SEGURIDAD DEL COMERCIO ELECTRÓNICO EN COLOMBIA DESDE UNA PERSPECTIVA JURÍDICA

ANEXOS

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

INDICE DE ANEXOS

ANEXO A: OBTENCIÓN DE LA MUESTRA DE SITIOS WEB

El primer paso para realizar una evaluación de seguridad es localizar el conjunto de sitios Web que se desean evaluar. Aunque al inicio de este trabajo se intento localizar únicamente los sitios Web con dominio regional ".co", en el proceso de búsqueda se vio que la muchos de los sitios representativos en Colombia no cuentan con dominio genéricos, además para las obligaciones legales en Colombia lo mas importante es que tengan su asiento principal en este país. Por estos motivos se decidió considerar tanto los sitios Web con dominio regional como genérico.

Inicialmente se recolectaron por medio de búsqueda manual mas de 80 diferentes sitios Web que al parecer contaban con comercio electrónico directo ya que por su mayor grado de vulnerabilidad son mas relevantes para el estudio. Posteriormente se empezó con una búsqueda manual ingresando a cada sitio y verificando efectivamente la posibilidad de realizar compras en línea. El principal inconveniente en esta parte es que la gran mayoría de los sitios requieren que los usuarios estén registrados en el sitio para poder realizar compras, como una medida de seguridad y control estadístico de quien realiza las compras. Esto demoró la búsqueda ya que implicó realizar registros en los sitios Web.

En el proceso de cuantificación se encontraron varias empresas ".com.co" pero que al empezar el proceso de compra en línea se redirecciona a una pagina genérica que es solo .com. Sin embargo se dejaron varias de estas empresas "..com" para el análisis.

Otro punto importante en el proceso de selección de la muestra fueron las corporaciones financieras. Estas entidades en su gran mayoría ofrecen servicios sobre Internet como el pago de servicios públicos o consultas bancarias. No se incluyeron estas corporaciones en la muestra a analizar porque se quiso escoger sitios de compra-venta directa entre el cliente y las empresas y no actividades financieras.

Inicialmente se planteó automatizar la búsqueda de estos sitios pero se encontraron los siguientes impedimentos.

- No están claros todos los dominios asignados en Colombia y en muchas ocasiones sitios netamente colombianos tiene sus Host en otros países.

- No es fácil buscar puertos abiertos o servicios ofrecidos por los servidores porque la gran mayoría cuentan con Firewall.
- En caso que se pueda verificar los puertos abiertos esto tomara mucho tiempo por el amplio rango de direcciones que se tendrían que analizar. A manera de ejemplo la herramienta Nmap tardó 62292 segundos equivalente a 17.3 horas en escanear 77 direcciones IP con la opción de escaneo -sS -O -P0 -D.
- Muchos sitios Web ofrecen servicios y conexiones tanto por el puerto 80 como conexiones seguras a través del 443 y no ofrecen servicios de comercio electrónico y muchos sitios de comercio electrónico lo prestan por otros puertos.
- Se planteo también la opción de utilizar un Script realizado en Perl y Netcat o utilizar un programa extractor de texto como el Web Data Extractor pero ambas opciones resultaron ineficientes porque muchos de los sitos utilizan las palabras que se intentaron buscar en artículos, noticias y demás lo que produjo que esta técnica arrojara un margen de error muy alto.

Después del proceso de búsqueda los sitios Web y de la depuración de las listas iniciales que se obtuvieron se obtuvo la siguiente lista de sitios Web a los que posteriormente se le aplicaron las pruebas y evaluaciones de seguridad:

Empresa	Dirección electrónica	Dirección IP
Almacenes Éxito	www.virtualexito.com	200.31.19.19
Papiros Ltda.	www.papiros.com	130.94.243.4
Diario La Opinión	www.laopinion.com.co	208.56.184.2
Almacenes la 14	www.la14.com	66.128.34.122
Deremate.com	Colombia.deremate.com	216.25.288.80
Virtualtiendas	www.virtualtiendas.com	209.15.164.247
El mercado de las Pulgas	www.mercadodelaspulgas.net	65.167.61.58
Mercadolibre	www.mercadolibre.com.co	216.35.213.254
Compaq	Web1.compaq.com/store	161.114.23.250
Almacenes Carulla	www.telleva.com.co	64.86.184.9
	Secure.iquiero.com/colombia/	207.22.51.88
Casa Musical Alcibíades Bedoya	www.casamusical.com	64.77.113.185
Tornillos & Partes	www.tornillosypartes.com.co	216.36.252.3
WilkinsonPC Computadores y Partes	www.willkinsonpc.com.co	200.31.19.121

Colombia Típica	www.typicalcolombia.com/es	65.161.248.24
Alianza Summa	www.summan.com	200.13.224.105
Cekit Electrónica	www.cekit.com.co	204.174.223.36
Ecomerz	www.ecomerz.com.co	200.25.22.40
Bellsouth	www.bellsouth.com.co	200.32.80.238
Comcel	www.comcel.com.co	64.239.37.21
	Comercio.ccb.org.co/tienda/	200.31.65.25
	www.timoteo.com	130.94.243.104
Tienda de la Rosas	www.latiendadelasrosas.com	130.94.243.102
Tu importas.com	www.tuimportas.com	130.94.243.100
Cinecolombia	www.cinecolombia.com.co	200.14.205.51
	Sun19061.dn.net/perl/	130.94.68.103
	www.comprarnet.com	208.221.129.29
Ancora Editores	www.elancoraeditores.com	200.31.19.32
	www.emultired.com	200.24.70.82
PC Madrigal	www.pcmadrigal.com	209.15.76.242
Zona Virtual	www.zonavirtual.com	209.15.10.232
	www.geo.net.co	200.69.97.16
Villega Editores	www.villegaseditores.com	64.225.117.114
Tiendas del Color	www.tiendasdelcolor.com	200.13.224.100
Almacenes Mercomas	www.mercomas.com	200.75.78.11
Almacenes Mercomucho	www.mercomucho.com	200.75.78.11
	www.ecolombia.com.co	139.81.148.130
Magisterio de Colombia	www.magisterio.com.co	200.25.22.1
Orbitel	www.orbitel.com.co	200.30.64.66

ANEXO B: EVALUACIÓN DE LAS SEGURIDAD DE LOS SITIOS WEB DE COMERCIO ELECTRÓNICO EN COLOMBIA

Para proponer soluciones tecnológicas a los problemas del comercio electrónico se deben seguir varios pasos, además que el análisis tecnológico es una base para poder plantear soluciones jurídicas certeras y muy acercadas a la realidad. Aquí es importante mencionar que con el solo análisis tecnológico no se pueden plantear soluciones jurídicas, es necesario, llevar esos análisis tecnológicos a uno conjunto de problemas (vulnerabilidades), formas de aprovecharse de esos problemas (ataques) y consecuencias (efectos).

1. Evaluación del estado actual de la seguridad del comercio electrónico

El proceso para la evaluación de seguridad de los sitios Web de comercio electrónico colombianos se dividió en dos fases. Una primera fase que consistió en obtener la información relevante para el análisis. Esta fase requirió de mucha paciencia ya que hay que recolectar y analizar gran cantidad de información y muchas de las herramientas software utilizadas requieren de varios días par obtener algunos datos.
Un factor importante en esta primera fase es que se debe realizar en un periodo de tiempo largo porque en muchas ocasiones la configuración de los servidores cambia con los meses, así como se descubren nuevas vulnerabilidades.

1.1 Fase I

La primera fase de dividió en tres partes:

1.1.1 Recolección información: Una vez que se tenían los nombres de los sitios Web a analizar se empezó el proceso de recolección de toda la información posible de los sitios. Este proceso se realizo básicamente visitando uno a uno los sitios Web para identificar información importante colocada en el mismo sitio, además se utilizo la herramienta de exploración de texto de sitios Web llamada Web Data Extractor versión 3.7[1] con la que se obtuvo información sobre correos electrónicos, números telefónicos y algunas palabras claves contenidas en las páginas.

[1] Ver información adicional de la herramienta en el Anexo C

1.1.2 Enumeración de la red: En este proceso se utilizó la herramienta Sam Spade versión 1.14 y la pagina Web de DNSstuff.com[2] para realizar búsquedas Whois, traceroute para poder identificar la procedencia del Servidor, su lugar físico de ubicación, información relevante sobre los administradores del dominio y titular de sitio. En la mayoría de los casos no se obtuvieron buenos resultados.

1.1.3 Ejecución de las herramientas de escaneo: Por ultimo en este proceso se utilizaron las diferentes herramientas de recolección de información de las conexiones del Servidor.
Estas herramientas fueron: Lan Guard Network Sacanner versión 2.0 Beta, Nmap, Netcat, Super Scan y Port Scan.

Con la primera lista de sitios que al parecer prestan servicios de comercio electrónico se realizó un primer escaneo remoto utilizando la herramienta nmap con las opciones -sS -O -P0 -D 209.123.16.20 -i archivo_entrada -o archivo_salida.

1.2 Fase II

En la segunda fase se realizo una análisis de las empresas para así proporcionar concepto sobre la seguridad de los sitios Web.

