ADMINISTRACION Y REGULACION DE LOS DERECHOS DIGITALES PARA MUSICA EN INTERNET

CESAR HERNANDO VALENCIA NIÑO
JOSE GABRIEL CORREDOR POVEDA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERIA ELECTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2004

ADMINISTRACION Y REGULACION DE LOS DERECHOS DIGITALES PARA MUSICA EN INTERNET

CESAR HERNANDO VALENCIA NIÑO

JOSE GABRIEL CORREDOR POVEDA

Monografía para optar al título de
Especialista en Telecomunicaciones

Director
MSC. JORGE HERNANDO RAMON SUARES

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERIA ELECTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2004

A mis padres Hernando
Y Flor Marina, a mis
Hermanos Laura y
Carlos a mi Novia
Catalina y a DIOS.

Cesar Hernando

A mi familia, a
Mis compañeros
Y a DIOS.

José Gabriel

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Dr. Jorge Hernando Ramón Suárez, Director de la Monografía y Docente de la Universidad por su colaboración, orientación y paciencia a lo largo de este proceso.

A la parte administrativa de la Especialización por su apoyo constante e incondicional para satisfacer nuestras necesidades, especialmente a la Ing. Leydi Barco, a Shirly y demás colaboradores.

A todos los profesores que tuvimos durante el curso por su paciencia y comprensión.

A todos los compañeros de clase por hacer de esta una experiencia enriquecedora no solo de aprendizaje sino también de vida.

CONTENIDO

Pág

LISTA DE FIGURAS

GLOSARIO

BITS: Sucesión de caracteres numéricos que pueden ser “1” o “0”.

CD: Formato Digital de Discos Compactos especiales para almacenar información.

CIFRAR: Proceso mediante el cual se oculta una información dentro de otra.

CD-ROM: Unidades Lectoras de Discos Compactos incorporadas en las computadoras personales.

CLAVE: Conjunto de caracteres alfanuméricos designados como secretos y conocidos solamente por el dueño.

CNUDMI: Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil.

CRIPTOGRAFIA: Ciencia que se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial.

DESCIFRAR: Procedimiento mediante el cual se obtiene una información oculta en otra.

DIGITALS WATERMARKS: (Marcas de Agua Digitales). Utilizadas para marcar el contenido de los medios digitales y preservar los derechos de autor.

DRM: (Digital Rigths Management). Administración de Derechos Digitales. Tecnología utilizada para la distribución de información en Internet respetando los derechos de autor.

DVD: (Disco de vídeo digital). Dispositivo de almacenamiento masivo de datos cuyo aspecto es idéntico al de un disco compacto, aunque contiene hasta 15 veces más información.

FIRMA DIGITAL: Es la versión computarizada de la firma manual, indispensable para la identificación del usuario.

HACKERS: Sujetos que utilizan Internet para fines no autorizados de copiado y espionaje también conocidos como Piratas Informáticos.

HARDWARE: Son todos los componentes materiales de un computador bien sea personal o industrial.

MD5: (Message Digest 5). Programa utilizado para procesar el resultado de pasar un texto plano por una función Hash.

MEMORIA FLASH: Tipo de memoria programable electrónicamente para almacenar datos y además es reescribible.

MP3: (Motion Picture Experts Group-1, Audio Layer 3). Formato de compresión digital de audio que permite reducir el tamaño de una canción 10 veces sin que haya pérdida notable en la calidad de sonido.

NAPSTER: Mayor comercializador de música por Internet antes de la aparición de DRM.

OMPI: Organización mundial de Propiedad Intelectual.

ONE WAY HASH FUNCTION: (Función de Hash Unidireccional). Función que toma el contenido con cualquier longitud a modo de entrada y produce un pequeño mensaje de longitud fija a la salida.

P2P: (Peer to Peer). Redes en las que cada nodo tiene las mismas responsabilidades y capacidades.

PC: Sigla que define a los Computadores personales, que contienen aplicaciones para desarrollo de tareas domésticas.

PLUG-INS: Son todas aquellas aplicaciones que tiene el cliente en su computador personal para el desarrollo de cualquier tarea.

RIAA: Asociación que reúne a las discográficas de Estados Unidos.

SDMI: (Secure Digital Music Initiative). Componente de DRM encargada de la seguridad digital musical.

SOFTWARE: Componentes informáticos de un computador como programas y aplicaciones.

SSL: Protocolo encargado de autenticación de mensajes.

TEXTO CIFRADO: Resultado de aplicar un algoritmo criptográfico al texto plano.

TEXTO PLANO: Información original que no ha sufrido ningún cambio.

UIT: (Unión Internacional de Telecomunicaciones). Ente más importante encargado de regir todo proceso concerniente a las Telecomunicaciones a nivel mundial.

WMA: Extensión usada para archivos protegidos contra copias.

WOOFERS: Parte de la salida de sonido que se encarga de las frecuencia más bajas.

RESUMEN

TITULO:
ADMINISTRACIÓN Y REGULACION DE LOS DERECHOS DIGITALES PARA MUSICA EN INTERNET*.

AUTORES:
VALENCIA NIÑO, Cesar Hernando;
CORREDOR POVEDA, José Gabriel**2.

PALABRAS CLAVES:
Administración, Tecnología, Criptología, Música, Firma Digital, Normatividad, Función HASH, Derechos Digitales.

DESCRIPCIÓN:

El objetivo primordial de este trabajo es realizar un compendio de las Características técnicas y normas legales existentes, para la administración de derechos digitales en Internet para música.

Se realizó una recopilación literaria sobre los conceptos y técnicas utilizadas En la implementación de la tecnología DRM, tales como criptología, marcas De agua, funciones HASH, clave pública, clave privada y firmas digitales.

Se analizó la Ley 527 de Agosto 18 de 1999, el Decreto 1747 del 11 de Septiembre del 2000 y el Tratado Internacional de la OMPI referentes al Comercio electrónico en Colombia y además un cuadro informativo de legislación para comercio electrónico de países vecinos.

Como conclusión, la existencia del la Ley 527 ubica a Colombia como uno de los países Latinoamericanos que ha partido en punta referente a este tema con el fin de garantizar lo derechos de autor.

En el ámbito tecnológico es mucho lo que hay que hacer, puesto que para la implementación gran parte de esta tecnología viene del exterior; la adquisición y comprensión de estos modelos dan una orientación a los sectores privados y públicos para una posible implementación de este esquema a tareas realizadas por los mismos.

---

* Monografía.

** Facultad de Ingeniería Físico-mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones. Jorge Hernando Ramón Suárez.

ABSTRAC

TITLE:
DIGITAL RIGHTS MANAGEMENT AND REGULATION FOR MUSIC IN THE INTERNET[*].

AUTHORS:
CORREDOR POVEDA, José Gabriel; VALENCIA NIÑO, Cesar Hernando[**].

KEY WORDS:
Administration, Technology, Cryptology, Music Digital Signatures, laws, HASH Function, DRM.

DESCRIPTION:

This work principal objective is to make a compendium from the technical characteristics and law for the administration of the digital rights for music in the Internet.

A literary recopilation about the conceptions and the technics used in the implementation of the DRM technology, as cryptology, water marks, HASH functions, public passwords, private passwords and digital signatures, was made.

The law 527 from august 18th, 1999; decree 1747 from September 11 th, 2000 and the international treaty of the OMPI, that´s about electronic business in Colombia and an informative picture of the law for electronic business among near countries were analyzed.

In conclusion, the 527 law puts Colombia as one of the countries in Latin America that has left in point in this theme and it warrants the author rights.

In the technologic world there is a lot to do because to implement this technology many things come from the other countries, with the acquisition and comprehension of these models the private and public sectors will receive orientation for a possible use of this way in the tasks made by themselves.

---

[*] Monograph

[**] Faculty of Engineering Physique-Mechanics. School of Electric, Electronic and Telecommunications Engineering. Jorge Hernando Ramon Suarez

INTRODUCCION

Los estudios de Administración y Regulación de Derechos Digitales para Música en Internet que se presentan en este trabajo, quieren mostrar al lector una recopilación sobre la información que existe, tales como: Métodos orientados a Medios Físicos, Métodos orientados a programación y Métodos orientados a Normas Legales que dan protección a los derechos de autor.

Es de especial importancia divulgar el trabajo que han hecho algunos expertos en la materia, apoyados en ciencias como, la Electrónica, la Informática, el Derecho y otras disciplinas para dar un aporte a aquellos que desean hacer parte de este proceso; a continuación se presenta un resumen de los temas que trata el presente trabajo.

La utilización de computadoras, y más especialmente de Internet, ha creado una cultura diferente en la forma de vida de las personas, convirtiendo este medio en un elemento más en la conformación del hogar, la oficina y empresa, puesto que desde un computador personal se puede acceder a todo tipo de información como por ejemplo: libros, videos, música, juegos e imágenes. A través de este medio existe la posibilidad de comunicación con los diferentes usuarios que se encuentren conectados a la red.

