legislaciones extranjeras se ha regulado la responsabilidad legal derivada de este bien jurídico cuando han ocurrido casos de mensajes difamatorios que afectan la honra de un particular. El caso es el siguiente: en una página web que ofrece el servicio de opinión sobre temas de interés, ingresa un usuario y envía mensajes difamatorios, groseros y obscenos referidos a una determinada

persona. En este caso la Corte de Inglaterra determinó que “la empresa que presta los servicios de hosting (hospedaje) no puede eximirse de responsabilidad, después de haber sido fehacientemente notificada de la existencia de los mensajes en su servidor”. La doctrina jurídica de varias partes del mundo ha concluido que no es coherente derivarle responsabilidad a las empresas que prestan el servicio de hospedaje pues al existir miles y miles de páginas, la responsabilidad legal se vuelve subjetiva, es decir que se debe entrar a probar la culpa o el dolo de la empresa que presta los servicios de hosting para poder derivarle responsabilidad legal, que se transformaría finalmente en una indemnización pecuniaria.

La posición de la responsabilidad subjetiva que plantea la doctrina jurídica internacional no tiene en cuenta el concepto tecnológico ya que se podrían aplicar filtros software que eviten que palabras o frases consideradas obscenas se encuentren en las páginas hospedadas lo que haría que la responsabilidad se inclinara más hacia la responsabilidad objetiva, pero no de forma plena pues la ausencia de palabras o frases obscenas no impide que se cometan injurias o calumnias contra el buen nombre y la dignidad de las personas.

Al existir un riesgo de daño, si este ocurre debe necesariamente existir una responsabilidad legal, y si hay una responsabilidad lo más adecuado es que la asunción del riesgo la asuma una entidad aseguradora a través de una póliza de seguro, es por eso que se están expidiendo nuevas pólizas donde se incluyen daños producidos por: violación de la propiedad intelectual, transmisión de virus, violación de la privacidad, difamación y mal uso de la información.

### 1.1.6 NATURALEZA JURÍDICA DE UN SITIO WEB.

Las páginas de Internet son la forma como se presenta la información de una empresa de Internet, entonces por ser esta la principal herramienta que se utiliza para la realización del comercio electrónico se hace necesaria establecer su naturaleza jurídica.

Un sitio web no es lo mismo que una página web aunque a veces se utilizan como sinónimos. Un sitio web esta formado por un conjunto de páginas web a las que se pueden acceder por medio de un enlace (link) o a través de la dirección electrónica de la

página. Por ejemplo al ingresar al sitio web de la Universidad del Cauca cuya URL es http://www.unicauca.edu.co lo primero que se ve es la página principal que en la que se muestran los diferentes contenidos del sitio, al dar clic en uno de estos iconos se sigue navegando dentro del sitio web pero se ingresa a otra página de este, por ejemplo: http://www.unicauca.edu.co/~gseguridad.php, que corresponde a la página del área de seguridad del sitio web de la Universidad del Cauca.

Se puede catalogar un sitio web como un establecimiento de comercio sui-generis, es decir como un establecimiento de comercio muy especializado y que no se puede catalogar dentro del género clásico de los establecimientos de comercio planteados por el Código de Comercio. Además también se la considera como una obra intelectual que requiere la protección de los derechos de autor.

El Código de Comercio (Decreto 410 de 1971) en el artículo 515 dice: "*Se entiende por establecimiento de comercio el conjunto de bienes organizados por el empresario para realizar los fines de la empresa. Una misma persona podrá tener varios establecimientos de comercio y a su vez un solo establecimiento de comercio podrá pertenecer a varias personas y destinarse al desarrollo de diversas actividades* ".

Aunque la ley es clara y precisa en la definición, es conveniente aclarar que no se debe confundir establecimiento de comercio con local comercial, pues por local comercial nos referimos al inmueble destinado a un establecimiento de comercio. Tampoco es correcto atribuirle la calidad de persona jurídica a un establecimiento de comercio como lo hacen otras legislaciones como la alemana pues nuestra legislación se limita a reconocerlo como una universalidad jurídica.

Con lo anterior surge el interrogante de si un establecimiento de comercio físico tiene un local comercial, así mismo se puede asimilar las páginas de un sitio web como un local comercial virtual. Esto para poder determinar hasta donde tiene libertad de ingreso los usuarios del sitio web. Al respecto no existe ningún precedente que de solución al interrogante. La respuesta que se plantea en este documento se basa en un simple análisis analógico con los locales comerciales físicos y se responde que está permitido el ingreso de los usuarios hasta donde lo permita el local comercial avanzando mas en la

respuesta lo importante no es a donde se ingrese sino el posible daño o perjuicio que pueda causarse dentro de este es decir que aquí se debe tener muy en cuenta la intención dolosa del usuario.

Los elementos del Establecimiento de Comercio son:

- La enseña y el nombre comercial. La enseña según la legislación mercantil (Decisión 486/00 de la CAN[7]) es el signo que utiliza el empresario para identificar su establecimiento. En el caso de un sitio web el nombre de dominio cumple la función de nombre comercial.
- Las marcas de productos y servicios. En el caso del comercio electrónico se genera un riesgo para el empresario que no tiene su marca registrada en Colombia pues se pueden cometer infracciones contra dicha marca. Para el consumidor existiría el riesgo de ser confundido sobre el origen de dichos bienes y servicios.
- Las mercancías. Entendidas como los bienes a comercializar, ubicando dentro de estos a la información como un bien mueble.
- El mobiliario y las instalaciones. Que permiten desarrollar la actividad mercantil. Acondicionándolo a los sitios web este elemento puede ser muy simple o no existir.
- Los derechos del Empresario sobre las invenciones o creaciones industriales o artísticas que se utilicen en las actividades del establecimiento.
- El derecho a impedir la desviación de clientela y la protección de la fama comercial. Con respecto a este derecho es de analizar ¿qué ocurre en los casos en los que al abrir una página web determinada aparecen links que muestran otras páginas de temas totalmente diversos que lo que logran es desviar la clientela y puede atentar contra el buen nombre del sitio web? Seria posible entonces a través de la aplicación de la ley comercial adelantar una acción preventiva o condenatoria contra esta forma de ofrecer productos que constituiría competencia desleal según lo consagra el artículo 8 de la Ley 256 /96 que regula el tema de la competencia desleal.

Se afirma que un Sitio web es un establecimiento de comercio sui-generis porque las negociaciones se establecen a través de un medio electrónico que evita la mediación directa de las partes, es por eso que la doctrina jurídica habla de Establecimiento de

[7] CAN: Comunidad Andina

Comercio virtual. Surgen algunas complicaciones al respecto pues se debe determinar cuando se trata de un establecimiento comercial virtual que opera como tal en Colombia o se trata mejor de almacenes virtuales que están establecidos y operan fuera de Colombia lo que impediría la aplicación de la legislación colombiana.

Para la creación de un sitio de Internet se deben observar procedimientos legales y tecnológicos:

**A).** Desde el punto de vista legal se debe obtener un nombre de dominio. A nivel internacional existe la International Corporation for Assigned Names and Numbers[8] que es una entidad privada, esta entidad ha delegado sus funciones en otros registradores quienes tiene la capacidad de otorgar los nombres de dominio, para el caso colombiano estas funciones son ejercidas por la Universidad de los Andes.

**B).** Desde un punto de vista tecnológico requiere una serie de actividades que tendrán en algunos casos repercusiones en el campo jurídico.

Entre esas actividades de creación de un sitio de Internet se encuentran:

**El diseño del sitio**: Esto implica la creación de logotipos, marcos, enlaces y demás diseños gráficos y ayudas de navegación que son los que observaran los visitantes al sitio.

**Desarrollo de códigos:** Para todas las interacciones de los sitios Web como los contadores de visitantes, relojes y animaciones interactivas, es necesario realizar una codificación en un lenguaje de programación, tal es el caso de las inserciones de código realizado en lenguaje de programación Java en las páginas Web.

**Integración del sistema:** Es hacer del sitio de Internet un tramo más de la red, integrándolo con buscadores de páginas, portales de comercio, o cualquier otro relacionado con el sitio web que se este creando.

[8] Organización que adopto las funciones de la IANA.

En estos tres aspectos que se acaban de referir se manejan los derechos de autor, se podría decir a manera de ejemplo que la persona natural o jurídica que realice el diseño de la página web tendría derecho sobre esa creación intelectual logrando con esto que no pueda ser utilizada sin autorización por otras personas, esto según la ley 23 de 1982 sobre derechos de autor que en su artículo 4 dice "Son titulares de los derechos reconocidos por la ley: a) El autor de la obra. Pero tratándose de sitios web ha hecho carrera la tesis de que se ceden los derechos de autor que existan a raíz de la construcción de un sitio web, pasando su titularidad a los propietarios del sitio, lo anterior lo realizan basándose en el artículo 20 de la misma ley que dice: "Cuando uno o varios autores, mediante contrato de servicios, elaboren una obra según plan señalado por persona natural o jurídica y por cuenta y riesgo de esta solo percibirán, en la ejecución de ese plan, los honorarios pactados en el respectivo contrato. Por este solo acto, se entiende que el autor o autores transfieren los derechos sobre la obra, pero conservaran las prerrogativas consagradas en el artículo 30 de la presente ley en sus literales a y b". Esos literales que menciona el artículo 30 son sobre el derecho a que aparezca el nombre del autor cuando vayan a reproducir, traducir o comunicar la obra, y el derecho a que no se modifique su obra sin su consentimiento.

Posteriormente a la elaboración del sitio web se logra su colocación en la red a través de un proveedor de servicios de Internet que tiene una conexión con la estructura básica de interconexión de Internet. Para esto se debe realizar un contrato de Hosting (Contrato de Hospedaje) que es una derivación del contrato de arrendamiento, donde se paga una cantidad determinada de dinero por poder tener el sitio web en el proveedor de servicios de Internet por un determinado tiempo.

### 1.1.7 CONSECUENCIAS JURÍDICAS DE LOS ENLACES O LINKS

Los Links o enlaces electrónicos cumplen la función de permitir la interrelación de los sitios web de Internet, permitiendo entonces poder pasar de una página web a otra sin necesidad de utilizar un buscador o de escribir la dirección electrónica de este.

Lo positivo de los enlaces es que permiten encontrar más información sobre un tema determinado en páginas similares. Esto hace que Internet sea más interactiva, más ágil y

completa, pero también puede generar inconvenientes para los propietarios de páginas de Internet que pueden ver afectado el derecho al buen nombre al aparecer el acceso a sus páginas a través de un link de otro sitio web que no goce del prestigio o confianza del público. Para evitar una posible reclamación jurídica por utilizar links sin autorización del sitio web destinatario se debe celebrar un contrato no convencional que la doctrina denomina contrato de Linking, este contrato lo realiza con el sitio web con el que se quiere construir un vinculo electrónico que permita su acceso.

### 1.1.8 LA MONEDA ELECTRÓNICA

El comercio electrónico fuera de la utilización de los medios de pago convencionales como podría ser la entrega personal del precio del bien también se vale de mecanismos electrónicos como lo son las tarjetas de crédito. La larga historia del papel moneda y la moneda acuñada esta por terminar para dar paso a lo que se ha llamado moneda electrónica, un buen antecedente de la moneda electrónica es el sistema EDI (Electronic Data Interchange System), aunque en Colombia este sistema no es muy conocido, sino que se da más la utilización de la moneda electrónica por medio de tarjetas de crédito.

La moneda electrónica es entonces una unidad de valor monetario que puede ser transmitido por medio de un sistema de redes computacionales. Esas unidades de valor son adquiridas por los consumidores de las entidades financieras, se puede entonces pagar con moneda electrónica debitando de la cuenta del usuario cuando este lo autorice utilizando una contraseña que ordene la transferencia.

Las transacciones con moneda electrónica requieren de la existencia de una cuenta virtual en una entidad financiera, esta cuenta utiliza una contraseña o clave que sirve como llave, de esta forma el cuentahabiente puede enviar dinero virtual para el pago de sus transacciones.

La moneda electrónica es una realidad que no se puede desconocer y que cada día toma más auge en la economía y poco a poco ha ido remplazando al papel moneda. El derecho y la economía no pueden detenerse y desconocer esta realidad, por el contrario deben como es su función entrar a regularlas, lastimosamente nuestra legislación ni siquiera ha

considerado la regulación de este tema. Podemos al menos plantear algunas situaciones de conflictos jurídicos que surgen a raíz de la implementación de la moneda electrónica.

Una primera situación es acerca del control de cambio de la moneda nacional que ejerce el Banco de la Republica según lo estipula el artículo 371 de la Constitución Política, surge entonces la función de regular la entrada y salida de divisas a través de las pasarelas de pago interbancarias. Esto nos describe una de las características de la moneda electrónica que es la supranacionalidad.

El otro inconveniente que puede surgir a raíz de la moneda electrónica es la vulnerabilidad ante las actividades criminales, atrás quedaron los grandes asaltantes de bancos, ahora los asaltos bancarios se dan a través de la informática, lo que revalúa conceptos de la investigación criminal desde elementos como el estudio de la escena del crimen por parte de la criminalística hasta la extraterritorialidad de la ley penal, pues la conducta punible puede ser cometida desde otro Estado. Este es el tema central del presente estudio pues como se ha dicho reiteradamente la solución está en tomar soluciones tecnológico – jurídicas que protejan y den seguridad a las transacciones y al ejercicio del comercio a través de medios electrónicos

Los retos que enfrenta la moneda electrónica son:

- Ampliar su campo de acción para que pueda estar al alcance de todos los usuarios.
- Ser aceptada de forma internacional.
- Servir para grandes y pequeñas transacciones.
- Lograr una alta seguridad y confidencialidad que den confianza al usuario.

Las transacciones a través de la Internet pueden ser principalmente de tres clases:
a) Transacciones bancarias, como consulta de saldos, constitución de depósitos a término fijo o cualquier otra actuación bancaria.
b) Transacciones bursátiles, que serian las referidas a las bolsas de valores como compra de acciones y colocación de bonos.
c)Transacciones comerciales como lo seria la compraventa de un bien mueble a través de la red.

Para la correcta realización de una transacción a través de Internet, la doctrina ha establecido cinco pasos, que ayudaran a actuar de forma diligente a las partes de la transacción, estos pasos son:

**1 ) Autenticación:** También podría llamarse identificación, es decir que se debe verificar que las partes intervinientes son quienes dicen ser. Esto se logra a través de los mecanismos de identificación modernos como: las contraseñas o los métodos de identificación biométrica.

**2 ) Autorización**: Hace referencia a la capacidad legal de las partes para poder realizar la transacción.

**3 ) No repudiación**: Es el compromiso o la obligación que adquieren los intervinientes, esto impide la facultad de retractarse de las obligaciones que han contraído. Para esto se requiere un reconocimiento legal de dichas transacciones. Es lo que hizo la ley 527/99 al reconocerle valor probatorio a los mensajes de datos, permitiendo exigir ante los estrados judiciales el cumplimiento de las obligaciones contraídas a través de este mecanismo.

**4 ) Integridad de la información**: Es una garantía que consiste en impedir que los documentos o datos que constituyen la transacción sean alterados después de realizada la transacción, y de ocurrir dicha alteración esta pueda ser detectada. El documento electrónico es de más difícil falsificación que el documento normal.

**5 ) Privacidad:** Consiste en garantizar la confidencialidad a través de mecanismos que prohíban el acceso a la transacción por parte de terceros.

**Medios de pago**

Los medios de pago más comunes utilizados por Internet son:
**1 ) El pago directo**: Es cuando el pago se realiza por fuera de Internet. Tal seria el caso de compra de un bien a través de la red que se paga cuando ocurre la entrega de este, esto obedece a un sistema de *comercio electrónico incompleto* explicado anteriormente.

**2 ) Las Tarjetas de Crédito**: En esta forma de pago el comprador debe suministrarle el número de la tarjeta de crédito al vendedor quien se encargará a través de una *pasarela de pagos* de realizar el intercambio monetario entre los bancos del comprador y del vendedor.


**Gráfica 4.**

Una pasarela de pagos es el sistema que permite realizar intercambio monetario entre el Banco del vendedor y el del comprador. Es un segmento de red ubicado después del servidor del vendedor y es transparente o totalmente ajeno al cliente, como se explica en la gráfica 4.

Es riesgoso porque el usuario o comprador debe desprenderse del número de cuenta, es por eso que en este tipo de pago se debe actuar con diligencia calificada para evitar la exoneración de responsabilidad por parte del vendedor al alegar culpa exclusiva de la víctima dentro de un eventual litigio. Dentro de la modalidad de pago por tarjeta de crédito se incluye la **Tarjeta de Crédito Virtual**, esta consiste en un número asignado por el banco al comprador para que lo utilice en compras a través de Internet del mismo modo que una tarjeta de crédito convencional, con la diferencia que esta es solo un número y no existe una tarjeta física.

**3 ) El Cheque electrónico**: (e – cheque). Se implantó por primera vez en Estados Unidos en 1998. Se realiza por las mismas partes que intervienen en el libramiento de un cheque

tradicional, es decir, participa un librador que llena los requisitos del cheque virtual y el beneficiario que lo envía a una entidad bancaria encargada de hacer la transacción. El e-cheque es un instrumento de pago de fácil uso en otros países que gracias a sus avances tecnológicos hacen mas fácil su expedición. En Colombia esta el vacío jurídico de si es posible la utilización del cheque electrónico. En principio se considera que al reconocer la ley 527/99 valor probatorio a los mensajes de datos se da cumplimiento a los cuatro principios que rigen para los títulos valores que son: principio de la Literalidad, principio de la Autonomía, principio de la Incorporación y el principio de la Legitimación. Estos principios por ser materia exclusiva de los títulos valores no consideramos fundamental detenernos en ellos.

**4 ) E – Cahs:** Es la moneda electrónica propiamente dicha, se lo define entonces como el dinero electrónico que puede ser almacenado y gastado de distintas forma. Son tarjetas que contienen un chip que puede ser recargado, este chip indica la cantidad de dinero disponible y se va descargando cada vez que se utiliza la tarjeta al realizar un pago. La utilización de estas tarjetas implica la necesidad de los dispositivos que leen los chips.

### 1.1.9 EL DOCUMENTO ELECTRÓNICO:

Es este un tema nuevo dentro de la ciencia del derecho que implica cambios en la forma de hacer negocios y que repercute en la mentalidad de las personas que siempre han depositado su confianza en el papel. Muchos de los negocios jurídicos del campo laboral, civil y comercial contienen la exigencia legal de realizarse en forma escrita. La lenta y paulatina implementación de tecnologías en la aplicación del derecho han ido modificando la forma tradicional de los documentos hasta el punto de que ya nuestra legislación le reconoce valor legal al documento electrónico. Lo mismo está haciendo la administración de justicia que pretende implementar la notificación personal por medio del correo electrónico y la notificación por estados a través de una página web, lo que traerá agilidad y descongestión a los despachos judiciales y una considerable reducción de gastos por concepto de correo y papelería.

La definición jurídica de documento la presenta el artículo 251 del Código de Procedimiento Civil que dice:

***Artículo 251:***

*"Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, contraseñas, cupones, etiquetas, sellos y, en general todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lapidas, monumentos, edificios o similares".*

Se puede decir entonces que el documento es un producto de la conducta humana, se tenga o no la voluntad de hacerlo. El documento es siempre representativo, y en ocasiones es declarativo, pues puede contener una declaración de ciencia, conocimiento o voluntad.

El objeto del documento es demostrar un hecho del pasado, por lo que siempre debe tener una connotación probatoria.

La ley 527/1999 en su artículo 10 complemento el Código de Procedimiento Civil en lo referente a los documentos, dándole admisibilidad como medios de prueba a los mensajes de datos. Dice el inciso final del artículo 10 "*... En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original".* La misma ley en su artículo 2 trae la definición de mensaje de datos que se puede sintetizar como toda información que se puede transmitir por medios electrónicos.

El documento electrónico no es tangible, no esta expresado en un papel, pero si es visible y accesible para una posterior consulta. La mayoría de documentos electrónicos corresponden a títulos valores electrónicos pues son estos los que determinan derechos y obligaciones de carácter económico. Actualmente se manejan los títulos valores electrónicos a través de una Entidad de Deposito que conserva un documento tradicional es decir plasmado sobre un papel donde se autoriza la creación de títulos valores electrónicos. Hacia futuro se pretende omitir el trámite ante las entidades de depósito para que las negociaciones sean directas entre las partes y por lo tanto más ágiles y fáciles.

Pese al reconocimiento legal que se le ha otorgado al documento electrónico este presenta algunas limitaciones que las da la misma ley pues el derecho privado exige en algunos casos que se otorgue Escritura Pública más el correspondiente registro, como ocurre en el caso de compraventa de inmuebles y de aeronaves, en estos casos no se podría realizar la compraventa por medio de un documento electrónico.

Existen muchas lagunas jurídicas sobre la aplicación del documento electrónico y es tarea de la jurisprudencia y de la doctrina orientar. Tales lagunas jurídicas si tienen una respuesta desde lo tecnológico. Dichos interrogantes son entre otros muchos:

- ¿Cuándo y como se debe determinar la autenticidad de los documentos electrónicos?. Tecnológicamente puede ser posible determinar la autenticidad dependiendo del tipo de documento y la tecnología utilizada para su creación y manipulación.
- ¿Cómo se realizarán las copias de los documentos electrónicos y que valor probatorio tendrán?. Tecnológicamente es posible desarrollar programas software que permitan identificar la primera copia de un documento electrónico y que garanticen su valor probatorio.

### 1.1.10 EL NEGOCIO JURÍDICO ELECTRÓNICO

Se planteará a continuación las grandes cuestiones jurídicas acerca del Comercio electrónico, partiendo de que este no es una modificación de los principios básicos del negocio jurídico sino que se debe entender y aplicar como una modalidad del negocio jurídico donde tiene plena cabida los principios tradicionales de este. Se establece entonces una equivalencia funcional, que no es otra cosa que equiparar la utilización de medios electrónicos al uso común de los documentos en papel. Lo importante entonces no es modificar el régimen actual en materia de contratación sino darle reconocimiento legal a la utilización de todas las nuevas tecnologías en la formación de contratos.