1.2.1 Sitios con antecedentes
Es muy importante para un análisis de seguridad considerar los antecedentes de ataques del país. A continuación se relacionan en una tabla todos los sitios a los que les ha sido vulnerada la seguridad según el sitio Web Zone-H con su correspondiente fecha, atacante, nombre de dominio y cuando se pudo determinar también el sistema operativo.

Fecha	Atacante	Nombre	Sistema Operativo

[2] http://www.dnsstuff.com

22/01/2000	sh00ter	kaplan.com.co	Windows
10/11/2000	Prime Suspectz	visa.com.co	Windows
16/11/2000	Prime Suspectz	la-republica.com.co	Windows
24/11/2000	Prime Suspectz	nec.com.co	Windows
03/12/2000	WFD	redcolombia.com.co	Windows
23/01/2001	Furia.BR	coopserv.com.co	Linux
29/01/2001	Silver Lords	informatica.com.co	Windows
17/02/2001	Hi-Tech Hate	okidata.com.co	Windows
01/03/2001	Supreme Entity	petrobras.com.co	Windows
10/03/2001	ReFLuX	mcdonalds.com.co	Windows
18/03/2001	Prime Suspectz	netxos.com.co	SolarisSun OS
17/04/2001	pr0phet	netxos.com.co	SolarisSun OS
29/04/2001	f0ul	coopserv.com.co	Linux
11/05/2001	cr1m3 0rg4n1z4d0	telefonica-data.com.co	Windows
05/06/2001	Perfect.br	sfi.com.co	Windows
05/06/2001	NAsh	aia.com.co	Windows
07/06/2001	Cyb3r Attack	gec.com.co	Windows
09/06/2001	King420	parche.telesat.com.co	Windows
15/06/2001	Demoniados.Br	digitalware.com.co	Windows
15/06/2001	Demoniados.br	bancomercantil.com.co	Windows
27/06/2001	Web Pirates	canooutsourcing.com.co	Windows
28/06/2001	web pirates	convergencia.com.co	Windows
28/06/2001	Web Pirates	eluniversal.com.co	Windows
28/06/2001	Web Pirates	ecogas.com.co	Windows
30/06/2001	Web Pirates	finotex.com.co	Windows
30/06/2001	Web Pirates	executrain.com.co	Windows
01/07/2001	Web Pirates	gmac.com.co	Windows
02/07/2001	Web Pirates	ingetec.com.co	Windows
02/07/2001	Web Pirates	hq.com.co	Windows
05/07/2001	Web Pirates	intesa.com.co	Windows
06/07/2001	Web Pirates	naturesunproducts.com.co	Windows
06/07/2001	Web Pirates	lowe-sspm.com.co	Windows
06/07/2001	Web Pirates	meltec.com.co	Windows
07/07/2001	Perfect.br	bostonsci.com.co	Windows
07/07/2001	Web Pirates	proware.com.co	Windows
07/07/2001	Web Pirates	sistecredito.com.co	Windows
07/07/2001	Web Pirates	sodexho.com.co	Windows
07/07/2001	Web Pirates	schradercamargo.com.co	Windows
08/07/2001	Web Pirates	surtigas.com.co	Windows
08/07/2001	Prime Suspectz	pinel.com.co	SCO Unix
09/07/2001	SecureInfo	abs.com.co	Windows
26/07/2001	Tissia	digitalware.com.co	Windows
08/08/2001	Cyb3r Attack	canooutsourcing.com.co	Windows
08/08/2001	RB Team	colombiacompite.com.co	Windows

09/08/2001	RB Team	comline.com.co	Windows
09/08/2001	Cyb3r Attack	proware.com.co	Windows
10/08/2001	Cyb3r Attack	naturesunproducts.com.co	Windows
14/08/2001	BHS	polaroid.com.co	Windows
27/09/2001	BFH	boterosoto.com.co	Windows
27/09/2001	BFH	antivirus.com.co	Windows
01/10/2001	nu|L	telecaqueta.com.co	SolarisSun OS
11/10/2001	nu|L	eevvm.com.co	IRIX
12/10/2001	Eagle	bostonsci.com.co	Windows
21/10/2001	LinuxLover	zeus.eevvm.com.co	SCO Unix
05/11/2001	WINSATANIC	heel-colombia.com.co	Windows
08/11/2001	WINSATANIC	lau.com.co	Windows
08/11/2001	Unknown	mapfre.com.co	Windows
09/11/2001	WINSATANIC	paisas.com.co	Windows
11/11/2001	Unknown	sofasa.com.co	Windows
11/11/2001	WINSATANIC	psl.com.co	Windows
11/11/2001	WINSATANIC	tdm.com.co	Win NT9x
11/11/2001	Unknown	solutech.com.co	Windows
14/11/2001	Silver Lords	domicilios.com.co	Unknown
15/11/2001	WINSATANIC	semagroup.com.co	Windows
18/11/2001	S0l4ris	suncamps.com.co	Windows
09/12/2001	BHS	pinel.com.co	SCO Unix
17/12/2001	M4fia.Br	paisas.com.co	Windows
21/12/2001	Hack00x Killers	fanadis.com.co	Windows
22/12/2001	Hack00x Killers	ferrogruas.com.co	Unknown
26/12/2001	w0n4d	heel-colombia.com.co	Windows

14/01/2002	H.i.S	boterosoto.com.co	Windows
19/01/2002	M4F14	paisas.com.co	Windows
19/01/2002	hax0rs lab	unitel.com.co	Unknown
20/01/2002	BaXiM_MsN	sido.com.co	Windows
20/01/2002	BaXiM_MsN	boterosoto.com.co	Windows
21/01/2002	BaXiM_MsN	telegirardot.com.co	Unknown
22/01/2002	BaXiM_MsN	tdm.com.co	Win NT9x
23/01/2002	BaXiM_MsN	ferrogruas.com.co	Unknown
31/01/2002	hax0rs lab	colombiavirtual.com.co	Linux
12/03/2002	Trippin Smurfs	...aniasdecolombia.com.co	SolarisSun OS
21/03/2002	Trippin Smurfs	pinel.com.co	SCO Unix
24/03/2002	Trippin Smurfs	coopetrol.com.co	Linux
25/03/2002	Grupo NG	tdm.com.co	Win NT9x
27/03/2002	spabaton	tdm.com.co	Win NT9x
29/03/2002	woot-project	vsr.com.co	Linux
06/04/2002	iS	texaco.com.co	Linux
06/04/2002	iS	texaco.com.co	Linux
06/04/2002	BlooDMASK	correo.webdepot.com.co	Linux

14/05/2002	Innocent Boys	amg.com.co	Win 2000
14/05/2002	S4t4n1c_S0uls	polaroid.com.co	Win NT9x
12/06/2002	MedanHacking	...anizales.com.co/mh.htm	Win NT9x
08/07/2002	Fatal Error	...mbia.com.co/index.html	Win NT9x
08/07/2002	xsun	emcali.com.co	Win 2000
09/07/2002	xsun	aerodinamica.com.co	Win NT9x
18/07/2002	xsun	guianza.com.co/index.htm	Win NT9x
22/07/2002	ISOTK	seaboardcolombia.com.co	Win NT9x
06/08/2002	g0pher	guianza.com.co	Win NT9x
07/08/2002	Cyb3r Attack	aldato.com.co	Win NT9x
20/08/2002	Shellc0d3	seaboardcolombia.com.co	Win NT9x
10/09/2002	Arabian_Sniper	abs.com.co	Win NT9x
11/09/2002	BreaKIce	...news/_notes/index.html	Win 2000
26/09/2002	Arabian_Sniper	abs.com.co	Win NT9x
23/10/2002	Suicidal Pigs	repremundo.com.co	Linux
02/11/2002	BreaKIce	...c146.uolpremium.com.co	Unknown
05/11/2002	cybers satans	alfaomega.com.co	Win 2000
05/11/2002	cybers satans	controlambiental.com.co	Win 2000
18/11/2002	NixGr0up	imbanaco.com.co	Linux
27/11/2002	gB	telecom.com.co	SolarisSun OS
08/12/2002	delirium	celsa.com.co	Linux
10/12/2002	Fatal Error	geca.com.co	Win 2000
23/12/2002	MHA	mail.melianelight.com.co	Linux

19/05/2003	kn0w	dino.com.co	Linux
11/05/2003	BloodBR	muebleselemperador.com.co	Linux
11/05/2003	BloodBR	mipc.com.co	Linux
11/05/2003	BloodBR	melec.com.co	Linux
11/05/2003	BloodBR	intermec.com.co	Linux
11/05/2003	BloodBR	itsystems.com.co	Linux
11/05/2003	BloodBR	interseguros.com.co	Linux
11/05/2003	BloodBR	index.com.co	Linux
11/05/2003	BloodBR	hotellaesperanza.com.co	Linux
11/05/2003	BloodBR	geovision.com.co	Linux
11/05/2003	BloodBR	festytortas.com.co	Linux
11/05/2003	BloodBR	fanty.com.co	Linux
11/05/2003	BloodBR	unidata.com.co	Linux
11/05/2003	BloodBR	tourcolombia.com.co	Linux
11/05/2003	BloodBR	ecostick.com.co	Linux
11/05/2003	BloodBR	racomex.com.co	Linux
11/05/2003	BloodBR	syac.com.co	Linux
11/05/2003	BloodBR	sanagustin.com.co	Linux
11/05/2003	BloodBR	seduceme.com.co	Linux
11/05/2003	BloodBR	polarix.com.co	Linux
11/05/2003	BloodBR	pcmicros.com.co	Linux