La música, videos, juegos, libros e imágenes son servicios digitales ofrecidos por Internet, con los cuales no se ha logrado maximizar su productividad por la poca seguridad que existe para garantizar los derechos de autor, la privacidad, la confidencialidad y autenticidad. La reproducción ilegal de estos servicios sin contar con la autorización de sus propietarios origina que alguna información no sea publicada por Internet, por el temor a ser plagiada.

Los servicios digitales son de fácil reproducción y distribución a través de servidores, usando principalmente conexiones punto a punto donde los usuarios intercambian ficheros por lo cual este método toma gran fortaleza y propone un crecimiento acelerado con el aumento de ancho de banda. Hoy los usuarios quieren hacer descargas (downloads) de información, como videos y música en el menor tiempo posible adquiriendo nuevas tecnologías como ADSL y fibra óptica para sus conexiones las cuales están haciendo presencia en las ciudades capitales de nuestro país. El usuario ya no tiene que dirigirse a centros comerciales para buscar información, ahora lo pueden hacer desde su casa, oficina o sitio de trabajo. Sin embargo los dueños de la información con el propósito de hacer proteger sus derechos han limitado los contenidos que publican por Internet.

Estas preocupaciones han hecho que las empresas y los computadores personales puedan intercambiar cada vez más información pero controlando a su vez quien podrá y como utilizarla mediante la implementación de métodos como el uso de claves.
Como resultado de lo anterior surge DRM (Digital Rights Management) en el comercio electrónico para ofrecer seguridad.

La administración de derechos digitales ayudará a dar privacidad, confidencialidad y seguridad conservando la autenticidad para motivar e impulsar el comercio electrónico contribuyendo de esta forma a mejorar la economía de los países.

El desconocimiento y la escasa legislación en materia de regulación de los servicios de derechos digitales contribuyen a que haya desconfianza por los propietarios de la información. Sin embargo en Colombia ya se dio un avance significativo con la promulgación de la ley 527 de 1999 y con la firma de un tratado internacional con la O.M.P.I[3]

3 Organización Mundial de Propiedad Intelectual.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Recopilar información acerca de los métodos y de la regulación existente para protección de los derechos digitales de música en Internet.

1.2 OBJETIVOS ESPECIFICOS

- Conocer las generalidades 7del crecimiento en el uso de Internet.
- Describir los diversos métodos implementados para la protección de los derechos de autor.
- Explicar los conceptos y características de la administración de derechos digitales para música en Internet.
- Realizar una síntesis de las normas legales existentes en materia de derechos digitales para Internet en Colombia y algunos países latinoamericanos.

2. GENERALIDADES DEL CRECIMIENTO EN EL USO DE INTERNET

Cada vez los servicios digitales prestados a través de Internet contribuyen a masificar su uso, ya que el aumento de computadores personales sigue en crecimiento en todos los países de América Latina; a pesar de que la situación económica en este sector del continente ha estado en deterioro, los usuarios de Internet continúan en ascenso. También contribuye al uso del Internet la publicación electrónica de un número significativo de artículos en español, lengua que ocupa el cuarto lugar en el mundo.

Hoy en día la cultura adoptada por gran parte de la humanidad ubica a Internet como uno de los medios masivos de comunicación, compartiendo honores con la televisión, la prensa y la radio, puesto que en este medio las distancias son insignificantes para quienes toman la decisión de establecer comunicación. Este fenómeno del crecimiento no solo es evidente por el auge en la comunicación sino que también toma una parte muy relevante en la obtención de información en diferentes formatos tales como:

- Datos.
- Audio.
- Video.
- Imágenes.

Todos estos formatos ofrecen un sinnúmero de posibilidades a la hora de ser ejecutados con programas muy novedosos, que han sido puestos en el mercado ya sea por los publicantes de la información, casas disqueras, casas editoriales, compañías de software, universidades y en algunos países por dependencias oficiales dedicadas a este oficio. Como resultado de estos esfuerzos no solo cada formato se puede reproducir en cualquier punto donde esté Internet, sino que además este tipo de Software ofrece multifuncionalidad en la ejecución de estas tareas, por ejemplo, Windows Media ofrece la posibilidad de ver videos, imágenes y escuchar sonidos todo en un solo programa.

Los dispositivos con los cuales se puede establecer una conexión, se han diversificado de manera tal, que hoy en día se cuenta con al menos cinco alternativas de conexión para llevar a cabo esta tarea:

- Inalámbricas.
- Vía Línea Telefónica.
- Vía Satelital.
- Vía Fibra Óptica.
- Banda Ancha.

Este tipo de conexiones en general son ofrecidas por las empresas nacionales de comunicaciones en cada país dando la posibilidad de que cualquier persona que pueda pagar por el servicio lo obtenga. En un comienzo los costos de conexión fueron bastante elevados pero con el transcurrir del tiempo y el avance tecnológico, no solo se han masificado sino que ha demostrado tener una baja ostensible en lo que a precios se refiere.

Dentro de los paquetes ofrecidos por las empresas prestadoras de este servicio se han adoptado diferentes tipos de clientes en el mercado como:

- Empresas.
- Hogares.
- Instituciones Educativas.
- Negocios que comercializan este servicio.

La competencia está planteada con promociones y tarifas competitivas para cada tipo de cliente, otorgando ventajas que en el pasado solo podrían ser una utopía. Además, la integración de los estos servicios ofrece la posibilidad de obtener en un mismo paquete comercial, conexión a Internet, televisión por cable y línea telefónica.

Con el firme propósito de globalizar este servicio los países en vía de desarrollo, mediante planes de expansión están instalando terminales públicos o cafés Internet para que sean utilizados por aquellos usuarios que no pueden tener su computador personal, prestando entonces estos servicios a las clases más desprotegidas. Estos sistemas o similares han sido implementados en varios países latinoamericanos dando buenos resultados. En el siguiente cuadro, se describen los diferentes programas adoptados por algunos países:

Cuadro 1. Programas pilotos adoptados por algunos gobiernos

PAIS	PROGRAMA	OBJETIVOS
ARGENTINA	TELECENTROS	Instalación de mil telecentros, que proveerán Internet a los lugares más distantes y de bajos recursos.
BARBADOS	EN ESCUELAS DE PRIMARIA Y SECUNDARIA	Las escuelas de primaria y secundaria tendrán instalados equipos de informática durante los próximos años.
BELICE	INTERNET PARA ESCUELAS	Prestar el servicio gratuito para todas las instituciones de educación secundaria y universitaria.
CHILE	TELECENTROS	El Fondo para las Telecomunicaciones está instalando telecentros para garantizar la conexión a todas las comunas chilenas para el 2006
COLOMBIA	COMPARTEL	Compartel está llevando el Internet a todos los municipios y espera prestar el servicio gratuito para los municipios más pobres, de igual forma en convenio con el Ministerio de Educación esperan colocar Internet a dos mil escuelas

PERU	CENTROS PUBLICOS DE INTERNET	La red científica peruana se ha hecho famosa por la instalación de centros públicos de Internet y esperan colocar cinco mil cabinas para Internet semejantes a los teléfonos públicos
URUGUAY	TERCER MILENIO	El proyecto tercer milenio y mediante la compañía estatal ANTEL, espera colocar veinticinco centros digitales en las capitales de departamento y en las grandes ciudades, estos centros prestarán el servicio de Internet y videoconferencia

4. Fuente: (I.T.U) Unión Internacional de Telecomunicaciones., www.itu.int.

3. METODOS IMPLEMENTADOS PARA LA PROTECCION DE LOS DERECHOS DE AUTOR

Actualmente Internet está inundado de mucha información, como se menciona en el capítulo anterior. Es el propósito de este texto tomar como caso de estudio la distribución y la vigilancia de los derechos de autor para la música en Internet.

La música en Internet es uno de los servicios más utilizados y fue implementado para dar a conocer los artistas desconocidos, con el fin de aumentar la popularidad y las ventas en las tiendas discográficas de algunos intérpretes, para quienes era prácticamente imposible realizar una gira a nivel mundial para exponer su música. En este punto juega un papel muy importante el formato MP3.

El formato MP3 (Motion Picture Experts Group-1, Audio Layer 3), es el responsable de la avalancha de intercambio y reproducción de música a través de Internet, fomentando con ello la piratería digital. MP3 es un formato de compresión que reduce el tamaño de los archivos hasta en 10 veces; un archivo de 30 Mb fácilmente se convierte en otro de solo 3 Mb, omitiendo en la pista las frecuencias que no son perceptibles por el oído humano sin que haya pérdida notable de la calidad del sonido.

El formato MP3 ha llamado la atención de los usuarios de Internet, ya que facilita la descarga de canciones en menos tiempo e inclusive reproducirlas sin la autorización de los dueños, violando los derechos de autor. Por lo tanto el buen uso del formato MP3 es legal, pero la

reproducción o el intercambio de material protegido sin las autorizaciones respectivas es ilegal y ha causado grandes pérdidas a la industria discográfica y a los artistas de música.