Sin entrar a sentar doctrina acerca del Negocio Jurídico, pues ya se ha escrito suficiente sobre él, bastará con afirmar que el Negocio jurídico es un Acto Jurídico querido por las partes, donde lo importante es el acuerdo de voluntades que mueve a una persona a obligarse con respecto a otra persona.

El negocio jurídico electrónico o la contratación electrónica se puede definir como aquella que se realiza mediante la utilización de algún elemento electrónico que sirva para perfeccionar el contrato, es decir para expresar las voluntades de las partes a obligarse.

EL contrato electrónico es posible realizarlo en Colombia y puede probarse su existencia por medios electrónicos según lo afirma el artículo 14 de la ley 527 / 99 que dice:

***Artículo 14 ley 527/99:***

*"En la formación del contrato, salvo acuerdo expreso de las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos".*

Desglosando el contenido del artículo para intentar materializarlo se debe saber como se hace para lograr la oferta y la correspondiente aceptación de los contratantes, pues mientras no coincidan la oferta y la aceptación no hay contrato. Cuando se está entre presentes no habría inconveniente en manifestar la voluntad, pero entre ausentes se debe determinar el momento en que se perfecciona el contrato.

En la contratación electrónica puede darse la contratación entre presentes cuando se utiliza un medio de comunicación que permita la simultaneidad, tal seria el caso del teléfono, los servicios de mensajería instantánea, los chats[9]. Lo contrario será la comunicación entre ausentes que es cuando no hay una simultaneidad en la comunicación. En este caso se deberá analizar según la clase de contrato, si se trata de un contrato unilateral bastará la expresión de la voluntad de la parte que se obliga, pero si se trata de un contrato bilateral este se perfeccionará cuando se de la contestación aceptando la obligación.

Sin pretender profundizar en la cantidad de escollos que pueden surgir en la realización de un negocio jurídico electrónico bastará con decir que se debe analizar cada caso

[9] Tecnológicamente la diferencia entre el sistema de mensajería instantánea (messenger) y los chats consiste en que el messenger es un sistema de mensajería limitado mientras los chats son sistemas de intercambio abierto de mensajes.

concreto intentando obviar las normas especializadas del derecho civil y del comercial para dar aplicación a principios del derecho Informático, sin distinguir entre si la comunicación es entre ausentes o entre presentes, o si se está ante un consumidor o ante un empresario y propendiendo siempre por la supranacionalidad, pues reiteradamente hemos dicho que la globalización de Internet reevalúa el concepto de territorialidad de la ley.

En la práctica existen *contratos de adherencia* elaborados por los sitios web que realizan comercio electrónico estos contratos sirven de sustento legal para dirimir los conflictos generados a raíz del comercio electrónico, aunque se hace la crítica de que por lo extensos y rigurosos de estos contratos se ve afectada la libertad contractual del usuario.

## 1.2 EL DERECHO INFORMÁTICO Y EL DERECHO PENAL

Dentro del tema central del estudio sobre seguridad del comercio electrónico, es de suma importancia hacer la relación entre el derecho informático y el derecho penal, ya que este como ultima instancia jurídica, es el que garantiza la protección de los derechos de los usuarios del comercio electrónico.

Es entonces el Derecho Penal el que respalda las actividades del Derecho Comercial al tipificar las conductas delictivas en contra del comercio electrónico.

Ya fue materia de detenido estudio todo lo relacionado entre el Derecho Informático y el derecho comercial analizando también en ocasiones su ingerencia con el Derecho Civil. Corresponde ahora nuevamente tratar los conceptos básicos del Derecho Informático pero desde la perspectiva del Derecho Penal. Se pasa entonces del ámbito del Derecho Privado al ámbito del Derecho Público.

El Derecho Informático tiene como objeto de estudio o como bien jurídico a tutelar la información. Se hace necesaria la explicación de bien jurídico: es un concepto que pertenece al derecho penal y se puede definir como un valor social que se pretende proteger a través de la tipificación de una conducta punible, es decir a través de la consagración de un delito; Se puede entender mejor con un ejemplo: En el caso del delito de homicidio consagrado en el artículo 103 de nuestro Código Penal, la conducta que se

prohíbe es *matar a otro,* esto con la finalidad de proteger la vida, debemos entender entonces que la vida es ese valor social o bien jurídico que protege este tipo penal. En el caso del derecho informático el bien jurídico tutelado es la información que encuentra regulación en nuestro Código Penal en diferentes tipos penales como el Artículo 195 al que se remitirá constantemente.

Al detenerse en la naturaleza de un bien jurídico surge la pregunta si es la información un verdadero valor social, un fin en si mismo que debe ser tutelado a través de la tipificación de conductas, o si por el contrario es solo un medio para cometer otros delitos como el hurto, la estafa, las falsificaciones y cualquier otra modalidad de conducta punible que se puede realizar por medio de la utilización de nuevas tecnologías como Internet.

Un sector de la doctrina se inclina a pensar que la información es un fin en si mismo, (la información por la información), se basa en que si se tiene la capacidad de almacenamiento, tratamiento y transmisión de la información, esta por si sola constituye un valor económico de la actividad de empresa. Otro sector de la doctrina considera que la información solo cumple una mera función de medio para la comisión de una conducta punible. Tal seria el caso de un cracker que logra introducirse en el sistema informático de una entidad bancaria y obtener los códigos de acceso de cuentas con el fin de traspasar una cantidad de dinero a una cuenta personal; en este caso dice la doctrina no seria viable tutelar la información obtenida del sistema de la entidad bancaria, sino que lo que se debe proteger es el patrimonio económico y tal conducta seria encuadrada dentro del tipo penal de hurto.

Aparece como reacción a las dos posiciones anteriores una tesis ecléctica que cataloga a la información como un bien jurídico intermedio. El planteamiento de este trabajo se inclina por esta teoría que desarrollará mas adelante.
Se parte entonces de la base de la información como bien jurídico tutelado por los delitos informáticos. A continuación se verá que se entiende por Delito Informático:

**Algunas definiciones doctrinales sobre el delito informático son las siguientes:**

1. ***Carlos Sarzana****. Es cualquier comportamiento crimogenio en el cual la computadora ha estado involucrada como material o como objeto de la acción crimogenea o como mero símbolo*[10].

Esta es una definición muy amplia que no permite una plena delimitación del delito informático, habla de computadoras como material o como objeto de la acción delictual, según esta definición una persona que en una riña arremete a otra pegándole con un computador en la cabeza comete un delito informático.

2. *El profesor mexicano Julio Téllez Valdez define: " Es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin"*[11].

3. Se comparte la siguiente definición de los delitos informáticos dada por Sandra Jeannette Castro: *Aquellas conductas típicas, antijurídicas y culpables que lesionan la seguridad informática de los sistemas tecnológicos y dirigidas contra bienes intangibles como datos, programas, imágenes y voces almacenados electrónicamente*.

Las anteriores definiciones brindan una delimitación de lo que se ha entendido por delito informático, que protege la información, ya se dijo que la posición de este trabajo es la de considerar la información como un bien jurídico intermedio, tema que se desarrollará enseguida:

### 1.2.1 LA INFORMACIÓN COMO BIEN JURÍDICO INTERMEDIO.

Un ejemplo de la utilización de un bien jurídico intermedio ayudará a entender su definición: Se puede causar la muerte de una persona haciéndole tomar un vaso de agua envenenada, esto seria homicidio, el mismo resultado se obtendría si se contamina las aguas del acueducto de una población. En ambos casos se tutela el bien jurídico Vida, con la condición de que en el segundo caso también se constituye un delito contra el

[10] SARZANA, Carlos. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2. Ano 1. 1979. Roma,Italia. P.53

[11] TELLEZ, Valdez, Julio. Derecho informático 2º ed. Mc Graw Hill 1996. México

medio ambiente que se podría tipificar como contaminación de aguas, que en ultimas también pretende proteger la vida. Lo que se quiere dar a entender es que el bien jurídico final es la vida y el bien jurídico intermedio es el medio ambiente. Se concluye que un bien jurídico intermedio es aquel que tutela intereses colectivos conjuntamente con intereses particulares que se encuentran en una misma línea de ataque.

Se han señalado como requisitos de los bienes jurídicos intermedios los siguientes:

a. Son supra-personales.
b. Están ligados a un bien jurídico personal
c. Hay una relación de medio entre el bien colectivo y el bien individual, el primero es medio o paso previo necesario para la lesión del segundo. Hay entonces un bien jurídico medio que es colectivo y un bien jurídico final que es el individual.
d. *Cuando se lesiona el bien jurídico intermedio hay una alto riesgo potencial de que se lesionen varios intereses individuales*.

Es la ultima característica de los bienes jurídicos intermedios la que fundamenta su razón de ser. El legislador lo que pretende es sobre-tutelar los bienes jurídicos finales como la vida a través de la tipificación de conductas que vulneren bienes jurídicos relacionados o antecedentes a estos y que pueden afectarlos, tal es el caso de cuando se atenta contra el medio ambiente. Entrando mas en el tema central del estudio, el ejemplo seria el de un atacante que logra conseguir información a través de Internet como datos personales de varios usuarios de un sitio web en el que han realizado una compraventa de un bien. Hasta aquí se ha vulnerado el bien jurídico intermedio es decir la información y se ha creado un fuerte riesgo de vulnerar intereses particulares que se daría cuando el atacante efectivamente utilice la información para obtener un beneficio económico en perjuicio de cada usuario individualmente considerado. La ley se adelanta a que ocurra el delito individual, no espera a que ocurra el hurto a cada usuario de Internet y considera como delito el haber adquirido la información de forma violenta así esta no llegue a utilizarse para cometer otro delito.

Los delitos que consagran bienes jurídicos intermedios no se deben confundir con los delitos de mero peligro como seria el caso del *Concierto para delinquir* del artículo 340 del Código Penal, en este artículo se sanciona la simple reunión de personas que tenga como

finalidad el cometer un delito, delito que aun no se ha cometido pero que se está planeando y que existe el peligro de que llegue a materializarse. En cambio en los delitos que protegen bienes jurídicos intermedios no hay un peligro de que se cometa una lesión futura sino que ya hay una lesión a un bien jurídico como ocurre con los delitos contra el medio ambiente o la información. En los delitos de peligro la lesión aun no se presenta es solo potencial, puede o no ocurrir, pues a nadie se lesiona con el simple hecho de reunirme con un grupo de personas cualquiera que sea el tema de conversación. Teniendo claro cual es el bien jurídico que tutelan los delitos informáticos se puede pasar a analizar cuales son las conductas que se pueden catalogar como delito informático.

La doctrina ha desarrollado conceptos que se catalogan como Delitos Informáticos, pero se aclara que son criterios doctrinales que no tienen fuerza de ley pues no puede la doctrina crear tipos penales ni seria viable que por analogía o por aplicación extensiva se juzgue a un atacante que ha realizado una conducta que no se encuentra expresamente regulada en la ley, esto es lo que hace necesaria la creación de una ley que complemente el Código Penal en materia de Delitos Informáticos, pues este se queda corto en la tipificación de conductas delictivas que utilizan nuevas tecnologías, permitiendo que conductas que no se encuentran consagradas en el Código Penal y que lesionan bienes jurídicos queden en la impunidad por falta de legislación. A lo anterior cabe agregársele que en Derecho Penal no tiene cabida la Interpretación extensiva ni la analogía por lo que no se puede acondicionar una conducta no tipificada a otra que si lo este y que sea similar a la primera. Se crean conductas lesivas de la confidencialidad, la integridad y la disponibilidad de la información.

**1. Conductas lesivas de la Confidencialidad:**

Se debe entender la confidencialidad como el derecho que tiene toda persona sea natural o jurídica a guardar reserva de su información, este derecho es de rango constitucional y solo podría desvirtuarse dentro de nuestra legislación por una orden judicial.

- **El espionaje informático**: Siempre que la obtención de la información sea con animo de lucro y que no medie autorización alguna. Técnicamente se podrían catalogar como espionaje informático las puertas traseras (backdoors), los olfateadores de conexiones (sniffers), el pinchado de líneas telefónicas, la apropiación de

informaciones residuales o archivos temporales y las llaves maestras que consiste en la utilización de programas no autorizados con el fin de modificar, destruir, copiar, insertar o impedir el uso de datos archivados en los sistemas de información.

- **La intrusión informática:** Aquí ya no existe el ánimo de lucro si no que es el simple acceso al sistema informático sin fines específicos, simplemente curiosidad o por encontrar las vulnerabilidades de los sistemas. Tal es el caso de los Hackers que a diferencia de los Crackers que buscan un interés propio estos solo pretenden según ellos, contribuir al progreso de la seguridad informática[12].

2. **Conductas lesivas de la Integridad:**

   Lo que se pretende aquí es obstaculizar el normal funcionamiento de un sistema informático. Son las conductas que regularmente realizan los Crackers que persiguen conseguir un sabotaje informático, ejemplos de tipos de sabotaje informático que atenta contra la integridad de los sistemas son los virus informáticos, que son un tipo de código malicioso que se copia en el sistema y busca dañar partes sensibles de las aplicaciones y sistema operativo, y además intenta reproducirse copiándose a otros sistemas valiéndose de diferentes medios como los correos electrónicos, las carpetas compartidas, disquetes infectados. Ejemplos de virus pueden ser: RedCode, Nimda y el W32.Jeefo.

3. **Conductas lesivas de la Disponibilidad**

   Es cuando se logra bloquear un sistema informático a través ya sea de un virus, en cualquiera de sus formas: Gusano, Troyano o bomba lógica[13] o de un ataque de denegación de servicio DoS (Denial of Service), que es uno de los ataques más comunes actualmente. También se encuadra aquí los famosos Spam o correos basura, que en ocasiones bloquean cuentas de usuario de correo por sobrepaso de cuotas de almacenamiento de discos duros.

[12] La diferenciación entre un Hacker y un Cracker se ampliará en la parte final del capítulo III.

[13] En la actualidad no se puede establecer diferencias claras entre los diferentes tipos de virus informáticos como gusanos, troyanos o bombas lógicas debido a que la gran mayoría de los nuevos programas de código malicioso integran todas estas características en uno solo.

Se acaba de hacer un estudio desde un punto de vista jurídico de conceptos básicos al comercio electrónico como lo es los Delitos Informáticos, las entidades de certificación, firmas electrónicas, mensajes de datos entre otros; continuando con el tema del comercio electrónico a continuación se abarcará el tema de la seguridad de los sistemas computacionales desde un punto de vista tecnológico, profundizando en los conceptos de vulnerabilidades, ataques y efectos.

# CAPITULO II

# ANÁLISIS DE LA SEGURIDAD DE LOS SISTEMAS COMPUTACIONALES

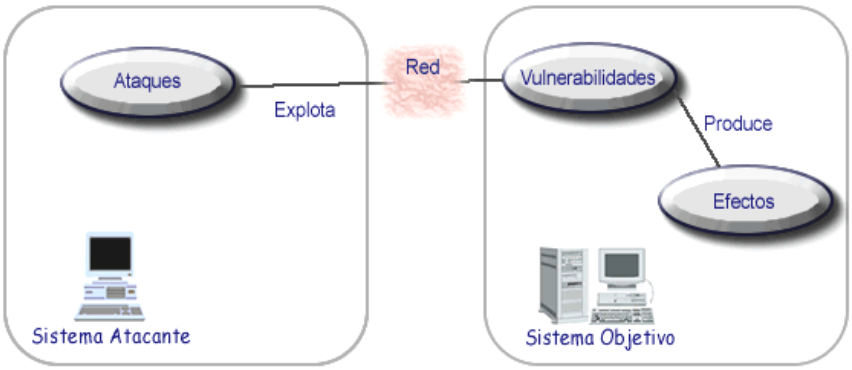
## 2.1 ASPECTOS GENERALES

La búsqueda de soluciones a la inseguridad del comercio electrónico empieza con el análisis del manejo tecnológico que se le da a esta manera de hacer comercio, para posteriormente identificar las maneras con que se le puede hacer daño a un sistema, el origen de estas maneras y que daños pueden llegar a causar al comercio electrónico. Posteriormente a este análisis se puede empezar a buscar las soluciones.

Inicialmente el análisis netamente tecnológico puede parecer un poco alejado de la idea de comercio electrónico pero los conceptos tecnológicos de seguridad computacional que atañen a los sistemas informáticos en general, se aplican a los sistemas de comercio electrónico, ya que este esta soportado sobre un sistema informático.

En el análisis tecnológico de la seguridad del comercio electrónico se debe tener en cuenta en primera medida la estructura y funcionamiento de estos sitios Web para poder encontrar así sus principales vulnerabilidades y la forma como son explotadas. Con este análisis se puede emprender la búsqueda de los métodos y tecnologías para defensa y evitar la ruptura de esta seguridad.

Para entender los problemas del comercio electrónico, y analizar sus problemas de seguridad se debe considerar que existe una amplia gama de estrategias y ataques que se pueden dirigir contra los sitios de comercio electrónico. Todos estos ataques aprovechan una vulnerabilidad o punto débil del sitio determinado; vulnerabilidades que se podrían minimizar. Todos estos ataques una vez ejecutados producen sobre el sistema cierto tipo de efectos en donde se pueden encontrar las marcas de un delito. Esta relación diferenciando entre sistema atacante y sistema objetivo se puede ver en la gráfica 5.




**Gráfica 5. Relación Atacante-Objetivo.**

Antes de proseguir con el análisis de la seguridad de los sitios Web de comercio electrónico en Colombia, es necesario que se consideren los siguientes elementos en la seguridad:

## 2.2 FACTORES TÉCNICOS QUE INTERVIENEN EN LA SEGURIDAD DE UN SISTEMA

### 2.2.1 Métodos de cifrado

Dentro de los métodos de cifrado para conexiones con páginas web que se han considerado están el SSL y el SET, por ser los métodos mas estandarizados.

SSL por sus siglas en ingles Secure Socket Layer, capa de conexión de seguridad es de los dos sistemas el más utilizado debido a la mayor facilidad en su implementación. Los Sitios Web que cuentan con un sistema de cifrado SSL se identifica por un pequeño icono de un candado cerrado en la parte inferior derecha de la ventana del navegador Internet Explorer y una llave o un candado cerrado en la parte inferior izquierda en la ventana del navegador Netscape Navigator.

Los sistemas de cifrado son un elemento fundamental en la seguridad de un sistema de comercio electrónico y es el encargado de convertir la información que se está intercambiando a una forma ininteligible gracias a una operación matemática en la que se oculta la información. El proceso de cifrado es necesario debido a que Internet funciona con tiempo compartido, es decir, la información de todos los usuarios viaja por los mismos

canales de comunicación y cada equipo usuario toma solo la información que va dirigida hacia él.

### 2.2.2 Los Certificados Digitales

Los certificados digitales son un sistema de cifrado de llave asimétrica en el que una Entidad Certificadora (EC) como GeoTrust o VeriSign firma los certificados otorgados a una organización garantizando la identidad de su Servidor; de esta manera un cliente cifra la información que va a enviar al servidor con la llave Pública de éste, una vez ha sido certificado.

Los certificados digitales son los encargados de dar confianza en las relaciones de comercio electrónico. En Colombia se observa una carencia de certificados digitales debido a los costos que estos implican para un pequeño comerciante. Un claro ejemplo de esto es la Universidad del Cauca que hasta ahora esta en proceso de compra de certificado digital, proceso que ha sido demorado por la cantidad de requisitos necesarios para obtención del certificado, además del alto costo de este.

### 2.2.3 Sistema Operativo

El sistema operativo, entendido como la plataforma de operación encargada de gestionar los recursos del equipo computacional por ejemplo Windows y Linux es determinante en la seguridad de un sitio Web debido a que cada sistema operativo tiene sus propias vulnerabilidades que influyen sobre las aplicaciones funcionando sobre él. Por ejemplo si se explota una vulnerabilidad del sistema operativo a tal punto que este deje de funcionar necesariamente todas las aplicaciones corriendo en este momento sobre el sistema operativo se van a ver suspendidas también.

Otro factor importante consiste en que del sistema operativo depende en gran medida el tipo de aplicaciones y la tecnología software con la que funciona el servicio Web.

### 2.2.4 Herramientas de desarrollo de las páginas Web

En la creación de las páginas Web de un sistema de comercio electrónico se encuentra pluralidad de herramientas de desarrollo que se ven reflejadas en las diferentes extensiones de las páginas: ASP, HTM, JSP, PHP, flash, entre otras. Cada una de estas

herramientas de codificación tiene sus propias vulnerabilidades y por lo tanto crean páginas con ciertas vulnerabilidades que están directamente ligadas a la herramienta de desarrollo.

### 2.2.5 Servidor Web

Cada sitio Web de comercio electrónico debe contar con un servidor Web, aplicación que debe estar operando sobre un determinado sistema operativo.

El servidor Web es la aplicación que ofrece los servicios que permiten a un visitante ver un conjunto de páginas Web alojadas en un equipo Servidor, definiendo Servidor como la máquina en la que se instala el Servidor Web.

### 2.2.6 Las Bases de Datos

Un sistema de comercio electrónico debe contar necesariamente con bases de datos para el almacenamiento de la información de sus productos, precios, etc. La accesibilidad a esas bases de datos es un factor importante en la seguridad debido a que estas bases de datos contienen información muy sensible.

## 2.3 ANÁLISIS DE SEGURIDAD

Para realizar un análisis concienzudo de la seguridad de un sistema informático es necesario considerar la relación entre vulnerabilidades-ataques-efectos, porque de esta relación depende el grado de afección que pueda tener un sistema.

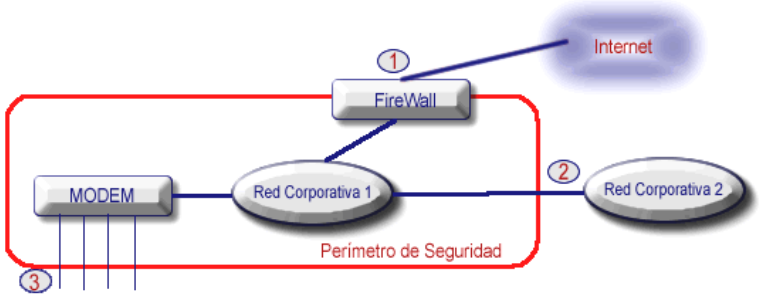
### 2.3.1 Vulnerabilidades

El concepto de vulnerabilidad, hace referencia a la capacidad de un equipo o sistema de equipos a la que se podría llamar red de computadores, para hacer frente a amenazas especificas en un momento particular. Como tal, vulnerabilidad es un concepto dinámico y relativo que depende del grado de riesgo frente a una amenaza, la cual depende del valor de los datos del sistema y del servicio prestado, de la preparación para hacerle frente con herramientas como antivirus y administradores de procesos, de las posibilidades de soporte como la redundancia de la información y datos de las configuraciones de las que se dispongan una vez se desencadene la amenaza.