11/05/2003	BloodBR	comfacundi.com.co	Linux
11/05/2003	BloodBR	competition.com.co	Linux
11/05/2003	BloodBR	colmedia.com.co	Linux
11/05/2003	BloodBR	boxer.com.co	Linux
10/05/2003	BloodBR	valoresyvalores.com.co	Linux
10/05/2003	BloodBR	directorio.com.co	Linux
10/05/2003	BloodBR	autosderisaralda.com.co	Linux
01/05/2003	jacXall	tdm.com.co/hack.asp	Win XP
28/04/2003	BI0S	dzm.com.co	Linux
28/04/2003	TNT	...et.com.co/default.html	Win 2000
20/04/2003	TechTeam	ax.axiscom.com.co	Linux
20/04/2003	TechTeam	axiscom.com.co	Linux
20/04/2003	infected hax team	intranet.merco.com.co	Linux
14/04/2003	Bug-Travel	c3116-51.impsat.com.co	Linux
14/04/2003	Bug-Travel	crisa.reinita.com.co	Linux
12/04/2003	uname-a	....alianzavalores.com.co	Linux
27/03/2003	DeathSymb0L	contacto.bolnet.com.co	Linux
23/02/2003	cyberlords	coltabaco.com.co	Win 2000
23/02/2003	cyberlords	conelec.com.co	Win 2000
23/02/2003	cyberlords	balmoralbulldog.com.co	Win 2000
23/02/2003	cyberlords	C2C.com.co	Win 2000
23/02/2003	cyberlords	belomatic.com.co	Win 2000
23/02/2003	cyberlords	Benedan.com.co	Win 2000
23/02/2003	cyberlords	codintex.com.co	Win 2000
23/02/2003	cyberlords	cooperenka.com.co	Win 2000
23/02/2003	cyberlords	compelect.com.co	Win 2000
22/02/2003	cyberlords	cademac.com.co	Win 2000
22/02/2003	cyberlords	bagatela.com.co	Win 2000
22/02/2003	cyberlords	altamira.com.co	Win 2000
22/02/2003	cyberlords	aquapruf.com.co	Win 2000
22/02/2003	cyberlords	clinicarosario.com.co	Win 2000
22/02/2003	cyberlords	cri.com.co	Win 2000
22/02/2003	cyberlords	corpo.com.co	Win 2000
22/02/2003	cyberlords	comercarne.com.co	Win 2000
22/02/2003	cyberlords	autoamerica.com.co	Win 2000
21/02/2003	cyberlords	...viciosdelacosta.com.co	Win 2000
21/02/2003	cyberlords	access.com.co	Win 2000
21/02/2003	cyberlords	aerovision.com.co	Win 2000
21/02/2003	cyberlords	...icentrodelprado.com.co	Win 2000
08/02/2003	CyPeRtRoN	e-learning.com.co	Win 2000
06/02/2003	nitr0x	contacto.bolnet.com.co	Linux
22/01/2003	Cyb3r Attack	country.com.co	Linux
14/01/2003	Rooting Sabotage Forced	sysentec.com.co	FreeBSD
03/01/2003	r00t_System	todoraquira.com.co	Unknown
03/01/2003	r00t_System	aldato.com.co	Unknown

1.2.2 Tabla Resumen del análisis

Después de correr las herramientas Lan Guard Network Scanner, Nmap, Super Scan y Port Scan, de resumir la información obtenida con estas herramientas se realizó la siguiente tabla que resume el análisis de la seguridad de los Sitios Web analizados. Para la construcción de esta tabla se utilizo básicamente la información obtenida a través del programa Nmap, la información sobre sistemas operativos y servidores Web que se puede obtener del sitio http://www.netcraft.com.

Se tomaron los datos recolectados en el mes de noviembre, diciembre, mayo y junio y se observo la evolución y cambios que presentaron algunos sitios Web.

También, de acuerdo al tipo de puertos abiertos que se encontraron en cada uno de los sitios se corroboraron con las listas conocidas de puertos que utilizan los troyanos. Aunque eso no afirma que el sitio Web pueda estar infectado por algún tipo de troyano si aumenta las posibilidades.

Algunos de los puertos comúnmente abiertos en varios de los sitios Web ya analizados son:

Puerto 80:
711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Seeker, WAN Remote, Web Server CT, WebDownloader

Puerto 21: Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, FreddyK, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, RTB 666, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash

Puerto 23: ADM worm, Fire HacKer, My Very Own trojan, RTB 666, Telnet Pro, Tiny Telnet Server - TTS, Truva Atl

Puerto 25: Ajan, Antigen, Barok, BSE, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Stukach, Tapiras, Terminator, WinPC, WinSpy

Dirección electrónica	Respuesta desde el Host	Dirección IP	Sistema Operativo aparente	Puertos Abiertos	Comentarios
www.virtualexito.com		200.31.19.19	FreeBSD 2.2.1 - 4.1, Windows Millennium Edition (Me), Windows 2000, o WinXP	80, 443	Sitio Web con buena seguridad, solo cuenta con dos puertos abiertos y están filtrados
www.papiros.com		130.94.243.4	Windows NT v4 o Windows 98		Todos los puertos escaneados están filtrados. Aparentemente el servidor Web es IIS 4.0.
www.laopinion.com.co		208.56.184.2	Linux Kernel 2.4.0 - 2.5.20	80, 110, 143, 443, 995, 3000, 3001, 3306,	Todos los Puertos están filtrados han cerrado 21 22 25 y otros han actualizado el linux
www.la14.com	ip-34-122.telesat.com.co	66.128.34.122	Windows NT v4 o Windows 98	25, 80, 43, 507, 522, 637, 1002, 1032, 1058, 1059, 1433, 1723, 2301, 3128, 5555, 8007, 8000	Este sitio cuenta con muchos puertos abiertos. El servicio de FTP Ha abierto recientemente, además durante el seguimiento a este sitio nunca ha mostrado mejoras en la seguridad Aparentemente el servidor Web es IIS 4.0.
Colombia.deremate.com	Paradigmcsi.com	216.25.288.80	Windows 2000		Buena seguridad, todos los puertos están filtrados. Aparentemente cuenta con Microsoft-IIS v 5.0
www.virtualtiendas.com	Bio-normalizer.com	209.15.164.247	Solaris 2.6 - 7 (SPARC)	21, 23, 25,80, 443, 1234, 3306.	Este sitio Web dedicado a la venta de tiendas virtuales tiene activado el servicio Telnet y FTP. Posibles troyanos en el puerto 1234: Sub Seven Java client y/o Ultors Trojan, aunque es probable que los troyanos no estén afectando el sitio

					gracias al sistema operativo que aparenta tener.
www.mercadodelaspulgas.net	adsl_pool_216761-58.007mundo.com	65.167.61.58		6667, 21, 25, 53, 80, 443, 5380, 1025 entre otros.	Este sitio Web a pesar de tener 21 puertos abiertos, algunos con peligro de troyanos como por ejemplo el 6667 Dark FTP, EGO, Maniac rootkit, Moses, ScheduleAgent, SubSeven, Subseven en el puerto 6667 no ha presentado mejoras durante el tiempo de seguimiento. Aparentemente utiliza IIS de Servidor Web
www.mercadolibre.com.co	www.mercadolibre.com	216.35.213.254	Unix	80 y 443	Se presento dificultad para obtener información Sitio aparentemente soportado en Oracle HTTP Server y Apache/1.3.19
Web1.compaq.com/store	vlaecwspro.zcce.compaq.com	161.114.23.250	Windows 2000	80 y 443	Servidor Web Microsoft-IIS/5.0
www.telleva.com.co		64.86.184.9	Windows NT v4 o Windows 98		Apache/1.3.12
Secure.iquiero.com/colombia/		207.22.51.88	Windows 2000/XP/ME	21, 25, 80, 81, 135, 443, 1025, 1026, 1433, 2301, 3372, 3389, 8080, 49400.	Este sitio Web esta dividido en secciones por países. Presenta posibles troyanos por el gran numero de puertos abiertos: Puerto 1025: Fraggle Rock, md5 Backdoor, NetSpy, Remote Storm Puerto 1025 (UDP) - Remote Storm
www.casamusical.com	casamusical.com	64.77.113.185	IRIX 6.5-6.5.15m	21, 80, 443, 111, 3306	A este sitio Web que aparenta estar seguro lo beneficia el sistema operativo poco utilizado.

