Indicaciones

PROYECTO DE LEY CHILENO SOBRE FIRMAS Y DOCUMENTOS ELECTRÓNICOS BOLETÍN Nº 2571-19

Documento Público (Versión 1)

Acepta.com S.A.

Agosto 2001

Contacto: Roberto Opazo Gazmuri
Gerente General de Acepta.com
roberto@opazo.cl

Paseo Bulnes 241, piso 5, Santiago, Chile.
Fono: (56 2) 496 8100 Fax: (56 2) 496 8130
www.acepta.com
info@acepta.com

RESUMEN EJECUTIVO

El objetivo de este documento es entregar un aporte crítico y constructivo al proyecto de ley de firma electrónica que en este momento se discute en el honorable Senado de Chile. Las ideas se han organizado en 3 grandes capítulos: "Introducción", contiene una descripción del estado actual del proyecto y un marco de apoyo que permite abordar temas técnicos sin ser un experto en esta tecnología; "Observaciones Generales", describe en térmicos de su contenido las observaciones de los puntos que se deben defender y los que se deben mejorar; y finalmente "Indicaciones", muestra en forma ordenada el estado actual de cada cláusula y las indicaciones propuestas, junto con una breve justificación para cada una.

Las propuestas presentadas apuntan a mejorar los siguientes puntos generales:

- **Rigor conceptual**: El proyecto confunde insistentemente la certificación de una firma electrónica con la certificación electrónica de una identidad, a partir de la cual es posible generar electrónicamente una firma factible de ser validada. Esto hace que sea urgente modificar varias cláusulas e incluso el título de la ley.
- **Diferencias entre públicos y privados**: La confusión mencionada en el punto anterior lleva a establecer distintos mecanismos de certificación de funcionarios públicos y el resto de los chilenos. Esto es un error ya que la forma en que se certifica la identidad de una persona no implica de manera alguna regulación sobre las atribuciones de esa persona y además, es contrario al espíritu de la ley en cuanto a homologar el valor de una firma electrónica con el de una manuscrita. Finalmente, esto lleva a la pre-acreditación de cualquier ministro de fe del estado, lo que omite todos los requisitos tecnológicos, de procedimientos y de interoperabilidad que llevan a recomendar la acreditación ante un órgano acreditador.
- **Sistema de acreditación**: La definición actual de la ley respalda un sistema de acreditación abierto, lo que pone en peligro la compatibilidad internacional de los mecanismos de certificación electrónica de identidad en Chile y la libertad económica de los usuarios y certificadores.
- **Otros puntos**: También se hace referencia a otros puntos como la definición del tipo de certificados que esta ley regula, de Autoridades de Registro, la venta de software con capacidades de firma electrónica, el respaldo de información del archivo nacional y la delimitación de responsabilidades.

ÍNDICE

1.- INTRODUCCIÓN

En este momento el Honorable Senado de la República de Chile discute un visionario proyecto de ley sobre firma electrónica, impulsado por el Poder Ejecutivo de Chile y ya aprobado por la Cámara de Diputados. A partir de este proyecto se espera dar un importante desarrollo al comercio electrónico en Chile.

Sin embargo, aun cuando la intención del proyecto y el momento de su propuesta son idóneos, el tema abordado es tecnológicamente desconocido para la mayoría de los profesionales que deben participar en su redacción. De hecho, las empresas privadas que se encuentran operando en Chile, exceptuando a Acepta.com que desarrolló localmente la tecnología ocupada de acuerdo a estándares internacionales, son sólo representantes de tecnologías extranjeras que ellos no desarrollaron. En consecuencia, los expertos consultados tampoco han tenido la capacidad de orientar adecuadamente la redacción de la ley para que esta sea tecnológica y comercialmente aplicable en Chile.

Este informe ha sido preparado en armonía con los criterios definidos por el Grupo de Trabajo sobre Comercio Electrónico de las naciones unidas (UNCITRAL), integrado por los siguientes **Estados miembros** del Grupo de Trabajo: Alemania, Argentina, Australia, Austria, Brasil, Camerún, China, Colombia, Egipto, España, Estados Unidos de América, Federación de Rusia, Francia, Honduras, Hungría, India, Irán (República Islámica del), Italia, Japón, México, Nigeria, Reino Unido de Gran Bretaña e Irlanda del Norte, Rumania, Singapur y Tailandia. Además, asisten **observadores** de los siguientes Estados: Arabia Saudita, Bélgica, Canadá, Costa Rica, Cuba, Ecuador, Eslovaquia, Guatemala, Indonesia, Irlanda, Jordania, Líbano, Malasia, Malta, Marruecos, Nueva Zelandia, Países Bajos, Perú, Polonia, Portugal, República Checa, República de Corea, Suecia, Suiza, Túnez, Turquía, Ucrania, Uruguay y Yemen. Y asisten observadores de las siguientes **organizaciones internacionales**: Comisión Económica para Europa de las Naciones Unidas, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), Banco Mundial, Banco Africano de Desarrollo (BAD), Secretaría del Commonwealth, Comisión Europea, Agencia Espacial Europea (ESA), Organización de Cooperación y Desarrollo Económicos (OCDE), Centro Regional de Arbitraje Mercantil Internacional de El Cairo, *European Law Students' Association* (ELSA), Asociación Internacional de Puertos (APH), Asociación Internacional de Abogados, Cámara de Comercio Internacional (CCI), y *Union internationale du notariat latin* (UINL). Como puede apreciarse, Chile no ha tenido ninguna participación en esta importantísima instancia mundial de discusión sobre el uso de la firma electrónica.

En el Informe de este grupo, acerca del 38º período de sesiones, se sugirió que se debería expresar más enérgicamente la idea de que "para lograr un grado

satisfactorio de armonización y certeza se recomienda que los Estados hagan el menor número posible de modificaciones al incorporar la nueva Ley Modelo a su derecho interno".

La propiedad intelectual de las indicaciones aquí propuestas no pertenece a Acepta.com, ya que se han considerado los valiosos aportes de la UNCITRAL, el abogado don Renato Jijena, la comisión de trabajo de la SOFOFA para mejorar esta ley, las consideraciones del Honorable Senador don José Antonio Viera-Gallo y su equipo de asesores y las leyes de otros países, entre muchas otras fuentes. Se ha tomado como base el proyecto actual y buscado mejorarlo por la vía de indicaciones y no un reemplazo del proyecto.

La recopilación, filtro y aportes propios han sido realizados con el único fin de realizar un profundo aporte al país mejorando este proyecto. No se han tomado en cuenta intereses personales, ni políticos; no se ha buscado eliminar temas importantes para acelerar el trámite, ni se ha sacrificado contenido para evitar herir susceptibilidades; tampoco se ha buscado elegir los temas más importantes para evitar confundir a los legisladores; sólo se ha pensado en mejorar el proyecto.

Por lo tanto, este informe puede ser reproducido en forma total o parcial sin previa autorización y sin obligación de citar la fuente. En particular, las indicaciones propuestas pueden ser aprovechadas por cualquier persona o grupo.

Estas indicaciones representan lo que Acepta.com considera sería un proyecto idóneo para el país, dado el estado actual de la tecnología y de los temas tratados en profundidad por el proyecto.

Aun cuando el problema que se busca resolver es de fácil comprensión, las soluciones que se deben poner en marcha, de acuerdo al estado del arte en Internet, involucran una serie de conceptos relacionados con criptografía, matemática discreta y comunicaciones electrónicas, los que por su naturaleza altamente especializada, no son plenamente comprendidos por quienes analizan y recomiendan sobre estas materias. Esta situación lleva a la necesidad de utilizar analogías que permitan pensar y entender conceptos abstractos, basándose en lo que los legisladores comprenden y conocen.

Lamentablemente, las analogías comúnmente utilizadas no son rigurosas en su equivalencia con la firma electrónica, lo que lleva a afirmaciones completamente herradas que pueden fácilmente transformar esta ley en letra muerta. Así por ejemplo, debemos decir que un Prestador de Servicios de Certificación no es análogo a una notaría; una firma electrónica avanzada no funciona como si se usara un lápiz pasta en vez de uno a mina y otras simplificaciones utilizadas tampoco logran establecer una equivalencia que realmente permita entender y por lo tanto legislar adecuadamente sobre la materia.