Al hablar de vulnerabilidades se introduce el concepto de amenaza. Como amenaza se considera cualquier evento o suceso que pueda atentar contra la integridad del sistema ya sea por pérdida de datos de operación del sistema o de la información contenida en él, suspensión de actividades o modificación de las mismas. Cuando se ha aprovechado una debilidad y se desencadena una amenaza, se considera que se ha violado la seguridad, es decir, se ha penetrado uno de los perímetros de seguridad causando necesariamente efectos sobre el sistema, en este caso se habla de un equipo o sistema vulnerado.

También se deben considerar aquí los incidentes de seguridad, un *Incidente de Seguridad* es cualquier intento, exitoso o no, de obtener acceso no autorizado a un sistema informático. Se deben tener muy en cuenta los incidentes porque registran no solo que tan vulnerable es el sistema sino también la capacidad para soportar un determinado ataque.

Para cualificar la vulnerabilidad de un sistema es importante que cada equipo o sistema de equipos defina claramente su perímetro de seguridad, es decir, hasta donde llega el territorio lógico del sistema, este territorio esta definido por el dominio de direcciones IP, así como la estructura física de la red. También se deben identificar los puntos de acceso a este perímetro. Como se muestra en el caso característico de la gráfica 6 se muestran tres puntos en los que es posible traspasar el perímetro de seguridad: En el punto uno en la conexión de la red interna con Internet, en el punto dos una línea de enlace directa con otra red corporativa y en el punto tres por las conexiones a través de MODEM a la red corporativa. Existen varias líneas de defensa, como por ejemplo los corta fuegos o Firewalls que pueden estar ubicadas en algunos de estos puntos para ofrecer mayor seguridad.




**Gráfica 6. Perímetro de Seguridad**

Con esta información sobre los puntos débiles para acceder a un sistema se debe crear una estrategia adecuada para defender sus datos. Existen muchas técnicas de seguridad perimetral, pero lo importante es definir cual es la mas útil para el sistema de tal forma que no queden puntos débiles en la seguridad.

**Las siete vulnerabilidades más comunes**

Para poder profundizar en las vulnerabilidades de un sistema computacional se han analizado las principales listas sobre sucesos de seguridad publicadas en Internet, realizadas por diferentes tipos de organizaciones interesadas en la seguridad como el instituto SANS, el CERT y el FBI. Aunque estas listas de seguridad son de carácter internacional se aplican al caso de Colombia debido a que las vulnerabilidades que allí se analizan dependen en gran medida de los sistemas operativos y aplicaciones de los sistemas computacionales que son del mismo tipo en todo el mundo, además y gracias a la interconexión mundial que ofrece Internet un atacante puede llegar a su objetivo desde cualquier lugar del mundo.

Las vulnerabilidades mas explotadas en la generalidad de los sistemas informáticos del mundo incluyendo Colombia son:

**Instalaciones por Defecto.** Instalaciones de los diferentes programas y sistemas operativos con las opciones que están señaladas por defecto, esto hace referencia a los valores que traen de forma predeterminada los programas en el momento de la instalación de los mismos. Los creadores de estas aplicaciones acostumbran dejar señaladas en las instalaciones muchas opciones que dejan partes del sistema vulnerable, con valores estándares que son conocidos por los atacantes. Debido a que un gran número de usuarios no son cautelosos en las instalaciones y los desarrolladores de software no tienen la seguridad como estandarte, estos valores se convierten en uno de los problemas de seguridad más frecuentes.

También esta el caso de los usuarios anónimos, es decir, sin contraseña que se conectan a través de conexiones anónimas tipo NULL creadas como la cuenta invitado para que un usuario ajeno al sistema se pueda conectar con privilegios muy básicos y que esta por

defecto en muchos sistemas, pero el problema está en que un atacante puede utilizar estas conexiones para escalar privilegios y tener un mayor acceso a la información.

Otro problema relacionado con las instalaciones son las carpetas compartidas por defecto que traen algunos sistemas operativos y que no tienen contraseña de acceso, tal es el caso de la versión HOME del sistema operativo Windows XP.

**Vulnerabilidades de los Servicios Web.** El gran auge de Internet ha hecho que sean los servicios ofrecidos por los servidores web unos de los más comunes y por lo tanto las vulnerabilidades de estos Servidores también unas de las más regulares. Este tipo de servicios permite la visualización de páginas web alojadas en un equipo Servidor por múltiples clientes que se conectan a él. Las vulnerabilidades más críticas de este tipo se encuentran sobre el servidor web de Microsoft Internet Información Server que es muy utilizado en todo el mundo; se encuentran diversas vulnerabilidades, por ejemplo en el componente RDS (Remote Data Services), en las extensiones ISAPI y en Unicode. Un ejemplo de estas vulnerabilidades es el virus Código Rojo, que se beneficia de un error en la extensión ISAPI de Index Server para ejecutar código propio en un sistema infectado.

Las vulnerabilidades para Servidores Web como Apache considerados hasta ahora más seguros están aumentando cada día mas, sin embargo siguen teniendo la ventaja de tener código abierto (OpenSource) y esto hace que las correcciones de seguridad al código, es decir, los llamados Parches de seguridad se desarrollen con mayor rapidez.

**Carencia de Registros de Sucesos del Sistema.** Cada sistema debe crear periódicamente un registro de todos los sucesos que ocurren en él, como por ejemplo el nombre y hora en la que acceden los usuarios, para poder identificar los posibles errores y vulnerabilidades del sistema que lo pueden dejar sensible a algún ataque. Por lo regular los sistemas no conservan registros de eventos adecuados y si los hay no son revisados e interpretados correctamente por el personal calificado y a tiempo de prevenir o contrarrestar los daños.

También se deben registrar y documentar todos los eventos que el usuario o administrador del sistema considere extraños o inesperados como la aparición de

archivos de origen desconocido o de extensiones poco comunes, procesamiento muy lento, mensajes de error, etc.

**Puertos Software de Comunicación.** Los protocolos de comunicación utilizados en redes de computadores necesitan de puntos de comunicación, pero de manera similar como funciona una central telefónica que no tienen una conexión física por cada abonado que se conecta, los equipo computacionales tienen un determinado número de puertos software de comunicación que permiten la conexión de múltiples servicios por una sola conexión física, estos puertos los provee el sistema operativo y se utilizan dependiendo de los diferentes servicios: Servicio Web - puerto 80, servicio SSH – puerto 22, servicio NetBios – puerto 139, entre otros que esta ofreciendo el sistema, es decir, que por cada servicio que se ofrezca que implique comunicación deber existir un puerto abierto, un equipo computacional tiene 65535 puertos disponibles según parámetros definidos en el RFC1010[14]. Existen muchos sistemas con un gran número de puertos innecesarios abiertos o listos para conexión, esto por errores en su configuración y por falta de utilizar herramientas que verifiquen esta situación.

Cada puerto abierto sin necesidad es un potencial ataque al sistema, es como dejar las puertas y ventanas abiertas en una casa. Puede suceder también que el sistema este infectado con algún tipo de programa que abra uno de los puertos para crear lo que se llama "***Puertas traseras***", es decir puertos abiertos sin el consentimiento del usuario o administrador del sistema y que son utilizadas para fuga de información o para que un atacante manipule el sistema remotamente, en ocasiones estas puertas traseras son detectadas demasiado tarde cuando el sistema ya ha sufrido daños.

**Confianza de Usuarios y Administradores.** La vulnerabilidad más importante de todas es la confianza humana, es decir que los usuarios actúen confiadamente y no tomen las medidas necesarias para proteger su información, la prueba de esto es que se utilizan contraseñas débiles, que han sido usadas en otros sistemas y en ocasiones ni siquiera utilizan contraseñan sin advertir que están creando un problema de seguridad para todo el

[14] RFC 1010 - Assigned Numbers Mayo de 1987

sistema en el que se encuentran, y están exponiendo otros usuarios. Por esto un tipo de ataque muy común es el de *Ingeniería Social*.

También existe el problema de la seguridad por oscuridad. Este es un error muy común que cometen los administradores de sistemas o equipos que creen que haciendo mas complicado y confuso sus equipos y utilizando programas poco conocidos y documentados están aumentando la seguridad de su sistema cuando en lugar de ello están aumentando el riesgo de un ataque ya que también desconocen la forma correcta de administración de estas aplicaciones, además de no tener una acertada documentación de estas.

**Vulnerabilidades de los Servicios (Bugs).** En general todos las aplicaciones para computadores son hechas por el hombre y como tal son susceptibles a errores. Un bug es precisamente un error de programación, pueden existir gran número de errores de programación en los diferentes software, cuando esto ocurre se hace más vulnerable el sistema donde esta funcionando el programa.

Un ejemplo de lo anterior es el NetBIOS y el servidor de correos Sendmail, estos son dos servicios de comunicación que utilizan muchos sistemas computacionales y que dependiendo de sus versiones tienen determinados bugs que convierten el sistema en vulnerable. Como ocurre con las distribuciones anteriores a la 8.12.5 de Sendmail en donde por un error en la aplicación se producía un desbordamiento de buffer cuando el mapa DNS se especifica usando expedientes TXT.[15]

**Vulnerabilidades Relacionadas con las Formas de Pagos.** El comercio electrónico utiliza protocolos como Secure Electronic Transaction (SET), Secure Socket Layer (SSL) y Transport Layer Security (TLS). Estos son los protocolos encargados de brindarles seguridad a los intercambios de datos en las relaciones de comercio electrónico.

Los *Certificados Digitales* aunque no son protocolos son un mecanismo de seguridad encargado de brindarle confiabilidad a los sitios web. Las vulnerabilidades inherentes al

[15] Información ampliada sobre errores en SendMail se puede encontrar en el sitio www.senmail.org

comercio electrónico que se refieren a los medios de pago son las relacionadas con los protocolos mencionados en el párrafo anterior y con los Certificados Digitales

El protocolo de seguridad SSL cuando se trata de una conexión segura se caracteriza por presentar un icono en forma de candado en la parte inferior de la ventana del navegador. Uno de los problemas que se pueden presentar con SSL es que el icono del candado puede ser generado por un Script de Java haciendo creer al usuario que esta realizando una conexión segura cuando en realidad no lo es. También existen vulnerabilidades directas de los protocolos que permiten ataques como el Klima-Pokorny-Rosa, Bleichenbacher y por control de tiempos[16] que permite deducir clave privada de una instalación OpenSSL observando las pequeñas diferencias en el tiempo de ejecución de las operaciones criptográficas a medida que se van introduciendo diferentes argumentos. Este ataque se ha utilizado de forma clásica, por ejemplo, para obtener las claves privadas de las tarjetas inteligentes.

Suponiendo que los servidores de comercio electrónico son seguros se puede ver su funcionamiento de la siguiente manera*:* Un cliente accede a la dirección del web seguro a través de la URL correspondiente, como por ejemplo, https://www.objetivo.com. Una vez establecida la conexión, el visualizador o navegador solicita una conexión segura. Si el servidor a que se accede es un servidor seguro, responderá afirmativamente a la solicitud, enviándole un certificado electrónico de tipo RSA. Tras recibir este certificado, el navegador lo desempaquetara con la clave de la entidad de certificación, ya integrada en el software, obteniendo de este modo la clave según el algoritmo RSA. Por ultimo, el cliente genera una clave de encriptación simétrica según el algoritmo RC4 y se la envía cifrada al servidor (con su llave pública). A partir de este momento, tanto el cliente como el servidor pueden establecer una comunicación segura basada en esta clave simétrica, que ambos, y sólo ellos conocen.

El inconveniente con los Certificados Digitales es que en ocasiones la autenticación es realizada por una entidad certificadora secundaria, es decir, una entidad certificada por una EC primaria que no cumple con todos los requisitos de seguridad, si un navegador

[16] La información sobre las vulnerabilidades reconocidas de OpenSSL se puede encontrar en www.openssl.org en la sección de announce.

como Internet Explorer no verifica toda la cadena se corre el riesgo que exista un certificado falso.

También se puede ver que las vulnerabilidades de los medios de pago están dispuesta por el grado de fortaleza de los algoritmos de cifrado como RSA y RC4

### 2.3.2 Ataques Informáticos

Se puede definir un ataque como emprender una acción ofensiva de parte de un atacante contra un sistema con el fin de causar un efecto dañino sobre él, como la modificación de sus datos o la alteración de sus servicios. No se deben confundir los ataques informáticos con los ya mencionados incidentes de seguridad pues estos hacen referencia a los sucesos generados a raíz de un ataque exitoso o no, además los incidentes se deben valorar desde el punto de vista del atacado mientras que los ataques informáticos hacen referencia a la forma de emprender el ataque y se observa desde el punto de vista del atacante. Los atacantes pueden ser externos al sistema o internos es decir, que esta ubicado dentro de la red donde sucede el ataque.

Por cada vulnerabilidad encontrada existe un ataque por realizar. Existen diferentes técnicas para realizar ataques a los sistemas pero todas están gracias a que se aprovechan de las vulnerabilidades encontradas y de los errores de administración.

A continuación se describen los diferentes tipos de ataques que se realizan a los sitios en Internet, también se mencionan los efectos que estos ataques pueden causar y que más adelante en este capítulo serán descritos.

**Ataques Denegación del Servicio (DoS).** Estos ataques se hicieron sumamente populares entre 1997 y 1998 y aunque este es uno de los últimos recursos de un atacante, es poco elegante y no ofrece grandes beneficios, es sin embargo uno de los ataques que más daño puede causar, tal es el caso de portales como yahoo, e-bay y bay.com que en febrero del 2000 fueron víctimas de este tipo de ataques por parte de una

joven de 17 años apodado Mafiaboy, según una corte canadiense[17], que produjeron perdidas que ascienden a 1.700 millones de dólares.

Estos ataques básicamente consumen todo el ancho de banda disponible en una red o en otros casos consume todos los recursos del sistema (saturación de la CPU, memoria o cuotas del disco duro). El problema principal de los ataques DoS es que son datos legítimos en cantidades enormes, por eso los sistemas de detección y protección perimetral no pueden evitarlos fácilmente y es necesario emplear otros métodos mas avanzados que implican revisión minuciosa de los paquetes de datos para evaluar su procedencia, tamaño, servicio, entre otros. Sin embargo en muchas ocasiones esto no es suficiente; Un tipo especial de estos ataques es el Ataque de Denegación del Servicio Distribuido (DDoS), que consiste en infectar múltiples equipos con un programa tipo gusano programado para hacer que todos los equipos infectados realicen una determinada petición a un mismo sitio web produciendo la saturación de éste.
*Efectos sobre el Sistema:* Denegación del Servicio.

**Ataques de Suplantación (Spoofing).** Estos son ataques que utilizan el engaño. Existen diferentes técnicas para efectuar este tipo de ataques en donde se busca básicamente hacerle creer al usuario víctima que está accediendo a un recurso determinado en Internet, cuando en lugar de ello está accediendo a otro en donde pueden estar capturando datos valiosos sobre él o enviándole información errónea.

*Correos Falsos:* Es la técnica más simple de este tipo de ataques, consiste en enviar correos en los que el remitente es modificado alterando la estructura del paquete que se pone en la red. El uso de estos correos falsos o FakeMails es muy variado pero su principal aplicación esta en la complementación de los ataques de Ingeniería Social.

*Suplantación en el DNS:* Esta técnica aprovecha las vulnerabilidades de los servidores de Nombres de Domino (DNS), lo que hace es engañar al Servidor de Nombres de Domino modificando su base de datos para que al recibir una petición de encontrar la dirección IP

[17] La sentencia fue dictada el 12 de septiembre de 2001 según el sitio Web Delitos Informáticos (http://www.delitosinformáticos.com)

equivalente a un nombre de dominio el Servidor resuelva otra dirección diferente a la que el usuario esta solicitando de esta manera accede a un recurso no deseado.

*Suplantación de Dirección IP:* En la suplantación IP el atacante logra identificarse con una IP que no es la suya, entonces el visitante cree que esta visitando su IP de confianza cuando en lugar de ellos esta en el sitio Web del atacante.

*Suplantación Web:* Esta es una técnica muy usada en la que el atacante crea un sitio Web idéntico al del sitio que desea atacar, posteriormente pone en otras páginas enlaces a su página gemela con el fin de que un visitante incauto entre a ésta y crea que esta en la página original. Por lo regular en esta técnica se oculta la barra de direcciones del navegador para que el visitante no se percate de su error y pueda enviar información valiosa a un sitio Web desconocido.

*Efectos sobre el Sistema:* En este tipo de ataque los efectos sobre el sistema atacado son principalmente económicos y sociales como perdida de credibilidad y prestigio. El efecto de perdida de información en este caso recae sobre el visitante.

**Ataques de Fuerza Bruta.** Es la forma de ataque más básico, aunque ha perdido popularidad por su falta de "estilo" para los atacantes y por las nuevas tendencias a realizar ataques que no solo causen daño sino que también creen algún beneficio al atacante como la obtención números de tarjetas de crédito, nombres y claves de usuarios. Consiste en estimar una combinación de nombre de usuario y contraseña probando el mayor numero posible de combinaciones; Obviamente esto es una tarea bastante dispendiosa, para esto existen en Internet un gran número de herramientas software como el John the Ripper que automatizan este proceso. Un ataque de fuerza bruta depende mucho de la velocidad del procesador del sistema desde el que sé esta efectuando el ataque; Algunos ataques de este tipo pueden durar días en su ejecución. Un tipo de ataque de Fuerza Bruta muy frecuente es el ataque de diccionario, en el que las palabras que se prueban para encontrar la combinación nombre de usuario-contraseña provienen de un diccionario de palabras relacionadas con la víctima, por ejemplo si la víctima es un médico el diccionario tendrá bastantes términos relacionados con la medicina.

*Efectos sobre el sistema:* Denegación del Servicio, Pérdida de información

**Ataques Dirigidos a Datos.** Estos ataques se dividen en dos tipos: ataques por desbordamiento de buffer y ataques por validación de entrada[18].

Los ataques de desbordamiento de buffer son los más comunes. Cada día se encuentra en Internet varios nuevos desbordamientos de buffer. Se produce una situación de desbordamiento de buffer cuando un usuario o un proceso intenta introducir en el buffer o Arreglo de tamaño fijo mas datos de los permitidos, el sistema al no saber que hacer con estos datos se altera permitiendo ejecución de código arbitrario, un ejemplo de estos ataques es la creación de una página maliciosa que al ser cargada por un usuario con un navegador Internet Explorer versiones 5.01, 5.5 o 6.0 permite un desbordamiento de buffer en la librería URLMON.DLL permitiendo ejecución de código arbitrario en el sistema del usuario según el boletín de seguridad MS03-015 publicado el 23 de abril del 2003 por la página Web de soporte de Microsoft[19].

Los ataques de validación de entrada son menos comunes pero igualmente efectivos. Estos se producen cuando un programa o proceso no logra reconocer la entrada sintacticamente incorrecta o se produce un error de correlación de valor de campo produciéndose el mismo efecto de ejecución de código arbitrario en el sistema. Por ejemplo, Un servicio Web XML que espera que se escriba un nombre de usuario como parámetro. Si se asume que el nombre de usuario sólo contiene una cadena ASCII y por tanto, se coloca directamente en la consulta SQL, el servicio puede encontrarse expuesto a los ataques. Por ejemplo, si tiene una consulta SQL en el código creada de la siguiente forma:

*sqlQuery = "SELECT * FROM Users WHERE (Username='" & UsernameInput & "')*

Si en el parámetro UsernameInput se incluyera algo similar a *Bob') or not (Username='0* el servicio podría devolver todos los registros y no únicamente uno correspondiente a un usuario específico.

[18] La subdivisión realizada de los ataques dirigidos a datos se realizó con base una propuesta presentada en el libro Hackers de Stuart McClure, Joel Scambray y George Kurtz. Ed. McGraw Hill.
[19] http://www.microsoft.com/technet/

*sqlQuery = "SELECT * FROM Users WHERE (Username='" & Bob') or not (Username='0 & "')*

*Efectos sobre el sistema:* Denegación del Servicio, perdida de información, sustitución de datos.

**Ataques de Ingeniería Social.** Esta es sin lugar a dudas la técnica que mejores resultados puede alcanzar, por lo que requiere mayor atención, se vale del engaño y de la utilización de toda la información que se ha recolectado de la víctima mediante las diferentes técnicas de seguimiento del rastro, exploración y enumeración para obtener información valiosa como nombres de usuario, claves de acceso y contraseñas de red por parte del mismo usuario o administrador del sistema para luego emplear esta información para conseguir mas información o para vulnerar el sistema objetivo. Un típico ataque de Ingeniería Social es el caso del usuario que recibe un correo electrónico aparentemente del administrador del sistema, pero que en realidad ha sido falsificado el remitente (FakeMail), este correo ya contiene algunos datos del usuario como su nombre y la división donde trabaja y le solicita que le envié a un determinado correo electrónico su clave de acceso para labores de mantenimiento del sistema cuando en realidad este valioso dato se envía a una persona desconocida en un lugar indeterminado.

*Efectos sobre el sistema:* Perdida de información, sustitución de datos. También existe un efecto de perdida de credibilidad que recae sobre la persona natural o jurídica a nombre de quien fue enviado el correo falso.

Es importante ver que una vez uno de estos ataques haya alcanzado su objetivo y el sistema es vulnerable se pueden presentar múltiples efectos.

Se pueden ver a continuación un ejemplo de los 10 ataques específicos más importantes, de acuerdo a los daños producidos, el número de ataques registrados y su popularidad, para el año 2002 según SecurityFocus (www.securityfocus.com) para hacer una idea de los nombres de los ataques más populares en Internet. También se debe recordar que estos ataques son en muchas ocasiones completados con ataques de ingeniería social y de suplantación en la etapa de enumeración y recolección de datos de las víctimas.