www.tornillosypartes.com.co		216.36.252.3	Linux Kernel 2.4.0 - 2.5.20 O FreeBSD	20 21 22 25 80 443 110	Apache/1.3.27 para Unix y FrontPage/5.0.2.2623
www.willkinsonpc.com.co		200.31.19.121	Linux Kernel 2.4.0 - 2.5.20	21, 80, 8080	Aunque tiene el puerto 8080 abierto es difícil la existencia de troyanos debido a el tipo de sistema operativo
www.typicalcolombia.com/es	65-161-248-24.servdns.com	65.161.248.24	Windows XP professional	21 25 80 135 443, 8080	Posibles troyanos en el puerto 8080: Brown Orifice, Generic backdoor, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero
www.summan.com	atelopus.epm.net.co	200.13.224.105	Windows 2000.	21, 80, 443, 3306	Este sitio Web dedicado a vender tecnología cerro recientemente el puerto 3306 mysql. Aparentemente utiliza Microsoft-IIS/5.0.
www.cekit.com.co	front.netnation.com	204.174.223.36	Linux Kernel 2.4.0 - 2.5.20	21, 22, 25, 23 80, 110, 443.	Servicio Telnet activado
www.ecomerz.com.co	Rds.org.co	200.25.22.40	Linux 2.1.19 - 2.2.20,	21, 22, 25, 80, 109, 110, 443, 554	Vende artesanías, Telnet.
www.bellsouth.com.co	c3280-238.impsat.com.co	200.32.80.238	Windows 2000	80	Microsoft-IIS/5.0
www.comcel.com.co		64.239.37.21	Windows Server 2003		Microsoft-IIS/6.0
Comercio.ccb.org.co/tienda/	www.ccbvirtual.com.co	200.31.65.25	Windows XP Professional	80, 443	
www.timoteo.com		130.94.243.104	Windows Millennium Edition (Me), Win 2000, o WinXP	21, 25, 80, 110 443, 1433, 3372, 3389	Puerto 110 posible troyano ProMail
www.latiendadelasrosas.com		130.94.243.102	Windows Millennium Edition (Me), Win 2000, o WinXP	21, 25, 80, 110, 443, 1433 3372, 3389	Puerto 110 posible troyano ProMail
www.tuimportas.com		130.94.243.10	Windows Millennium	21, 25, 80,	Puerto 110 posible troyano ProMail

		0	Edition (Me), Win 2000, o WinXP	110, 443, 1433 3372, 3389	
www.cinecolombia.com.co	cineco1.att.net.co	200.14.205.51	Windows XP Profesional o Windows 2000	80, 443, 5800, 5900, 8080	Este sitio Web utiliza el software de gestión remota VNC que puede ser inseguro. Posible servidor Web Microsoft-IIS/5.0
Sun19061.dn.net/perl/		130.94.68.103			Viene de tarjetasnico.com/co. No se puede obtener mucha información. Cerro 11 puertos recientemente.
www.comprarnet.com	comprarnet.andinet.com	208.221.129.29	Windows 2000.	80 y 443	Posible servidor Web Microsoft-IIS/5.0
www.elancoraeditores.com	www.hostingred.com	200.31.19.32	Windows 2000	21, 25, 80, 110, 2048	Posible servidor Web Microsoft-IIS/5.0
www.emultired.com		200.24.70.82	Windows 2000	7, 88, 5900, 21	Sitio Web que probablemente instalo un Firewall porque cerro 31 puertos en los últimos meses. Posible servidor Web Microsoft-IIS/5.0
www.pcmadrigal.com	pcmadrigal.com	209.15.76.242	Solaris 2.6 - 7 (SPARC)	21, 23, 25, 514, 3306, 80, 110, 111, 6000 911	Servicio Telnet habilitado
www.zonavirtual.com	zonavirtual.com	209.15.10.232	Solaris 2.6 - 7 (SPARC)	21, 23, 25, 514, 3306, 80, 110, 111, 6000 911	Servicio Telnet habilitado Paso de 16 a 22 puertos abiertos. Probablemente disminuyo el nivel de seguridad.

www.geo.net.co	Web.geonetsa.com	200.69.97.16	Windows Millennium Edition (Me), Win 2000, or WinXP	21, 25, 80, 135, 139, 443 1027, 1029, 1032, 3372, 7000, 7007, 8000, 8080.	A pesar del gran numero de puertos abiertos no se observan mejoras en la seguridad de este sitio.
www.villegaseditores.com	villegaseditores.com.co	64.225.117.114			Sitio Web que probablemente instalo un Firewall porque cerro 16 puertos en los últimos meses.
www.tiendasdelcolor.com		200.13.224.100	Solaris 8	21 80 443	
www.mercomas.com		200.75.78.11	Compaq Tru64		Posible servidor Web Microsoft-IIS/5.0
www.mercomucho.com		200.75.78.11	Compaq Tru64		Posible servidor Web Microsoft-IIS/5.0

2. Identificación del problema

Se identificaron básicamente dos problemas en la seguridad de algunos sitios Web dedicados al comercio electrónico:

1. Existe un exceso de puertos abiertos innecesariamente. Se puede deducir que en muchos casos no existe un monitoreo de estos puertos.

2. Muchas de las vulnerabilidades de los sistemas de comercio electrónico están ligadas a las vulnerabilidades del sistema operativo y Servidor Web. En el caso de los muchos sitios Web que utilizan aplicaciones que demoran en ofrecer las correcciones a las vulnerabilidades descubiertas crean un problema de seguridad.

3. Existe una falencia en la seguridad causada por los usuarios de las redes por falta de conocimientos técnicos básicos.

4. Existe una falta de uso de la tecnología informática y los sistemas de pago como la tarjeta de crédito. Existen otras alternativas como la tarjeta de crédito virtual de instituciones bancarias como Bancolombia.

ANEXO C: HERRAMIENTAS SOFTWARE UTILIZADAS PARA LA EVALUACIÓN DE SEGURIDAD

La cantidad de programas o herramientas software utilizadas en seguridad computacional puede ser abrumadora. Uno de los principales problemas para mantener la seguridad en un sistema, en el caso de comercio electrónico es que existe una gran variedad de programas para atacar, indiscriminadamente puestos en Internet al alcance de cualquier persona.

Los programas más importantes y los que le dan origen a casi todo lo que aparece en Internet son los muy famosos NMAP y NETCAT. Estas dos aplicaciones pueden servir tanto como para administrar el sistema como para atacarlo.

Netcat: Este es un pequeño pero muy potente programa creado originalmente para administración de redes, fue creado por el Hobbit y hoy en día es una de las herramientas mas utilizadas tanto por los atacantes como por los administradores de redes. Netcat trabaja sobre el protocolo TCP/IP y le da a los equipos con sistema operativo Windows mayor manejo de este protocolo, ventaja que solo se podía encontrar en los sistemas operativos tipo Unix. Netcat es básicamente un manejador de puertos y conexiones que utiliza todas las ventajas y versatilidad de TCP/IP cuyo funcionamiento se basa en el uso de paquetes tipo ICMP. Netcat puede por ejemplo permitir realizar y aceptar conexiones tanto TCP como UDP desde y hacia cualquier puerto, realiza conversiones de DNS y de DNS inverso, puede leer líneas de comando de la entrada estándar, puede comportarse como un demonio Telnet.
Netcat se puede encontrar en: http://www.l0pht.com/~weld/netcat.

Nmap: Es una herramienta de exploración de red y escáner de seguridad creada por Fyodor y diseñada para permitir a administradores y usuarios de sistemas el escaneo de grandes redes para determinar que Servidores se encuentran activos y que servicios están ofreciendo. Este programa es un escáner tanto UDP como TCP.

Nmap proporciona también características avanzadas como la detección remota del sistema operativo por medio de rastros TCP/IP, escaneo tipo oculto, retraso dinámico y cálculos de retransmisión, escaneo paralelo, detección de servidores inactivos por medio de pings paralelos, escaneo con señuelos, detección de filtrado de puertos, escaneo por fragmentación y especificación flexible de destino y puerto.
Nmap puede se puede encontrar en http://www.insecure.org/nmap.
Se utilizó la versión Nmap para Windows versión 3.0

Perl: Usado como lenguaje de programación, debido a su potencia y facilidad para trabajar a nivel de scripts. Perl trabaja sobre sistema operativo Linux. Inicialmente se desarrollo un script que aprovechara la potencialidad de Netcat pero debido a la imposibilidad de automatizar el proceso de obtención de los sitios Web de Comercio Electrónico no fue necesario utilizarlo.

Lan Guard Network Sacanner: Es un escáner muy funcional con una excelente interfaz grafica que permite elegir fácilmente el objetivo a escanear. Ofrece unas muy completas funcionalidades entre las que se encuentran: Resolución DNS, Obtención de Sistema operativo, obtención y crack de carpetas compartidas cuando el sistema objetivo utiliza Windows 98, nombres de Netbios, nombres de usuarios, puertos abiertos y la más importante, expone las diferentes vulnerabilidades encontradas en el equipo objetivo de acuerdo a una clasificación según su grado afección. El LanGuard también permite generar los reportes como una página Web.
Se utilizó la versión 2.0 Beta de este programa de la empresa GFI Software Ltda., que se puede encontrar en http://www.gfisoftware.com/lannetscan/.

Sam Spade: Se utilizó la versión 2.0 de esta herramienta Freeware que funciona sobre Windows y ofrece una interfaz grafica para diversas tareas de exploración de redes. Este programa integra diversas capacidades como Traceroute, ping, búsquedas whois y transferencia de zona DNS en una clara interfaz por medio de ventanas.
La información completa y el programa para Windows se pueden obtener en http://www.samspade.org/ssw/.