En las siguientes líneas de explica una analogía rigurosamente construida con el objeto de ayudar a personas que no tienen los conocimientos matemáticos de criptografía requeridos. Esta analogía debería permitir que distintos actores relevantes en la definición de esta ley (senadores, diputados, ministros, asesores, representantes de empresas privadas, entre otros) puedan desarrollar una opinión bien fundamentada sobre cada uno de los puntos tratados.

1.1.- Analogía con el mundo físico

La siguiente tabla muestra una comparación estableciendo relaciones de equivalencia respecto del funcionamiento de la firma manuscrita en comparación con la firma electrónica.

Esta comparación está construida sin comprometer a la firma electrónica con una tecnología en particular, respetando así uno de los principios que inspiran este proyecto de ley. En su lugar se han utilizado las propiedades que la firma electrónica requiere para tener valor probatorio. De esta forma se evita explicar la criptografía asimétrica, la cual agrupa una serie de métodos matemáticos que pueden utilizarse para implementar firmas electrónicas. Toda la infraestructura requerida para implementar la firma electrónica basándose en criptografía asimétrica o criptografía de llaves públicas es denominada PKI por su sigla en inglés Public Key Infrastructure. Se incluyen notas al pie de página con referencia a los elementos de la tecnología PKI que se están abstrayendo, a fin de permitir una validación de la analogía por parte de asesores especializados, pero no con la intención de explicar los métodos criptográficos. En general se recomienda leer el capítulo haciendo caso omiso de las notas al pie.

	Firma Manuscrita	Firma Electrónica
Lo firmado	Una persona puede firmar un documento escrito sobre papel usando un lápiz pasta.	Una persona puede firmar un correo electrónico usando mecanismos que puede mantener bajo su exclusivo control [1].
El soporte	Una persona puede usar una firma manuscrita en otros soportes físicos distintos al papel, como la madera, piedra y metales entre otros, así como puede utilizar elementos distintos de un lápiz pasta para dibujar la firma.	Una persona puede firmar un documento electrónico usando distintos medios de almacenamiento, protocolos, formatos y medios de transmisión, como por ejemplo e-mail, documentos Word, páginas Web y otros.

[1] Usando PKI, el mecanismo citado es una llave privada (un número secreto), la cual puede estar protegida en diferentes medios: Disco duro, tarjeta inteligente, llavero y otros.

	Firma Manuscrita	Firma Electrónica
La firma	El receptor de un documento firmado con una firma manuscrita puede validar a simple vista que la firma efectivamente fue colocada sobre el papel del documento. En rigor la firma podría haberse colocado en el papel antes que el texto, o el texto podría haberse complementado sin que el receptor tenga forma de notar el engaño.	El receptor de un documento electrónico puede validar que el documento tiene una firma electrónica y puede detectar si el contenido del documento ha variado desde que se generó la firma electrónica[2]. En este aspecto las firmas electrónicas son más seguras que las firmas manuscritas.
El certificado	El receptor del documento firmado no puede estar seguro de la persona a la que corresponde la firma a menos que vea un carné emitido por una organización de confianza en la que se establezca la relación entre el nombre o Rut del firmante y su firma manuscrita. Este carné es un certificado físico de la identidad de una persona. Normalmente se utiliza la cédula emitida por el Servicio de Registro Civil e Identificación (SRCEI).	El receptor del documento firmado electrónicamente no puede estar seguro de la identidad del firmante a menos que cuente con un certificado electrónico de identidad, a partir del cual pueda obtener acceso a los mecanismos públicos[3] requeridos para validar la firma electrónica generada a partir de los mecanismos que la persona certificada puede mantener bajo su exclusivo control.
PSC	Las personas pueden obtener certificados físicos de identidad emitidos por distintas instituciones, por ejemplo la licencia de conductor, su tarjeta de crédito, un carné de club social, un carné de club de videos y muchos otros, todas estas organizaciones de alguna forma están dando fe pública sobre la identidad de la persona.	Las personas pueden obtener certificados electrónicos de identidad emitidos por diferentes Prestadores de Servicios de Certificación, los cuales dan fe pública sobre la identidad de la persona, proveen de la tecnología necesaria para crear y validar certificados electrónicos, publican y cumplen prácticas de certificación y ofrecen servicios para que las personas puedan revocar la vigencia de sus certificados electrónicos.

[2] Usando PKI, para hacer esta validación se requiere conocer la llave pública que le corresponde a la llave privada con que se generó la firma. Además, debe saber el método usado para firmar (formatos de archivos, función de hashing, algoritmo de encriptamiento asimétrico).

[3] En PKI, el certificado contiene información que identifica a la persona certificada y una llave pública (número público) con la que se pueden validar todas las firmas electrónicas generadas con la llave privada que le corresponde a dicha llave pública.

	Firma Manuscrita	Firma Electrónica
PSR	En la lógica de los carnés de identidad, no existe un equivalente claro para diferenciar a un Prestador de Servicios de Certificación de un Prestador de Servicios de Registro porque normalmente las 2 funciones son desempeñadas por la misma organización, pero la diferencia se puede entender con la siguiente analogía de otro ámbito: Cuando una persona necesita un examen clínico, puede ir a una Unidad de Toma de Muestra (UTM), en donde por ejemplo, se extrae la sangre necesaria para el examen y se almacena en tubo especial. Luego esta muestra es enviada a un laboratorio, en el que se utilizan equipos biomédicos y otras tecnologías para realizar el examen y preparar un informe. En este caso la UTM actúa como PSR porque valida presencialmente la información relevante del solicitante y el laboratorio actual como PSC porque provee de la tecnología, supervisa a la UTM, cumple un procedimiento y emite un certificado.	El Prestador de Servicios de Registro se encarga de validar presencialmente al solicitante de un certificado electrónico de identidad. Actúa coordinadamente con un Prestador de Servicios de Certificación para completar el proceso con todas las características señaladas en el punto anterior.
La confianza	Quien recibe un documento firmado en forma manuscrita puede libremente tomar la decisión de confiar en un carné distinto del emitido por el Servicio de Registro Civil e Identificación sin que una ley tenga que autorizar esta elección, pero la posibilidad de exigir que se cumpla con un compromiso formalizado usando una firma manuscrita distinta de la informada en el carné de identidad emitido por SRCEI es muy baja.	Quien recibe un documento firmado electrónicamente puede libremente elegir si confía en el PSC que firma el certificado electrónico de identidad del firmante del documento.
La falsificación	Las personas se pueden construir sus propios certificados físicos de identidad, pero es difícil construir uno creíble por el tipo de papel y otras barreras comúnmente utilizadas para dificultar la falsificación.	Las personas pueden fácilmente emitir sus propios certificados electrónicos de identidad, los que salvo por no contar con la firma electrónica de un PSC auténtico tienen un aspecto igual a los originales. La única forma en que el receptor puede validar quién emitió el certificado es comparando la firma electrónica del certificado. Por lo tanto, el receptor no debería aceptar certificados emitidos por un PSC que no conozca.