Napster llego a ser el programa más importante utilizado para intercambiar música en formato MP3, permitiendo ver los ficheros ubicados en los discos duros de los usuarios y facilitando la posibilidad de escoger la música que se quiere bajar o intercambiar. El MP3 alcanza su mayor auge en las universidades, ya que allí se tiene mayor velocidad y ancho de banda, requisitos esenciales en el intercambio de información digital.

Con el fin de contrarrestar esta reproducción ilegal, se han implementado diferentes métodos a los cuales nos referimos a continuación:

3.1 METODOS ORIENTADOS A MEDIOS FISICOS.

Como primera medida para contrarrestar este flagelo, se pensó en bloquear la posibilidad de realizar dichas copias no autorizadas mediante diferentes sistemas, algunos sugeridos y otros implementados en los medios físicos como reproductores y discos compactos.

Los dueños de las casas disqueras quisieron hacer su aporte y por otro lado ganar un poco más, sugiriendo que se considerara la posibilidad de crear un CD degradable inmediatamente fuera escuchado, dando la oportunidad de ser oído una o máximo dos veces. Al conocer esta propuesta la comunidad en general manifestó su rechazo, pues con

este tipo de implementaciones se estarían violando los derechos del comprador al no permitir que el mismo conserve sus canciones para oírlas cada vez que así lo quiera; con todo lo anterior, esta idea no prosperó.

Otra alternativa utilizada y llevada a cabo era la de ofrecer al mercado discos compactos que solo pudiesen leerse en los reproductores de música pero carecieran de esta facultad en los Computadores personales. Este método fue rechazado por los usuarios, quienes lo manifestaron simplemente no adquiriendo los productos que tuvieran esta característica, obligando de esta manera a ser retirados del mercado en poco tiempo.

Con un método un poco mejor elaborado, de nuevo las casas disqueras contrataron los servicios de científicos para que hicieran una investigación exhaustiva y desarrollaran un producto para prevenir este problema; fue así como un nuevo producto nació y se trataba de un disco compacto con un cierta combinación binaria mediante la cual estos no podían ser reproducidos por los equipos de sonido pero sí por los Computadores personales.

En un comienzo fue incómodo para muchos usuarios pero paulatinamente fue afianzándose hasta que se descubrió que al subir el volumen este código producía unas frecuencias que deterioraban los Woofers (salidas de los Bajos) y por consiguiente tuvo que retirarse del mercado.

Por último se desarrolló con gran dedicación un disco compacto que contenía una pista oculta que impedía la reproducción y copia de los temas en los Computadores personales, para poder lograr este avance, se hizo una inversión millonaria con muchos científicos a la cabeza para dicha implementación; este invento no duró mucho tiempo y no por que a los usuarios no les gustara, sino que un grupo de cibernautas encontró la forma de inutilizar la pista trazando una raya transversal con un marcador y de paso dejando en ridículo a sus fabricantes[5].

3.2 METODOS ORIENTADOS A PROGRAMACION.

Dentro de los métodos orientados a programación, el esfuerzo realizado tanto por las casas disqueras como por la industria tecnológica son evidentes y tuvieron mejor aceptación dentro de los usuarios, la evidencia está en que la mayoría de estos métodos aún están funcionando en buena medida.

Para iniciar el recuento traemos a colación los diferentes programas que se implementaron en los dispositivos reproductores con el fin de que solo pudieran oír algunos tipos de pistas exclusivas de ciertos vendedores, es decir cada CD de música ofrecido por alguna compañía se podía escuchar con el software correspondiente.

Mediante el uso de temporizadores la música puede ser reproducida en cierto lapso de tiempo que es especificado por el proveedor; este tiempo está dado por el monto pagado, así se puede disponer de las pistas por semanas, meses o tan solo horas.

5. Fuente: www.uberbin.net/archivos/000108.php

El modelo de pagar por oír es muy utilizado actualmente y de hecho tiene que ver mucho con el método anterior y con el próximo pues aunque para muchos usuarios no resulta muy satisfactorio pagar por un servicio que antes era gratuito, esta nueva modalidad ha tomado fuerza y se ha convertido en un pilar de la industria en Internet.

Como resultado final se ha implementado el Modelo de Administración de Derechos Digitales (Digital Rights Management o DRM) por parte del consorcio Microsoft e inclusive siendo compatible con otra plataforma como Unix.

En el siguiente capítulo hablaremos del modelo más utilizado para el comercio de música por Internet.

3.3 METODOS ORIENTADO A RECURSOS LEGALES.

En febrero del año 2003 la asociación que reúne a las discográficas en Estados Unidos (RIAA)[6], presentó una demanda que para fortuna de los mismos obtuvo muy buenos resultados. En la sentencia de la novena corte de California se estableció que está terminantemente prohibido el intercambio gratuito de temas musicales que estén amparados por derechos de autor y fonográficos.

6. Asociación que reúne a las discográficas de Estados Unidos.

4. CONCEPTOS Y CARACTERISTICAS DE LA ADMINISTRACION DE DERECHOS DIGITALES PARA MUSICA EN INTERNET

La administración de derechos digitales es una metodología implementada en un software que se encarga básicamente de verificar la autenticidad de las licencias de reproducción para temas musicales que se encuentran bajo las leyes de derechos de autor; las siglas con las cuales es conocido mundialmente son D.R.M. que significa Digital Rights Management, y su funcionamiento se basa en los cánones de la criptografía de clave pública y clave privada, así como marcas de agua y firmas digitales.

La D.R.M., tiene como ventaja la flexibilidad de aplicación en las diversas plataformas, como por ejemplo: computadores personales, portátiles y celulares. También controla el flujo de información enviado a través de medios magnéticos como discos compactos, discos de video digital y memorias flash.

El uso de licencias digitales es muy versátil permitiendo agrupar diferentes características como: frecuencia de acceso, fecha de vencimiento, restricciones para transferencias a otros dispositivos y permisos de copiado.

En el desarrollo de este capítulo se realiza un detallado seguimiento a todos los procesos por los cuales pasa un tema musical desde su grabación hasta su distribución.

4.1 MÉTODOS DE PROTECCIÓN DIGITAL UTILIZADOS POR DRM

Actualmente la Administración de Derechos Digitales emplea dos métodos para la protección de la propiedad intelectual: La Cifrado de Datos y Las Marcas de Agua Digitales (Digitals watermarks).

4.1.1 Cifrado de Datos: El cifrado es una conversión de datos, de un texto plano a un texto cifrado, mediante el uso de una clave o código secreto. Esta es la forma de brindar seguridad ya que el usuario que desea acceder a la información debe descifrar el texto cifrado usando la clave respectiva.

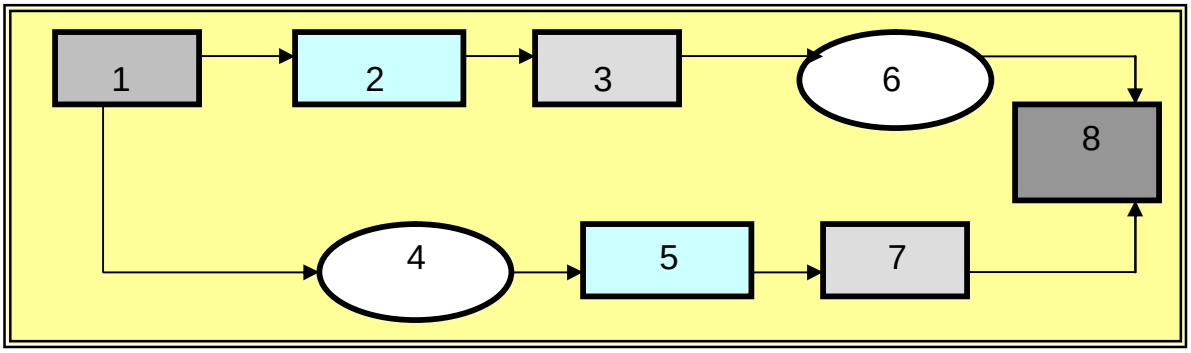
La Administración de derechos Digitales utiliza un programa llamado algoritmo criptográfico, para cifrar los temas musicales. Emplea una clave que puede ser una frase o una serie de números para encriptar el tema musical, y sólo el poseedor de este código podrá abrir y escuchar el tema; de lo contrario será inaudible. Por lo tanto se debe tener un buen control en la entrega de estas claves.

En criptografía digital entre más dígitos tenga la clave, más difícil será descifrarla y necesitará procesos mucho más complejos. Una clave que posea 16 caracteres cada uno de 8 bits hace que sea imposible descifrar el código por los hackers de la informática. “Si un computador tuviese la posibilidad de probar un billón de claves por segundo, y a su vez un billón de estos computadores estuvieran trabajando en forma concurrente con el descifrado de dicha clave: podría tomarles 10.000.000.000.000 años probar cada clave posible[7]”. Por lo cual todos

los contenidos encriptados por D.R.M. garantizan seguridad en alto grado.