Se han dejado los nombres originales con los que fueron creados y con los que son conocidos en todo el mundo. La mayoría de los ataques son de tipo dirigidos a datos ya que aprovechan una de las principales vulnerabilidades en los sistemas informáticos, los Bugs.

1. Red Code- MS Indexing Server/Indexing Services ISAPI. Ataque de desbordamiento de Buffer.
2. Nimda - Microsoft IIS 4.0/5.0 Extended UNICODE Ataque de directorio transversal.
3. Matt Wright Ataque de formulario de correo.
4. WU-FTPD File Globbing Heap Ataque de corrupción.
5. SSH CRC32 Compenation Detection Attack
6. Generic CDE dtspcd Ataque de desbordamiento de Buffer.
7. Generic System V Derived Login Ataque de desbordamiento de Buffer.
8. Generic SNMP PROTOS Test Suite Attacks.
9. Shaft DDoS Ataque de manipulación al cliente.
10. PHP Post File Upload Ataque de desbordamiento de Buffer.

Según CERT han nacido nuevas tendencias de ataque con gran fuerza. Entre ellas, destaca la habilidad de las herramientas de ataque para borrar sus huellas y auto-reconfigurarse para intrusiones más profundas, una permeabilidad creciente de los Firewalls (por mala configuración y falta de política global), un índice mayor de vulnerabilidades debida a la complejidad inherente de los nuevos programas, y una mayor habilidad de los Hackers gracias al rápido intercambio de información que pueden perpetrar con colegas de todo el mundo.

### 2.3.3 Efectos

Un efecto es la situación o resultado de una determinada acción. Para el caso de la seguridad computacional la acción es un ataque informático y los efectos recaen sobre el sistema atacado.

Como es tarea del legislador establecer si una conducta es o no delictiva, serán estos los encargados de tipificarla. Desde un punto de vista netamente tecnológico solo se determinará en que momento un sistema no conserva su integridad, entendiendo

integridad como que el sistema conserve los mismos datos, con la misma estructura y que no hayan sido accedidos arbitrariamente. Aunque es importante decir que el legislador no se puede aislar de la parte tecnológica a la hora de construir normas que regulen los delitos informáticos ya que de ser así estas carecerían de aplicación eficaz.

Los diferentes efectos jurídicos que generan las conductas tecnológicas lesivas se analizarán en el capítulo siguiente buscando la equivalencia entre los modus-operandi de los delitos informáticos y los ataques informáticos.

**Efectos en un sistema Vulnerado**

Los efectos tecnológicos que se pueden encontrar en un sistema vulnerado o que ha sido atacado son bastante amplios pero se pueden agrupar o clasificar de la siguiente manera:

**Denegación del Servicio.** Un computador o sistema de computadores cuenta con diferentes servicios que pueden ser: el servicio Web, servicio de Cliente DHCP, servicio de Telnet, entre otros, que varían de acuerdo al sistema operativo y a las aplicaciones instaladas especificas del sistema. Estos servicios son lo que el sistema ofrece a sus usuarios y el motivo por el que existe. Cuando se aprovecha una vulnerabilidad del sistema para hacer que uno de estos servicios deje de funcionar se produce una situación de *Denegación del Servicio,* mas comúnmente conocida como *DoS* por las siglas en ingles de Denial of Service.

Las técnicas para Denegación del Servicio son muchas y muy variadas, dependen del tipo de servicio que se desea bloquear y del sistema operativo que los soporta.

Es muy común que al producirse la suspensión de uno de los servicios del sistema esto provoque la suspensión de otros servicios o del sistema completo. El caso más común es el de denegar el servicio Web de un sistema causando que los clientes no puedan acceder al sitio Web de la empresa afectada.

**Perdida de Información del Sistema.** La información que se pierde puede ser de la integridad del sistema, es decir, código de programas instalados o información contenida en el sistema, por ejemplo datos almacenados en una base de datos.

Se pueden presentar dos casos con la pérdida de información, cuando el administrador o responsable del sistema está al tanto de la pérdida y cuando el robo de información no es descubierto, en ocasiones el robo nunca es descubierto dejando el sistema aun más vulnerable porque el problema de seguridad o vulnerabilidad explotada para efectuar esta extracción de información no es corregida, y en este caso el atacante puede reincidir en sus acciones. Una variable de este efecto es cuando datos son modificados, en este caso sigue habiendo presencia física de datos pero la información se pierde.

**Sustitución de Datos.** Sustitución de datos en el sistema modificando la configuración de este. Es cuando el ataque permite que ciertos datos esenciales para el funcionamiento del sistema sean alterados, los datos modificados pueden ser tanto del sistema operativo como de las aplicaciones instaladas produciendo en ocasiones la modificación, pero *no cancelación* de los servicios activos.

En el caso de sustitución de datos pueden existir diferentes finalidades: Modificación del servicio Web, ocultar rastros de accesos no autorizados al sistema o implantar programas para espiar el sistema atacado o tener control de él; Este tipo de programas son conocidos como Caballos de Troya, por ejemplo NetBus, BackOrifice y Sub7, y son pequeñas aplicaciones que se ocultan en el sistema o se camuflan en otro programa, aparentemente de propósitos muy útiles e interesantes para que el usuario no se percate de él mientras realiza conexiones no autorizadas, llamadas puertas traseras, que permiten la fuga de la información.

Los anteriores efectos recaen sobre cualquier sistema informático y naturalmente sobre los sitios Web dedicados al comercio electrónico, pero existen ciertos efectos que están implícitos en la naturaleza comercial de algunos sitios Web y son los relacionados con los medios y formas de pago. Aunque en el comercio electrónico los efectos que se pueden considerar son más de carácter económico, debido a la perdida de prestigio de una organización por causa de un incidente de seguridad, incidente que si es conocido por la comunidad usuaria de ese sitio causaría la perdida de confianza en él y por lo tanto la perdida de clientes.

## 2.4 LAS EMPRESAS COLOMBIANAS DE COMERCIO ELECTRÓNICO

Las grandes empresas colombianas cuentan con un sitio en Internet para su finalidad económica. Algunas empresas solo utilizan su presencia en Internet con fines publicitarios y como soporte a su actividad económica, en cambio otras la utilizan para relaciones de comercio electrónico indirecto, es decir intercambio de bienes tangibles usando el sitio Web para las etapas de publicidad, venta y algunas veces pago, pero para la parte de distribución es necesario emplear medios de transporte físicos. Relaciones de comercio electrónico directo en el que la parte de distribución se puede hacer a través del mismo sistema web, debido a que son bienes intangibles como servicios y software. Para el caso de este trabajo se hace referencia a los sitios que realizan las relaciones de comercio electrónico directo e indirecto, pero en todo caso comercio electrónico completo, es decir, que la etapa de pago se realice utilizando los medios de pago electrónicos porque es en esta etapa que los efectos en el sistema vulnerado pueden ser mas graves.

En el Anexo B se puede encontrar la lista de los sitios Web colombianos, es decir aquellos que tienen el sufijo ".com.co", a los que se les ha logrado traspasar la seguridad hasta mayo del 2003. según lo divulga el sitio Web ZoneH[20] especializado en recolección de datos sobre sistemas vulnerados o Defaced. Se puede observar en esta lista la gran variedad de empresas y organizaciones a las que les han sido vulnerados sus sistemas y lo que es peor, muchas de estas empresas han sido vulneradas en varias ocasiones como por ejemplo la empresa alojada en el dominio www.paisas.com.co. Esto indica la gran falta de interés en la seguridad de sus sistemas informáticos de algunas empresas colombianas. Existen también algunos casos de empresas a las que les han vulnerado su sitio Web porque simplemente el dominio esta registrado a nombre de la empresa pero este no esta siendo utilizado, esto implica la creación de mal prestigio en el nombre de dominio que a su vez trae connotaciones económicas como la desvalorización de este dominio.

### 2.4.1 Obtención de la muestra de los sitios Web

El proceso de cuantificación de las empresas colombianas que realizan actividades de comercio electrónico completo es bastante complicado debido a que según la Universidad

[20] http://www.zone-h.com

de los Andes existen 7047 (15 de mayo de 2003) empresas registradas con dominios comerciales en Colombia pero muchas de estas empresas utilizan los sitios Web únicamente para una parte de comercio como lo es la publicidad. Ya que todos los sitios utilizan los mismo puertos de comunicación digitales, por lo regular puerto 80 o puerto 443, es difícil emplear métodos automáticos para detectar los sitios que en realidad ofrecen servicios de comercio electrónico completo.

En el Anexo A se encuentra la tabla con la lista de los sitios Web obtenidos en el proceso obtención de la muestra para los correspondientes análisis de seguridad, así como la descripción del proceso técnico que se siguió para la obtención de esta lista.

En este punto es importante notar que las empresas mas conocidas, visitadas y utilizadas en el campo del comercio electrónico en Colombia, empresas que son sinónimo de comercio electrónico no son empresas colombianas, tal es el caso de Deremate.com, empresa Argentina que cuenta con una sección en su sitio dedicada a Colombia, colombia.deremate.com y utiliza un dominio genérico. También se debe notar que muchas de las reconocidas empresas colombianas con presencia en el comercio electrónico no utilizan un nombre de domino con el sufijo identificador del país, un ejemplo de esto es VirtualEXITO[21] que aunque pertenece a CADENALCO no tiene el indicativo “co.”. La Universidad de los Andes como entidad encargada del registro de dominios a nivel nacional únicamente realiza los registros con el indicador referente a Colombia, es decir, “.co”.

### 2.4.2 Las vulnerabilidades más explotadas en los sistemas informáticos en Colombia

Si se analizan los sistemas vulnerados en Colombia en los últimos años se puede ver que se encuentran 177 sitios con dominios comerciales colombianos reportados como vulnerados entre los años 2000, 2001, y 2002 y hasta 20 de mayo de 2003. Se aclara que existen muchos sitios que se quedan por fuera en esta parte del análisis, sitios cuyo nombre de dominio no se incluye el indicativo del país (.co) aunque su sede principal este ubicada en Colombia, esto sucede porque las empresas se constituyen legalmente en

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

Colombia pero registran el dominio solo como comercial, es decir, ".com". También se aclara que se están considerando solo los sitios Web identificados por Zone H, ya que pueden existir algunos sitios que Zone H no logre identificar como vulnerados.

De estos sitios 108 tienen o tenían en el momento del ataque sistema operativo Windows, es decir, el 61.01% de los sitios, aunque se muestra una tendencia a cambiar este sistema operativo por otros, tanto así que los sitios vulnerados en el 2000 todos tenían sistema operativo Windows, mientras que en el 2001 solo el 83,1% tenían Windows, en el 2002 el 41.7% y hasta mayo del 2003 el 37.8% de los sitios vulnerados tenían este sistema operativo. Las estadísticas muestran que está aumentado el número de ataques contra otro tipo de sistemas operativos diferentes de Windows, sobre todo a los tipo Unix, por ejemplo para el año 2003 se incremento notablemente los ataques contra sitios que funcionan sobre sistemas operativos tipo Unix, a tal punto que si se observa el reporte de sitios Web vulnerados en todo el mundo según Zone-H, de un promedio de 700 sitios (mayo 2003) solo el 13 % en promedio utilizan sistemas operativos diferentes de Linux. Esto se puede explicar en parte con el creciente aumento en la utilización de sistemas operativos Linux[22], es decir, los ataques son dirigidos contra servidores que utilizan sistemas operativos tipo Linux porque la gran mayoría de servidores utilizan este sistema operativo, aclarando que estos datos son para equipos tipo servidor y no para estaciones de trabajo. El aumento en la utilización de sistemas operativos Unix a contribuido con el aumento en sus vulnerabilidades, sin embargo los Sitios Web dedicados a la seguridad como Security Focus e Hispasec los siguen considerando más seguros.

Los análisis de los sitios vulnerados se realizaron con base en la información proporcionada por Zone-H.org[23]

### 2.4.3 Evaluación de seguridad

Para plantear las soluciones a los problemas de la seguridad del comercio electrónico se ha realizado una evaluación de seguridad a un conjunto de sitios Web ya definidos como

[22] La utilización de Linux aumenta cada vez mas. Según la empresa de análisis de mercado International Data Corporation (IDC) prevé que el gasto en sistemas operativos Linux pase de 80 millones de dólares en 2001 a 280 millones en 2006, lo que equivale a una tasa de crecimiento anual compuesta del 28%. (www.idc.com).
[23] www.zone-h.org.

muestra. Esta evaluación se dividió en dos fases: La primera que buscaba recolectar la información relevante a los sitios Web y la segunda fase que utilizaba esta información para ejecutar diferentes herramientas de seguridad como el Nmap que arrojaran la información suficiente para después de un proceso de análisis generar un conocimiento sobre el estado de la seguridad. El análisis se ha realizado considerando la vulnerabilidad de los Sitios Web a los distintos ataques ya mencionados en este Capítulo.

De lo anterior se incluye un resumen estadístico de todos los datos recolectados en esta parte y que aparece de forma completa en el anexo B.

**Organismos internacionales de asignación de direcciones IP.**

La Corporación de Internet para nombres y números asignados (ICANN)[24] es una corporación sin animo de lucro del sector privado formada por una amplia coalición de las comunidades de Internet, de negocios, técnicas académicas y de usuarios. La Corporación ICANN ha sido reconocida por los gobiernos como la entidad de consenso global para coordinar la administración técnica del sistema de nombres de dominios de Internet, la asignación de espacio de direcciones de IP, la asignación de parámetros de protocolos, y la administración del sistema de servidores de raíz. El objetivo de la Corporación ICANN es el de operar como un cuerpo abierto, transparente y basado en el consenso, ampliamente representativo de las diversas comunidades accionarías de la Internet global.

A nivel regional existen tres organizaciones encargadas de la asignación de bloques de asignaciones IP y políticas para el manejo de estos, dichas entidades regionales son: La ARIN para América, el caribe y África subsahariana; la APNIC para la región de África y el pacifico y la RIPE NCC para Europa y su área de influencia[25].

[24] http://www.icann.org. La ICANN asumió las funciones que venia prestando desde la década de los 80´s la IANA (Internet Assigned Numbers Authority) http://www.iana.org

[25] ARIN American Registry for Internet Numbers, APNIC Asia Pacific Network Information Centre, RIPE-NCC Reseaux IP Numbers Network Coordination Centre.

**¿Cómo se realiza una firma electrónica?**

El software del firmante aplica un algoritmo hash sobre el texto a firmar, obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor. Los algoritmos hash más utilizados son el MD5 ó SHA-1. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits (según el algoritmo utilizado), se somete a continuación a cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA. De esta forma se obtiene un extracto final cifrado con la clave privada del autor, el cual se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

**¿Cómo se comprueba la validez de la firma digital?**

Para poder verificar la validez de un mensaje de datos es necesario la clave pública del autor.

El procedimiento sería el siguiente: el software del receptor, previa introducción en el mismo de la clave pública de remitente (obtenida a través de una Autoridad de Certificación), descifraría el extracto cifrado del autor y a continuación calcularía el extracto hash que le correspondería al texto del mensaje y, si el resultado coincide con el extracto anteriormente descifrado, se considera válida; en caso contrario significaría que el documento ha sufrido una modificación posterior y por lo tanto no es válido.

**¿Qué es el cifrado?**

Hay dos tipos de cifrado o encriptación, el simétrico que obliga a los dos interlocutores (emisor y receptor) del mensaje a utilizar la misma clave para encriptar o desencriptar el mismo (como por ejemplo el criptosistema DES, Data Encription Standard, desarrollado por IBM), y la encriptación asimétrica o criptográfica de claves públicas que está basada en el concepto de pares de claves, de forma que cada uno de los elementos del par (una clave) puede encriptar información que solo la otra componente del par (la otra clave) puede desencriptar. El par de claves se asocia con un solo interlocutor, así un componente del par (la clave privada) solamente es conocida por su propietario mientras

que la otra parte del par (la clave pública) se Pública ampliamente para que todos la conozcan (en este caso destaca el famoso criptosistema RSA cuyas iniciales son las de sus creadores: Rivezt, Shamir y Adelman).

**VIRUS**

Aunque de acuerdo a la delimitación de este documento no corresponde desarrollar el tema de los virus informáticos, si se hace relevante realizar ciertos comentarios al respecto.

Para fines prácticos en este estudio se han clasificado los virus informáticos solo en dos tipos de acuerdo a su finalidad:

1) Virus cuya finalidad es causar únicamente y exclusivamente daño en el sistema infectado, ya sea con borrado o degeneración de archivos, con la relentización del equipo o cualquier otro método.

2) Virus cuya finalidad es obtener ventaja del sistema infectado, es decir, todos aquellos que buscan una fuga de información sobre la víctima, ya sea enviando información a una determinada dirección de correo electrónico, publicando información valiosa del sistema, entre otros métodos.

Esta clasificación se realiza porque para el documento se considera el primer tipo de virus como entes autónomos en los que una persona natural o jurídica ya no tiene un control directo sobre él o su origen.

El segundo tipo de virus se considera para el estudio no como virus sino como una técnica de ataque que busca obtener una ventaja de una víctima y se enmarcará en una de las técnicas mencionadas en este capítulo y así mismo se le da el tratamiento jurídico al acto delictivo.

## 2.5 ANÁLISIS SOCIOLÓGICO DE LOS HACKERS

*“ Si, soy un criminal*
*Mi crimen es la curiosidad.*
*Mi crimen es el juzgar a las personas por lo que dicen y piensan,*
*no por lo que aparentan.*
*Mi crimen es ser más inteligente, algo por lo cual nunca me olvidarás.*
*Soy un Hacker, este es mi manifiesto.*
*Tu podrás detener este esfuerzo individual, pero nunca podrás detenernos a todos ...*
*después de todo, todos somos iguales.”*

***Parte final del Manifiesto Hacker, escrito por The Mentor***.

Las personas que comenten los delitos informáticos son de difícil aprehensión, se plantea el interrogante de quienes son estas personas, que clase de comportamientos y modos de vida tienen. Existe cierta subcultura denominada en algunos textos y sitios web como underground, esta subcultura tiene un lenguaje, un manual de ética, códigos de honor y costumbres.

Existe una diferencia entre los conceptos de Hacker y Cracker que radica en los fines de sus conductas, los primeros realizan sus actos sin la intención de causar un daño grave o destrucción a los demás, su justificación es propender por la seguridad de los sitios web al demostrar su vulnerabilidad, muchos de los Hackers utilizan la tecnología como una forma de revolución social y política. Los Crackers por el contrario tienen intereses económicos individuales o por la simple diversión al causar daño y destrucción a otros. Un común denominador en el comportamiento de estas personas es la paranoia por la seguridad computacional y el delirio de persecución por parte de las autoridades de su país, lo que conlleva a que sean personas solitarias que manejan un bajo perfil social, a pesar de su elevado ego que se alimenta con cada nueva intrusión informática que logran realizar. Los Hackers han sido llamados en libros y muchos sitios Web los Robin Hood de la era informática, pero lo cierto es que estos realizan sus actos mas por un sentido de vanidad y auto superación.

Los Hackers son por lo regular jóvenes que no superan los 26 años con una situación económica estable en la mayoría de los casos subsidiada por sus padres, lo que ayuda a que puedan dedicar el mayor tiempo posible a las investigaciones informáticas.

A pesar de los factores psicológicos como la vanidad y egocentrismo de los Hackers es muy difícil capturarlos. Primero que todo porque manejan un bajo perfil al realizar sus actos a tal punto que en muchos de los casos de jóvenes capturados ni siquiera sus padres sabían de sus actos. También porque se cuidan mucho de no dejar ningún rastro cuando realizan ataques. Aunque la mayoría de los Hackers trabajan desde el mismo sitio, o en ocasiones solo se mudan de barrio dentro de la misma ciudad, desde el punto de vista informático se mueven por todo el mundo ocultando sus rastros. Por ejemplo para realizar un ataque a un Servidor en Estados Unidos donde se encuentran, primero toman el control de un servidor débil ubicado en algún país del lejano oriente y una vez tengan el control de ese equipo lo pueden administrar remotante como si estuvieran allá. Desde ese nuevo equipo realizan un ataque contra el Servidor en Estados Unidos, una vez ocurrido el incidente de seguridad el administrador de ese Servidor intenta seguir los rastros y se encuentra con que el ataque fue realizado desde un país lejano que no presta mucho interés en colaborar con el caso y en donde la barrera del idioma hace más difícil analizar los Logs del sistema.

Desde el punto de vista de la criminalística informática para el seguimiento de los procesos de los delitos informáticos y de los Hackers se han definido una serie de pautas en el RFC3227 en donde aparecen los pasos que se deben seguir para la correcta recolección de evidencia digital, se definen elementos importantes como el orden de volatilidad de los datos, pasos para la recolección de evidencia y las consideraciones de privacidad. También se cuenta con la guía del RFC2350 que define la forma de conformación de equipos de respuesta a incidentes de seguridad y el RFC2828 que define los términos seguros en la operación de Internet y sirve de punto de referencia para las evaluaciones de seguridad y recolección de evidencia digital.

Hasta aquí se ha realizado en este documento un análisis tanto jurídico como tecnológico de la seguridad del comercio electrónico. Haciendo énfasis en este capítulo en el análisis de vulnerabilidades de sitios web colombianos. Ahora se cuenta con elementos necesarios para realizar en el siguiente capítulo un estudio de casos en los que se resuelven jurídicamente situaciones en las que se ve vulnerada la seguridad del comercio electrónico.

# CAPITULO III
# ESTUDIO DE CASOS

## 3.1 CASO: Acceso al Servidor

El sujeto que para el estudio de este caso se le llamará usuario del sistema, se conecta utilizando la tecnología Internet y la infraestructura que ofrece la red telefónica pública conmutada a un sitio Web que para el estudio de casos se le llamará *Objetivo.com* y se le identificará con la dirección www.objetivo.com.co. El sitio Web Objetivo es un sitio de naturaleza jurídica comercial, registrado ante la Cámara de Comercio de una ciudad de Colombia donde se encuentran sus oficinas principales y con el correspondiente nombre de dominio asignado por la Universidad de los Andes. El usuario se conecta con el fin de realizar la compra de un artículo cualquiera. Después de realizar el proceso de búsqueda y análisis de los productos en el sitio, el usuario se decide por un artículo determinado y procede a realizar el proceso de compra en línea del producto.