	Firma Manuscrita	Firma Electrónica
La expiración	Normalmente los carné de identidad tienen definido un periodo de valides, una vez cumplido dicho plazo estos documentos se consideran expirados y por lo tanto no deben ser reconocidos por quien valida una firma.	Los certificados electrónicos de identidad tienen definido un período de vigencia, una vez cumplido este plazo no se deben aceptar firmas generadas por los mecanismos asociados a dichos certificados.
La vigencia	Cuando una persona quiere validar la firma manuscrita de un documento acompañado de un carné, no es necesario que la institución que emitió el carné participe de alguna forma, a menos que quien recibe el documento quiera asegurarse de que el carné recibido no ha sido revocado por extravío, robo u otra circunstancia. No todas las instituciones que emiten carné tienen mecanismos para validar su vigencia, por ejemplo las tarjetas de crédito tienen mecanismos para validar su vigencia, pero las licencias de conducir no.	Cuando una persona quiere validar la firma digital de un documento electrónico acompañado de un certificado electrónico de identidad no es obligatorio que el PSC que emitió el certificado participe en la operación, a menos que se desee validar la vigencia del certificado de identidad digital.
La notarización	Para la firma de documentos que requieren mayor nivel de seguridad respecto de la firma se recurre a un notario que da fe del momento en que se realizó la firma y que valida presencialmente a quienes están firmando, a menos que use la figura de autorización de firma que permite al notario dar fe, aun cuando no estén presentes todos los firmantes, pero estableciendo validaciones adicionales a la mera firma del documento.	Para la firma de documentos electrónicos que requieren mayor nivel de seguridad se han desarrollado técnicas de notarización electrónica que permiten agregar niveles de seguridad respecto del momento en que se generó la firma electrónica y de la vigencia de los certificados de los firmantes, sin embargo, estas técnicas no incluyen una nueva validación presencial de los titulares de los certificados electrónicos de identidad.
La individualización	Cuando un servicio requiere de la individualización de una persona, por ejemplo en la aduana antes de entregar un envío, se pide que la persona presente su carné de identidad y comparando con la foto presente en este certificado físico, el funcionario toma la decisión de confiar en que la persona es quien dice ser.	Cuando un servicio requiere la individualización de una persona, por ejemplo cualquier sitio Web que requiera saber quién se está conectando, la persona puede usar su identidad digital, para lo que tendrá que enviar el certificado de identidad y utilizar los mecanismos que el titular puede mantener bajo su exclusivo control. En este caso, en forma muy simple, el usuario está firmando electrónicamente una solicitud de entrada al sitio, por lo tanto se valida la firma y no la foto como en el caso físico.

1.2.- Diferencias con el mundo físico

Si se analiza la analogía presentada entre las firmas manuscritas y las firmas electrónicas es posible comprender que existe una gran cantidad de similitudes entre estas 2 formas de firmar, pero también es importante comprender las principales diferencias y las consecuencias que generan estas diferencias:

- **Seguridad del contenido**: La firma electrónica brinda mayor nivel de seguridad respecto de que no podrá modificarse el mensaje firmado sin que este cambio sea detectado.
- **Falsificación de certificados**: La firma manuscrita está asociada a certificados físicos de identidad que se pueden definir fácilmente de modo que su falsificación no sea trivial, en cambio en el caso electrónico lo único que permite confiar en la autenticidad de un certificado es la firma del PSC. En consecuencia, es irresponsable incentivar a que los usuarios utilicen y reconozcan certificados emitidos por PSC que no sean acreditados, esta condición no es análoga en el caso de las firmas manuscritas.
- **Aspecto de la firma**: Las firmas electrónicas son diferentes para cada firmante y cada mensaje firmado, a diferencia de las firmas manuscritas que son diferentes para cada firmante, pero iguales en todos los documentos firmados por una misma persona.
- **Rol del PSC**: El rol de un PSC es asegurar que la persona que administra los mecanismos que permiten generar una firma electrónica es la misma persona que se individualiza en el certificado emitido, el cual habilita el acceso a los mecanismos de validación de la firma. Además, el PSC provee de mecanismos para validar la vigencia de los certificados emitidos. Por lo tanto, su actividad no es comparable a la de un notario, ya que tanto las competencias requeridas como las actividades realizadas son diferentes.

2.- OBSERVACIONES GENERALES

Tanto el espíritu del proyecto como su diagnóstico inicial son acertados, sin embargo algunos aspectos de redacción y otros de fondo deben ser corregidos antes de aprobar el texto definitivo, en algunos casos para evitar que la ley sea inaplicable y en otros casos para generar las condiciones necesarias para que se desarrolle el comercio electrónico en Chile.

A continuación se explican los conceptos generales que inspiran las indicaciones propuestas. En el capítulo siguiente se presenta el texto actual y las indicaciones que se debería considerar a fin de mejorar el proyecto.

2.1.- Rigor conceptual

Como se ha visto en la analogía presentada, para implementar un sistema de firmas electrónicas en el ámbito nacional y compatible con las iniciativas internacionales en la materia, lo que se requiere es definir los mecanismos que se utilizarán para que las personas cuenten con certificados electrónicos de identidad. Es decir, la forma en que se certifica la identidad de las personas en la red y no su firma electrónica. A partir de una identidad certificada digitalmente es posible generar firmas electrónicas confiables, pero los Prestadores de Servicios de Certificación (PSC) no participan en el proceso de generación de la firma electrónica, por lo tanto afirmar que los PSC certifican firmas electrónicas es una simplificación aceptable en lenguaje coloquial, pero es un grave error en la redacción de una ley que puede transformar todo el texto en letra muerta. Esta consideración genera la necesidad de modificar varias cláusulas.

Incluso el título de la ley debería ser modificado por “Documentos electrónicos, firma electrónica y los servicios de certificación del titular de dicha firma”.

2.2.- Diferencia entre públicos y privados

Se debe eliminar la confusión que nace de tener certificados electrónicos de identidad diferentes, unos para funcionarios públicos y otros para el resto del país. Esta diferencia no tiene ningún sentido y atenta contra la homologación del valor de la firma electrónica con el valor de la firma manuscrita. Es necesario corregir los siguientes conceptos:

- **Certificación de personas, no cargos**: Así como hoy tanto los funcionarios públicos, como cualquier ciudadano del país, utilizan la cédula emitida por el SRCEI para acreditar su identidad, todas las personas deberían usar certificados electrónicos emitidos por cualquier PSC acreditado para probar electrónicamente su identidad y validar su firma electrónica. Esto no tiene relación con la diferencia que existe por ley entre públicos y privados en el sentido de que los primeros sólo estarían facultados para hacer lo que la ley

explícitamente les autoriza, mientras que los segundos pueden hacer todo aquello que no esté explícitamente prohibido. No hay relación porque tan solo se está certificando su identidad y no el contenido de los documentos que eventualmente sean firmados electrónicamente.

- **Preacreditación automática**: Adicionalmente, el artículo 9, preacredita a todos los ministros de fe de órganos del estado sin que medie alguna validación sobre las prácticas y políticas de certificación que ellos utilizarán.
- **Rol del Servicio de Registro Civil e Identificación**: La ley debe autorizar explícitamente al SRCEI para actuar como Autoridad de Registro (o Prestador de Servicios de Registro). En el proyecto se ha optado por encargarle a empresas privadas el rol de organizar e impulsar la utilización de tecnologías de firma electrónica. Una alternativa habría sido encargarle esta función al SRCEI, ya que esta repartición actualmente se encarga de entregar los certificados físicos de identidad más confiables en el país. La elección tomada, se respalda en la innumerable cantidad de nuevas funciones y competencias requeridas para la certificación electrónica y es coherente con la tendencia mundial, pero la eficiencia demostrada por el SRCEI, la infraestructura disponible en el país y las economías que se pueden lograr al juntar la validación presencial de las personas al solicitar un certificado físico y electrónico de identidad en forma simultanea, mueven a autorizar a esta repartición a actuar como Autoridad de Registro o Prestador de Servicios de Registro. El SRCEI debería tener la facultad de definir los términos bajo los cuales un PSC acreditado podrá coordinar sus servicios para interactuar con el SRCEI, pero no debería poder discriminar entre PSC que cumplan los requisitos establecidos.

2.3.- Sistema de Acreditación

El sistema de acreditación debe ser obligatorio, es decir, otorgarle valor legal sólo a los certificados emitidos por un PSC previamente acreditado. A continuación se resumen algunas de las múltiples razones que respaldan esta medida:

- **Confianza**: El objetivo central de la ley es regular el uso de la firma electrónica para que se puedan realizar intercambios de información electrónica en un clima de confianza entre personas que no necesariamente se conocen. Por lo tanto, darle valor legal a certificados emitidos por cualquier persona, natural o jurídica, chilena o extranjera, sin importar las políticas y prácticas que esta siga en la emisión de certificados es un contrasentido, ya que tiende justamente a eliminar la confianza en las comunicaciones electrónicas.