Con el fin de evitar manipulaciones digitales DRM utiliza una Función Hash unidireccional. “ONE WAY HASH FUNCTION” la cual toma el contenido de cualquier longitud y produce un resumen de 128 bits llamado “Message Digest”, para hacer la comparación a la salida del mensaje y si no ha sufrido alguna alteración o modificación debe dar igual.

Figura 1. Función Hash



Convenciones:

1- Texto plano.
2- Función Hash antes de ser enviado.
3- Resumen Hash listo para ser enviado.
4- Medio Inseguro.
5- Función Hash después de ser enviado.
6- Medio Inseguro
7- Resumen Hash después de ser enviado.
8- Comparador.

7. Fuente: www.idc.com/spain/prensa “Protección y nuevas posibilidades”.

En la función Hash se toma el texto plano que está identificado con el número 1 y se realiza una función hash con el fin de obtener un resumen hash que está identificado con el número 3; posteriormente se envía al destino, de igual forma se envía el texto plano por un medio inseguro el cual antes de llegar al destino tiene el mismo proceso con el fin de comparar los dos resúmenes y constatar que la información que llegó es auténtica y que no ha sido modificada.

De esta forma el proveedor de la música garantiza la autenticidad mediante el message digest, el cual es guardado de manera segura y al que puede acceder el usuario para verificar si el producto que adquirió es el legítimo respondiendo al "message digest". Para procesar el anterior mensaje se usa un algoritmo ampliamente conocido como el MD-5 (Message Digest 5).

4.1.2 Criptografía de Clave Pública: En 1976 Martín e. Hellman y Whitfield Diffie, desarrollaron origen a la criptografía de clave publica. Con este sistema se conocen dos tipos de claves: Clave privada (KR) y la clave pública (KU), la primera se conserva secreta y la segunda se entrega libremente.

El cifrado se puede realizar con cualquiera de las dos claves, obteniéndose un mensaje C, el cual se debe descifrar con la clave apropiada para obtener el mensaje original M.

Si cifro con KR (M) se obtiene C y si descifro con KU(C) se obtiene M.

Si cifro con KU (M) se obtiene C y si descifro con KR(C) se obtiene M.

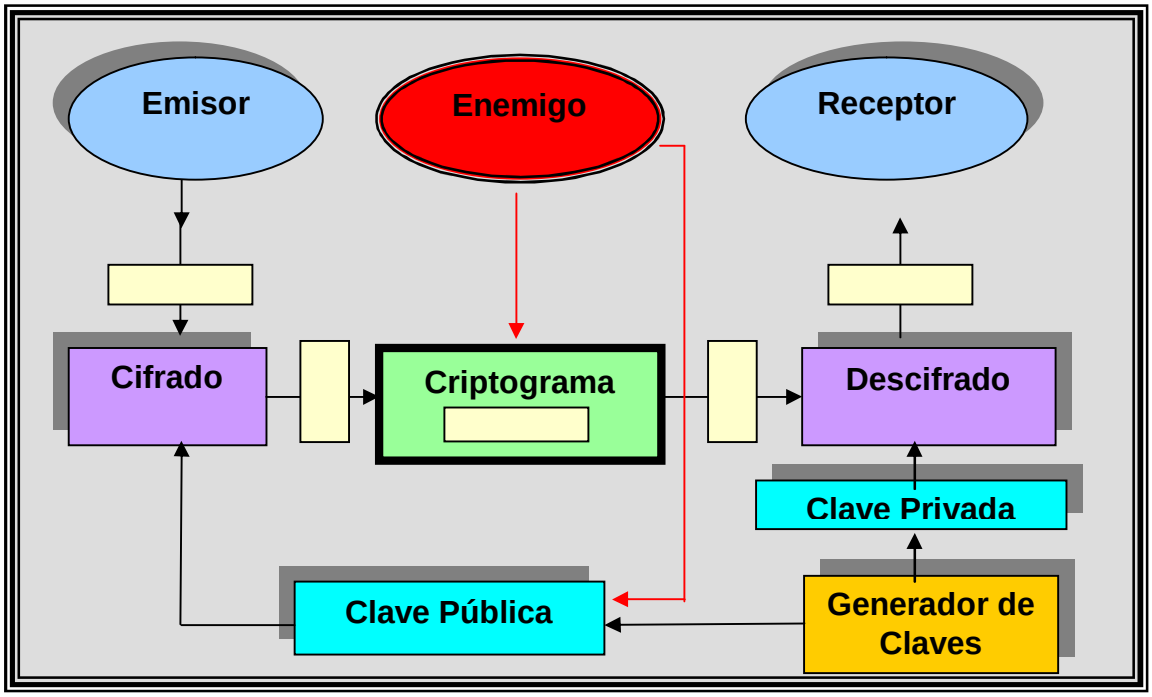
Cuando se trabaja con criptografía de clave pública se pueden obtener algunos postulados en los cuales basamos la confianza de este sistema y ellos son:

- Computacionalmente fáciles para que un usuario genere las dos claves, la pública y la privada.
- Es computacionalmente fácil para un emisor A, que conociendo la clave pública, genere un texto cifrado,
- Es computacionalmente fácil para el receptor B, descifrar el mensaje cifrado conociendo la clave privada para obtener el mensaje original.
- Resulta computacionalmente infactible para un oponente hallar la clave privada a partir de la clave pública.
- También es computacionalmente infactible para un oponente, recuperar el mensaje conociendo la clave pública y un texto cifrado[8].

En la Figura 2, se observa cómo el Emisor envía un mensaje al receptor cifrado con la clave pública y este sólo lo puede descifrar sin ningún problema usando su clave privada de descifrado. Aunque el mensaje cifrado o criptograma y la clave pública pueden ser vistos por el enemigo, éste no podrá descubrir qué dice en el mensaje gracias a que no posee la clave privada.

8. Fuente: Técnicas Criptográficas de Protección de datos – Fúster Sabater, Amparo, Editorial Computec.

Figura No 2 – Sistema Asimétrico de Clave Pública – Fuente: Seguridad Informática, Caballero Pino, Editorial Computec.



4.1.3 Marcas de Agua Digitales: son usadas para marcar el contenido y así de esta manera los medios digitales no pueden ser distribuidos libremente. Básicamente están compuestas por un patrón de bits insertados en una imagen digital, archivo de vídeo o de sonido mediante el cual se identifica la información del autor. El principal objetivo es dar protección a la propiedad intelectual que se encuentra en formato digital. Lo elemental es que este patrón sea totalmente invisible y para el caso de archivos de sonido no audibles.

A través de los estándares SDMI[9] los distribuidores de música se encargan de asegurar los archivos MP3 de copias y distribuciones no autorizadas, asegurando la remuneración desde el artista hasta los distribuidores en línea.

Entonces, de alguna manera los sistemas DRM necesitan saber cuándo la copia es permitida y cuándo no. Por ejemplo, los usuarios tienen derecho a hacer copias a sus familiares más cercanos. Para esto se usan los "hops" que consisten en que el archivo original puede ser copiado, pero la copia del original no puede ser copiada y así sucesivamente. Obviamente esto genera un inconveniente, si el usuario por accidente borra el archivo original así tenga la copia de este archivo no podrá hacer un duplicado.

4.1.4 Firma Digital: La firma digital es la versión computarizada de la firma manual. Durante el desarrollo de las telecomunicaciones en estos últimos años, se ha creado toda una variedad de nuevas necesidades, dado que en la mayoría de las entidades bancarias es necesario firmar los documentos. Con el uso de los computadores se requiere un nuevo planteamiento donde la firma digital cumple las mismas propiedades que la firma manual.