Para la compra en línea del producto o compra a través de Internet, el usuario envía los siguientes datos personales: Nombres y apellidos, empresa a la que pertenece, documento de identidad, teléfonos, correo electrónico, dirección completa del sitio de entrega del producto y la forma de pago que desea utilizar; el usuario elige utilizar su tarjeta de crédito VISA entonces envía adicionalmente los siguientes datos: el número de la tarjeta, titular, la fecha de vencimiento y el número de cuotas. El usuario termina la fase de envío de datos satisfactoriamente y el sitio o la empresa Objetivo.com a través de su pasarela de pagos se encarga de realizar el traslado de fondos del banco del usuario a su banco.

En los días posteriores a la transacción un atacante logra entrar arbitrariamente aprovechando un error de programación en una de sus páginas de extensión php al servidor donde Objetivo.com tiene almacenados todos los datos de las transacciones que ha realizado. El atacante que hábilmente sustrae toda la base de datos de los clientes de Objetivo.com tiene acceso a los datos necesarios del usuario como su nombre y número

de la tarjeta de crédito para realizar compras a nombre del usuario. Debido al tipo de técnicas que utiliza el atacante no es descubierto.

Aquí aparece un punto importante. La información no fue robada directamente del usuario, es decir, aparece Objetivo.com como víctima del robo de la información, información que consistía en datos confidenciales que el usuario le había confiado con compromiso de confidencialidad, compromiso que aparece con los mensajes donde objetivo.com advierte que se está a punto de entrar a un sitio seguro. El usuario sufre un perjuicio debido a la perdida de dinero de su cuenta bancaria.


**Gráfica 7. Acceso al servidor.**

**Hipótesis de Solución:**

En este caso como en la mayoría de casos donde hay que derivar responsabilidad, esta se puede dividir en dos, la responsabilidad penal y la responsabilidad civil, se analizará a continuación cada una de ellas, para acentuar las diferencias existentes entre estas y entender a cabalidad la hipótesis de solución planteada en cada uno de los casos.

La responsabilidad penal, grosso modo es la que plantea nuestro Código penal para cada uno de sus delitos. Consiste esta responsabilidad en la imposición de una pena o de una medida de aseguramiento según se haga referencia a un mayor de edad o a un menor de edad. Nuestro Código Penal Ley 599/ 2000 dice en su artículo 35 que las penas principales consistirán en Pena privativa de la libertad o prisión, la pena pecuniaria de Multa y las penas privativas de otros derechos según lo consagre cada delito en particular. La sanción de los delitos le corresponde al Estado por ser este el encargado de

la seguridad y el orden social, es por eso que se ubica el Derecho penal dentro del Derecho Público.

La Responsabilidad Civil corresponde al derecho privado, aquí el Estado no actúa directamente como parte sino que por el contrario las partes intervinientes son personas particulares. En la responsabilidad Civil ya no se persigue la responsabilidad personal, que es lo que pretende el derecho penal, sino que lo que se pretende conseguir es una responsabilidad patrimonial, monetaria, que tendría como finalidad lograr el restablecimiento del derecho, ya sea intentando volver las cosas a su estado anterior o cancelando una indemnización pecuniaria.

La responsabilidad civil puede ser contractual cuando se deriva de las obligaciones de un contrato celebrado entre las partes y puede ser extra-contractual cuando se deriva de un hecho ajeno al derecho como podría ser un accidente de tránsito pero que genera repercusiones jurídicas.

Una vez entendido los conceptos generales de las responsabilidades Penal y Civil, se dará paso a la hipótesis de solución del caso planteado.

**Responsabilidad Penal**

Se debe determinar si la conducta descrita en el planteamiento del caso es una conducta punible, es decir si es típica, antijurídica y culpable. **Típica**: Se puede entender como el proceso que sigue el Legislador de tomar comportamientos humanos que se consideran dañinos a la sociedad para definirlos como conductas punibles, penarlos e incluirlos en una norma penal. Se dice entonces que una conducta es Típica cuando se puede encuadrar dentro de un tipo penal. **Antijurídica**: Una conducta es antijurídica cuando además de ser típica lesiona o pone efectivamente en peligro, sin justa causa un bien jurídicamente tutelado por la ley. **Culpable**: Se puede entender la culpabilidad como el juicio de reproche que se le hace a una conducta típica y antijurídica de una persona que actúa de una manera pudiendo hacerlo de otra.

En el caso planteado se debe tener en cuenta que no se trata de una comunicación porque lo que se ataca es un sistema de almacenamiento y no un canal de comunicación entre dos personas.

La responsabilidad penal del caso planteado se puede encuadrar en los artículos 195 y 239 - 240 Numerales 1º y 4º del Código Penal utilizando la figura del concurso de delitos.

**Artículo 195 Código Penal:**

*"El que se introduzca abusivamente a un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa".*

**Artículo 239 Código Penal:**

*Hurto. El que se apodere de una cosa mueble ajena con el propósito de obtener provecho para si o para otro, incurrirá en prisión de dos a seis años.*

*La pena será de prisión de uno (1) a dos (2) años cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales.*

**Artículo 240 Código Penal.**

*"Hurto calificado, La pena será de prisión de tres (3) a ocho (8) años, si el hurto se cometiere:*

*1. Con violencia sobre las cosas.*

*2. Colocando a la víctima en condiciones de indefensión o inferioridad o aprovechándose de tales condiciones*

*3. Mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores.*

4. *Con escalamiento o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes.*

*La pena será prisión de cuatro (4) a diez (10) años cuando se cometiere con violencia sobre las personas*

*Las mismas penas se aplicarán cuando la violencia tenga lugar inmediatamente después del apoderamiento de la cosa y haya sido empleada por el autor o partícipe con el fin de asegurar su producto o la impunidad".*

Según la forma de ataque que se efectúe contra el sistema informático, se puede establecer si existió o no violencia contra el sistema, por ejemplo, en un ataque de fuerza bruta en el que se genera un daño, se puede establecer claramente que existió violencia sobre el sistema informático; lo mismo se podría decir de un ataque de desbordamiento de buffer en el que se induce un error contra el sistema, error que puede implicar daños lógicos contra el sistema.

Se puede encuadrar también dentro del numeral cuarto del artículo 240, ya que se pueden incluir las llaves virtuales y contraseñas de acceso dentro del concepto de llave sustraída o falsa que plantea el artículo.

Téngase en cuenta que en esta clase de delitos se hace muy difícil lograr dar con el paradero del delincuente ya que por lo general son Crackers que se cuidan de dejar evidencias, mas aun con la posibilidad de que no se encuentre en el territorio nacional haciendo más difícil su aprehensión. Por lo que la materialización de la sanción penal en un eventual proceso se hace casi imposible.

**Responsabilidad Civil:**

Para establecer si existe una responsabilidad civil se deben analizar las circunstancias que plantea el problema.

- El usuario del servicio ingresa al sitio Objetivo.com con la garantía que este le presenta de que está ingresando a un sitio seguro.
- La información no fue robada directamente al usuario ni en el canal de comunicación entre este y el sitio web.
- La información es extraída ilícitamente del servidor donde Objetivo.com almacena la información. Siendo este la verdadera víctima del hurto.

Como el sitio web en el caso planteado se encuentra registrado en la Cámara de Comercio de una ciudad colombiana, esto facilita la instauración de un proceso de responsabilidad civil contra el sitio web, en este proceso el usuario del servicio utilizando la libertad probatoria que concede nuestra legislación deberá entrar a demostrar tecnológica y jurídicamente que el hurto se cometió en el servidor de almacenamiento del

sitio web, siendo este el único responsable de la custodia de dicha información, por lo que el sitio web debe responder por los daños y perjuicios que se le hayan podido causar al usuario con la sustracción del dinero de sus cuentas bancarias, pues el sitio web le garantizó que se estaba ingresando a un sitio seguro lo que permitió que el usuario depositara sus datos, se puede agregar aquí que el actuar del usuario en el caso planteado es diligente.

En un eventual proceso judicial el usuario demandaría a la página web en virtud de su responsabilidad del robo de la información la indemnización por daños y perjuicios que se le hayan podido causar al usuario a raíz del hurto del dinero de sus cuentas bancarias.

**Conclusión:**

En este primer caso la responsabilidad penal recae sobre el atacante, el cual es muy difícil de ubicar. Si se lograra ubicar e instaurar una acción penal en su contra la ley permite constituir la parte civil dentro del proceso penal. Es decir las dos responsabilidades analizadas, la civil y la penal dentro de un solo proceso de tipo penal. En la hipótesis contraria de que no se pueda dar con el paradero del Atacante la responsabilidad penal se desvirtúa por falta de sujeto, y la responsabilidad civil recaerá sobre el sitio web que es la verdadera víctima del delito.

EL artículo 195 hace referencia a los *sistemas informáticos protegidos con medida de seguridad*, como por ejemplo contraseñas de acceso o Firewall. El artículo no prevé los casos de aquellos sistemas que no están protegidos por medidas de seguridad, lo que generaría una atipicidad de la conducta. Se debe entrar a definir en un caso concreto por un perito si se esta frente a un sistema con medida de seguridad o no.

### 3.2 CASO: Olfateo de conexiones

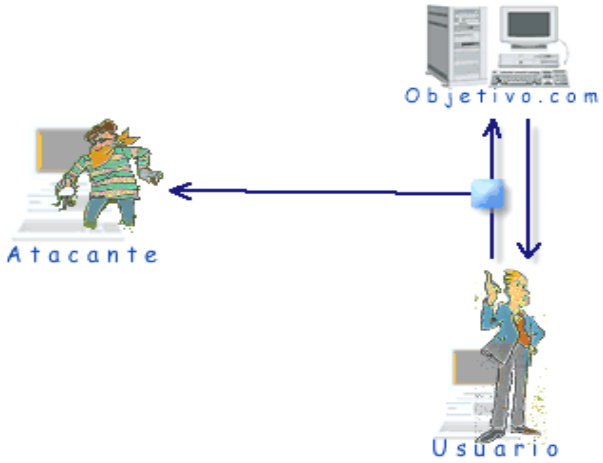
Nuevamente hay un sitio, Objetivo.com con todas las características ya mencionadas y un usuario que accede a este sitio para realizar la compra a través de Internet de un determinado producto. El usuario elige pagar con su tarjeta de crédito VISA y envía los datos personales y posteriormente los datos de su tarjeta de crédito.

La conexión que se establece con el sitio Objetivo.com para enviar esta información es a través del protocolo SSL pero la configuración realizada en el servidor de Objetivo.com solo establece el cifrado en el momento de enviar los datos mas críticos, es decir, los datos de la tarjeta de crédito.

Cuando esta establecida la conexión un atacante la intercepta utilizando un programa tipo Sniff (olfatedador que se aprovecha que en Internet el tiempo es compartido) y logra capturar datos personales de la víctima como su nombre, edad, y que tipo de producto esta comprando. El atacante que ha obtenido estos datos los vende a una empresa de publicidad que aprovecha esta información para ofrecer publicidad personalizada a la víctima.

Surgen dos puntos importantes. Primero si la responsabilidad es del sitio Objetivo.com por no garantizar la seguridad de todos los datos de sus clientes.

El segundo punto consiste en que la víctima de este Hurto de información esta en la libertad de elegir en que sitios compra y decidió hacerlo en Objetivo.com. También se debe considerar si la víctima envió sus datos a sabiendas que podían ser capturados por un tercero o sino lo sabia por una labor de desinformación del sitio Objetivo.com.




**Gráfica 8. Olfateo de conexiones**

**Responsabilidad Penal**

A un primer análisis se podría catalogar que la conducta se encuadra en los artículos 192 y 239 del Código Penal referentes a Violación ilícita de Telecomunicaciones y Hurto respectivamente. Sin embargo si se analiza la antijuridicidad de la conducta no seria posible encasillarla dentro del delito de hurto ya que la información plagiada no se puede considerar como una información valiosa que deba ser guardar con recelo, pues como lo plantea el caso se refiere a los datos generales y públicos de la persona como lo es el nombre la dirección electrónica y la edad, por lo que con su adquisición no se está poniendo efectivamente en peligro el patrimonio económico que es el bien jurídico que tutela el delito de Hurto.

La adecuación típica se encuadraría únicamente en el artículo 192 del Código Penal referente a la violación ilícita de comunicaciones y el sujeto activo de la acción penal seria el Cracker que obtuvo ilícitamente la información. Se encuadra en este tipo penal por el verbo rector Sustraer que plantea el artículo y por tratarse de una comunicación, en el caso 1 se trataba de una información que se caracterizaba por estar almacenada, mientras que es este caso se trata de un intercambio de información es decir de una comunicación.

Tampoco es correcto el pretender derivar una responsabilidad de carácter penal contra el sitio Web por no cifrar los datos ya que su conducta no es típica, es decir que no encuentra asidero en ningún artículo del Código Penal.

**La responsabilidad Civil**

En el caso planteado para que exista una responsabilidad civil se debe configurar un daño al usuario, como ya se analizó hay ausencia de daño o este no se puede determinar de forma clara en un eventual proceso ni mucho menos fijar su tasación, por lo que se puede concluir que en este caso no hay responsabilidad civil.

**Conclusión.**

Para lograr una mejor adecuación punitiva de la conducta dentro de uno de los verbos rectores que plantea el artículo 192 es conveniente hacer una diferenciación entre *Interrupción* e *intercepción*. La interrupción impide el paso de los datos que viajan a través

de un canal impidiendo así la comunicación entre las partes, en tanto que la *intercepción* no la impide y solo busca conocer la información sin evitar el paso de los datos.

En el caso planteado por tratarse de un olfateo de conexiones en la que no se impide el paso de la comunicación entre el servidor que contiene la página y el usuario se habla de una intercepción de comunicaciones que tiene como fin la sustracción de una información.

### 3.3 CASO: DoS

Para este caso la víctima es directamente el sitio Objetivo.com que ofrece el servicio de venta de sus productos a través de Internet. Un atacante que se aprovecha de una vulnerabilidad de desbordamiento de buffer causa la suspensión de los servicios Web del sitio por un lapso de dos horas durante la noche, después de las cuales el administrador de Objetivo.com se percata del hecho y reanuda el servicio. Durante el tiempo de suspensión del servicio dejaron de acceder, según las estadísticas de Objetivo.com, un promedio de 1000 visitantes al sitio lo que representa graves perdidas en términos de ventas y publicidad.

Después de realizar un análisis de los registros de sucesos del sistema, el administrador de Objetivo.com determinó la dirección IP del atacante y corresponde a una universidad de una ciudad cercana.


**Gráfica 9 Denegación del servicio.**

### Responsabilidad Penal

Como se ha venido diciendo la responsabilidad penal es de carácter personal. En el caso planteado la responsabilidad penal solo podría recaer sobre la persona que realizó el ataque contra el sitio Web y no contra la entidad a la que pertenece el equipo atacante, en este caso la Universidad. La conducta del atacante se podría tipificar dentro del delito de

Daño en bien ajeno, teniendo en cuenta que la información es un bien mueble, consagrado en el artículo 265 del Código penal en concurso con el delito de acceso abusivo a un sistema informático del artículo 195.

El artículo 265 del Código penal dice:

**Daño en bien ajeno:**

*"El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno mueble o inmueble incurrirá en prisión de uno (1) a cinco (5) años y multa de cinco a veinticinco salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor".*

Es importante tener en cuenta la cuantía del daño sobre el objeto del delito para establecer los agravantes que consagra la ley penal.

**Responsabilidad Civil:** Esta si podría recaer en un eventual proceso contra la entidad a la que pertenece el equipo atacante y la dirección IP. En el caso planteado a una Universidad. Se debe entrar a determinar en el campo procesal si la universidad es de carácter público o privada para entrar a establecer si corresponde al derecho administrativo o al derecho civil.

**Conclusión.**

El daño no es tanto sobre el servidor como tal, es decir el equipo no sufre daños físicos ni en su lógica, simplemente es una saturación que induce a un bloqueo temporal del equipo, sino que el daño recae sobre la imagen y buen nombre del sitio web, además de las perdidas económicas que implica la falta de acceso a este por parte de los usuarios.

### 3.4 CASO: Suplantación

Como en el caso número uno, existe una víctima que se conecta a un sitio Objetivo.com para realizar una transacción comercial sobre la plataforma que ofrece Internet.

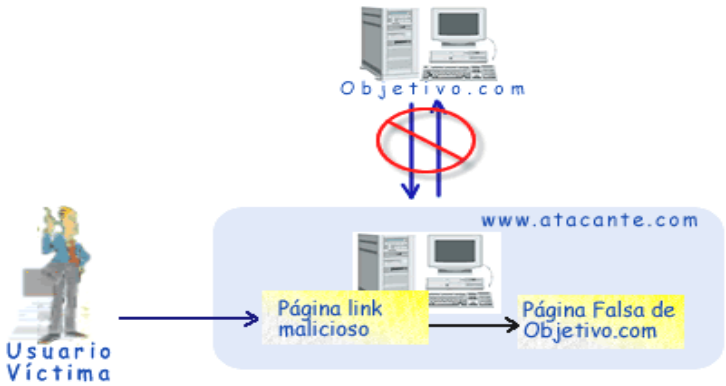
La víctima está navegando en un sitio Web que se llamará Atacante.com en el que encuentra un enlace interesante para realizar sus compras a través de Internet. El enlace supuestamente es hacia Objetivo.com. La víctima verifica la dirección a la que apunta el

enlace mirando en la barra de estado de su navegador y efectivamente aparece la dirección electrónica de Objetivo.com, así que la víctima decide entrar al nuevo sitio a través de ese enlace. Cuando carga la página principal del supuesto sitio Objetivo.com se percata que no aparece la barra de direcciones en su navegador pero no le parece un detalle importante. La página en la que está la víctima es idéntica en cuanto a su presentación gráfica a Objetivo.com pero corresponde a una falsificación elaborada por Atacante.com, así se logra engañar a la víctima y esta procede a ordenar sus productos y a llenar los formularios de información confidencial, que en realidad está enviando hacia el sitio atacante.com que para esta caso se podría denominar sitio atacante.

Para evitar sospechas, una vez Atacante.com ha recolectado la suficiente información de la víctima muestra un mensaje de error falso que supuestamente se produjo al enviar los formularios con la información y redirecciona a la víctima al verdadero sitio Objetivo.com.

En este caso se puede considerar a Objetivo.com también como una víctima debido a la perdida de credibilidad y prestigio que puede sufrir.

Es importante notar que todo este proceso es totalmente independiente de Objetivo.com, que no participa ni se percata del hecho. De todas maneras si se debe considerar que Objetivo.com, aunque podría tener implementado un servicio de cifrado de sus datos como SSL, no cuenta con un certificado digital que garantice a un visitante a su sitio que efectivamente esta en él.




**Gráfica 10 Suplantación**

**Responsabilidad Penal**

El usuario entrega datos importantes que aunque no han sido utilizados existe un alto riesgo de que sean utilizados, por lo que según la teoría de la Información como bien jurídico intermedio, esta es protegida así no haya sido utilizada para cometer un delito individual.

La adecuación punitiva del caso planteado correspondería a los artículos 192 y 239 del Código Penal que corresponden a los delitos de Violación ilícita de comunicación y hurto respectivamente, se utiliza aquí también la figura del concurso de delitos. Si con la información obtenida se persigue un provecho económico no encuadraría dentro de la figura del hurto sino de la estafa ya que se esta engañando al usuario a traves de al suplantación de páginas web.

Se encuadra dentro del artículo 192 porque existe una sustracción de información por medio de la interrupción de una comunicación privada. Aquí se nota mas la actitud dolosa del atacante, que tiene que diseñar la falsa página y la página donde se encuentra el link malicioso con el fin de engañar al usuario víctima del robo de información.

En el caso planteado es más fácil ubicar al delincuente, que seria el dueño del sitio web Atacante.com, puesto que este debe dejar algún registro al momento de comprar el dominio del sitio web.

**Responsabilidad Civil**

Según el grado de conocimiento que tenga el usuario víctima del hurto se puede establecer si existe falta de diligencia o no, puesto que él verifica en el enlace con el sitio web que la dirección electrónica aparezca en su barra de estado, se da cuenta de que no aparece la dirección electrónica en la barra de direcciones y a pesar de eso continua navegando. La responsabilidad civil recaerá sobre el propietario del sitio web atacante.com sea este una persona natural o jurídica.

Por otra parte el sitio Objetivo.com también se ve afectado, ya no por el robo de información sino porque su nombre se ve en medio de una conducta criminal, lo que

afectaría su buen nombre y su credibilidad frente al público quienes quedarán prevenidos en el momento de querer realizar un acto de comercio electrónico con este.

Que el sitio Objetivo.com no tenga el certificado que garantice que se esta navegando en él no constituye una causal que permita derivarle responsabilidad civil a este, pues la función que cumple el certificado es la de brindar seguridad a los usuarios y no constituye un requisito legal.

**Conclusión:**

Para este caso se puede concluir que no es suficiente las regulaciones jurídicas si no que la solución principal esta en aumentar el grado de conocimiento y de prudencia por parte de los usuarios a la hora de utilizar el comercio electrónico.

### 3.5 CASO: Troyano

La víctima que esta navegando desde su equipo llega a un interesante sitio Web, Objetivo.com que le ofrece una determinada herramienta software para encontrar promociones en Internet, pero que hace la aclaración que no se responsabiliza por las aplicaciones software proveídas allí. La víctima, que no nota el mensaje de advertencia, efectivamente descarga el software a su equipo y lo instala. La herramienta software cumple con las características anunciadas y la víctima lo sigue utilizando con frecuencia. Pero en realidad cada vez que se conecta a Internet y utiliza la herramienta, esta está recolectando información personal del equipo de la víctima y la envía a una cuenta de correo electrónico en Internet que no es posible rastrear. El software con código malicioso no es creado por el sitio Objetivo.com, en la mayoría de estos casos es creado por un tercero ubicado en Internet fuera del dominio de Objetivo.com que es el directo beneficiado con la información sustraída al usuario.

Cuando la víctima se da cuenta del fraude y de la perdida de información ya han pasado varios meses y no es posible determinar que información ha sido extraída de su equipo.

Cabe recordar que el sitio Objetivo.com que provee el programa con el que se engaña la víctima coloca un mensaje en el que expresa no hacerse responsable por los programas que está suministrando al público.