- **Libertad económica de usuarios y certificadores**: Este es el primer principio que guía la redacción de la ley, pero se cae en una contradicción al darle valor probatorio a un certificado emitido por cualquier empresa, nacional o internacional. Esto deja expuestos a todos los chilenos a responder por actos realizados al amparo de un certificado electrónico de identidad emitido por una organización con la que nunca han interactuado y por lo tanto no han depositado su confianza en ella en forma individual y tampoco como sociedad.
- **Compatibilidad internacional**: Este es el cuarto principio que inspira la redacción de ley, sin embargo un sistema de certificación abierto no brinda ninguna garantía respecto de que los certificados con valor legal en Chile sean tecnológicamente compatibles con los estándares mundialmente utilizados. Adicionalmente, con un sistema de acreditación obligatorio, cuando una persona en el extranjero reciba una firma electrónica y la valide a partir de un certificado emitido por un PSC acreditado en Chile, podrá confiar en este certificado tanto como confía en un pasaporte chileno o en una cédula nacional de identidad.
- **Interoperabilidad**: Todos los certificados emitidos por cualquier PSC acreditado deben ser aceptados por las empresas Chilenas que utilicen certificados electrónicos de identidad. En un sistema de acreditación voluntario existe la posibilidad de discriminar a uno o más PSC lo que pone en riesgo la libre competencia y también la interoperabilidad en la red. Esto permitiría crear grupos de servicios a los que se pueda acceder gracias a los certificados emitidos por un PSC y otros grupos de servicios para los que se requiera utilizar los certificados de otro PSC. Una situación así obligaría a los usuarios a comprar varios certificados, encareciendo el sistema y además, permitiría aprovechar el control sobre algunas empresas para privilegiar en forma desleal a un PSC.

2.4.- Seguro obligatorio

El proyecto de ley establece la obligatoriedad de que los PSC que quieran acreditarse demuestren que han contratado un seguro por el 2% del monto máximo autorizado en los certificados vendidos o una garantía equivalente. Esto se opone a otras realidades del mercado actual en Chile. La corte suprema no exige ni capital mínimo ni garantía a los abogados que juran y que les permite ejercer la profesión. Los notarios tampoco están sujetos a restricciones financieras para garantizar sus actos. Tampoco se les exige a arquitectos, ingenieros que firman planos o a contadores que firman balances.

Este tipo de seguro no tiene precedentes en el mercado, no hay historia. Las empresas aseguradoras no sabrán como evaluar el riesgo y por lo tanto el inciso tiende a encarecer y frenar el desarrollo del uso de la tecnología.

2.5.- Tipos de certificados

El texto propuesto deja abierta la posibilidad de que los certificados emitidos incluyan información relacionada con representantes de personas naturales y jurídicas, pero no aborda el tema de los poderes de estos representantes. Por ejemplo, no se menciona el cambio de cargo o empresa entre las causales de revocación de un certificado; se exige validación presencial del titular del certificado, pero esto no es necesario para informar a un representante legal, para esto se requiere estudiar escrituras de poderes; tampoco se menciona el rol del Conservador de Bienes Raíces y su relación con información de poderes otorgados y revocados a representantes legales; o las formas de actuar exigidas para representar al mandante (se podría exigir la firma de 2 personas para ejerser una facultad). En resumen, la ley está pensada para certificar electrónicamente la identidad de personas naturales y es evidente que no se ha pensado en el funcionamiento de la certificación de representantes legales, sin embargo, el texto deja abierta la posibilidad de usar esta ley para informar representantes legales, sin pensar en las consecuencias de esta posibilidad.

El sistema de certificación de representantes abierto por esta ley no sólo está mal definido en el texto propuesto, sino que se trata de una forma de trabajo probadamente inoperante. Las recomendaciones de la IETF (Internet Engineering Task Force, organización internacional que ha liderado la definición de estándares de uso de firma electrónica) apuntan a que los certificados electrónicos de identidad sean puros, es decir, contengan sólo información permanente asociada a la persona y a que los poderes se informen a través de otros mecanismos, que pueden incluir bases de datos o certificados adicionales que complementen al certificado de identidad.

No es necesario cambiar la forma en que se informa a los representantes legales para impulsar el comercio electrónico, ya que existen muchas organizaciones que tienen resuelto el problema a través de bases de datos de poderes. Estas bases de datos pueden usarse para validar las facultades de una persona certificada en forma física o electrónica.

Se propone modificar la redacción de esta ley para aclarar que el único tipo de certificación electrónica de identidad normado es el de personas naturales. De esta forma también se excluyen otro tipo de certificados, como el de sitio Web o agentes computacionales.

Es necesario definir una ley sobre certificación de identidad de representantes legales, sitios Web y agentes computacionales, pero el texto propuesto está muy lejos de lo requerido para legislar sobre estos temas.

2.6.- Autoridades de Registro

Es importante distinguir jurídicamente el rol de un Prestador de Servicios de Certificación (Autoridad Certificadora) y un Prestador de Servicios de Registro (Autoridad de Registro). La segunda realiza la validación de antecedentes de quién solicita ser titular de un certificado electrónico de identidad. Una AR actúa de acuerdo a las políticas y prácticas de certificación que haya definido la AC con la que trabaja coordinadamente. La AC emite los certificados, administra los repositorios públicos de consulta sobre los certificados y su vigencia, provee de toda la tecnología necesaria, se preocupa de que se cumpla con las políticas y prácticas de certificación definidas y se asegura de que la AR realice adecuadamente su función.

2.7.- Venta de Software

Se debe prohibir la venta de software que traiga preconfigurada la confianza en PSC distintos de los acreditados en Chile. Es aceptable que no se pre-configure ninguno, o sólo los acreditados, pero la situación actual es un abuso de confianza con el usuario. El proyecto no toca el tema de la venta de software nacional o importado que utiliza firma electrónica. Actualmente, se venden en el país programas que traen pre-configurada la confianza en algunos PSC, por ejemplo, empresas tan desconocidas en Chile como “PTT Post Root CA” (Empresa Holandesa) vienen preinstaladas en Microsoft Internet Explorer y los usuarios no son advertidos al recibir firmas que se validen con certificados emitidos por esta empresa, pero si reciben una advertencia cuando reciben un certificado emitido por Acepta.com y otros PSC Chilenos, a menos que se deposite explícitamente la confianza en estos PSC. Las personas que compran e instalan estos programas no reciben ninguna advertencia que les avise que la firma electrónica que están recibiendo fue emitida por un PSC en el cual no han depositado su confianza, sin embargo esta advertencia sí aparecería con los certificadores Chilenos acreditados, lo cual es un contrasentido.

2.8.- Archivo Nacional

Se debe permitir que el Archivo Nacional respalde documentos utilizando imágenes escaneadas y firmadas electrónicamente usando una identidad acreditada en Chile. Actualmente una microficha tiene igual valor que el documento original y por lo tanto se utiliza para respaldar los gigantescos volúmenes de información que maneja el Archivo Nacional, sin embargo no se puede utilizar una imagen escaneada y firmada electrónicamente como medio de

respaldo. La ley 18.845 de 1989 del Ministerio de Justicia, establece un sistema de microcopia o micrograbación de documentos que otorga competencia al Archivo Nacional en materias relativas a la conservación de documentos. Y el DFL N° 4 de 1991 del Ministerio de Justicia, faculta al Archivo Nacional para llevar el registro de las entidades que se dediquen a microfilmar documentos otorgándoles a estas copias el mismo valor del documento original.

3.- INDICACIONES Y JUSTIFICACIÓN

A continuación se propone un conjunto de indicaciones que permitirán mejorar drásticamente la ley, cada indicación está acompañada de una justificación.