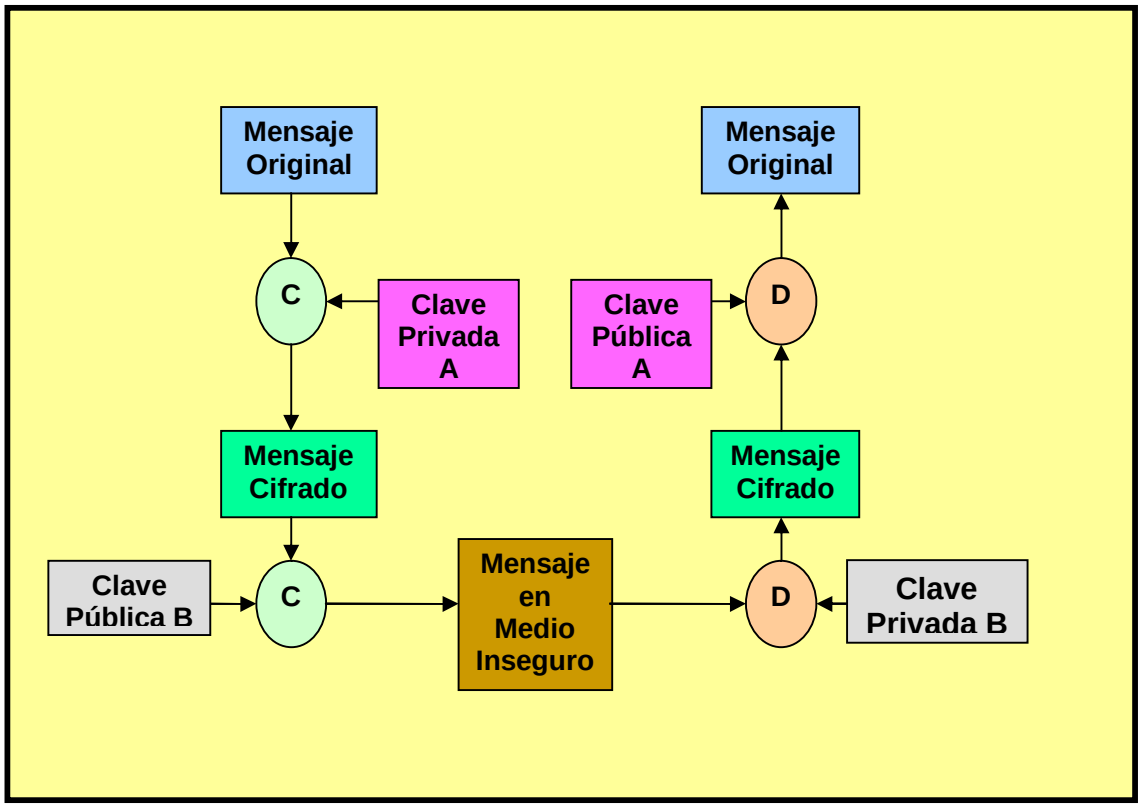
Se puede distinguir la firma:

- Implícita: Es aquella que está dentro del contenido digital.
- Explícita: Aquella que está añadida al texto como una marca inseparable.
- Privada: Legible sólo para quien comparte cierto secreto con el emisor.
- Pública: Legible para todo el mundo.

9. Componente de DRM encargada de la seguridad digital musical.

- Revocables: Si el remitente puede, posteriormente, negar que la firma digital en cuestión le pertenece.
- Irrevocables: Si el receptor puede probar que el remitente escribió el mensaje[10].

Figura 3 – Firma Digital – Seguridad En Redes, Martínez Juan Carlos.



La Firma Digital debe ser:

- Única, así solo puede ser generada por el usuario legítimo.

10. Fuente: Sistemas de Autentificación para Seguridad en Redes. – Oppliger Rolf, Editorial Computec.

- No falsificable. Cualquier intento de falsificación conlleva a un problema intratable matemáticamente.
- Fácil de autenticar, otorga facilidades para determinar su autenticidad aún después de mucho tiempo.
- Irrevocable, será innegable para el autor de una firma su autoría.

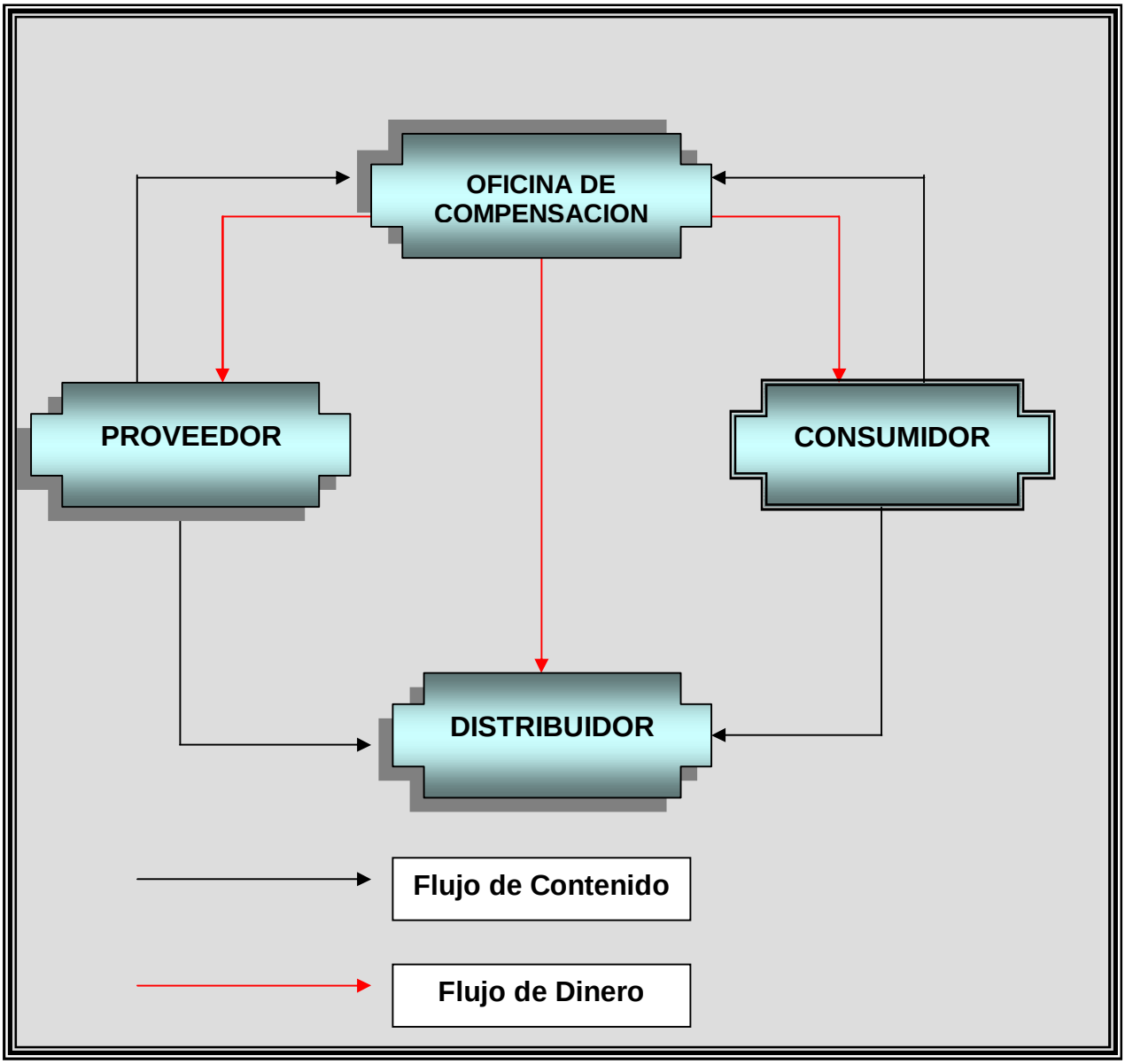
4.2 MODELO TIPICO DRM

Si se toma por ejemplo la implementación DRM con sus nombres y maneras de especificar las reglas de uso, se concluye que en el procedimiento se involucran cuatro partes esenciales que son:

- El proveedor de contenido (content provider).
- El distribuidor.
- La oficina de compensación interbancaria (clearing Mouse).
- El consumidor.

DRM integra un sistema de comercio electrónico (e-commerce) que se ocupa de los pagos por medio de la red. En la Figura 4, están esquematizados los elementos que comúnmente hacen parte de una implementación DRM así como el flujo del contenido representado por la línea continua y el flujo del dinero representado por la línea punteada:

Figura 4 – Implementación DRM[11]



11. Fuente: www.microsoft.com/windows/windowsmedia/wm7/drm/ architecture.aspx

4.2.1 El Proveedor de Contenido: Está representado por una casa disquera o un estudio cinematográfico. Es el dueño del contenido digital y el que desea proteger sus derechos digitales.

4.2.2 El Distribuidor: Posee el canal de distribución. Pueden ser los almacenes en línea y los minoristas de la Red. El distribuidor recibe la información digital del proveedor del contenido y crea un catálogo de presentación en la Red para ofrecer éstos productos.

4.2.3 El Consumidor: Obtiene el contenido a través de la Red y luego paga por la licencia digital. El software o hardware (viewer o player) que utiliza el consumidor para visualizar o escuchar el contenido adquirido, es el encargado de solicitar la licencia a la oficina de compensación interbancaria y obliga al contenido a manejar los derechos de uso.

4.2.4 La Oficina de Compensación Interbancaria: Es aquella que maneja las transacciones financieras que realiza el consumidor para comprar la licencia digital y pagar los derechos de autor respectivos al distribuidor de contenido.

4.3 FASES DE UN MODELO TIPICO DRM

Las siguientes son las fases que un comprador debe llevar a cabo para acceder a un producto a través de un modelo DRM vía Internet:

4.3.1 Primera Fase – Codificación del Contenido Digital: El proveedor codifica el contenido digital en un formato que soporte el sistema DRM. Cada sistema DRM ofrecido debe estar en capacidad de soportar contenidos con diferentes formatos. El contenido digital luego es cifrado y empaquetado como método de preparación para la distribución. El proveedor de contenido utiliza las marcas de agua para convertir el código digital en contenido digital, el cual tiene identificado su dueño y las reglas de uso.