**Gráfica 11 Troyano**

**Hipótesis de Solución**

El que el sitio web tenga un mensaje dirigido al público en el que advierte no hacerse responsable sobre los programas ahí suministrados no implica la total exclusión de responsabilidad de este, se debe entrar a analizar otros factores como la buena fe por parte del sitio Objetivo.com y la diligencia calificada por parte del usuario. En otras disciplinas como en el derecho médico se ha ido construyendo derecho en contra de las cláusulas de los contratos en los que las clínicas se eximen de responsabilidad por los actos médicos, en el caso planteado no existe un precedente doctrinal ni jurisprudencial que permita sentar una posición en la que se derive algún tipo de responsabilidad al sitio web.

**Responsabilidad Penal**

La responsabilidad penal recaería sobre el tercero que creó el software malicioso, y que se beneficia con el robo de la información.

La adecuación punitiva se da en los artículos 192 violación ilícita de comunicaciones y 239 Hurto. Es de tener en cuenta que si lo que se persigue con la conducta engañosa es un provecho económico se tipificaría como Estafa del articulo 246 del Código penal. Si no existiera dicho provecho económico seria simplemente hurto de información.

La efectividad de la sanción penal se hace de difícil aplicación porque se desconoce el paradero del atacante y no deja rastros que permitan su captura.

**Responsabilidad Civil**

Como se planteó en la hipótesis de solución, no es posible establecer con certeza la responsabilidad civil del sitio web que suministra el programa malicioso.

Se podría argumentar en defensa del sitio web que este no fue el creador del programa, que no se beneficia con el robo de la información y que actuó de buena fe, por lo que no es responsable civilmente del ilícito. Por otra parte se puede argumentar en contra del sitio web que éste estaba en la obligación de revisar los programas en él ofrecidos evitando los programas maliciosos, por lo que si seria responsable civilmente. En este trabajo se considera que el sitio Objetivo.com, si es responsable civilmente porque tecnológicamente es posible detectar Spyware.

**Conclusión:**

Se hace necesaria la expedición a nivel nacional de una ley sobre los delitos informáticos que complemente el código penal y permita castigar con penas de prisión las conductas criminales de los Crackers, además de la unificación mundial de la consagración de los delitos informáticos que permita su castigo en cualquier parte del mundo sin necesidad de trámites engorrosos sobre equivalencia de penas de un país a otro, ni los relacionados con la extradición.

La escasez de casos sobre el tema en los estrados judiciales no permite crear un precedente jurisprudencial que sirva de base argumentativa en futuros litigios, además la doctrina no es lo suficientemente profunda sobre el tema de los delitos informáticos como para tomarla de punto de referencia y los análisis realizados por esta son desde el punto de vista jurídico sin tener en cuenta el componente tecnológico.

## 3.7 ADECUACIÓN DE LOS ATAQUES INFORMÁTICOS A LOS VERBOS RECTORES DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL A TRAVEZ DE LOS MODUS OPERANDI DE ESTOS.

Se han planteado una serie de técnicas de ataque desde el punto de vista netamente tecnológico y unos artículos del Código Penal que consagran como delitos algunas conductas o verbos rectores. Nos proponemos ahora encuadrar dichas formas de ataques

en los verbos rectores de los artículos, para esto nos valemos de los modus operandi que se puede entender como la forma de realizar un delito. Presentamos a continuación una tabla en la que se plantea una secuencia lógica entre los ataques tecnológicos, la forma en que estos se materializan o sea los modus operandi, los efectos tecnológicos que los modus operandi pretenden conseguir para finalmente encuadrarlos en los verbos rectores de los artículos 192 y195 del código penal.

Los efectos tecnológicos parten de la hipótesis de que estos son lo más dañinos posibles para poder así, sin entrar a analizar casos concretos plantear categorías que demuestren que es posible con nuestra precaria legislación penalizar las conductas de los Crackers.

| Ataques | Modus-Operandi | Finalidad | Verbos Rectores |
|---|---|---|---|
| Ataques dirigidos a datos | Introducción de datos maliciosos en un campo de texto de una página Web | Sustitución de datos del sistema, denegación del servicio | Destruir, controlar, Introducirse abusivamente |
| | Desbordamiento de buffer | Ver información del sistema, ejecución de código arbitrario | Controlar, sustraer, Introducirse abusivamente |
| | Virus informáticos: Gusanos, troyanos y bombas lógicas | Daño del sistema, perdida de información | Destruir, sustraer, impedir, introducirse abusivamente |
| Ataques de Ingeniería Social | Obtener información de conversaciones en Chats | Perdida de información potencialmente peligrosa | No hay adecuación posible |
| | Recolección de información en comunidades virtuales | Perdida de información potencialmente peligrosa | No hay adecuación posible |
| | Análisis del contenido de un sitio Web | Perdida de información | No hay adecuación posible |

| | | | |
|---|---|---|---|
| Ataques de fuerza bruta | Métodos de diccionario | Perdida de información, intrusión arbitraria, | Introducirse abusivamente, sustraer |
| | Métodos de pruebas masivas aleatorias | Perdida de información, intrusión arbitraria, | Introducirse abusivamente |
| Ataques de Suplantación | Correos de falso remitente | Engaño, perdida de información | Desviación |
| | Falsificación del contenido páginas Web | Engaño, robo de información | Introducirse, interceptar |
| | Actos tendientes a suplantar un sitio Web utilizando un dominio similar | Robo de información, suplantación, engaño | Introducirse abusivamente, desviación |
| Ataques de Denegación del Servicio | Inundación de pings | Denegar el servicio | Destruir, impedir |
| | bombardeo de e-mails | Denegar el servicio | Destruir, impedir |

**Tabla 1**

Se concluye que la ley 599 de 2000**,** actual código penal regula de manera dispersa y sin criterio de unificación el tema de los delitos informáticos, a diferencia de las legislaciones española y alemana que si los consagran de manera mas explicita y organizada. También consagra el Código Penal el pinchado de líneas que para este caso se puede referir a un sniffer y la fuga de datos que se puede dar en el aprovechamiento de puertas traseras, estas conductas no fueron incluidas en la tabla anterior porque no se pueden catalogar como ataque informático como tal porque no constituyen un modus oprendi sino que aprovechan unas circunstancias de falta de diligencia y cuidado del administrador del sistema, es decir, en estos no se planea un ataque sino que se aprovecha una oportunidad evidente. En la cotidianidad se puede comparar con un ladrón que ingresa a

robar a una casa que tiene la puerta abierta, aquí igual se comete un delito pero no un ataque para ingresar existiendo culpa de la víctima.

Existen también conductas que aunque utilicen líneas telemáticas o sistemas informáticos pueden ser sancionados dentro de la descripción de otros delitos de nuestro código penal sin que se requiera una lesión al bien jurídico intermedio, se hace referencia por ejemplo a la manipulación fraudulenta de cajeros automáticos que puede encuadrarse en el daño en bien ajeno y hurto.

Se acaba de hacer un estudio tecnológico de la seguridad del comercio electrónico desarrollando conceptos de ataques, vulnerabilidades y efectos enfocados al análisis de una muestra de los Sitios web colombianos que realizan comercio electrónico. Se pasa a continuación a un estudio de casos en el que se interrelaciona los conceptos jurídicos y tecnológicos estudiados hasta el momento.

Hasta este momento se analizado y clarificado la situación de la seguridad del comercio electrónico en Colombia. Pero antes de plantear las recomendaciones derivadas de este trabajo es importante buscar puntos de referencia a nivel internacional para situar el trabajo en un contexto mas real. En el siguiente capítulo se realizará una comparación de la situación de la seguridad del comercio electrónico de Colombia y algunos otros países.

# CAPITULO IV
# SEGURIDAD DEL COMERCIO ELECTRÓNICO DESDE LA PERSPECTIVA JURÍDICA A NIVEL INTERNACIONAL

## 4.1 Conceptos generales sobre la legislación internacional

Como se ha reiterado en los capítulos anteriores no se pueden tomar las legislaciones internas de los Estados de forma independiente sino que por el contrario debido a la globalización de Internet es necesario que se busque parámetros de unificación de las normas de cada Estado. En este capítulo se utiliza entonces el derecho comparado como mecanismo para la evaluación de la seguridad del comercio electrónico desde la perspectiva jurídica.

Antes de empezar a realizar los análisis de las legislaciones internacionales en materia de comercio electrónico y de los delitos informáticos se debe considerar que el acceso a la tecnología informática tiene las misma facilidades desde cualquier lugar del mundo, es decir, una persona desde cualquier parte del mundo puede comprar una máquina Servidor directamente en Estados Unidos e instalarlo como servidor Web en cualquier país y así mismo cualquier usuario de Internet podrá acceder a ese servidor. Existen barreras económicas en el acceso a la tecnología que para el caso no son tan influyentes debido a la operación de empresas transnacionales que pueden acceder a la tecnología e instalarla en cualquier país. Con esto lo que se pretende es argumentar que el objeto de regulación de las legislaciones de cada Estado es el mismo.

Se puede decir que los sistemas informáticos tienen las mismas características y arquitecturas a nivel mundial, a pesar que la infraestructura informática en los países desarrollados es más robusta los tipos de aplicaciones y sistemas operativos son los mismos que en Colombia. Las tecnologías para brindar seguridad a los sistemas de comercio electrónico con SSL y los certificados de confianza otorgados por entidades de certificación que operan a nivel mundial.

El factor en el que definitivamente están más adelantados ciertos países como España, Argentina y Estados Unidos es en el uso y manipulación de sistemas de pago no tradicionales como las tarjetas de crédito y los cheques electrónicos. Factor que aunque es beneficioso para su economía y desarrollo de tecnologías los coloca en una situación más vulnerable a los delitos informáticos relacionados con las transacciones electrónicas comerciales.

Para hacerse una idea de una manera global de la tecnología que se maneja a nivel mundial para demostrar que tecnológicamente Colombia no tiene gran diferencia con otros países que tienen una legislación sobre delitos informáticos más avanzada, aunque puedan existir diferencias económicas que hagan que la penetración de las tecnologías no sea de la misma manera y con la misma profundidad, se analizaron los sitios Web de 5 de las empresas transnacionales proveedoras de tecnología hardware reconocidas a nivel nacional: Ericsson, Cisco Systems Inc, Nortel Networks Limited, IBM y Siemens AG[26].

Las entidades de certificación en muchas ocasiones son internacionales y prestan sus servicios a Sitios Web de origen colombiano, y las que son empresas Colombianas como Certicamara S.A. que siguen los lineamientos de las empresas internacionales perfiladas por la Ley modelo de la CNUDMI.

A nivel de software es claro el dominio mundial de las tecnologías de Microsoft en especial los sistemas operativos Windows y el Internet Information Server. Y con la creciente aceptación de los sistemas operativos Unix se corrobora una vez más la universalidad en cuanto a tecnología de los sistemas informáticos.

Si tecnológicamente no existe gran diferencia entre los sistemas informáticos utilizados por otros países y los utilizados en Colombia, teniendo en cuenta además que por la globalidad de Internet los delitos informáticos se pueden realizar desde cualquier parte del mundo, las regulaciones jurídicas para los delitos informáticos deberían estar unificadas o guardar relación y coherencia que permita su fácil aplicación entre Estados.

[26] Ericsson (www.ericsson.com), Cisco Systems, Inc (www.cisco.com), Nortel Networks Limited (www.nortelnetworks.com), IBM (www.ibm.com) y Siemens AG (www.siemens.com).

Se tomará para el presente análisis de Derecho comparado las dos ramas del derecho que se han manejado a lo largo del documento. El derecho Comercial haciendo énfasis en la ley modelo de la Comisión de las naciones unidas para el Comercio electrónico y por el Derecho penal ya que es el eje fundamental la penalización y normalización de los delitos informáticos para poder proteger el comercio electrónico.

### 4.2 Antecedentes

#### 4.2.1 Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y sus efectos se adoptó la "Segunda Ley contra la Criminalidad Económica" de 1986 en la que se contemplan los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos. Tipificando la cancelación, inutilización o alteración de datos.
- Sabotaje informático. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos.
- Utilización abusiva de cheques o tarjetas de crédito.

Es de anotar que Alemania es un Estado que ya en el año 1986 tenia una ley con contenido tecnológico y que tipificaba conductas que aun no están como punibles en Colombia.

Los delitos mencionados anteriormente son solamente parte de la doctrina en nuestro país, ya que en nuestra legislación no existe un artículo del código penal ni mucho menos de una ley que lo complemente que haga mención, por ejemplo al sabotaje informático el cual se puede entender como: El acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

#### 4.2.2 Austria

El Estado austriaco en la ley de reforma de su Código Penal de diciembre de 1987 consagró los siguientes delitos:

- Destrucción de datos. En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática. En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

### 4.2.3 Francia

El parlamento francés expidió la ley número 88-19 de 5 de enero de 1988 sobre el fraude informático. Las conductas que se tipifican como delitos en esta ley son:

- Acceso fraudulento a un sistema de elaboración de datos. Que sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático. Se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos. Se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informáticos. Se sanciona a quien de cualquier modo falsifique documentos informáticos con intención de causar un perjuicio a otro.
- Uso de documentos informáticos falsos.

### 4.2.4 Chile

El Estado chileno fue el primer país de Latinoamérica en aprobar una ley relativa a los delitos informáticos en 1993 con la Ley No. 19223, la cual cuenta solo con cuatro artículos, pero que son precisos y enfocados en los delitos informáticos.

La ley 19223 de Chile maneja como tema central y único el de los delitos informáticos a diferencia de otros países que incluyen el tema de los delitos informáticos dentro de otras leyes que manejan como tema central otro diferente.

### 4.2.5 Costa Rica

La asamblea legislativa de la Republica de Costa Rica adiciono por medio de la Ley No.8148 del 25 de octubre de 2001 tres nuevos artículos; los 196bis, 217bis y 229bis al código penal Costarricense para el tratamiento especifico de los delitos informáticos. Actualmente Costa Rica tiene un proyecto de Ley sobre firmas y documentos electrónicos.

### 4.2.6 Perú

En agosto del 1999 el gobierno peruano incorporó dos nuevos artículos también a su código penal referentes a los delitos informáticos.

Aunque la normatividad peruana es corta cubre un campo bastante amplio de los delitos informáticos y es asertiva.

### 4.2.7 Venezuela

La Ley especial contra los delitos informáticos de Venezuela es una de las más extensas de Latinoamérica, cuenta con treinta y tres artículos. Esta ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas. Esta ley que fue firmada en septiembre de 2001 y consagra los delitos contra los sistemas, la propiedad, la privacidad con sus correspondientes definiciones y agravantes. A diferencia de otras legislaciones de otros países que dedica un artículo a cada tipo de delito, la legislación venezolana dedica un titulo a cada tipo.

Es de resaltar que en el artículo 3º de la ley Especial Contra Delitos informáticos expedida en octubre de 2001 hace referencia a la extraterritorialidad de la ley y dice:
*“Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido*

*juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros".*

### 4.3 Parámetros de referencia legislativa

Se puede ver que las legislaciones de otros países apuntan a penalizar delitos específicamente informáticos, es decir, no utilizan conceptos que surgen de otros delitos tradicionales para tipificar delitos informáticos sino que crean los nuevos conceptos que se adaptan de una manera más precisa a las acciones, por ejemplo las legislaciones de Alemania, Francia y Austria que expresan específicamente la destrucción de datos como delito.

Aunque se realiza un breve repaso a la legislación de varias naciones que tratan las conductas que afectan el comercio electrónico, se hará énfasis a continuación en el análisis a las legislaciones española, estadounidense y argentina que servirán como punto de comparación con la legislación colombiana.

España porque es uno de los países europeos que más a tratado el tema de los delitos informáticos. En España se encuentra una de las comunidades Hackers más extensa y fuerte del mundo. Otra razón para considerar a España es la afinidad con el idioma.

Se analizó la legislación Estadounidense porque aunque jurídicamente es bastante diferente a Colombia por su sistema jurisprudencial[27], Estados Unidos tiene una clara influencia social, política y económica en Colombia. Además Estados Unidos fue uno de los primeros países en el mundo en penalizar delitos informáticos y tienen un excelente sistema criminalístico de persecución de Hackers y Crackers.

A nivel de Latinoamérica se decidió analizar la legislación Argentina ya que es el país Latinoamericano que hace un tratamiento mas profundo a los delitos informáticos. Otro

[27] El derecho estadounidense se basa en la jurisprudencia es decir en las decisiones judiciales y no en la codificación de normas como es el caso de Colombia. Este tipo de derecho jurisprudencial es herencia del derecho ingles. En Colombia las decisiones de los jueces no son fuente formal de derecho pues el artículo 330 de nuestra Constitución política reconoce como única fuente formal de derecho a la ley y la jurisprudencia es fuente auxiliar.

punto importante que se considero es que tanto Argentina como Estados Unidos cuentan con importantes comunidades Hackers.

### 4.3.1 España:

**Legislación comercial española en relación con la seguridad del comercio electrónico.**

En las legislaciones de Colombia y la legislación española existe equivalencia entre el Real Decreto ley 14/1999, de 17 de septiembre, sobre firma electrónica y la Ley 527 sobre comercio electrónico.

En términos generales el Real Decreto español es mas técnico, de la simple lectura del articulado se establece que en su elaboración colaboraron profesionales de la ingeniería lo que le da una visión más exacta de los conceptos. Lo que no se presenta por ejemplo en los artículos 192 y 195 del código penal colombiano mencionados en el capítulo anterior.

El antecedente principal de la ley 527 de 1999 de Colombia fue la ley modelo para el comercio electrónico creada por la CNUDMI y se había afirmado en el primer capítulo que era una fiel copia de esta, el Real Decreto Español aunque también habla de las firmas digitales y de las entidades de certificación no es una copia idéntica de la ley modelo de la CNUDMI sino que va más allá dando definiciones tecnológicas sobre la creación y verificación de firmas electrónicas. Su contenido es más amplio pues no se centra en el comercio electrónico sino que su tema central es el de la firma electrónica que puede ser utilizada en general en cualquier intercambio electrónico de datos.

El Real Decreto hace una diferencia entre firma electrónica y firma electrónica avanzada, la cual consiste en que la primera no tiene validez legal mientras la segunda si la tiene, al igual que en la ley 527 colombiana la firma electrónica avanzada puede estar certificada por una entidad de certificación que avalará la firma, con esto se presume la autenticidad de la firma. En este punto se concluye que no existe ninguna diferenciación de fondo entre la legislación colombiana y la española.

En la legislación española la supervisión de las entidades prestadoras de servicios de certificación está a cargo de la Secretaría General de Comunicaciones del Ministerio de Fomento mientras que en Colombia la encargada de la supervisión y control es la Superintendencia de Industria y Comercio. El Real Decreto español logra un mayor conocimiento de los inconvenientes de las firmas electrónicas y del comercio electrónico desde lo tecnológico, mientras que la ley 527 lo abarca mas desde lo comercial.

De manera similar tanto el Real Decreto español como la Ley 527 de Colombia establecen una lista de obligaciones a las entidades de Certificación haciendo énfasis en garantizar la seguridad del certificado, el real decreto establece en el numeral c del artículo 11 la prohibición de almacenar y copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en el caso de que ésta lo solicite.

El Real Decreto español establece en el artículo 14 de forma muy acertada las Responsabilidad de los prestadores de servicios de certificación. Dicho artículo reza así: *"Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia."* No se consagra aquí una responsabilidad objetiva pues se debe entrar demostrar la negligencia de la Entidad Certificadora, la ley 527 no trae un artículo similar pero igualmente nuestra legislación permite responsabilizar a la Entidad Certificadora por los daños causados cuando esta ha actuado con negligencia.

Finalmente establece el Real Decreto una serie de infracciones y sanciones para el incumplimiento de lo establecido en el Real decreto acarreando multas de distinto grado según la infracción. Estas multas no son penas si no que son sanciones pertenecientes al derecho disciplinario y no al penal. La ley 527 las establece de forma mas general y delega la facultad en la Superintendencia de Industria y Comercio.

También es conveniente citar como parámetro de la legislación española referente al comercio electrónico y firmas electrónicas la LSSI (Ley 34 / 2002, de 11 julio, sobre Servicios de la sociedad de la información y de comercio electrónico). LA LSSI es una ley

española que habla sobre la protección de los datos y el derecho a la privacidad sobre estos. Ha sido una ley muy controvertida por muchas comunidades expertas en informática entre ellas por la comunidad Hackers.

**Legislación penal española en relación con la seguridad del comercio electrónico.**
España ha sido un país muy preocupado por la regulación de los delitos informáticos, pretendiendo así por la seguridad del comercio electrónico, además como se había dicho anteriormente España tiene una de las más grandes comunidades de Hackers.

El Código Penal español tipifica aunque no en un capítulo especial las conductas que lesionan bienes jurídicos a través de la utilización de tecnologías principalmente de Internet.

El Art. 197 del Código Penal español tipifica conductas como apoderarse de mensajes de correo electrónico ajenos. Tal seria el caso de instalación de programa Sniffer, troyanos o el aprovechamiento de bugs o cualquier otra técnica de Hacking que permitan el acceso a un correo electrónico.

Los artículos 164 y 178 hacen referencia a la destrucción, alteración o daño de programas o documentos contenidos en ordenadores, esto se puede hacer a través de la instalación de un virus o de cualquier programa malicioso. El Art. 178 también tipifica el apoderamiento o difusión de documentos o datos electrónicos de empresas. Respecto al apoderamiento de secretos de empresas se presento un caso donde por primera vez en España se sentencio a una Hacker a tres años de cárcel más multa por descubrir secretos de empresa. La sentencia marca un precedente en delitos de revelación de secretos informáticos empresariales, dando aplicación al nuevo Código Penal.

El condenado de 26 años quien esta terminando sus estudios de ingeniería trabajaba como programador desde su casa para una empresa. En su defensa argumento que considera que *“el juez desconoce la informática, al llamar al código fuente abierto, código secreto"*, además *“si tener el código fuente de programas que estás haciendo para tu empresa en casa significa ir a prisión, tendrán que encerrar a todos los programadores”*

Más relacionada con la protección del comercio electrónico el Art. 248 del Código penal tipifica la estafa a través de la manipulación informática. Tal seria el caso de compras fraudulentas a través de Internet o fraudes en la banca electrónica a través de la usurpación de la identidad de la víctima. Por su parte el Art. 256 tipifica la utilización no consentida de un ordenador sin la autorización de su dueño causándole un perjuicio económico superior a 300,5 €. Unos 963,690.25 pesos colombianos a julio de 2003.