Zone Alarm: Es muy importante cuando se hacen pruebas de seguridad y vulnerabilidad usar un Firewall que proteja el equipo que desde el cual se están haciendo las pruebas. Zone Alarm es un firewall personales muy popular creado por la empresa Zone Labs Inc,. Ofrece la posibilidad de gestionar que programas pueden acceder a Internet, también genera mensajes en pantalla y logs en los casos que detecta intentos de conexión al equipo, además de bloquear el acceso. Se utilizo la versión de prueba de este software que se puede encontrar en http://www.zonelabs.com/store/content/download.jsp.

Super Scan: Super Scan es un escáner de puertos TCP basado en conexiones, ofrece verificaciones por medio de pings y resuelve rangos IP. El código fuente no es accesible. Es una herramienta muy popular y usada dentro de algunas comunidades de seguridad.

PortScan: Se utilizó la herramienta Port Scan Versión 1.2 Basic codificada creada por Rhad como un escáner sencillo de puertos, principalmente para tener una opción diferente del Nmap que permitiera tener factores de comparación de los resultados de las herramientas. El Port Scan permite escanear los puertos de solo un host al tiempo pero es eficiente y veloz en sus tareas.

Limpiadores de Spyware como AD-Aware: Es importante contar con una herramienta que elimine los programas spyware, es decir aquellos que ofrecen buenas utilidades pero que abren puertos que permiten la fuga de información del equipo. Esto sobre todo porque para el proceso de evaluación de seguridad es necesario probar numerosas herramientas hasta encontrar las adecuadas y en este proceso se puede ver afectada la integridad del equipo, además obviamente del Antivirus. Se utilizó la herramienta AD-Aware versión 5.83 estándar free de la empresa Lavasoft Inc, que examina la memoria, registro, unidades de discos duros y discos flexibles en busca de programas que puedan poner en riesgo los datos del equipo. El programa AD-Aware se puede encontrar en el sitio Web http://www.lavasoftusa.com/software/adaware/.

Es importante aclarar que muchas de estas herramientas a pesar de sus excelentes características en muchas no arrojan ningún resultado debido a que no pueden romper la seguridad de los objetivos, es por esto, que se deben usar un conjunto de herramientas para obtener los mejores resultados.

ANEXO D: EL CONTRATO DE TRASPROTE EN LA LEY 527 / 99

La Ley 527/ 99 a diferencia de la Ley modelo de Comercio Electrónico elaborada en 1996 por la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil Internacional (CNUDMI), como una guía para su incorporación al derecho interno de cada uno de los países, introduce un capítulo que se refiere al Contrato de trasporte que no se encontraba en la ley modelo. Aunque ese no es el tema de estudio de este trabajo de grado si guarda relación ya sea formal por encontrarse en la misma ley, esto en virtud del principio de unidad de materia consagrado en el artículo 158 superior y también guarda una relación material con el tema del presente documento por permitir la ley 527/99 la aplicación de lo referente al comercio electrónico al Contrato de trasporte. Por lo anterior se puede pasar por alto esta parte de la Ley objeto de estudio.

Como se decía anteriormente la ley 527/ 99 establece en el literal b) del artículo 2º, que la regulación del comercio electrónico resulta aplicable a todas las modalidades de transporte tanto de pasajeros como de carga, sin embargo la segunda parte de la Ley 527 de 1999 se refiere en forma específica a las aplicaciones del comercio electrónico en materia de transporte de mercancías, que comprende igualmente las modalidades terrestre, marítima, aérea, férrea y multi-modal. Lo anterior se debe complementar con la excepción consagrada en el artículo primero de la ley que dice que su contenido no se aplicará a las obligaciones contraídas por el Estado colombiano en virtud de Convenios o Tratados internacionales; Colombia ha ratificado muchos convenios internacionales en materia de trasporte en el que podemos citar como principal el convenio de Varsovia que regula el transporte aéreo internacional de pasajeros y mercancías, por lo que se quedaría gran parte de nuestra realidad contractual por fuera del ámbito de aplicación de la Ley 527/ 99.

En el campo probatorio el billete o el boleto de pasaje en el transporte terrestre, aéreo, marítimo o férreo de pasajeros, que cumplen funciones probatorias se pueden sustituir por las diferentes modalidades de mensajes de datos, sin que se afecte la constitución, desarrollo y ejecución del contrato de transporte, dificultad que puede existir para

identificar con claridad a las diferentes partes de un contrato que se perfecciona a través de cualquiera de las modalidades de mensajes de datos.

Una critica a la inclusión del contrato de trasporte en el texto final de la Ley 527 / 99 es que se colocan trabas que impiden la unificación de legislaciones internas respecto al tema del comercio electrónico.

ANEXO E: LA INEFICACIA DE LOS DERECHOS DE AUTOR A RAIZ DE LA IMPLEMENTACION DE NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN.

A pesar de los múltiples esfuerzos por proteger los derechos de autor de la utilización de nuevas tecnologías de la información, estos se encuentran cada vez más amenazados, aun más en Colombia donde abunda la piratería de obras intelectuales, es así como existen programas de sistemas como Kazaa que permiten adquirir en pocos minutos canciones, videos, imágenes o libros.

El problema de la piratería se ha salido de las manos de las autoridades nacionales quienes no pueden revisar cada equipo computacional para verificar si almacena información pirata, lo mismo ocurre con los vendedores informales de información pirata.

La cultura de los colombianos de falta de sentido de pertenencia hacia las políticas que adopta el Estado ha permitido que se acepen y se recupere fácilmente a la adquisición por medio de Internet de toda clase de productos.

La posible solución a manera de conclusión es que las autoridades como la DIAN o en general el gobierno nacional elimine la gigantesca diferencia de precios que existe entre un producto que paga derechos de autor a uno que no lo hace, esto se podría lograr a través de políticas enfocadas a disminuir los excesivos gravámenes que presentan productos como la música y los libros, pues estos impuestos hacen que las autoridades y en si los derechos de autor pierdan aceptación por parte de la comunidad que optan por aceptar la piratería. Lo anterior debe complementarse con un estricto control sancionatorio basado en inspecciones continuas a focos de piratería para frenar la venda, suministro y compra de información pirata.

Tecnológicamente es muy difícil hacer un control por parte de las autoridades nacionales para impedir la practica de la piratería, mas sin embargo se puede bloquear o sancionar la utilización de ciertos programas de sistemas que permiten extraer información sin ningún control. Como ocurre con todo lo relacionado con Internet, se debe llevar al campo internacional y asumir políticas globalizadas pues de nada sirve prohibir la utilización de

un programa en los sitios web con dominios colombianos si se puede acceder a ellos desde otro sitio web.

La conclusión general se debe realizar una reforma legal y política acerca de los derechos de autor, pues lo que hasta el momento existe se queda en letra muerta que no logra ser realmente efectiva.

Existe una posición distinta respecto de la propiedad intelectual sobre software impulsada por la Free Software Fundation (FSF), que propone Software libre. Software libre no significa gratis, significa acceso al código fuente de los programas.
Este tipo de programas quedaran cubiertos bajo una licencia especial llamada licencia GPL.

ANEXO F: LEY NO 527 / 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:

PARTE GENERAL

CAPITULO I

Disposiciones Generales

Artículo 1. 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. 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.

Artículo 2. 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; **f) Sistema de Información**. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3. 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.

Artículo 4. 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.

Artículo 5. 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.

CAPITULO II

Aplicación de los requisitos jurídicos de los mensajes de datos

Artículo 6. 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.

Artículo 7. 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.

Artículo 8. 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; 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.

Artículo 9. 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.

Artículo 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.

Artículo 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.

Artículo 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, y 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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, o3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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; 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.

Artículo 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. 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

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

Artículo 27. Documentos de transporte. Con sujeción a lo dispuesto en el inciso tercero (3°) 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 expresado 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

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.

CAPÍTULO II

Entidades de certificación

Artículo 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. 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.

Artículo 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.

Artículo 31. Remuneración por la prestación de servicios. La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

Artículo 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; j) Llevar un registro de los certificados.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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, y 7. Por orden judicial o de entidad administrativa competente.

Artículo 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

Artículo 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.

Artículo 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

Artículo 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 auditoría 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.

Artículo 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

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

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

ANEXO G: DERECHO DE PETICIÓN ELEVADO AL ADMINISTRADOR DE LOS DOMINIOS ".CO": UNIANDES.

A raíz de la duda del artículo 91 de la ley 663 / 2000 surgió la duda de ¿Qué se debía entender por sitio web de origen colombiano?. Si se hacia referencia al país donde está registrado el dominio, o por el contrario se refiere al país donde se encuentra las instalaciones físicas? Esto con fines tributarios y fiscales.

Con la respuesta obtenida se sacaron varias conclusiones:

1. El artículo 91 de la ley 663 / 2000 Al hacer alusión a los sitios de origen colombiano se refiere a aquellos que tiene sus instalaciones físicas en el territorio nacional. Así no estén registrados en Colombia.
2. Con respecto al derecho de petición consagrado en el artículo 23 de la constitución como un derecho fundamental que tiene toda persona a elevar solicitudes respetuosas a las autoridades, se verificó satisfactoriamente que es posible su realización a través de medios electrónicos.
3. Con la reforma al código de procedimiento civil se establece la posibilidad de realizar notificaciones a través de correo electrónico economizando los gastos de correo y papelería.