Artículo	Proyecto Original	Indicaciones
Nombre *	Sobre firma electrónica y los servicios de certificación de dicha firma.	Sobre documentos electrónicos, firma electrónica y los servicios de certificación del titular de dicha firma. Fundamento: De esta forma se evita generar confusión respecto de la certificación de una firma, ya que lo que se certifica es la identidad del firmante y no cada una de las firmas que posteriormente este pueda generar. Si se certificara cada firma, se obligaría al PSC a validar presencialmente al firmante cada vez que firma, eso sería inaplicable, además no existen PSC en Chile, ni en el mundo que brinden este tipo de servicios.
	"TITULO I DISPOSICIONES GENERALES	
1 **	Artículo 1º.- La presente ley regula la firma electrónica, sus efectos legales, la prestación de servicios de certificación de estas firmas y el procedimiento voluntario de acreditación de prestadores de servicio de certificación, para su uso en documentos electrónicos a través de medios electrónicos de comunicación.	Artículo 1º.- La presente ley tiene por objeto regular la utilización de firmas y documentos electrónicos mediante mecanismos de seguridad y autentificación electrónica, la prestación de servicios de certificación electrónica de identidad y sus efectos legales, de manera tal que ellos puedan ser aceptados válidamente conforme a derecho. Fundamento: Así se obtendría mayor claridad, se corregirían errores conceptuales de fondo (como el señalar que se certifica “la firma digital” cuando lo respaldado es “la identidad” de la persona que firma), y se eliminaría la afirmación de que “la ley regula el procedimiento voluntario de acreditación de prestadores de servicios de certificación”. El procedimiento de acreditación debiera ser obligatorio.
	Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.	
	Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.	
2	Artículo 2º.- Para los efectos de esta ley se entenderá por:	

Artículo	Proyecto Original	Indicaciones
	a) Electrónico: relacionado con tecnología que tenga capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;	a) Electrónico: Tecnología que tenga capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares; Fundamento: Se debe eliminar "relacionado con" a fin de evitar que cualquier cosa relacionada con algo electrónico sea también electrónica.
**	b) Certificado de firma electrónica: certificación electrónica que da fe sobre los datos referidos a una firma electrónica;	b) Certificado electrónico de identidad: Mensaje de datos, documento electrónico u otro registro que confirme el vínculo entre un firmante o titular del certificado y los datos de creación de la firma; Fundamento: Se cae en un grave error conceptual al confundir la certificación de una firma, con la certificación de la persona que generó dicha firma. El texto propuesto está tomado de la ley modelo de la UNCITRAL.
*	c) Certificador: entidad prestadora de servicios de certificación de firmas electrónicas;	c) Prestador de Servicios de Certificación: Entidad que expide certificados electrónicos de identidad y puede prestar otros servicios relacionados con las firmas electrónicas; Fundamento: Se define "Certificador", pero a lo largo del proyecto de habla de Prestador de Servicios de Certificación y se omite explicitar la función más importante de un PSC que es emitir certificados electrónicos de identidad. El texto propuesto está tomado de la ley modelo de la UNCITRAL.
		x) Prestador de Servicios de Registro: Entidad que actúa coordinada por un Prestador de Servicios de Certificación para realizar la validación de antecedentes de una persona que solicita ser titular de un certificado. Fundamento: Se agrega esta distinción para mejorar la técnica de delimitación de responsabilidades y para permitir la interpretación de que el Registro Civil actualmente es un Prestador de Servicios de Registro.
	d) Documento electrónico: toda representación electrónica que dé testimonio de un hecho, una imagen o una idea;	d) Documento electrónico o mensaje de datos: Información generada, enviada, recibida o archivada por medios electrónicos; Fundamento: Se propone una definición de "Documento Electrónico" innecesariamente restrictiva. El texto propuesto está tomado de la ley modelo de la UNCITRAL.

Artículo	Proyecto Original	Indicaciones
*	e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción;	e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción y todo otro órgano público que leyes especiales le otorguen competencia de tal; Fundamento: Dejar habilitada la competencia que hoy en día tienen organismos como el Servicio Nacional de Aduanas y el Servicio de Impuestos Internos.
*	f) Firma electrónica avanzada: es aquella creada usando medios que el titular mantiene bajo su exclusivo control, de manera que esté vinculada únicamente al mismo y a los datos a los que se refiere, y permita que sea detectable cualquier modificación ulterior de éstos, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento y la integridad del mismo;	f) Firma electrónica: conjunto de datos en forma electrónica o digital, consignados en un mensaje de datos, o adjuntados lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos; Fundamento: Las letras f) y g) dan una definición confusa de distintos tipos de firmas, una que prueba lo firmado y otra que puede ser cualquier cosa. No tiene sentido legislar y darle un valor probatorio distinto al de cualquier documento electrónico a mecanismos de firma que no aportan nada tecnológicamente en términos de prueba. El texto propuesto está tomado de la ley modelo de la UNCITRAL.
*	g) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor, y	Eliminar. Fundamento: Sólo se considerarán firmas electrónicas que cumplan con aportar tecnológicamente algo más que un documento electrónico común y corriente.
	h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica.	h) Titular del certificado: persona natural identificada en la información contenida en un certificado electrónico de identidad. Fundamento: La letra h) hace que una firma electrónica deje de serlo si el titular no utiliza bajo su exclusivo control los mecanismos de creación de la firma y por lo tanto podría ser usada para eludir responsabilidades. Además se recomienda aclarar aquí que la presente ley sólo será aplicable en la certificación de personas naturales a fin de evitar que se utilice la ley para certificar a personas jurídicas, sitios Web, procesos computacionales u otros agentes distintos de las personas naturales. Esto es importante porque estos otros certificados siguen reglas y procedimientos distintos de las personas naturales y esta ley no ha sido pensada para dar confianza respecto de esa certificación.

Artículo	Proyecto Original	Indicaciones
3	Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan por escrito.	
	Lo dispuesto en el inciso anterior no será aplicable a los actos y contratos otorgados o celebrados en los casos siguientes:	
	a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;	
	b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes; y,	
	c) Aquellos relativos al derecho de familia.	
	La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en el artículo siguiente.	

Artículo	Proyecto Original	Indicaciones
**		Se presume que una firma electrónica tiene el mismo efecto legal que una firma manuscrita u ológrafa, en la medida que ella sea verificada por referencia a un certificado electrónico de identidad válidamente emitido por un Prestador de Servicios de Certificación previa y debidamente acreditado. Se presume legalmente que la firma electrónica aplicada en un documento electrónico constituye una manifestación de voluntad de su signatario, respecto de su envío, contenido, oportunidad y lugar de despacho. La firma digital o electrónica sustituirá el uso de cualquier sello, timbre, visto bueno u otra marca distintiva que se requiriese para la validez del documento si este hubiere sido escrito sobre un soporte de papel. Fundamento: El inciso tercero del artículo 3 señala que "la firma electrónica... se mirará como firma manuscrita para todos los efectos legales…". El artículo puede reforzarse con las presunciones legales señaladas.
	El reglamento determinará las normas técnicas para la generación, archivo, comunicación y conservación de la integridad del documento electrónico.	
4	Artículo 4º.- Los documentos electrónicos podrán presentarse en juicio. En los casos en que dichos documentos se presenten como medios de prueba, se seguirán las siguientes reglas:	Observación: Este artículo es la norma que alude a la forma o a las reglas que habrán de seguirse para "presentarse" los documentos electrónicos en juicio y además formula o determina cual será "el valor probatorio" de dichos documentos. La gradación o los distintos valores probatorios establecidos, según exista firma digital respaldada por un certificado emitido por una entidad previamente acreditada, o no, es teoría jurídica y no solucionará el problema del valor probatorio en juicio de los documentos firmados y/o sólo soportados en forma electrónica. Lo que se busca es otorgar un mayor valor legal en caso de juicio a quienes utilicen documentos o mensajes electrónicos firmados y respaldados digitalmente por entidades previamente acreditadas. La firma digital debiera ser una sola desde el punto de vista de los requisitos y sus efectos legales, es decir, siempre debiera exigirse el respaldo de un certificado de identidad digital emitido por un prestador de servicios de certificación acreditado, para que produzca siempre los mismos efectos legales conforme a derecho.