En lo referente a derechos de autor la legislación española tipifica la copia no autorizada de programas de música o películas, fabricación o distribución de programas que vulneren los programas anti-piratería. El tema de los derechos de autor por no pertenecer al tema central del documento se tratará en el Anexo E.

Se concluye que la legislación penal española es muy severa y adecuada al consagrar conductas comunes en la utilización de Internet, seria un buen antecedente de una futura ley colombiana que complemente a nuestro código penal en materia de delitos informáticos.

La crítica a la legislación penal española es que conductas tan frecuentes como son el Spam o el simple escaneo de puertos, difícilmente encuentran cabida entre los delitos tipificados en el Código Penal, por lo que no son perseguibles por vía penal. Si serian punibles estas conductas cuando sean utilizadas en la comisión de un delito como la denegación de servicio en un servidor web.

### 4.3.2 Estados Unidos:

**Legislación comercial estadounidense en relación con la seguridad del comercio electrónico.**

En un país con una economía fuerte como la estadounidense y en donde el índice de uso de tarjetas de crédito es grande el comercio electrónico juega un papel importante.

En los Estados Unidos fue aprobada el 30 de junio de 2000 la Ley Federal Sobre Firma Electrónica (*Electronic Signatures In Global And National Commerce Act),* que es equivalente a la Ley 527/99 en Colombia.

La norma estadounidense le otorga los efectos legales a los documentos y firmas electrónicas, tal como lo hace la Ley 527/99. Aunque la finalidad de la norma es similar a la de la Ley 527 se puede ver que esta es mucho más precisa y entra mas en detalles que la Ley 527. Sin hacer tantas definiciones de términos tecnológicos se cuida de las incidencias en otras normas anteriores, de seguir protegiendo los derechos de los consumidores y del comercio en general, además menciona expresamente la aplicación de la norma en asuntos relacionados con pólizas de seguros. La norma sobre las firmas electrónicas en el comercio global y nacional, menciona también las excepciones y situaciones en las que no se aplica, lo que hace que a diferencia de la Ley 527 tenga un ámbito de aplicación mas preciso.

Aunque el acta estadounidense no incluye como la Ley 527 el tratamiento de las entidades de certificación ni del transporte de mercancías en el comercio electrónico si hace énfasis en la promoción del comercio electrónico internacional[28] y la protección infantil "on-line"[29].

**Legislación penal estadounidense en relación con la seguridad del comercio electrónico.**

En cuanto a los delitos informáticos, desde 1986 Estados Unidos introdujo en su legislación la penalización a estos, con el Acta de Fraude y Abuso computacional de 1986. Esta acta fue revaluada y modificada con el Acta Federal de Abuso Computacional (*18 U.S.C*[30]*. Sec.1030*) de 1994, con la finalidad de eliminar argumentos y definiciones demasiado técnicas sobre los diferentes tipos de virus informáticos. En cambio, la nueva acta determina la ilegalidad en la transmisión con conocimiento de cualquier dato que pueda causar daño (*18 U.S.C.: Sec. 1030 (a) (5) (A)* ).

Asimismo, en materia de estafas electrónicas y otros actos dolosos realizados a través de sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red

[28] Titulo III de la norma
[29] Término usado en la norma en los asuntos referentes a Internet
[30] U.S.C.: United States Code se puede encontrar en http://www4.law.cornell.edu/uscode/

informática. Es importante notar que el Acta de 1994 es federal, es decir, que tiene aplicación en cualquier estado del territorio estadounidense.

Los Estadounidenses han ido mucho mas allá de los delitos informáticos o cybercrime como lo llaman ellos y han tratado de penalizar explícitamente toda actividad maliciosa que haga uso de una u otra manera de Internet, como el espionaje industrial y actos considerados para ellos como de terrorismo, como publicidad subversiva y el suministro de información peligrosa.

Se puede ver la severidad de las normas estadounidenses en comparación con las de Colombia en donde por prácticas de Spam se puede imputar hasta un año de cárcel mientras que en nuestra legislación las penalizaciones son de multas muy bajas.

### 4.3.3 Argentina:

**Legislación penal argentina en relación con la seguridad del comercio Electrónico**

Existe actualmente en la legislación Argentina un proyecto de ley que solo contiene seis artículos en los que se trata temas como el acceso ilegitimo informático, el daño informático, el fraude informático y unas disposiciones comunes en donde se definen de forma tecnológica un poco ambigua conceptos como el sistema informático, dato informático o información.

Con relación a la seguridad del comercio electrónico el artículo 5 del proyecto de ley mencionado referente al fraude informático consagra como punible con pena de prisión de un mes a seis años, a *"el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".*

En el caso del párrafo anterior, si el perjuicio recae en alguna administración pública, o entidad financiera, la pena será de dos a ocho años de prisión. Es un artículo muy amplio que permite encasillar aquí cualquier clase de conducta dolosa de fraude a través del comercio electrónico, ya que la interpretación de *"Artificio tecnológico"* puede ser muy amplia.

No es conveniente profundizar mas sobre el proyecto de ley por faltarle a este fuerza de ley y estar sujeto a continuas e inesperadas modificaciones.

**Legislación argentina comercial en relación con la seguridad de comercio electrónico.**

El congreso argentino promulgó la ley 25.506 del 11 de diciembre de 2001 sobre Firma Digital, por los temas que trata y por la forma de ubicación de estos en los artículos de la ley se concluye que tuvo como antecedente la ley modelo de la CNUDMI de 1996, al igual que la ley 527 / 99 de Colombia y el Real decreto ley 14 / 99 de España.

En la ley argentina también se hace una diferenciación entre las firmas avaladas por una entidad de certificación que están cobijadas por la presunción de que la firma pertenece al suscriptor del documento, y aquellas firmas que no están bajo la presunción de autoría por faltarle uno de los requisitos que establece la ley teniendo que entrar a demostrar su validez. En la ley argentina se las llama firmas digitales a las que gozan de la presunción de autoría y firmas electrónicas a las que no, presentando así una forma de definir las firmas electrónicas y las digitales muy distinta de la planteada en el capítulo primero de esta monografía.

Las similitudes entre la ley 527 / 99 de Colombia y su homologa Argentina son principalmente en temas como las entidades de certificación llamadas en la ley argentina como Certificadores Licenciados, los certificados digitales, las obligaciones de las entidades de certificación, el cese de actividades de las entidades de certificación y los derechos y obligaciones del titular del certificado digital.

Por la cantidad de similitudes entre las legislaciones argentina y colombiana lo mas adecuado es compararlas identificando sus diferencias: La ley argentina crea una comisión Asesora para la Infraestructura de Firma Digital integrada por 7 miembros de profesiones afines a la utilización de la firma digital, su función principal es la de emitir recomendaciones acerca de los estándares tecnológicos, el sistema de registro a implementar y los métodos de resguardar físicamente la información. La ley colombiana no crea un órgano con dichas funciones pero las delega a la Superintendencia de Industria y Comercio quien debía asignar a una de sus dependencias las funciones de

inspección, control y vigilancia de las actividades realizadas por las entidades de certificación. En este punto es mas elaborada la disposición de la ley argentina pues al crear una comisión de profesionales de distintas áreas del saber sus recomendaciones serán mas acertadas y eficientes.

Se concluye que es favorable para el comercio electrónico en virtud de la globalización de este el que exista una homogeneidad entre la regulación del comercio electrónico en Argentina y Colombia ya que fuertes centros impulsadores de esta forma de comercio se encuentran en Argentina como es el caso de Deremate.com.

**4.4 Conclusiones de la legislación internacional con respecto a la colombiana**

Es importante notar que en materia de penalización a los delitos informáticos varios de los países latinoamericanos cuentan con legislación especializada en este tipo de delitos mientras en Colombia los artículos del código penal que se toman en este trabajo y que son los que más se adecuan al tratamiento de los delitos informáticos no fueron creados específicamente para este tipo de delitos sino que fueron creados para ser usados en temas como la violación a la intimidad y reserva e interceptación de comunicaciones.

En este momento se encuentra en trámite la resolución del Ministerio de Comunicaciones por la cual se regula la administración del dominio ".co" por parte del Ministerio de Comunicaciones que tiene su fecha de expedición programada para el 14 de agosto de 2003 según lo consagra la resolución 00020 del 14 de enero de 2003.

En Colombia las pocas normas que regulan los aspectos relacionados con Internet reflejan lo disperso de la legislación nacional ya que no se encuentran en una sola normatividad que unifique criterios y clarifique la labor para los usuarios de Internet, en especial los que desempeñan labores relacionadas con el comercio, sino que están en múltiples normas y decretos que pertenecen a diferentes partes del estado. Por ejemplo, el decreto 1524 es un decreto para la regulación de la pornografía infantil en Internet, pero también tiene medidas para la regulación técnica de los ISP y además toca tangencialmente la prohibición del Spam en Colombia. No existen unos lineamientos claros en la normalización de los delitos informáticos.

Actualmente por desconocimiento de la gran cantidad de equivalencias entre las legislaciones y para evitarse procesos con leyes extranjeras se ha optado por la resolución de los conflictos a través de los Tribunales internacionales de arbitramento por lo que es conveniente detenerse en este aspecto para decir que son los tribunales de arbitramento y como funcionan.

Un tribunal de arbitramento es un órgano colegiado integrado por un número impar de personas llamadas árbitros quienes decidirán en derecho o en equidad sobre un conflicto que les ha sido encomendado. Finalmente la decisión se presenta en un documento llamado laudo arbitral el cual se puede comparar por sus efectos con una sentencia, este será obligatorio para las partes, pues estas han manifestado su voluntad a través de un contrato en el que expresan la intención de resolver el conflicto en un tribunal de arbitramento y acoger su decisión cualquiera que esta sea.

Existen dos clases de tribunales en equidad y en derecho, los primeros tienen como finalidad la justicia de forma más abstracta, los árbitros no son necesariamente abogados y fallan conforme al sentido común y sana crítica. Los tribunales en derecho tienen como finalidad la correcta interpretación y aplicación de una norma legal o de un principio del derecho, sus árbitros son necesariamente abogados.

El gran inconveniente de los tribunales de arbitramento es su elevado costo económico lo que impide un fácil acceso a estos para dirimir pequeños litigios, por el contrario su mayor ventaja es el corto tiempo en que se realiza el proceso.

Para lograr que en Colombia exista una ley que establezca delitos informáticos se requiere de un proceso de expedición de esta por parte del Congreso, este procedimiento inicia con la presentación de un proyecto de ley por parte de uno de lo congresistas o por el Presidente de la Republica. Dicho proyecto para que sea útil debe ser elaborado conjuntamente sectores conocedores del Derecho como de las nuevas tecnologías dando así mayor precisión a las conductas punibles.

# CAPITULO V
# CONCLUSIONES Y RECOMENDACIONES

Este trabajo empezó con un análisis sobre la legislación con la que cuenta Colombia para enfrentar el reto del comercio electrónico, considerando temas como las firmas electrónicas, sitios Web y penalización de los delitos informáticos, para en el segundo capítulo, desde una perspectiva tecnológica, encontrar la situación real de la seguridad del comercio electrónico, en el tercer capítulo ya con elementos de juicio tanto jurídicos como tecnológicos se realizó un Estudio de Casos en las que se tomaron situaciones planteadas tecnológicamente para darle soluciones con los elementos jurídicos con que cuenta actualmente Colombia. Por ultimo con soluciones jurídicas planteadas y una idea más amplia de la situación de la seguridad del comercio electrónico en Colombia desde la perspectiva jurídica se realizó en el Capítulo IV una comparación con legislaciones extranjeras de la situación normativa del comercio electrónico, tanto desde el derecho penal como el comercial.

Durante todo este proceso se han gestado una serie de conclusiones y recomendaciones muy puntuales que pueden ser útiles para ayudar a la seguridad del comercio electrónico. Muchas de las siguientes recomendaciones se realizan para las empresas que pueden actuar como comprador o vendedor en las relaciones del comercio electrónico.

- Considerar a todas las empresas que tengan acceso a la tecnología Internet vulnerables a los diferentes tipos de ataques ya planteados en este trabajo, ya sea que la empresa sea prestadora de servicios de comercio electrónico, usuaria o utilice su sitio Web únicamente para la labor comercial de publicidad, cada usuario y administrador de un sistema debe actuar entonces de forma diligente.

- Implementar en las políticas de seguridad y administración de las empresas un formulario de registro de irregularidades para el público al igual que un detallado registro interno de incidentes de seguridad que deberá ser estrictamente administrado.

- Implementar políticas de administración de tecnología informática estables, consecuentes con las políticas generales de la empresa, tales como establecer contraseñas robustas por parte de todos los empleados de la empresa fortificando la seguridad de esta, ya que una contraseña débil perteneciente a un empleado hace vulnerable todo el sistema. Estas políticas deben ser implementadas a largo plazo.

- Es importante para los administradores, desarrolladores y usuarios tener una adecuada política de obtención de información, con fuentes confiables y actuales para de esta forma ser más asertivos en la administración de parches de actualización y en el tratamiento de virus informáticos. Existen numerosas supuestas listas de seguridad en Internet que son foco de transmisión de Spam y no ofrecen una información confiable. Se recomiendan como fuentes confiables las listas de seguridad de Hispasec, CERT, SANS y NSA[31].

- Informase sobre la situación normativa del comercio electrónico teniendo en cuenta que estas se encuentran dispersas y en algunos casos consignadas en normas sobre otros temas, por ejemplo la Ley 633/2000 por la cual se expiden normas en materia tributaria, se dictan disposiciones sobre el tratamiento a los fondos obligatorios para la vivienda de interés social y se introducen normas para fortalecer las finanzas de la Rama Judicial regula también de forma muy poco evidente y en un solo artículo la inscripción de sitios Web en la Cámara de Comercio.

- Se recomienda que cada empresa debe contar con personal capacitado en la recolección de evidencia digital, análisis forense y formación de equipos de atención de incidentes en caso de presentarse ataques informáticos.

- Se debe tener en cuenta que en ocasiones los puntos más vulnerables en la seguridad de una empresa están ubicados dentro de la misma empresa y es importante determinarlo y contrarrestarlo con capacitaciones a los usuarios ubicados dentro de la red de computadores de la empresa, que los concienticen de los peligros del mal uso de los sistemas informáticos. Tales Políticas podrían ser: Simulacros

[31] http://www.hispasec.com, http://www.cert.org, http://www.sans.org, http://www.nsa.gov.

sobre parálisis del sistema informático, capacitaciones sobre el manejo de los formularios de incidentes, capacitaciones continuadas sobre la actualidad de los sistemas informáticos, distribución en la organización de las noticias sobre las penalizaciones nacionales e internacionales sobre delitos cometidos con tecnología y sobre el uso moderado de recursos computacionales de acuerdo a su finalidad dentro de la organización.

- Se recomienda a los usuarios acceder únicamente a sitios Web de comercio electrónico certificados por una entidad certificadora reconocida, verificar la validez del certificado y el sistema de cifrado que utiliza el sitio Web. No se debe confiar solamente en la verificación del icono del candado en la parte inferior de la ventana del navegador pues este puede colocar engañando al visitante. Se debe tener en cuenta el impedir la ejecución automática de scripts de Java y controles active X

- No ocultar nunca la barra de direcciones al navegar para evitar ataques de suplantación.

- Se debe actuar cuidadosamente en foros y servicios de mensajería instantánea como los Chats donde se comparten datos personales que puedan servir para ataques de ingeniería social.

- El sector financiero y empresarial, deberán hacer un gran esfuerzo económico y profesional para interconectarse y permitir el flujo de operaciones interbancarias que brinden un soporte tecnológico e industrial que ayude a crecer el comercio electrónico en Colombia y así los colombianos no sigan realizando sus compras en sitios web internacionales.

- El Estado colombiano debe fortificar la infraestructura de telecomunicaciones y acceso a Internet, y estimular el comercio electrónico por ejemplo concediéndole exención del IVA, a fin de ayudar a los empresarios a crear las poderosas organizaciones financieras, tecnológicas y logísticas que esta actividad requiere. Al igual de ayudar a constituir alianzas que puedan ser competitivas con centros de comercio electrónico de otros países.

- Las empresas deben transformarse para poder hacer mercadeo vía Internet aprendiendo a mantener una clientela virtual, a diseñar páginas web, pensar sus productos para un mercado globalizado con el grado de competitividad que esto implica.

- Los administradores deben utilizar programas de seguridad software que revisen en los equipos de la red la existencia de puertos abiertos no deseados. En este sentido es muy recomendable utilizar un Firewall ubicado en el acceso a Internet de la red y además Firewalls personales en los equipos de usuario.

- Los desarrolladores de software y sitios Web deben conocer muy bien las herramientas de desarrollo para que sus productos no hereden vulnerabilidades dependientes de las herramientas de desarrollo.

- Los desarrolladores deben ser muy cuidadosos en no utilizar imágenes y logos de otros sitios Web al diseñar un sitio Web para evitar problemas con los derechos de autor.

- Se concluye que al igual que las legislaciones de España y Argentina es importante que exista en Colombia una ley de protección de datos o Habeas Data.

- A pesar de no existir en Colombia una ley sobre delitos informáticos es posible realizar la adecuación punitiva de las conductas delictuales informáticas a los artículos de Código Penal como se planteó en el estudio de casos del Capítulo III.

- Comercialmente los usuarios de los sitios web de comercio electrónico deben actuar con diligencia calificada, leer todas las opciones que presenta el sitio web y las cláusulas de los contratos de vinculación al sitio, más aun cuando algunos sitios web tienen en letra menuda una aceptación tácita de los términos del sitio web por el solo hecho de acceder a estos.

# GLOSARIO

**GLOSARIO TECNOLÓGICO**

ADMINISTRADORES DE PROCESOS: aplicación que corre en un equipo o sistema y que permite la administración y manejo de los procesos que funcionan en este equipo.

ARCHIVO ADJUNTO (ATTACHMENT): fichero o archivo que se envía junto a un mensaje de correo electrónico. Puede contener cualquier objeto digitalizado: textos, gráficos, archivos de sonidos e imágenes fijas o en movimiento.

ANCHO DE BANDA: medida de capacidad de comunicación o velocidad de transmisión de datos de un circuito o canal, también se puede interpretar como la cantidad de datos que puede ser enviada o recibida durante un cierto tiempo a través de un determinado circuito de comunicación. Técnicamente, es la diferencia en hertzios (Hz) entre la frecuencia más alta y más baja de un canal de transmisión.

ASP: Active Server Page. Paginas de servidor activa. Tipo de paginas activas que corren en el servidor Web y que permiten la interacción con el usuario. Estas paginas se pueden identificar mediante la extensión .asp.

BACKDOORS: puertas traseras. Puerto abierto en un equipo que permite la fuga de información. En la mayoría de las ocasiones el usuario no sabe de la existencia de estas y es instalada sin su autorización consciente.

BARRA DE DIRECCIONES: barra flotante ubicada en la parte superior del navegador que indica la dirección electrónica de la pagina a la que se esta accediendo. Esta es fácilmente removible.

BARRA DE ESTADO: barra fija ubicada en la parte inferior del navegador que indica el estado de la conexión con la pagina Web que se esta solicitando.

BASE DE DATOS: conjunto de información para varios usuarios. Suele admitir la selección de acceso aleatorio y múltiples "vistas" o niveles de abstracción de los datos subyacentes.

BIT: cantidad de información más pequeña que puede transmitirse. Una combinación de bits puede indicar un carácter alfabético, un dígito, una señal, un modificador u otras funciones.

BUG: término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en 1945 cuando uno de los pioneros de la programación moderna descubrió que un insecto (bug) había dañado un circuito de un ordenador.

BUSCADOR: sitios en la red que actúan como herramientas que recopilan y estructuran sistemáticamente la información contenida en ella. Ayudan a los usuarios a buscar datos específicos, para lo cual se organizan en buscadores por palabras o índices y buscadores temático o directories.

CADENA ASCLL: cadena de caracteres presentada en su equivalente según la organización American Standar Code for Information Interchange.

CANAL: vía (canalización) de telecomunicaciones con una determinada capacidad (velocidad) entre dos ubicaciones de una red.

CERT: Computer Emergency Response Team.

CGI: (Interfaz de gateway común). Interfaz para programadores que crean archivos de comandos o aplicaciones que se ejecutan internamente en un servidor de Web. Estos archivos de comandos pueden generar texto y otros tipos de datos de forma inmediata, en respuesta a una entrada del usuario, o bien tomando la información de una base de datos.

CHAT (Charla): comunicación simultánea entre dos o más personas a través de Internet. De ahí que se diga que los internautas “chatean” cuando intercambian mensajes

instantáneamente por este medio. Antes sólo se podía hacer en forma escrita, pero hoy también es posible comunicarse utilizando audio y video.

CIBER: término griego que significa “máquina” o “nave”. Se utiliza como prefijo de un sinnúmero de conceptos relacionados con la red. Por ejemplo: ciberespacio, cibernauta y cibercultura.

CIFRADO: operación que transforma datos legibles en ilegibles con el objeto de resguardar cierta información que viaja por la red. Por ejemplo, los números de las tarjetas de crédito son encriptados para luego ser desencriptados sólo por el destinatario mediante una clave especial.

CLIENTE: computador o programa que accede a los servicios ofrecidos por otro computador o programa denominado servidor. Todas las aplicaciones de Internet que tienen los computadores personales para usar los servicios de la red son clientes.

CLIENTE/SERVIDOR: sistema sobre el que funciona Internet y que implica la separación de computadores o programas en dos categorías: servidor (ofrece información) y clientes (piden y reciben esta información).

CONTRASEÑA (PASSWORD): conjunto de caracteres que permite acceder a un determinado contenido en la red o que sirve para discriminar el acceso de los usuarios.

CRACKERS: delincuente informático que se dedica a causar daño a los sistemas solo en busca de beneficio propio. Delincuente que accede ilegalmente a sistemas informáticos para destruir información, modificarla o, en general, causar daño**.**

DEFACED: palabra usada en el idioma ingles para definir un sitio Web que ha sido vulnerado.

DESCARGAR: término que, al igual que “bajar”, identifica el proceso de transferir información desde un servidor de Internet hasta un computador local.