Respuesta al derecho de petición:

Señor
ARCESIO BOLAÑOS ORDOÑES
fabolanos@unicauca.edu.co
ASUNTO : CONSULTA SOBRE PÁGINAS WEB DE ORIGEN COLOMBIANO – ART 91 LEY 633 DE 2000.

Estimado Señor:

En atención a su consulta formulada en ejercicio del Derecho de petición, referente al Art. 91 de la Ley 633 de 2000 (Reforma Tributaria de ese año), me permito presentarle los siguientes comentarios:

La Universidad de los Andes por delegación internacional de IANA (Internet Assigned Numbers Authority) e ICANN (Internet Corporation for Assigned Names and Number), es para Colombia la entidad encargada de la administración del dominio .co
Las asignaciones correspondientes fueron efectuadas desde 1991 por la IANA y, ratificadas en 1998 por la ICANN.
Los registros que hace la Universidad de los Andes a través de la Dirección de Tecnologías de Información (DTI), son de nivel local (ccTLD) con la partícula .co correspondiente al código local de Colombia. (com.co – edu.co – gov.co – net.co etc...).
Los registros de dominios de nivel general (gTLD) correspondientes a las partículas com – net – edu – gov – info – biz – aero - etc, son realizados por los más de ciento veinte (120) registradores de nivel general autorizados por la ICANN, que pueden ser consultados en el sitio web de esta entidad (www.icann.org).

Los nombres de dominio registrados en el nic Colombia, pueden ser consultados en https://www.nic.co, pudiendo obtener datos relativos a un nombres de dominio particular y determinar los datos correspondientes al solicitante y la fecha de aprobación del nombre de dominio.

Ahora bien, circunscribiéndonos al objeto especifico de su consulta, vale decir, que en torno a la obligación que se impone a todo pagina y sitio web de origen Colombiano de inscribirse en el registro mercantil y suministrar a la DIAN (Dirección de Impuestos y Aduanas Nacionales) la información de transacciones económicas; que efectivamente esa norma sigue vigente y no sufrió modificación alguna con la reciente reforma Tributaria aprobada en Colombia (Ley 788 de 2002, vigente desde enero de 2003).

A continuación me permito transcribir la correspondiente norma:
´´ [..] ARTÍCULO 91º. Todas las páginas Web y sitios de Internet de origen colombiano que operan en el Internet y cuya actividad económica sea de carácter comercial, financiera o de prestación de servicios, ***deberán inscribirse en el Registro Mercantil y suministrar a la Dirección de Impuestos y Aduanas Nacionales DIAN, la información de transacciones económicas (en los términos) que esta entidad (lo) requiera*** *[...].´´ (subrayado fuera de texto)*

Las expresiones anteriores que aparecen en paréntesis, fueron declaradas inexequibles por la Corte Constitucional de Colombia a través de la Sentencia C-1147 del 31 de octubre de 2001, Magistrado Ponente: Manuel José Cepeda, declarando su exequibilidad condicionada, estableciendo que la información que requiera la DIAN es la estrictamente necesaria para cumplir con sus funciones.

Uno de los puntos que más discusiones e interpretaciones ha suscitado, es el referente a establecer que es una página web de origen Colombiano, tal y como lo menciona la norma en comento. Sin embargo y como quiera que allí se menciona la inscripción en el registro mercantil, se ha entendido que tal inscripción se debe realizar en la Cámara de Comercio del lugar donde tenga su asiento principal, domicilio o residencia habitual.
De modo que pese a que el registro de nombre de dominio se encuentre en el nivel general (gTLD), o en el nivel local (ccTLD); lo que realmente es relevante para los efectos del Art. 91 ibidem.; es que la pagina web respectiva tenga su asiento principal, domicilio o residencia habitual en territorio Colombiano; pese a que el proveedor de servicio de conexión a la red (ISP), o proveedor del hosting (alojamiento) se encuentre dentro o fuera del País.

Así mismo vale mencionar los artículos 315 y 318 de la reciente reforma al Código de Procedimiento Civil Colombiano (Ley 794 del 8 de enero de 2003), estableció la obligación de suministrar e inscribir una dirección de correo electrónico que se deberá registrar por las personas jurídicas, comerciantes y personas jurídicas domiciliadas en Colombia al momento de registrarse en la Cámara de Comercio o cualquier otro registro competente; para efectos de notificaciones personales, y particularmente el tema de las notificaciones por aviso a través de Mensajes de Datos (EDI, Correo Electrónico, Internet, Fax, Telex).

El Art. 318 de la reforma procesal mencionada, establece que el Consejo Superior de la Judicatura realizara dentro del año siguiente a la vigencia de la Ley, la creación de las firmas digitales que utilizaran los secretarios de los Juzgados y Tribunales.

Finalmente, y por ser las entidades competentes para efectos de realizar la inscripción correspondiente de que trata el Art. 91 de la Ley 633 de 2000, le sugerimos que esta

misma consulta la eleve a la Superintendencia de Industria y Comercio (Cámaras de Comercio) y la Dirección de Impuestos y Aduanas Nacionales (DIAN).

Cordialmente,

WILSON RAFAEL RÍOS RUIZ
Abogado Dirección Jurídica
Universidad de los Andes

ANEXO H: ARTÍCULOS REFERENCIADOS DEL CODIGO PENAL

CODIGO PENAL COLOMBIANO

LIBRO SEGUNDO

TITULO III

DELITOS CONTRA LA LIBERTAD INDIVIDUAL Y OTRAS GARANTIAS

CAPITULO SÉPTIMO

DE LA VIOLACIÓN A LA INTIMIDAD, RESERVA E INTERCEPTACION DE COMUNICACIONES.

ARTÍCULO 192 - Violación ilícita de comunicaciones. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.
Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

ARTÍCULO 193 - Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

ARTÍCULO 194 - Divulgación y empleo de documentos reservados. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

ARTÍCULO 195- Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

ARTÍCULO 196 – Violación ilícita de comunicaciones o correspondencia de carácter oficial. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.

La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado.

ARTÍCULO 197. Utilización ilícita de equipos transmisores o receptores. El que con fines ilícitos posea o haga uso de aparatos de radiofonía o televisión, o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de uno (1) a tres (3) años.

La pena se aumentará de una tercera parte a la mitad cuando la conducta descrita en el inciso anterior se realice con fines terroristas.

ANEXO I: LEY ESPAÑOLA HOMOLOGA A LA LEY 527 / 99

REAL DECRETO LEY 14/1999, DE ESPAÑA, SOBRE FIRMA ELECTRÓNICA

TITULO PRIMERO

Disposiciones generales

CAPITULO UNICO

Disposiciones generales

Artículo 1. Ámbito de aplicación.

1. Este Real Decreto-ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. Definiciones.

A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:

a) "Firma electrónica": Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

b) "Firma electrónica avanzada": Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

c) "Signatario": Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

d) "Datos de creación de firma": Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica.

e) "Dispositivo de creación de firma": Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma.

f) "Dispositivo seguro de creación de firma": Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

g) "Datos de verificación de firma": Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

h) "Dispositivo de verificación de firma": Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma.

i) "Certificado": Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

j) "Certificado reconocido": Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

k) "Prestador de servicios de certificación": Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

l) "Producto de firma electrónica": Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

ll) "Acreditación voluntaria del prestador de servicios de certificación": Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Artículo 3. Efectos jurídicos de la firma electrónica.

1. La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que

se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21.

2. A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

TITULO II

La prestación de servicios de certificación

CAPITULO PRIMERO

Principios generales

Artículo 4. Régimen de libre competencia.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea.

2. La prestación de los servicios de certificación por las Administraciones o los organismos o sociedades de ellas dependientes se realizará con la debida separación de cuentas y con arreglo a los principios de objetividad, transparencia y no discriminación.

Artículo 5. Empleo de la firma electrónica por las Administraciones públicas.

1. Se podrá supeditar por la normativa estatal o, en su caso, autonómica el uso de la firma electrónica en el seno de las Administraciones públicas y sus entes públicos y en las relaciones que con cualesquiera de ellos mantengan los particulares, a las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento.

Las condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora, respecto de los documentos electrónicos integrados en un expediente administrativo. El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica a las que se refiere este apartado sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y se dictarán a propuesta del

Ministerio de Administraciones Públicas y previo informe del Consejo Superior de Informática.

2. Las condiciones adicionales a las que se refiere el apartado anterior deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o extranjeras.

3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

Artículo 6. Sistemas de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica.

1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios.

2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones; en la Ley 21/1992, de 16 de julio, de Industria, y en la demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1 establecerá las condiciones que permitan coordinar los sistemas de certificación.

3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen.

4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que

se haya pedido certificación. También tomarán en cuenta el cumplimiento, por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado.

5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

Artículo 7. Registro de Prestadores de Servicios de Certificación.

1. Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España.

Su regulación se desarrollará por Real Decreto.