4.3.2 Segunda Fase – Transferencia del contenido a los servidores: Posteriormente el contenido protegido es transferido a los servidores de distribución de contenido para que este sea distribuido en línea y las licencias digitales que contienen las llaves para descifrar y las reglas de uso son enviadas a la oficina de compensación interbancaria.

Las reglas de uso deben especificar como se usa el contenido, dando permisos de copiado, pagar por ver, renta por una semana, etc.

4.3.3 Tercera Fase – Acceso del consumidor al contenido digital: Por otro lado el consumidor baja el contenido digital del servidor Web. Para que el consumidor pueda utilizar el contenido debe hacer la solicitud de licencia a la oficina de compensación interbancaria. Después de recibir la solicitud de licencia la oficina de compensación verifica la identidad del usuario ya sea exigiéndole una Firma Digital para cargar su cuenta basándose en las reglas de uso y genera un reporte de la transacción al proveedor de contenido.

4.3.4 Cuarta Fase – Envío de Licencia: Finalmente la licencia es enviada al dispositivo del consumidor, una vez éste haya pagado a través de un sistema de e-commerce, después de esto el contenido puede ser descifrado y usado de acuerdo con las reglas de uso especificadas en la licencia.

En éste modelo los consumidores podrían pasar el contenido digital adquirido a otras personas, haciendo que los distribuidores dejen de vender a una gran gama de posibles clientes. Sin embargo el contenido digital puede ser distribuido libremente, pero el que lo ejecuta debe contactarse con la oficina de compensación interbancaria y gestionar el pago requerido para obtener la licencia.

Algunas veces, la licencia puede ser enviada a la aplicación antes o simultáneamente en el momento en que se transfiere el contenido digital. Esto se hace particularmente para licencias temporales. Por ejemplo una licencia temporal puede indicar tres accesos para una pieza musical digital, lo cual indica que el usuario podrá escucharla tres veces y posterior a esto tomar la decisión de comprar una licencia con un número ilimitado de accesos. Algunas compañías ofrecen el modelo "pruebe antes de comprar", el cual consiste en contactar al consumidor directamente con la oficina de compensación interbancaria donde puede comprar una licencia permanente una vez la licencia de "prueba" se haya vencido.

4.4 APLICACIONES DEL LADO DEL CLIENTE

Las aplicaciones del lado del cliente que permiten dar ejecución al contenido digital, tanto software como hardware, tienen un papel muy importante en las implementaciones DRM, ya que éstas son las encargadas de exigir la protección digital del contenido con base en las licencias.

La gran mayoría de proveedores ofrecen sus productos sin las funcionalidades DRM, pero existen los plug-ins que se encargan de incorporar el componente DRM al sistema. El proveedor de contenido incluye un archivo con una extensión especial que sirve de identificación del contenido digital protegido por un sistema DRM específico. Al utilizar un plug-in particular el programa que está siendo utilizado para visualizar o ejecutar el contenido abre y descifra el contenido digital apoyándose en las reglas de uso que tenga la licencia.

4.5 ESTADO DEL MERCADO

Los sistemas DRM pueden llegar a prevenir el consumo anónimo del contenido. Una gran posibilidad sería liderar una práctica estándar donde el dueño del contenido tenga una base de datos con la identificación de todos sus compradores.

En otras áreas donde se pueden prestar o comprar los medios, tales como almacenes de alquiler de video, están amparados legalmente; así se previene la transferencia de información personal que esté unida al contenido adquirido.

Como solución para prevenir el anonimato en el acceso a la información digital, DRM puede ser usado para facilitar el perfil de los usuarios o para limitar el acceso a ciertos contenidos. Esto se hace asignando un identificador al contenido o al programa que muestra el contenido y concatenándolo a la información personal del usuario. Como por ejemplo el Windows Media Player de Microsoft, que tiene incluido un identificador único (GUID Globally-Unique Identifier) que lleva el registro de los usuarios.

El poseer información personal de identificación trae como consecuencia una discriminación de precios, que es una práctica que consiste en vender el contenido digital a diferentes precios de acuerdo con el estado financiero del consumidor. Los sistemas DRM aparte de controlar el acceso al contenido, también permiten ajustar el precio del contenido basándose en la identidad del consumidor.

4.6 PROVEEDORES QUE OFRECEN EN EL MERCADO LOS SERVICIOS DE MUSICA UTILIZANDO DRM.

El desarrollo de sistemas DRM apenas está evolucionando pero en la actualidad muchas empresas le apuestan a esta tecnología, algunas de ellas son:

- Windows Media Rights Manager (WMRM) de Microsoft.
- Electronic Media Management System (EMMS) de IBM.
- InterTrust Rights System de InterTrust.
- RealSystems Media Commerce Suite (RMCS) de RealNetworks.
- MusicNow.

- Apple ITunes.
- Liquid Audio.
- Alchemedia.
- Musicmatch Mx Platinum.
- Emusic.
- SealedMedia.
- InterTrust DRM.
- Emediator DRM.
- Real One Rhapsody.
- Pressplay.

La mayoría de las compañías que tienen las canciones más populares están ansiosas por vender, pero esto solo lo pueden hacer una vez hallen la manera más conveniente de hacerlo tanto para los clientes como para los dueños de la información. "Digital Rights Management" está todavía en el inicio de su desarrollo y su difusión no está ampliamente alcanzada, aunque la atención está centrada en este tema; todavía hay gran discusión sobre como puede llegar a ser exitoso.

Como estrategia de mercadeo para motivar a los consumidores a comprar contenido digital en línea y aceptar los nuevos servicios, la industria discográfica necesita diseñar un modelo de negocio atractivo que sea de fácil uso y que además ofrezca precios cómodos respetando tanto los derechos de autor y el de los consumidores.

Algunos de los sitios en Internet que ofrecen el servicio de música incorporando DRM, han sido auspiciados por grandes disqueras tales como:

Web Site	Socios
MusicNet	Real Networks
Fullaudio	BMG
Radio Web	DMC
Napster 2.0	BMG, Warner, EMI, Roxio
Duet	Sony, Universal Music

4.6.1 Comparativo de ofertas: Los sitios que ofrecen música en Internet operan todos de forma diferente; por ello muchos factores influyen a la hora de seleccionar los temas musicales, por ejemplo; Si el tipo de conexión que se tiene es de banda ancha, el servicio de transferencia contínua es el adecuado. Así lo ofrecen algunas comercializadoras como Musicmatch MX Platinum o Rhapsody.

EMusic emplea un enfoque exclusivo para bajar la música. Es un servicio que utiliza las suscripciones por mes, trimestre o por año. Una vez obtenida, se puede bajar toda la música que se quiera del catálogo de disqueras independientes. Los archivos no tienen protección contra copias, así que se pueden grabar en discos compactos o ser transferidos a reproductores de MP3, el servicio no es ilimitado; si se bajan más de 2.000 canciones en un mes, se recibirá por correo electrónico un mensaje en el que se le previene con la cancelación de su cuenta si no reduce su actividad.

4.6.2 Calidad de Audio: La calidad de audio no siempre es la mejor y en algunos sitios este fenómeno es perceptible causando descontento en los usuarios quienes pagan por un producto con un mínimo de especificaciones

5. ENFOQUE REGULATORIO EN COLOMBIA CON RESPECTO A LA REPRODUCCIÓN DE MUSICA EN MEDIOS DIGITALES.

En Colombia se están dando los primeros pasos en materia de regulación de servicios digitales con la firma de una Tratado Internacional de la OMPI sobre la Interpretación y ejecución de fonogramas, la promulgación de la ley 527 de Agosto 18 de 1999 y el Decreto 1747 de Septiembre 11 del 2000 que la reglamenta.

5.1 TRATADO DE LA OMPI SOBRE INTERPRETACIÓN Y EJECUCIÓN DE FONOGRAMAS

Es un convenio para luchar contra la piratería musical en Internet. Entró en vigencia en mayo 20 del 2003 después de ser ratificado por 30 países. Este proyecto se ha adoptado hasta ahora por países tales como: Estados Unidos, México, Honduras, Costa Rica, El Salvador, Panamá, Colombia, Paraguay, Argentina, Ecuador, Chile.

Además de otros países Europeos y Africanos. Este tratado se encarga de proteger a los músicos y a la industria discográfica de la amenaza de piratería planteada por Internet y otras tecnologías digitales mejorando su protección internacional', y además reconoce los 'derechos exclusivos de reproducción, distribución, alquiler comercial y difusión pública en Internet'.

La corte constitucional Colombiana mediante revisión dío vía libre al Tratado internacional de la OMPI de reproducción de fonogramas en

Internet. El contenido del Tratado sobre la interpretación y ejecución de fonogramas fue declarado exequible (es decir, se ajusta a la Constitución) y por lo tanto es aplicable a la legislación colombiana.