DIGITAL: dispositivo o método que utiliza variaciones discretas en voltaje, frecuencia, amplitud, ubicación, etc. para cifrar, procesar o transportar señales binarias (0 o 1) para datos informáticos, sonido, vídeo u otra información.

DOMINIO: etiqueta o conjunto de caracteres que identifica el sitio de una persona u organización en la red y que permite el acceso de los usuarios. Está ubicado a la derecha del signo @ en la dirección de Internet e informa a un servidor hacia donde dirigir la solicitud de observación de una página web.

EDI: Intercambio Electrónico de Datos. Definido en la Ley 527/99 se refiere al intercambio de datos en entre sistemas informáticos.

E-Mail (Correo Electrónico): aplicación que permite a los usuarios de la red intercambiar y almacenar mensajes enviados desde cualquier parte del mundo. Cada mensaje también se denomina e-mail.

E-Mail Address (Dirección de Correo Electrónico): Conjunto de caracteres que identifican exclusivamente a un servidor, persona o recurso conectado a Internet y que le permite enviar y recibir mensajes. Está compuesto por la identificación del usuario, el signo @ y los dominios correspondientes.

EXTENSIONES: son las tres letras que están ubicadas después del punto en un archivo que identifican las características y el tipo de archivo.

FAQ (Frequently Asked Questions): Documentos que contienen las preguntas más habituales sobre un determinado tema y sus correspondientes respuestas. Por lo general, cada sitio tiene su sección FAQ para aclarar dudas.

FINGER: protocolo que permite localizar información sobre los usuarios en la red del host. Algunas redes no permiten su uso desde un sistema externo, y otras no lo permiten en absoluto.

FIREWALL (CORTAFUEGOS): mecanismo de seguridad que aísla redes locales. Impide que los usuarios no autorizados de Internet accedan a ciertos ficheros del sistema. Suelen incorporar elementos de privacidad y autentificación, entre otros.

FRAMES (MARCOS): posibilidad que ofrece el lenguaje HTML de dividir una página web en varias zonas. Cada una de estas secciones independientes o frames puede tener un contenido distinto a las demás.

FTP: (Protocolo de transferencia de archivos). Protocolo utilizado para transferir archivos a través de una amplia variedad de sistemas.

GPL: Licencia Pública general. Se refiere a un tipo de licencia para software en la que los usuarios no tiene que pagar derechos de autor aunque no esta permitido la modificación o usufructuacion del software.

HACKER: experto computacional que al penetrar en sistemas informáticos de alta seguridad deja de manifiesto sus puntos débiles u obtiene información restringida. Normalmente identifica a atacantes que realizan operaciones ilegales con fines de según ellos altruistas

HIJACKING: secuestro de sesión, es cuando un atacante se apodera de una sesión de inicio en un equipo contando con todos los privilegios de la cuenta.

HIPERTEXTO: describe un tipo de funcionalidad de exploración en línea interactiva. Los vínculos (direcciones URL) incrustados en palabras o frases permiten al usuario seleccionar texto (p. ejemplo. Haciendo clic con el mouse) y mostrar inmediatamente información relacionada y material multimedia.

HIPERVÍNCULO: conexiones entre una información y otra.

HOMEPAGE: primera página o página de acceso inicial a un sitio web. Suele presentar información general de las diferentes secciones que contiene. Es también el punto de inicio cuando un navegador se conecta por primera vez a la red.

HTML (Hypertext Markup Language): Lenguaje de "etiquetas" en el que se asigna formato a las páginas de Web y se distribuye la información.

HTTP (Protocolo de transferencia de hipertexto): Método mediante el que se transfieren documentos desde el sistema host o servidor a los exploradores y usuarios individuales.

INFORMÁTICA: (Del francés informatique) Disciplina que incluye las diversas técnicas y actividades relacionadas con el tratamiento lógico y automático de la información, en cuanto esta es soporte de conocimientos y comunicación humana.

INTERNET: es la red de redes. Conjunto de redes de computadores que conecta y comunica a millones de personas en todo el mundo. Es una red no comercial que nació en Estados Unidos en 1969 producto del interés por conectar universidad y centros de investigación. Está integrada por millones de computadores, llamados servidores, que comparten un lenguaje común. Los computadores personales que se conectan y consultan datos de los servidores se denominan clientes. Es el origen de la actual revolución de las comunicaciones, cuyos efectos se están sintiendo en todo el planeta.

INTRANET: red exclusiva de una organización, que es diseñada y desarrollada siguiendo los mismos principios de Internet, aunque no necesariamente conectada a ésta.

IP (Protocolo Internet): define la unidad de información enviada entre sistemas, que proporciona un servicio de entrega de paquetes básico.

IP ADDRESS (Dirección IP): número único asignado a cada computador que se conecta a la red. Es una dirección de 32 bites o cifras, que se divide en cuatro subgrupos, definida por el Protocolo Internet.

ISO: International Organization for Standardization. Organización de carácter internacional encargada de establecer estándares en los que se incluyen los de telecomunicaciones.

ISP (Internet Service Provider): compañía que, además de proporcionar acceso a la red, ofrece una serie de servicios, como consultoría de diseño e implementación de páginas web e Intranet. Por lo general, su accionar se circunscribe a un área geográfica, que puede ser un país o una zona más amplia.
JAVA: lenguaje de programación para elaborar pequeñas aplicaciones que les aportan dinamismo a las páginas web. Soporta, por ejemplo, animaciones, comercio electrónico y actualizaciones en tiempo real.

LENGUAGE DE PROGRAMACIÓN: conjunto de sintaxis y métodos que se integran para la creación de programas.

LINK (Enlace): conexiones, que pueden ser textos o gráficas, contenidas en una página web, que al ser activadas con un click permiten acceder a otras secciones del mismo documento, a otros documentos dentro de un sitio o a otros sitios, según la conveniencia del usuario. Cada uno de estos “saltos” también se denomina link.

LINUX: sistema operativo perteneciente a la familia LINUX. La licencia de Linux es GNU.

LOGIN: acción de conectarse a un computador con identificación de usuario y contraseña. Se ejecuta cuandO el cibernauta ingresa su nombre electrónico a través de su teclado para acceder a otro computador.

LOGS: Registro automático de un suceso en el sistema.

METATAGS: símbolos utilizados en los lenguajes de programación de marcaciones para indicar cada una de las características de la aplicación.

MODEM: Modulador/Demodulador. Dispositivo que convierte señales digitales en analógicas y viceversa para poder transferir datos entre computadores a través de una línea telefónica.

NAVEGADORES: también llamados browsers son las aplicaciones software que permiten la navegación en Internet a los clientes, realizando el intercambio de mensajes con los

servidores. Ejemplos de navegadores son Internet Explorer, Netscape Navegator y Opera.

NETBIOS: (Network Basic Input/Output System) es un programa que permite la comunicación de aplicaciones en diferentes computadores en una red de área local.

PÁGINA ASP: Pagina Web de extensión .asp, es decir, una página

PÁGINA WEB: documento de hipertexto. La página es cada uno de los elementos que puede presentar un cliente Web. Las páginas contienen texto, enlaces, imágenes, y otros elementos multimedia.

PAQUETE: pequeño conjunto de datos enviados desde un host en Internet.

PERL: *Practical Extraction and Report Language*, Lenguaje de programación similar a C, muy extendido en labores de administración de sistemas y programación CGI. Se puede obtener de forma gratuita para numerosos entornos.

PING: aplicación que permite la medición del tiempo de una conexión por medio del intercambio de paquetes específicos.

PLUG-IN: programa anexo que se puede usar e instalar fácilmente y que potencia las habilidades de un navegador y lo hace más funcional.

PORTAL: sitio web que ofrece a los usuarios la posibilidad de acceder en forma fácil e integrada a una serie de recursos y servicios como, por ejemplo, buscadores y salones para “chatear” o foros, entre otros. Es la puerta de ingreso para la mayoría de los internautas.

PROGRAMAS GUSANO: programa que se auto reproduce por sus propios mecanismos buscando propagarse por la Internet, en la mayoría de los casos son programas de finalidad dañina.

PROTOCOLOS: conjunto de reglas y de convenciones que rigen los intercambios de información entre ordenadores.

PUERTOS: conexión entre dos dispositivos o sistemas. Valor de 16 bits que hace posible que el destinatario de una información elija correctamente la aplicación correspondiente para su tratamiento o visualización.

RED: sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota (de voz, vídeo, datos, etc.) y facilitar el intercambio de información entre usuarios con intereses comunes.

REDES ABIERTAS: Redes con acceso a Internet.

REDES CERRADAS: Redes aisladas de Internet.

REQUEST FOR COMMENTS (RFC): Serie de documentos que contienen proposiciones, comentarios y estándares técnicos relacionados a la tecnología Internet, propuesta por el Internet Engineering Task Force (IETF).

RSA: Uno de los primeros sistemas criptográficos de clave pública**.**

SANS: SysAdmin, Audit, Network, Security.

SEGURIDAD PERIMETRAL: Área de la seguridad computacional encargada de definir y verificar la seguridad de un entorno computacional

SENDMAIL: Programa que se utiliza para el intercambio y manejo del servicio de correo electrónico en los servidores.

SERVICIO DHCP: DHCP (Dynamic Host Configuration Protocol). Servicio que administra la configuración de la red registrando y actualizando direcciones IP y nombres DNS.

SERVICIOS LOCALES: Servicios de un equipo computacional que corren en la misma maquina.

SERVICIOS REMOTOS: Servicios de un equipo que corren en otra maquina, por ejemplo los firewalls que reparten la carga de procesamiento en otra maquina.

SERVIDOR: Sistema que proporciona recursos, como servidores de ficheros y de nombres, y resuelve las peticiones emanadas desde los programas llamados clientes. Un servidor también es aquel computador que contiene dichos programas.

SISTEMA INFORMÁTICO: conjunto de procesos agrupados con el fin comun de procesar información.

SISTEMA OPERATIVO: aplicación fundamental del computador cuya función es básicamente la de establecer la comunicación lógica entre los diferentes elementos del ordenador para que puedan funcionar las diferentes aplicaciones. Ejemplos Linux Red Hat, windows 2000 y DOS.

SITIO WEB: normalmente es un conjunto coherente y unificado de páginas web almacenadas bajo una misma dirección y al que acceden los usuarios para obtener información. Un sitio web puede contener desde unas cuantas páginas hasta miles de páginas web.

SNIFFERS: programa malicioso que permite la intercepción mensajes de datos en Internet.

SOLARIS: sistema operativo de la empresa Sun Microsystems.

SPAM: correo basura o no deseado.

SPYWARE: software malicioso que aparenta ser una excelente aplicación que ofrece muchos servicios al usuario pero que en realidad

SQL: lenguaje de Definición de Datos (Structure Query Language). Potente lenguaje informático diseñado especialmente para la comunicación con bases de datos.

SSH: secure Socket Shell. Consola de comunicación segura o software que ofrece una conexión segura entre dos equipos utilizando el cifrado de la información.

SSL: secure Socket Layer. Capa de conexión segura. Protocolo de internet que ofrece seguridad en las conexiones.
Swift

TCP/IP: protocolo de control de transmisiones/Protocolo Internet. Es el protocolo estándar de comunicaciones en red utilizado para conectar sistemas informáticos a través de Internet.

TECNOLOGÍA: (de téchne, arte y lógos, tratado). sistematización de los conocimientos y practicas aplicables a cualquier.

TELEMÁTICA: ciencia y técnica que combina el tratamiento y la difusión de la información. La telemática es una disciplina híbrida, consecuencia de la simbiosis entre la informatica y las telecomunicaciones.

TELNET: servicio que permite a un usuario remoto iniciar sesión en el sistema local y ejecutar programas de consola utilizando la línea de comandos.

TERMINAL: estación de trabajo.

TIEMPO REAL: rápida transmisión y proceso de datos orientados a eventos y transacciones a medida que se producen, en contraposición a almacenarse y retransmitirse o procesarse por lotes.

TROYANO: Haciendo alusión a su nombre es un programa malicioso que se oculta dentro de otro programa llamativo, y permite la fuga de información del computador.

UNICODE: Es un sistema de conversión que provee un único número para cualquier caracter sin importa el idioma, plataforma o lenguaje de programación. Esto permite la integración de los sistemas computacionales.

URL (Uniform Resource Location): sistema unificado de identificación y localización de recursos de cualquier tipo en Internet, que permite acceder en forma sencilla y homogénea a los documentos que contiene. Por ejemplo, la dirección electrónica de una página web.

USER ID (Identificación de Usuario): conjunto de caracteres alfanuméricos que identifica a un usuario y permite su acceso a los recursos de la red. Normalmente se solicita junto a una contraseña o password.

USUARIO: cada computador conectado a la red. Se contabiliza como un solo usuario, aunque puede ser utilizado por muchas personas.

VISITANTE: usuario que ingresa a un sitio web, quien puede ser identificado por medio de diversos mecanismos

WWW: *World Wide Web*. sistema de organización y presentación de la información de Internet basado en hipertexto y multimedia que permite buscar y tener acceso a un conjunto muy variado de información en Internet. Actualmente es el servicio más utilizado junto con el correo electrónico.

## GLOSARIO JURÍDICO

APELACIÓN: recurso ordinario por el que unas decisiones judiciales se remiten a un juez superior, con la posibilidad de practicar nuevas pruebas para que revoque la decisión dictada por otro inferior.

ACCION DE INCONSTITUCIONALIDAD: Acción Pública de rango constitucional que permite un control de constitucionalidad de las leyes por parte de los ciudadanos. Se realiza directamente ante la Corte Constitucional.

ACCIÓN DE TUTELA: acción Pública judicial de rango constitucional que permite en un trámite especial lograr la efectiva protección de un derecho fundamental cuando este se encuentre en peligro de ser vulnerado.

ARBITRAJE: sistema de resolución de conflictos por fuera del sistema judicial en el que se faculta a un grupo de terceros imparciales llamados árbitros para que tomen una decisión justa. El arbitraje pretende evitar los engorrosos trámites de un proceso judicial.

BIEN JURÍDICO**:** valor social que requiere protección a través de la consagración de un tipo penal. Son ejemplos de bienes jurídicos: la vida el patrimonio, la buena fe, la seguridad del Estado, la familia etc.

CÓDIGO: conjunto articulado de normas con fuerza de ley.

CONSTITUCIÓN POLÍTICA: norma suprema del ordenamiento jurídico que regula la organización y funcionamiento de los órganos del Estado garantizando los derechos y las libertades de los ciudadanos. Cada Estado tiene una constitución política.

COSA JUZGADA: efecto producido por una sentencia en firme que impide volver a plantear de nuevo el mismo litigio.

CULPABILIDAD: principio general de los sistemas penales por el que de forma subjetiva se determina la idoneidad criminal del delincuente y su capacidad para asumir la responsabilidad del delito cometido.

DECRETO: norma jurídica creada por la rama ejecutiva, es decir por Autoridades administrativas como el Presidente de la República, Gobernadores, Alcaldes, Asambleas departamentales y Concejos municipales**.**

DERECHO FISCAL: Relativo a los tributos o impuestos que deben pagarse al Estado**.**

DERECHO PRIVADO: clasificación clásica del derecho que hace referencia al derecho en el que el Estado no actúa de forma directa, sino a través de la simple consagración de las normas que lo regulan. Corresponde a esta clasificación el Derecho Civil y el Derecho Comercial.

DERECHO PUBLICO: clasificación clásica del derecho que hace referencia al derecho en el que el Estado participa directamente. Corresponden a esta clasificación el derecho penal, el derecho administrativo, el derecho fiscal, el derecho policivo entre otros.

DIRIMIR: Dar solución a un conflicto.
DOCTRINA: fuente auxiliar de derecho que consiste en las opiniones dadas por los estudiosos de derecho en sus libros.

DOLO: es la intención de cometer un delito de manera deliberada y consciente.

ECLÉCTICA: posición intermedia entre dos ideas o tesis.

ESTADO: organización jurídico política de una población dentro de un territorio determinado. Se habla entonces del Estado Colombiano.

FALLO: parte final de una sentencia que contiene la decisión del juez sobre la controversia planteada en el proceso.

FUNCIÓN FEDAL: función de dar fe sobre algo. Es la que cumplen los notarios es sus actuaciones.

HABEAS DATA: Voz latina que significa protección de datos.

INDEMNIZACIÓN PECUNIARIA: relativa al pago de una suma de dinero determinada por un fallo judicial.

JURISPRUDENCIA: conjunto de decisiones o fallos emitidas por los jueces sobre un determinado tema.

LEY: Norma jurídica que se caracteriza por ser general, abstracta e impersonal y cuya creación es parlamentaria.

LEY ESTATUTARIA**:** tipo de ley que requiere de un proceso de formación mas expedito por parte del congreso; Se utilizan para la regulación de ciertas materias de especial relevancia dentro del contexto del ordenamiento jurídico. Están consagradas en el artículo 152 de la Constitución política.

LITIGIO: conflicto de intereses o derechos que se dilucida en un proceso judicial.

MAGISTRADO PONENTE: Integrante de un tribunal colegiado encargado de redactar la sentencia.

MEDIOS DE PRUEBA: instrumentos legalmente previstos para demostrar aquello que un una parte pretende demostrar a favor de su derecho. Son ejemplos de medios de prueba: Los documentos, Los indicios, los testimonios, los dictámenes periciales, las inspecciones judiciales, y la confesión.

MÉTODO EXEGÉTICO: método que concede a cada palabra un valor exacto, se centra en un análisis semántico y se profundiza en la gramática.

MULTA: sanción consistente en el pago de una suma de dinero.

PARTE ACTORA: aquella que impulsa o da inicio a un proceso judicial. Se le llama así a la parte demandante de un proceso civil o al denunciante en un proceso penal.

PERSONA JURÍDICA**:** entes colectivos a los que la ley extiende los atributos de una persona natural como lo son el tener un nombre, un domicilio y un patrimonio. Son sujetos de Derechos y obligaciones.

PERSONA NATURAL: son los seres humanos vistos como sujetos de derechos y de obligaciones.

PRESUNCIÓN LEGAL: Ficción jurídica que permite a partir de un hecho conocido dar por cierto otro desconocido. Estas presunciones pueden ser desvirtuadas demostrando prueba en contrario. Son ejemplos de presunciones legales: La presunción de paternidad, la presunción de inocencia y la presunción de buena fe.

RESARCIMIENTO DEL DAÑO: indemnizar o compensar un daño, jurídicamente se materializa en una indemnización pecuniaria.

RESPONSABILIDAD OBJETIVA: tipo de responsabilidad en la que no se tiene en cuenta la intención de la persona que causo el daño. Corresponde al derecho civil y esta prohibida en el derecho penal donde siempre se debe entrar a determinar la intencionalidad de la persona.

RESPONSABILIDAD SUBJETIVA: responsabilidad en la que se tiene en cuenta la intencionalidad del agente que causa el daño.

RIESGO: permanente posibilidad de daño o perdida de un bien o un derecho, su ocurrencia debe ser posible e incierta.

SENTENCIA: decisión judicial que pone fin definitivamente a un litigio. **Sentencia en firme**: Aquella contra la que no cabe ningún recurso, salvo el de revisión.

TÍTULO VALOR: documento que incorpora un derecho patrimonial en cabeza de quien lo posea, su principal característica es que sirve de prueba principal en los procesos de cobro ejecutivo. Son ejemplos de títulos valores: El cheque , la letra de cambio y el pagaré.

TRADICIÓN: modo de adquirir en propiedad una cosa y consiste en la entrega que hace el dueño de la cosa a otro que se llama adquirente. En los bienes muebles la tradición se agota con la entrega física del bien, en los inmuebles se agota con la constitución de la escritura pública mas el correspondiente registro.

TUTELAR: amparar o defender un derecho.

## BIBLIOGRAFÍA Y REFERENCIAS

Constitución Política de Colombia editorial Leyer colección códigos brevis.

Código penal colombiano Ley 599 / 2001 Editorial Leyer Colección códigos brevis.

Código Civil colombiano Editorial Legis Colección códigos básicos.

Código de procedimiento civil. Editorial Legis Colección códigos básicos.

Código de comercio Decreto 410 / 1971. Editorial Legis, Colección códigos básicos.

GARCES VELÁSQUEZ, Jaime. Derecho Penal General. Medellín. Diké, 3ª Edición. 2001.

MADRID PARRA, Agustín y otros. Derecho del comercio electrónico. Medellín. Colegio de abogados de Medellín, Biblioteca jurídica, y Cámara de Comercio de Medellín. 2002

Mc CLURE, Stuart; SCAMBRAY, Joel y KURT, George. Hackers secretos y soluciones para la seguridad de redes. Madrid. Osborne McGraw-Hill, 2000

LEON MONCALEANO, Willian Fernando. De la informática jurídica penal bancaria. Bogotá. Doctrina y Ley, 2001.

PEÑA VALENZUELA, Daniel. Los aspectos legales de Internet y del comercio electrónico ley 527 de 1999. Bogotá. Dupre Editores Ltda. 2001

RIASCOS GOMEZ, Libardo Orlando. La Constitución de 1991 y la informática jurídica. Pasto. Universidad de Nariño, 1997

Artículo de periódico: Ámbito Jurídico. Separata especial Seguridad del comercio electrónico, octubre de 2002.

Articulo de revista. Juego de manos: los delitos informáticos y electrónicos son muchos mas que una travesura de niños. La Nota Número 43. p 74-77, 1999.

Revista La propiedad inmaterial. Numero 4 primer semestre de 2002 edición especial Comercio electrónico y entorno digital.

http://whois.arin.net
http://www.cert.org
http://www.cibercrime.gov
http://www.criptonomicon.com
http://bachue.com/colibri
http://www.bib.minjusticia.gov.co/normas/
http://www.bufetalmeida.com
http://www.delitosinformaticos.com
http://www.derechos.org/nizcor/
http://www.dnsstuff.com
http://www.fbi.gov
http://www.gobiernoenlinea.gov.co
http://www.icann.org
http://www.insecure.org/tools/
http://www.i-uris.com/
http://www.law.cornell.edu/
http://www.netcraft.com
http://www.nic.co
http://www.nsa.gov.eu
http://webs.ono.com/usr016/Agika/
http://www.sans.org
http://www.securityspace.com
http://www.seguridata.com
http://servicios.att.net.co/traceroute/
http://www.sice.oas.org
http://www.uncitral.org