2. La solicitud de inscripción habrá de formularse, aportando la documentación que se establezca reglamentariamente, a efectos de la identificación del prestador de servicios de certificación y de justificar que éste reúne los requisitos necesarios, en cada caso, para ejercer su actividad. También será objeto de inscripción ulterior cualquier circunstancia relevante, a efectos de este Real Decreto-ley, relativa al prestador de servicios de certificación, como su acreditación o estar en condiciones de expedir certificados reconocidos.

La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente.

3. El Registro de Prestadores de Servicios de Certificación será público y deberá mantener permanentemente actualizada y a disposición de cualquier persona una relación de los inscritos, en la que figurarán su nombre o razón social, la dirección de su página en Internet o de correo electrónico, los datos de verificación de su firma electrónica y, en su caso, su condición de acreditado o de tener la posibilidad de expedir certificados reconocidos. En la citada relación figurarán, también, cualesquiera otros datos complementarios que se determinen por Real Decreto.

Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral. El suministro de esta información podrá sujetarse alpago de una tasa, cuyos elementos esenciales se determinarán por ley.

CAPITULO II

Certificados

Artículo 8. Requisitos para la existencia de un certificado reconocido.

1. Los certificados reconocidos, definidos en el artículo 2 j) de este Real Decreto-ley, tendrán el siguiente contenido: a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.

h) El comienzo y el fin del período de validez del certificado.

i) Los límites de uso del certificado, si se prevén.

j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Artículo 9. Vigencia de los certificados.

1. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias: a) Expiración del período de validez del certificado.

Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.

c) Pérdida o inutilización por daños del soporte del certificado.

d) Utilización indebida por un tercero.

e) Resolución judicial o administrativa que lo ordene.

f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.

g) Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.

h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

2. La pérdida de eficacia de los certificados, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado surtirá efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11.e).

3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación. Corresponderá al prestador de servicios la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

4. El prestador de servicios de certificación podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores.

Artículo 10. Equivalencia de certificados.

Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste,

expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumplan alguna de las siguientes condiciones:

a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.

b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.

c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPITULO III

Condiciones exigibles a los prestadores de servicios de certificación

Artículo 11. Obligaciones de los prestadores de servicios de certificación.

Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones: a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación, los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.

b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.

c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.

d) Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.

e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o perdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.

f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el apartado 1 del artículo 13, a los titulares de los certificados por ellos emitidos y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

Artículo 12. Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

a) Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

b) Demostrar la fiabilidad necesaria de sus servicios.

c) Garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.

d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

f) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.

g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.

Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación.

Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.

h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.

i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información, deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible.

Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.

j) Utilizar sistemas fiables para almacenar certificados, de modo tal que: 1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas.

2. Unicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.

3. Pueda comprobarse la autenticidad de la información.

4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

Artículo 13. Cese de la actividad.

1. El prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos y transferir, con su

consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

2. Si el prestador de servicios estuviere inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar a éste, con la antelación indicada en el anterior apartado, el cese de su actividad, y el destino que vaya a dar a los certificados especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto. Igualmente, indicará cualquier otra circunstancia relevante, que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de un procedimiento de quiebra o suspensión de pagos respecto de él.

3. La inscripción del prestador de servicios de certificación en el Registro de Prestadores de Servicios de Certificación será cancelada, de oficio, por el Ministerio de Justicia, cuando aquél cese en su actividad. El Ministerio de Justicia se hará cargo de la información relativa a los certificados que se hubieren dejado sin efecto por el prestador de servicios de certificación, a efectos de lo previsto en el artículo 12.h).

Artículo 14. Responsabilidad de los prestadores de servicios de certificación.

1. 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.

2. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

3. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extra contractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.

4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Artículo 15. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación al que se refiere este Real Decreto-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre.

Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

En todo caso, se estará a lo previsto en las normas sobre protección de datos indicadas en el apartado 1 de este artículo.

CAPITULO IV

Inspección y control de la actividad de los prestadores de servicios de certificación

Artículo 16. Supervisión y control.

1. El Ministerio de Fomento controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en este Real

Decreto-ley y en sus disposiciones de desarrollo. Asimismo, vigilará el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones establecidas en el artículo 11.

2. En el ejercicio de su actividad de control, la Secretaría General de Comunicaciones actuará de oficio, mediante petición razonada del Ministerio de Justicia o de otros órganos administrativos o a instancia de persona interesada. Los funcionarios de la Secretaría General de Comunicaciones adscritos a la Inspección de las Telecomunicaciones, a efectos de cumplir las tareas de control, tendrán la consideración de autoridad pública.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, de lo dispuesto en el artículo 11.c), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Esta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador, con arreglo a la legislación que regula su actividad.

Artículo 17. Deber de colaboración.

Los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría General de Comunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, referida siempre a datos que conciernan al prestador de servicios.

Artículo 18. Resoluciones del órgano de supervisión.

La Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan este Real Decreto-ley y sus disposiciones de desarrollo.

TITULO III

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

CAPITULO UNICO

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

Artículo 19. Dispositivos seguros de creación de firma electrónica.

A efectos del artículo 2 f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige: 1.º Que garantice que los datos utilizados para la

generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2.º Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3.º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4.º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Artículo 20. Normas técnicas.

1. Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de las Comunidades Europeas" son conformes con lo previsto en la letra e) del artículo 12 y en el artículo 19.

2. Sin perjuicio de esta presunción, los números de referencia de esas normas se publicarán en el "Boletín Oficial del Estado".

Artículo 21. Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica.

1. Los órganos de certificación a los que se refiere el artículo 6 podrán certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de evaluación acreditadas.

En la evaluación del cumplimiento de los requisitos previstos en el artículo 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el artículo anterior u otras que determinen los órganos de acreditación y de certificación, y cuyas referencias se publiquen en el "Boletín Oficial del Estado".

2. Se reconocerá eficacia a los certificados sobre dispositivos seguros de creación de firma que hayan sido expedidos por los organismos designados para ello por los Estados miembros de la Unión Europea, cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.

Artículo 22. Dispositivos de verificación de firma.

1. Los dispositivos de verificación de firma electrónica avanzada deben garantizar lo siguiente: 1. Que la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente.

2. Que el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

3. Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo.

4. Que se verifica de forma fiable el certificado.

5. Que puede detectarse cualquier cambio relativo a su seguridad.

2. El Real Decreto al que se refiere el artículo 6 podrá establecer los términos en los que las entidades de evaluación y los órganos de certificación podrán evaluar y certificar, respectivamente, el cumplimiento, por los dispositivos de verificación de firma electrónica avanzada, de los requisitos establecidos en este artículo.

TITULO IV

Tasa por el reconocimiento de acreditaciones y certificaciones

CAPITULO UNICO

Tasa por el reconocimiento de acreditaciones y certificaciones

Artículo 23. Régimen aplicable a la tasa.

1. La gestión precisa para el reconocimiento de las acreditaciones y de las certificaciones con arreglo a los artículos 6, 21 y 22, por los órganos públicos competentes, se grava con una tasa, a la que se aplicará el siguiente régimen: a) Constituye el hecho imponible el reconocimiento por dichos órganos de la acreditación de los prestadores de servicios o de la certificación de los dispositivos de creación o de verificación de firma a que se refieren los artículos 6, 21 y 22.

b) Es sujeto pasivo la persona natural o jurídica que se beneficie del reconocimiento de la correspondiente acreditación o certificación.

c) Su cuota es de 47.500 pesetas (285,48 euros) por cada acreditación o certificación reconocida. Esta cantidad podrá ser actualizada por Real Decreto.

d) Se devengará cuando se presente la solicitud de reconocimiento de la correspondiente acreditación o certificación.

2. La forma de liquidación de la tasa se establecerá reglamentariamente.

TITULO V

Infracciones y sanciones

CAPITULO UNICO

Infracciones y sanciones

Artículo 24. Clasificación de las infracciones.

Las infracciones de las normas reguladoras de la firma electrónica y los servicios de certificación se clasifican en muy graves, graves y leves.

Artículo 25. Infracciones.

1. Son infracciones muy graves: a) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h).

b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones impuestas en las letras c) a la j) del artículo 12, siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.

c) El incumplimiento grave y reiterado por los prestadores de servicios de certificación de las resoluciones dictadas por la Secretaría General de Comunicaciones, para asegurar el respeto a este Real Decreto-ley.

2. Son infracciones graves: a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones impuestas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h), siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.

b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones previstas en las letras a), b), y k) del artículo 12.

c) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones contempladas en las letras c) a la j) del artículo 12, cuando no concurran las circunstancias previstas en el apartado 1.b) de este artículo.

d) La falta de comunicación por el prestador de servicios de certificación al Ministerio de Justicia, en los plazos previstos en el artículo 13, del cese de su actividad o de la iniciación, respecto de él, de un procedimiento de suspensión de pagos o de quiebra.

e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo, con arreglo a este Real Decreto-ley.

f) El incumplimiento de las resoluciones dictadas por la Secretaría General de Comunicaciones para asegurar que el prestador de servicios de certificación se ajuste a este Real Decreto-ley, cuando no deba considerarse como infracción muy grave, conforme al apartado 1.c) de este artículo.