Artículo	Proyecto Original	Indicaciones
	1ª El juez aceptará su presentación como prueba, considerando los antecedentes de fiabilidad de la forma en que se generó, archivó o comunicó el respectivo documento y de la conservación de su integridad.	
*	2ª Los documentos cuya firma electrónica avanzada esté debidamente certificada por prestadores acreditados, tendrán el mismo valor probatorio que los instrumentos públicos o privados, según sea su naturaleza, de acuerdo con las reglas generales. Tratándose de instrumentos privados, se tendrán por reconocidas su autoría e integridad.	2ª Los documentos cuya firma electrónica cumplan los requisitos para ser aceptados por un juez, tendrán el mismo valor probatorio que los instrumentos públicos o privados, según sea su naturaleza, de acuerdo con las reglas generales. Tratándose de instrumentos privados, se tendrán por reconocidas su autoría e integridad. Fundamento: Se debe eliminar la palabra "avanzada".
*	3ª Los documentos electrónicos no comprendidos en la regla 2ª sólo podrán estimarse como base de una presunción judicial.	Eliminar. Fundamento: Se debe eliminar si se trabaja con acreditación obligatoria.
	4ª La producción de la prueba de los documentos electrónicos se regirá por las normas generales que sean aplicables en consideración a la naturaleza del documento.	Eliminar. Fundamento: Esta aclaración no aporta nada.
	5ª En aquellos procedimientos en los cuales el juez deba valorar el mérito probatorio de acuerdo a su libre convicción o según las reglas de la sana crítica no regirán las reglas 2° y 3°.	

Artículo	Proyecto Original	Indicaciones
		Artículo 4.1. - Los instrumentos y documentos soportados en papel podrán ser respaldados mediante imágenes digitales firmadas electrónicamente, tanto por órganos públicos actuando dentro de su competencia como por particulares, y su mérito probatorio se apreciará conforme a lo que establecen las normas generales en materia de prueba documental, en atención a la naturaleza pública o privada del instrumento o documento. Dichas imágenes se reputarán como microfilmadas, en todos los casos en que una ley o normativa admita usar técnicas de microcopia, microficha o de micrograbado de documentos como método de respaldo. Fundamento: Atendiendo las observaciones de la Subdirectora del Archivo Nacional, señora María Eugenia Barrientos, se propone esta cláusula que permitirá homologar el valor de respaldos de imágenes firmadas electrónicamente con el de las microficas. Esto es razonable, ya que la técnica de respaldo propuesta brinda más seguridad que las microfichas en términos de durabilidad y dificultad de falsificación, además es más económica y de fácil uso.

Artículo	Proyecto Original	Indicaciones
*		Artículo 4.2. - Los documentos contenidos en un soporte digital o electrónico y los actos y contratos que por su intermedio se celebren producirán los mismos efectos que los escritos en un soporte de papel, lo que será especialmente aplicable en los siguientes casos: a) cuando la ley exija que ciertos actos consten por escrito o prevea consecuencias jurídicas para su falta de escrituración; y, b) cuando se presenten o acompañen documentos electrónicos como prueba en un proceso". Artículo 4.3. - Cuando alguna disposición legal exija que una información deba constar por escrito y estar soportada en papel, o bien establezca la existencia de consecuencias jurídicas para su falta de escrituración en soporte papel, se entenderá que un documento digital o electrónico cumple con el requisito de escrituración si la información contenida en el mismo es legible, si está disponible para ser usada o presentada en cualquier momento, y si existe una razonable seguridad de que la información de que da cuenta o que contiene se ha mantenido íntegra desde el momento en que fue generada, salvo los necesarios cambios que sean consecuencia del archivo, de la recuperación y del envío o comunicación del documento. Artículo 4.4. - La posterior impresión en soporte papel de una copia de documentos digitales o electrónicos privados debidamente firmados con el respaldo de un certificado digital emitido por un Prestador de Servicios de Certificación acreditado, hará presumir que su contenido está o ha estado soportado en un archivo magnético o computacional, aún cuando dicha impresión no sea rubricada manualmente por la parte contra la cual se hace valer. Tratándose de documentos o declaraciones sometidas a consideración o presentadas digitalmente ante un órgano público, la posterior impresión en papel que efectúe el órgano o servicio de los informes o declaraciones presentadas en los referidos medios tendrá el valor probatorio de un instrumento privado emanado de la persona bajo cuya firma electrónica se presente. Fundamento: De manera general los artículos 3º, 4º y 5º discurren sobre el valor probatorio de los documentos electrónicos o digitales que son firmados de la misma manera. Pero el valor legal de estos documentos ya no soportados en papel debiera ser más amplio, es decir, poder ser presentados y valorados en un juicio, sea penal, civil, tributario, laboral, etcétera, aún cuando no

Artículo	Proyecto Original	Indicaciones
		Artículo 4.5. - Tratándose de sistemas electrónicos regulados por leyes especiales y sus respectivas disposiciones reglamentarias a la fecha de publicación de la presente ley, se estará a los requisitos, obligaciones y prohibiciones que para la intermediación de documentos, para la generación y certificación de firmas digitales y para la acreditación y licenciamiento de las personas jurídicas que actúen como Proveedores de Servicios de Certificación en ellas se establezca. Respecto de aquellas materias no reguladas para un ámbito particular, se aplicarán las disposiciones de la presente ley que sean compatibles con la naturaleza del servicio prestado, de los documentos transmitidos y de las firmas digitales utilizadas Fundamento: Como a esta fecha existen diversas regulaciones relacionadas con el uso de firmas y certificados digitales y con el valor probatorio de documentos electrónicos, todas las cuales priman por especialidad, debe considerarse un artículo que deje al margen de la aplicación de la futura ley dichas normas, a efectos de evitar conflictos de interpretación y de vigencia de la ley.
5 *	Artículo 5°.- Las partes podrán pactar libremente los procedimientos y métodos de autenticación que emplearán. Los documentos generados a partir de dichos procedimientos tendrán en juicio el valor que corresponda según las reglas generales del Código de Procedimiento Civil.	Eliminar. Fundamento: El artículo está pensado para respaldar el funcionamiento de un sistema de acreditación opcional y por lo tanto se debe eliminar a fin de proteger a los titulares potenciales por todas las razones ya explicadas para respaldar un sistema de acreditación obligatorio.
	Las cláusulas en que se pacten dichos procedimientos y métodos de autenticación se tendrán por no escritas cuando éstos no cumplan las condiciones de seguridad señaladas en la definición de firma electrónica avanzada del artículo 2º letra f). Corresponderá a quien alegue los procedimientos y métodos de autenticación comprobar dichas condiciones.	Eliminar. Fundamento: Eliminar acreditación voluntaria.

Artículo	Proyecto Original	Indicaciones
*	TITULO II USO DE FIRMAS ELECTRÓNICAS POR LA ADMINISTRACIÓN DEL ESTADO	Eliminar. Fundamento: Se debe eliminar el título 2 porque un certificado electrónico de identidad y las firmas electrónicas que con este se puedan validar no regula de ninguna forma el contenido de lo firmado, ni las facultades del firmante, tan sólo valida su identidad, por lo tanto no es necesario un título especial para la administración del estado.
6	Artículo 6º.- Los órganos de la administración del Estado señalados en el artículo 1º de la ley Nº 18.575, podrán efectuar actos y emitir documentos con firma electrónica para todas sus actuaciones, con los efectos indicados en los artículos 3º y 4º.	Artículo 6º.- Los funcionarios de todos los órganos del Estado, podrán efectuar actos y emitir documentos con firma electrónica para todas sus actuaciones, con los efectos indicados en los artículos 3º y 4º. Fundamento: Esta aclaración se mantiene sólo para reforzar la idea de que todas las personas podrán firmar electrónicamente. Se elimina la referencia a la ley nº 18.575 para incluir a todos los funcionarios públicos.
	Los actos y documentos referidos deberán respetar el ámbito de la competencia de dichos órganos.	Eliminar. Fundamento: Es innecesario y contraproducente ya que las facultades de firma de los funcionarios públicos no deben ser reguladas en una ley de firma electrónica, ya están reguladas.
7 *	Artículo 7º.- Las personas podrán relacionarse con los órganos de la administración del Estado a través de técnicas y medios electrónicos con firma electrónica, siempre que dichos organismos tengan los medios compatibles y se ajusten al procedimiento descrito por la ley.	Eliminar. Fundamento: La ley homologa el valor de la firma manuscrita con el de la firma electrónica salvo en un reducido grupo de excepciones. Por lo tanto, en todos aquellos casos en que de acuerdo a esta ley las firmas manuscritas y electrónicas sean homólogas, las personas se podrán relacionar con funcionarios del estado sin necesidad de que lo diga un artículo.
8 *	Artículo 8º.- En la utilización de firmas electrónicas por parte de los órganos de la administración del Estado, se deberá velar por el respeto a los derechos de las personas reconocidos por la Constitución Política y las leyes y evitar cualquier discriminación o restricción en el acceso a las prestaciones de los servicios públicos y a las actuaciones administrativas.	Eliminar. Fundamento: Esta ley no busca regular lo que deben o pueden hacer los funcionarios del estado, por lo tanto el artículo está descontextualizado.