La misma Corte en sus consideraciones establece que el tratado busca ampliar la protección de los derechos de propiedad intelectual adecuados a las necesidades impuestas por el desarrollo de la tecnología digital como forma de transmisión, reproducción y ejecución de obras sonoras.

Los acuerdos internacionales suscritos en el convenio OMPI obligan a los Estados miembros a incluir en sus correspondientes legislaciones las herramientas pertinentes para proteger las obras artísticas que se transmiten y se almacenan en Internet o en cualquier otro medio digital.

Así pues, la divulgación de esta clase de obras a través de la red mundial comienza a considerarse como una publicación.
De esta forma cualquier reproducción o almacenamiento en la memoria de un servidor, estará sujeta a la legislación de propiedad intelectual y derechos de autor.

5.2 LEY 527 DE AGOSTO 18 DE 1999.

Se Puede llamar a esta la ley marco por medio de la cual se define y reglamenta el acceso, uso de los mensajes de datos, del comercio electrónico, de las firmas digitales, y se establecen las entidades de certificación.

5.2.1 Aspectos de la Ley 527 de 1999: En sus primeras dos partes, se basan en los lineamientos fijados en el proyecto de Ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional -CNUDMI. La Ley 527 consagra el reconocimiento jurídico de los mensajes de datos de contenido comercial, como aporte fundamental en el comercio electrónico en Colombia.

En su tercera parte, la Ley 527 introdujo un elemento que no figura en la Ley Modelo de las Naciones Unidas. Se trata del mecanismo de certificación de firmas digitales, llevada a cabo por entidades especializadas, creadas bajo la autorización Estatal y supervisada por la Superintendencia de Industria y Comercio.

El Gobierno Nacional, mediante el Decreto 1747 del 11 de septiembre de 2000 define las condiciones que deben cumplir quienes aspiren a certificar las firmas digitales en Colombia.

5.2.1.1 Certificación de firmas digitales: La parte más extensa de la Ley 527, se dedica a legitimar en Colombia un aparato tecnológico teórico, el cual otorga condiciones materiales de integridad, confiabilidad y seguridad a los mensajes electrónicos que conlleven operaciones y transacciones comerciales, cuando se carece del contacto directo o físico entre las partes.

5.2.1.2 Entidades de Certificación: En el Capítulo II artículo 29 se establece que podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero

y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional.

5.2.1.3 Certificados: Sobre este tema el Capítulo III artículo 35 señala que un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

5.3 CUADRO INFORMATIVO DE LEGISLACIÓN EN COMERCIO ELECTRÓNICO.

Las siguientes son las leyes acerca de comercio electrónico que rigen en algunos países iberoamericanos[13]:

- ARGENTINA: Cuenta con la Ley 25.506, Mediante la cual se reconoce el empleo de la firma electrónica, de la firma digital y del certificado digital y su eficacia jurídica.

- BRASIL: Gestiona un Proyecto de Ley de la Cámara de Diputados N° 1.589, que dispone sobre el comercio electrónico, la validez jurídica del documento electrónico y la firma digital.

- CHILE: Posee el Decreto 81 de 1999 que regula la utilización de la firma digital y los documentos electrónicos como soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos de la administración del Estado.

- COSTA RICA: Desarrolla un Proyecto de Ley con el propósito de obtener la adecuada seguridad y certidumbre en las transacciones electrónicas basadas en la red de redes.

- ECUADOR: Hace uso de la Ley No. 67. R.O. Suplemento 557, Para regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

- GUATEMALA: Actualmente se encuentra en desarrollo una ley que será aplicable a todo tipo de información en forma de mensaje de datos.

13. Fuente: www.apc.org/español/rights/lac/clegislacion.sthml?x=1893

- MÉXICO: Se realizan esfuerzos conjuntos con el Proyecto de Decreto con reformas y adiciones al Código Civil Federal, al Código de Comercio y a la Ley Federal de Protección al Consumidor en materia de comercio electrónico.

- PANAMA: Se presentó el anteproyecto de ley por medio del cual se define y reglamenta el acceso y uso del comercio electrónico, firmas digitales y se autorizan las entidades de certificación.

- PERU: Cuenta con una ley que tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

- REPUBLICA DOMINICANA: Tiene la Ley No. 126-02, promulgada el 4 de septiembre del 2002.

- URUGUAY: Adelanta un proyecto de ley que regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

- VENEZUELA: Posee un Decreto-Ley que tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

6. CONCLUSIONES

- El crecimiento de Internet es evidente tanto en los países desarrollados como en vía de desarrollo. Según las estadísticas y planes de masificación propuestos por los diferentes gobiernos, se recomienda que además de hacer planes de expansión se deben realizar programas de capacitación orientado a los usuarios de todas las edades, con el fin de que puedan interactuar con este medio para obtener recursos como música, videos, imágenes, etc.

- Mediante la recopilación de información sobre derechos de autor, se pretende dejar un documento que centralice y sirva de guía o consulta para los estudiantes de la especialización y demás interesados en el tema de Administración de derechos digitales para Internet; ya que no existe un texto que abarque estos contenidos y por el contrario la información que existe se encuentra muy dispersa y superficial.

- De acuerdo con los temas abordados en el transcurso de la especialización y en especial de la asignatura de seguridad en redes, se puede afirmar que los sistemas utilizados por D.R.M, para cifrado de datos, como el uso de clave pública son apropiados y por lo tanto garantizan la confiabilidad que el propietario del contenido digital requiere en cuanto a fidelidad, integridad y seguridad.

- Con el ánimo de evitar la piratería digital, se recomienda a los entes estatales encargados de vigilar y hacer respetar los derechos de autor, ser drásticos y aplicar las normas vigentes con transparencia contando con el apoyo de la Policía Nacional, la Fiscalía y demás entes de control y vigilancia. La violación de los derechos de autor ha generado enormes pérdidas económicas para los propietarios de contenidos digitales, casas disqueras y artistas e inclusive para el mismo Estado por la evasión de impuestos que ello genera.

- La adopción de D.R.M como estándar en el mercado Colombiano, traerá como consecuencia la reducción significativa en las ventas al principio, debido a la inconformidad que se genera al pagar por lo que antes no costaba nada. Con base en lo anterior se aconseja dar incentivos a los usuarios como por ejemplos promociones y descuentos en las tarifas de los servicios digitales en Internet.

- En cuanto a la parte normativa se presenta una síntesis regulatoria en Colombia la cual es comparada con la de otros países latinoamericanos en lo que se refiere a derechos digitales. Con este análisis se busca dejar un material que sirva de consulta a los estudiantes, ya que en cuestión normativa Colombia es pionera en lo que se refiere a protección y derechos de autor.

- Colombia posee la Ley 527 de 1999, que es catalogada como uno de los pilares para el comercio electrónico y por consiguiente se considera al país como uno de los más avanzados en

infraestructura jurídica. Esta ley hace un reconocimiento jurídico para los datos de contenido comercial a través de las redes y que se creó con el propósito de brindar condiciones de confiabilidad y seguridad.

- La Ley 527 legitimó un mecanismo tecnológico complejo para las entidades de certificación y firma digital, pero no se tuvo en cuenta el costo para poderla implementar en Colombia. Además no contempla estímulos para el comercio electrónico, no ordena apoyo estatal para su desarrollo, tampoco resuelve aspectos tributarios, arancelarios y cambiarios. No se contemplan las responsabilidades que deben afrontar los actores del comercio electrónico como por ejemplo los comerciantes, los consumidores y entes financieros. Por lo tanto se deben tener en cuenta los anteriores aspectos en una reforma legislativa, para que el comercio electrónico no se detenga.

- El decreto reglamentario 1747 de 2000, define las condiciones que deben cumplir quienes aspiren a certificar las firmas digitales en Colombia. En sus primeros 27 artículos se definen condiciones complejas como por ejemplo la de cubrir todos los perjuicios contractuales y extra contractuales de los suscriptores y terceros por errores u omisiones de actos de mala intención de los administradores, empleados o representantes legales de la empresa certificadora.

- Los anteriores aspectos se deben tener en cuenta para una futura reforma legal, ya que se considera que estos requisitos son

muy exigentes y por lo tanto todavía no hay suficientes entidades de certificación en Colombia, hecho este que estanca el comercio electrónico.

- Una vez descritos los diferentes métodos de protección de derechos de autor, se observa que D.R.M, es el recurso más efectivo para preservar estos derechos y se ha destacado por su excelente aceptación por parte de los usuarios y propietarios de contenido digital. Por lo tanto se sugiere que este método sea implementado por los diferentes entes regulatorios en Colombia y sea adoptado como estándar por las casas disqueras.