3. Son infracciones leves: a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, excepto la c), cuando no deba considerarse como infracción grave, de acuerdo con lo previsto en el apartado 2 a) de este artículo.

b) La expedición de certificados reconocidos que incumplan alguno de los requisitos establecidos en el artículo 8.

c) No facilitar los datos requeridos, en el ámbito de sus respectivas funciones, por el Ministerio de Justicia o la Secretaría General de Comunicaciones para comprobar el cumplimiento de este Real Decreto-ley por los prestadores de servicios de certificación.

d) Cualquier otro incumplimiento de las obligaciones impuestas a los prestadores de servicios de certificación por este Real Decreto-ley, salvo el de la recogida en el artículo 11.c) o que deba ser considerado como infracción grave o muy grave, de acuerdo con lo dispuesto en los apartados anteriores.

Artículo 26. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones: a) Por la comisión de infracciones muy graves, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 1 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 5 por

100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 100.000.000 de pesetas (601.012,10 euros).

La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

Cuando la resolución de imposición de esta sanción sea firme, será comunicada al Registro de Prestadores de Servicios de Certificación para que cancele la inscripción del prestador de servicios sancionado.

b) Por la comisión de infracciones graves, se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 0,5 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 2 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 50.000.000 de pesetas (300.506,04 euros).

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 euros).

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional, una vez que aquélla tenga carácter firme.

3. La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, lo siguiente: a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El daño causado, siempre que no haya sido tomado en consideración para calificar la infracción como leve, grave o muy grave.

d) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

4. Se anotarán en el Registro de Prestadores de Servicios de Certificación las sanciones impuestas por resolución firme a éstos por la comisión de cualquier infracción grave o muy grave. Las notas relativas a las sanciones se cancelarán una vez transcurridos los

plazos de prescripción de las sanciones administrativas previstos en la Ley reguladora del procedimiento administrativo común.

5. Las cuantías señaladas en este artículo serán actualizadas periódicamente por el Gobierno, mediante Real Decreto, teniendo en cuenta la variación de los índices de precios al consumo.

Artículo 27. Medidas cautelares.

En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte. Estas medidas podrán consistir en la orden de cese temporal de la actividad del prestador de servicios de certificación, en la suspensión de la vigencia de los certificados por él expedidos o en la adopción de otras cautelas que se estimen precisas. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

Artículo 28. Procedimiento sancionador.

1. El ejercicio de la potestad sancionadora atribuida por este Real Decreto-ley corresponde a la Secretaría General de Comunicaciones del Ministerio de Fomento. Para ello, la Secretaría General de Comunicaciones se sujetará al procedimiento aplicable, con carácter general, al ejercicio de la potestad sancionadora por las Administraciones públicas.

2. El Ministerio de Justicia y los demás órganos que ejercen competencias con arreglo a este Real Decreto-ley y sus normas de desarrollo podrán instar la incoación de un procedimiento sancionador, mediante petición razonada dirigida a la Secretaría General de Comunicaciones

DISPOSICION ADICIONAL UNICA

Posibilidad de emisión por las entidades públicas de radiodifusión de una Comunidad Autónoma en el territorio de otras con las que aquélla tenga espacios radioeléctricos colindantes.

Las entidades autonómicas habilitadas, con arreglo a la Ley, para prestar el servicio de radiodifusión digital terrenal, podrán emitir en el territorio de otras Comunidades Autónomas con las que aquélla tenga espacios radioeléctricos colindantes. Para ello, será preciso que exista acuerdo entre las Comunidades Autónomas afectadas y que, en cada

territorio, se empleen los bloques de frecuencias planificados en el Plan Técnico Nacional de Radiodifusión Sonora Digital Terrenal, para el ámbito autonómico.

DISPOSICION TRANSITORIA UNICA

Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de este Real Decreto-ley.

Los prestadores de servicios de certificación ya establecidos en España y cuya actividad se rija por una normativa específica habrán de adaptarse a este Real Decreto-ley en el plazo de un año desde su entrada en vigor.

No obstante conservarán su validez los certificados ya expedidos que hayan surtido efectos.

DISPOSICIONES FINALES

Primera. Fundamento constitucional.

Este Real Decreto-ley se dicta al amparo del artículo 149.1.8.ª, 18.ª y 21.ª de la Constitución, que atribuye competencia exclusiva al Estado en materia de legislación civil, de bases del régimen jurídico de las Administraciones Públicas y de telecomunicaciones.

Segunda. Habilitación al Gobierno.

Se habilita al Gobierno para desarrollar, mediante Reglamento, lo previsto en este Real Decreto-ley.

Tercera. Entrada en vigor.

El presente Real Decreto-ley entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

ANEXO J: LEY ARGENTINA HOMOLOGA A LA LEY 527/99

FIRMA DIGITAL

Ley 25.506

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

LEY DE FIRMA DIGITAL

CAPITULO I

Consideraciones generales

ARTÍCULO 1º — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTÍCULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTÍCULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTÍCULO 4º — Exclusiones. Las disposiciones de esta ley no son aplicables:

A las disposiciones por causa de muerte;

A los actos jurídicos del derecho de familia;

A los actos personalísimos en general;

A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTÍCULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTÍCULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTÍCULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTÍCULO 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTÍCULO 9º — Validez. Una firma digital es válida si cumple con los siguientes requisitos:

Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTÍCULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTÍCULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTÍCULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos

digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II

De los certificados digitales

ARTÍCULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTÍCULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

Ser emitidos por un certificador licenciado por el ente licenciante;

Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan

Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

Ser susceptible de verificación respecto de su estado de revocación;

Diferenciar claramente la información verificada de la no verificada incluidas en el certificado

Contemplar la información necesaria para la verificación de la firma;

Identificar la política de certificación bajo la cual fue emitido.

ARTÍCULO 15. — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTÍCULO 16**.** — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III

Del certificador licenciado

ARTÍCULO 17. — Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

ARTÍCULO 18. — Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTÍCULO 19. — Funciones. El certificador licenciado tiene las siguientes funciones:

Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

Identificar inequívocamente los certificados digitales emitidos;

Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

A solicitud del titular del certificado digital.

Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

Por condiciones especiales definidas en su política de certificación.

Por resolución judicial o de la autoridad de aplicación.

Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTÍCULO 20. — Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTÍCULO 21. — Obligaciones. Son obligaciones del certificador licenciado:

Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

Mantener la confidencialidad de toda información que no figure en el certificado digital;

Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e interrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de

aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;

Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

Constituir domicilio legal en la República Argentina;

Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

ARTÍCULO 22. — Cese del certificador. El certificador licenciado cesa en tal calidad:

Por decisión unilateral comunicada al ente licenciante;

Por cancelación de su personería jurídica;

Por cancelación de su licencia dispuesta por el ente licenciante.

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTÍCULO 23. — Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

Para alguna finalidad diferente a los fines para los cuales fue extendido;

Para operaciones que superen el valor máximo autorizado cuando corresponda;

Una vez revocado.

CAPITULO IV
Del titular de un certificado digital

ARTÍCULO 24. — Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;

A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTÍCULO 25. — Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

Utilizar un dispositivo de creación de firma digital técnicamente confiable;

Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V

De la organización institucional

ARTÍCULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTÍCULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTÍCULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

CAPITULO VI

De la autoridad de aplicación

ARTÍCULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

ARTÍCULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:

Dictar las normas reglamentarias y de aplicación de la presente;

Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;

Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;

Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;

Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;

Determinar los niveles de licenciamiento;

Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;

Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;

Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

Aplicar las sanciones previstas en la presente ley.

ARTÍCULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;

Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;

Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;

Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTÍCULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII

Del sistema de auditoría

ARTÍCULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTÍCULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII
De la Comisión Asesora para la Infraestructura de Firma Digital

ARTÍCULO 35.— Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

ARTÍCULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

Estándares tecnológicos;

Sistema de registro de toda la información relativa a la emisión de certificados digitales;

Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

Metodología y requerimiento del resguardo físico de la información;

Otros que le sean requeridos por la autoridad de aplicación.

CAPITULO IX

Responsabilidad

ARTÍCULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

ARTÍCULO 38. — Responsabilidad de los certificadores licenciados ante terceros.

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

ARTÍCULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;

Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X

Sanciones

ARTÍCULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTÍCULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones: Apercibimiento; Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000); Caducidad de la licencia. Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTÍCULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos: Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado; No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones; Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTÍCULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos: Incumplimiento de las obligaciones previstas en el artículo 21; Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación; Omisión de llevar el registro de los certificados expedidos; Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere; Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante; Incumplimiento de las normas dictadas por la autoridad de aplicación; Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTÍCULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de: no tomar los debidos recaudos de seguridad en los servicios de certificación; Expedición de certificados falsos; Transferencia no autorizada o fraude en la titularidad de la licencia; Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa; Quiebra del titular. La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTÍCULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente. La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTÍCULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

CAPITULO XI

Disposiciones Complementarias

ARTÍCULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTÍCULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

ARTÍCULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTÍCULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTÍCULO 51. — Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTÍCULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTÍCULO 53. — Comuníquese al Poder Ejecutivo.

Dada en la sala de sesiones del Congreso argentino, en Buenos Aires, a los catorce días del mes de noviembre del año dos mil uno.