Artículo	Proyecto Original	Indicaciones
9 *	Artículo 9º.- La certificación de las firmas electrónicas de las autoridades o funcionarios de los órganos de la administración del Estado deberá contener, también, la fecha y hora de la emisión del documento.	Eliminar. Fundamento: No se certifica la firma, sino la identidad del firmante. Los documentos de nombramiento de funcionarios de órganos del estado ya están regulados al homologar la firma electrónica con la manuscrita se puede seguir usando esas normas. No le corresponde a una ley de firma electrónica normal la forma en que serán nombrados los funcionarios del estado.
*	Dicha certificación se realizará por los funcionarios que ejerzan como ministros de fe. En aquellos órganos de la Administración en que no se encuentre expresamente establecido el ministro de fe, el jefe de servicio deberá designarlo.	Eliminar. Fundamento: El artículo 12 es el que establece quienes pueden ser PSC, por lo tanto este artículo es innecesario. Es especialmente importante eliminar este inciso que preacredita en forma automática a todos los ministros de fe del estado, sin importar las políticas o prácticas de certificación que estos utilicen.
*	La certificación realizada por ministro de fe competente de los órganos de la administración del Estado, será equivalente a la realizada por un prestador acreditado de servicios de certificación.	Eliminar. Fundamento: Todos los PSC deben seguir las mismas reglas establecidas en esta ley.
10 *	Artículo 10.- Un reglamento establecerá las normas sobre certificación aplicables a la administración del Estado que garanticen la publicidad, fiabilidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas de este título.	Eliminar. Fundamento: Se debe eliminar porque al homologar la firma manuscrita con la electrónica se evita utilizar métodos diferentes para certificar electrónicamente a las personas y en consecuencia el mismo reglamento debe ser aplicable para públicos y privados.

Artículo	Proyecto Original	Indicaciones
		Artículo 10.1º.- El Servicio de Registro Civil e Identificación podrá actuar como Prestador de Servicios de Registro en coordinación con aquellos Prestadores de Servicios de Certificación acreditados que cumplan las condiciones establecidas en un reglamento especial preparado por esta repartición. Fundamento: El Servicio de Registro Civil e Identificación tiene como función principal registrar la identidad de las personas naturales que solicitan un certificado físico de identidad (carné de identidad). Por lo tanto resulta natural autorizar a esta repartición a desempeñar la misma función, pero orientándose a que las personas obtengan un certificado electrónico de identidad. En el fondo esto sólo representa una interpretación de acuerdo al estado de la tecnología de la forma en que el SRCEI puede desempeñar su función, no se trata de encomendarle una función nueva. Considerando las diferencias que existen en la operación y administración de un servicio de certificación electrónico en relación a uno físico y considerando la definición de encargar a empresas privadas la función de Prestador de Servicios de Certificación, se recomienda autorizar a esta repartición tan sólo a desempeñar la función de registro y no las tareas de certificación, ya que esto cambiaría las funciones del SRCEI y atentaría contra el sistema de libre competencia impulsado por la ley.
	TITULO III DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN	
11 *	Artículo 11.- La prestación de servicios de certificación de firma electrónica no estará sujeta a permiso o autorización alguna.	Eliminar. Fundamento: En consideración de los argumentos económicos, técnicos y jurídicos presentados en este informe, el artículo se debe eliminar para optar por un sistema de acreditación obligatorio.

Artículo	Proyecto Original	Indicaciones
12 *	Artículo 12.- Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, con domicilio en Chile que, entre otros servicios, otorguen certificados de firma electrónica.	Artículo 12.- Son Prestadores de Servicios de Certificación electrónica de identidad las personas jurídicas privadas, nacionales o extranjeras, domiciliadas en Chile, que, previa y debidamente acreditadas por la Entidad Acreditadora, en consideración al principio jurídico del necesario resguardo de la fe pública y para mantener el orden público económico involucrado en las transacciones electrónicas, tecnológica y legalmente asuman la responsabilidad de registrar los antecedentes de aquellas personas que serán certificadas mediante la emisión, publicación y mantención de un certificado electrónico de identidad que sirva de respaldo para demostrar su firma electrónica. Fundamento: Es necesario cambiar su redacción para definir acreditación obligatoria y evitar confundir la certificación de la firma con la certificación del firmante. Además, se elimina la posibilidad de que una persona jurídica pública sea PSC, ya que en el evento que una persona jurídica de Derecho Público quisiera competir en el mercado de las empresas Prestadoras de Servicios de Certificación, ya no para respaldar la identidad digital de sus funcionarios (lo que regula el DS Nº81) sino la de todos los chilenos, atendidas las implicancias y lo establecido por el artículo 19 Nº21 de la Constitución, dicha iniciativa debiera tramitarse en una ley especial.
*	Asimismo, son prestadores de servicios de certificación acreditados las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y, acreditadas en conformidad al Título V de esta ley que, entre otros servicios, otorguen certificados de firma electrónica.	Eliminar. Fundamento: Está fusionado con el inciso 1.

Artículo	Proyecto Original	Indicaciones
*	Los certificados de firma electrónica no podrán utilizarse en actos en que los prestadores de servicios de certificación que los hayan otorgado sean parte, o en que tengan cualquier tipo de interés económico directo y, cuando los hayan otorgado prestadores no acreditados en conformidad con el título V de esta ley tampoco podrán usarse en actos en que éstos tengan cualquier tipo de interés económico indirecto. Los certificados quedarán sin efecto desde el momento en que se empleen en contravención a este inciso.	Eliminar. Fundamento: Estaría orientado a proteger la libre competencia entre certificadores, porque impide usar los certificados electrónicos de identidad en aquellos casos en que los PSC que los hayan otorgado sean partes o en que tengan cualquier interés directo o indirecto (si no se han acreditado). Al parecer buscaría evitar situaciones de competencia desleal: por ejemplo, empresas preexistentes podrían aprovechar su participación de mercado para ofrecer certificados electrónicos de identidad en forma desleal aparentando un regalo de certificados a sus clientes, pero en realidad cobrando su valor en forma oculta a través precios en otros productos, a los que se accederá usando estos certificados y en los que tenga a sus clientes cautivos. Otros certificadores no podrían competir en un escenario de esta naturaleza. La cláusula es exagerada y su interpretación será conflictiva si se considera que una empresa asociada a una cámara de comercio no podría utilizar un certificado emitido por un PSC creado por dicha cámara, y en Chile existen dos instancias de certificación digital en este ámbito. Desde una perspectiva económica, y teniendo presente que el DL 211 llamado “ley antimonopolio” se hace cargo de violaciones a las normas de la competencia, no aparece conveniente que otras leyes entren en competencia con el DL 211. Es necesario tener presente que dicha ley establece que las violaciones a la libre competencia no sólo se refieren a conductas deliberadamente asumidas, sino también a conductas involuntarias que delimitan la competencia. El que empresas existentes comiencen a ofrecer servicios de certificación y que los ofrezcan a precios predatorios (bajo el costo) o que los regalen, lo que sería peor, significará que están violando las leyes de la competencia y será una conducta punible. Si una empresa “regala” certificados en forma promocional, no está violando ninguna norma, pero si el producto es permanentemente regalado, hay una conducta anticompetitiva porque en economía no hay milagros. Alguien está pagando por ello. Es lo que se denomina un “subsidio cruzado”. Este tipo de conducta ha sido penalizada por la comisión resolutiva en varios casos en el campo de la aviación comercial, telecomunicaciones, energía eléctrica.
	No se exigirá el establecimiento en el país, que señala este artículo, a los prestadores de servicios de certificación que estén establecidos en países con los cuales Chile se haya comprometido mediante tratados internacionales a no requerir la presencia local para la prestación de servicios transfronterizos.	