BIBLIOGRAFIA

ACLANTIS. Devela la Tecnología de Derechos Digitales. (On line) Agosto 2003, (España) Disponible en Internet.
http://www.aclantis.com/news.php

COLCIENCIAS. Distribución de Contenidos Digitales en Internet. (On line) Septiembre 2003, (Colombia) Disponible en Internet.
http://www.colciencias.gov.co/agenda/noticias_co.php

FUSTER SABATER, Amparo; DE LA GUIA MARTINEZ, Dolores; HERNANDEZ ENCINAS, Luis; MONTOYA VITINI, Fausto; MUÑOZ MASQUE, Jaime. TECNICAS CRIPTOGRAFICAS DE PROTECCION DE DATOS. Madrid, AlfaOmega. 1997. 279 p.

CABALLERO, Pino. SEGURIDAD INFORMATICA. Madrid, AlgaOmega. 1996. 137 p.

DENKEN UBER. Derechos Digitales...Soluciones Equivocadas. (On line) Mayo 2002, Disponible en Internet.
http://www.uberbin.net/archives/car_noticias.php

IDC. Gestión de derechos digitales: protección y nuevas posibilidades en la Red (on line) Octubre 2001, (España) Disponible en Internet.
http://www.idc.com/spain/newsletters/ebusiness_archivo.htm

NEXTANCE. End-to-End Rights and Asset Management (on line) Agosto 2003, Disponible en Internet. http://www.nextance.com//products/contract_management/nexrights/index .html

REDNET ARGENTINA. Principios Aceptables Que Rigen Para El Cliente En El Uso De Internet. (On line) Julio 2003, (Argentina) Disponible en Internet.

http://rednet.com.ar/servicios/normas.htm

OPPLIGER, Rolf. SISTEMAS DE AUTENTIFICACION PARA SEGURIDAD EN REDES, Madrid, AlfaOmega, 1998, 194 p.

Bibliografía relacionada directamente con DRM: (Disponible en Internet)

www.microsoft.com/windows/windowsmedia/wm7/drm/what.aspx

www.microsoft.com/windows/windowsmedia/9series/drm.aspx

www.devx.com/security/article/7868/0/page/1

ANEXO

LEY NÚMERO 527 DE 1999

(Agosto 18 de 1999)

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

El Congreso de Colombia,

DECRETA:

ÍNDICE

PARTE I: PARTE GENERAL
CAPÍTULO I: Disposiciones generales

ART. 1º. Ámbito de aplicación. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales, y

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

ART. 2º. Definiciones. Para los efectos de la presente ley se entenderá por:

a) Mensaje 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;

b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar

que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) Entidad de certificación. 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 transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

e) Intercambio electrónico de datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto, y

f) Sistema de información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

ART. 3º. 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 ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

ART. 4º. Modificación mediante acuerdo. Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III, parte I, podrán ser modificadas mediante acuerdo.

ART. 5º. Reconocimiento jurídico de los mensajes de datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

CAPÍTULO II: Aplicación de los requisitos jurídicos de los mensajes de datos

ART. 6º. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

ART. 7º. Firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

ART. 8º. Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma, y

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

ART. 9º. Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

ART. 10. Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil.

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 sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ART. 11. Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

ART. 12. Conservación de los mensajes de datos y documentos. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida.

3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

ART. 13. Conservación de mensajes de datos y archivo de documentos a través de terceros. El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPÍTULO III: Comunicación de los mensajes de datos

ART. 14. Formación y validez de los contratos. En la formación del contrato, salvo acuerdo expreso entre 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.

ART. 15. Reconocimiento de los mensajes de datos por las partes. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

ART. 16. Atribución de un mensaje de datos. Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador.

2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o

3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

ART. 17. Presunción del origen de un mensaje de datos. Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o

2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

ART. 18. Concordancia del mensaje de datos enviado con el mensaje de datos recibido. Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, éste último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

ART. 19. Mensajes de datos duplicados. Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o

debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

ART. 20. Acuse de recibo. Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

ART. 21. Presunción de recepción de un mensaje de datos. Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

ART. 22. Efectos jurídicos. Los artículos 20 y 21 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

ART. 23. Tiempo del envío de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté

bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

ART. 24. Tiempo de la recepción de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar:

1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o

2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos, y

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

ART. 25. Lugar del envío y recepción del mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

PARTE II: Comercio electrónico en materia de transporte de mercancías

ART. 26. Actos relacionados con los contratos de transporte de mercancías. Sin perjuicio de lo dispuesto en la parte I de la presente ley, este capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea taxativa:

a) I. Indicación de las marcas, el número, la cantidad o el peso de las mercancías.

II. Declaración de la naturaleza o valor de las mercancías.

III. Emisión de un recibo por las mercancías.

IV. Confirmación de haberse completado el embarque de las mercancías;

b) I. Notificación a alguna persona de las cláusulas y condiciones del contrato.

II. Comunicación de instrucciones al transportador;

c) I. Reclamación de la entrega de las mercancías.

II. Autorización para proceder a la entrega de las mercancías.

III. Notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;

e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;

f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías, y

g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

ART. 27. Documentos de transporte. Con sujeción a lo dispuesto en el inciso 3º del presente artículo, en los casos en que la ley requiera que

alguno de los actos enunciados en el artículo 26 se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El inciso anterior será aplicable, tanto si el requisito en él previsto está expreso en forma de obligación o si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o utilización de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del inciso tercero, el nivel de confiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 26, no será válido ningún documento emitido en papel para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos emitidos en papel. Todo documento con soporte en papel que se emita en esas circunstancias deberá contener una declaración en tal sentido. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento emitido en papel, esa norma no dejará de aplicarse a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en documentos emitidos en papel.

PARTE III: Firmas digitales, certificados y entidades de certificación

CAPÍTULO I: Firmas digitales

ART. 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.

PAR. 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.

CAPÍTULO II: Entidades de certificación

ART. 29. Características y requerimientos de las entidades de certificación. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;

b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la

autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley, y

c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

ART. 30. Actividades de las entidades de certificación. Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.

3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.

4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

ART. 31. Remuneración por la prestación de servicios. La remuneración por los servicios de las entidades de certificación será establecida libremente por éstas.

ART. 32. Deberes de las entidades de certificación. Las entidades de certificación tendrán, entre otros, los siguientes deberes:

a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;

c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;

d) Garantizar la prestación permanente del servicio de entidad de certificación;

e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;

f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;

g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

h) Permitir y facilitar la realización de las auditorias por parte de la Superintendencia de Industria y Comercio;

i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio, y

j) Llevar un registro de los certificados.

ART. 33. Terminación unilateral. Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

ART. 34. Cesación de actividades por parte de las entidades de certificación. Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte de la Superintendencia de Industria y Comercio.

CAPÍTULO III: Certificados

ART. 35. Contenido de los certificados. Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.

2. Identificación del suscriptor nombrado en el certificado.

3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.

4. La clave pública del usuario.

5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.

6. El número de serie del certificado.

7. Fecha de emisión y expiración del certificado.

ART. 36. Aceptación de un certificado. Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

ART. 37. Revocación de certificados. El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

1. Por pérdida de la clave privada.

2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

1. A petición del suscriptor o un tercero en su nombre y representación.

2. Por muerte del suscriptor.

3. Por liquidación del suscriptor en el caso de las personas jurídicas.

4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.

5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.

6. Por el cese de actividades de la entidad de certificación.

7. Por orden judicial o de entidad administrativa competente.

ART. 38. Término de conservación de los registros. Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

CAPÍTULO IV: Suscriptores de firmas digitales

ART. 39. Deberes de los suscriptores. Son deberes de los suscriptores:

1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.

2. Suministrar la información que requiera la entidad de certificación.

3. Mantener el control de la firma digital.

4. Solicitar oportunamente la revocación de los certificados.

ART. 40. Responsabilidad de los suscriptores. Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

CAPÍTULO V: Superintendencia de Industria y Comercio

ART. 41. Funciones de la superintendencia. La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones:

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.

2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.

3. Realizar visitas de auditoria a las entidades de certificación.

4. Revocar o suspender la autorización para operar como entidad de certificación.

5. Solicitar la información pertinente para el ejercicio de sus funciones.

6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.

8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.

9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.

10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.

11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

ART. 42. Sanciones. La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

1. Amonestación.

2. Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora.

4. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.

5. Revocar definitivamente la autorización para operar como entidad de certificación.

CAPÍTULO VI: Disposiciones varias

ART. 43. Certificaciones recíprocas. Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

ART. 44. Incorporación por remisión. Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por

remisión a ese mensaje de datos. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

PARTE IV: Reglamentación y vigencia

ART. 45. La Superintendencia de Industria y Comercio contará con un término adicional de doce (12) meses, contados a partir de la publicación de la presente ley, para organizar y asignar a una de sus dependencias la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella para tal efecto.

ART. 46. Prevalencia de las leyes de protección al consumidor. La presente ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

ART. 47. Vigencia y derogatorias. La presente ley rige desde la fecha de su publicación y deroga las disposiciones que le sean contrarias.

Publíquese y ejecútese.

Dada en Santa fe de Bogotá, D.C., a 18 de agosto de 1999.