Artículo	Proyecto Original	Indicaciones
		Artículo 12.1.- Son Prestadores de Servicios de Registro electrónico de identidad, las personas jurídicas públicas y privadas, nacionales o extranjeras, domiciliadas en Chile, que, previa y debidamente acreditadas por un Prestador de Servicios de Certificación acreditado, asuman la función de registrar los antecedentes de aquellas personas que serán certificadas. En el caso de personas jurídicas públicas esta función solo podrá ser desempeñada por reparticiones que ya tengan asignada entre sus funciones el registro presencial de personas. Fundamento: Este inciso define quienes pueden ser Prestadores de Servicios de Registro.
13 *	Artículo 13.- Son obligaciones del prestador de servicios de certificación de firma electrónica:	Artículo 13.- Son obligaciones de los Prestadores de Servicios de Certificación previamente acreditados, las siguientes: Fundamento: Se debe corregir el título del artículo para no indicar que se certifica la firma y fusionar con el artículo siguiente que norma a PSC no acreditados.
	a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano.	

Artículo	Proyecto Original	Indicaciones
*	b) Mantener un registro público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada.	b) Mantener un registro público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto y se consignen como atributos o campos del certificado, y no podrá utilizarlos para fines no establecidos en las respectivas políticas y prácticas de certificación. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. Se establece la obligación de secreto respecto a los antecedentes y datos personales o nominativos no contenidos en los certificados de quienes firmen y sean certificados digitalmente, que archiven o almacenen los Prestadores de Servicios de Certificación en bases de datos que para todos los efectos legales serán considerados de acceso reservado y restringido, con el objeto de asegurar la confidencialidad de la información y el respeto y la protección de la privacidad de las personas, salvo que un tribunal competente requiera el conocimiento u ordene la exhibición de dichos antecedentes por motivos fundados". Fundamento: En la letra b) es necesario aclarar los usos autorizados para la información recopilada por los PSC, ya que la ley 19.628 sobre protección de la vida privada es inaplicable y en la práctica legaliza el uso indiscriminado de la información de las personas naturales y jurídicas. Por otra parte, la información contenida en los certificados emitidos es por definición pública y por lo tanto es importante diferenciar las obligaciones que existirán sobre estos datos y las que se aplicarán sobre los datos no contenidos en los certificados y recopilados por los PCS.

Artículo	Proyecto Original	Indicaciones
	c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y podrán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.	c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de certificados electrónicos de identidad certificados por ellos, de la manera que establecerá el reglamento y podrán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad. Fundamento: Aclarar que se certifica la identidad de los titulares.
	d) Informar del inicio de las actividades de certificación a la Entidad Acreditadora y, una vez en operación, proporcionarle la información actualizada que ésta requiera y permitir las inspecciones necesarias. Dentro de la información que debe proporcionar estará comprendido el domicilio en el país y sus sucesivas modificaciones, así como demostrar que, antes del inicio de las operaciones, se ha contratado un seguro apropiado en los términos del artículo 15 de esta ley.	d) Informar del inicio de las actividades de certificación a la Entidad Acreditadora y, una vez en operación, proporcionarle la información actualizada que ésta requiera y permitir las inspecciones necesarias. Dentro de la información que debe proporcionar estará comprendido el domicilio en el país y sus sucesivas modificaciones. Fundamento: Exige un seguro que es definido en el artículo 15. Aun cuando el seguro fuera exigido, no tiene sentido repetirlo aquí.
	e) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten.	
	f) Cumplir con las demás obligaciones establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores y Nº 19.628, sobre Protección de la Vida Privada.	Eliminar. Fundamento: No hace más que señalar que los PSC deben cumplir con la ley, por lo tanto no aporta nada.
14	Artículo 14.- Serán obligaciones del prestador acreditado de servicios de certificación de firma electrónica, además de las indicadas en el artículo anterior, las siguientes:	Eliminar y renumerar para continuar con la numeración del artículo anterior. Fundamento: Este artículo se integra con el anterior si se norma sólo los PSC acreditados.

Artículo	Proyecto Original	Indicaciones
	a) Para el caso de la emisión inicial de un certificado de firma electrónica avanzada, el prestador requerirá previamente la comparecencia personal y directa del solicitante o del apoderado facultado si el solicitante es persona jurídica, ante sí o ante persona autorizada por él para tal efecto.	a) Para el caso de la emisión inicial de un certificado electrónico de identidad, el prestador requerirá previamente la comparecencia personal y directa del solicitante o del apoderado facultado si el solicitante es persona jurídica, ante sí o ante persona autorizada por él para tal efecto. Fundamento: Aclarar que se certifica la identidad de los titulares.
	b) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y una suma que será destinada a financiar el sistema de acreditación e inspección de los prestadores.	Eliminar. Fundamento: Se generan incentivos perversos al encargarle a los PSC que financien el funcionamiento de la entidad que los acreditará.
	c) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a dos meses cuando vayan a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.	
	d) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y podrán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario así lo consintiere.	
	e) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos.	

Artículo	Proyecto Original	Indicaciones
15	Artículo 15.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.	Artículo 15.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados electrónicos de identidad. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia. Fundamento: Aclarar que se certifica la identidad, no la firma.
	Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica avanzada.	Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado electrónico de identidad. Fundamento: Aclarar que se certifica la identidad, no la firma.
*	Para los efectos de las normas de este artículo los prestadores de servicios de certificación de firma electrónica deberán acreditar la contratación y mantención de un seguro o garantía, que cubra su eventual responsabilidad civil contractual y extracontractual por un monto equivalente a un mínimo de dos por ciento de la cantidad señalada como límite de los certificados que contengan limitación de responsabilidad y de cinco mil unidades de fomento para los demás certificados.	Eliminar. Fundamento: Se elimina la referencia al seguro obligatorio por todo lo señalado en el capítulo previo sobre "Observaciones Generales".
	El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado.	El certificado electrónico de identidad provisto por un prestador de servicios de certificación podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por terceros. El proveedor de servicios de certificación y el titular del certificado quedarán eximidos de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado a menos que se demuestre dolo. Fundamento: Aclarar que se certifica la identidad y excluir de responsabilidad al titular del certificado cuando la transacción aceptada exceda los montos de uso autorizados en el certificado.

Artículo	Proyecto Original	Indicaciones
**	En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.	Eliminar. Fundamento: El inciso 5 no tiene sentido, ya que elimina a los funcionarios públicos de todo aporte realizado por este proyecto de ley, en la práctica hará que la firma electrónica no sea usada para relacionarse con funcionarios y servicios públicos. Aparentemente está propuesto pensando privilegiar la certificación por parte de ministros de fe del estado, pero todos los PSC serán ministros de fe. Los Prestadores de Servicios de Certificación serán específicamente responsables respecto a la emisión de un certificado: En cuanto a la certeza de la información que él contenía al emitirse; a que en ese momento cumplía con los requisitos que establece la presente ley y el reglamento respectivo; y, a la efectiva vigencia y correspondencia existente entre los mecanismos de validación de la firma y la persona que sea titular de un certificado. Fundamento: Aclarar cuales son las responsabilidades del PSC.
*		Los Prestadores de Servicios de Certificación quedarán exentos de toda responsabilidad y liberados del cumplimiento de sus obligaciones cuando, por razones de caso fortuito o fuerza mayor tales como sismos, sobrevoltajes, cortes de suministro eléctrico y/o servicio telefónico y/o de líneas de transmisión de datos, actos terroristas, huelgas, etc., no se puedan generar las firmas digitales o emitir los certificados respectivos. Tampoco serán responsables de los perjuicios producidos como consecuencia del uso indebido o fraudulento de un certificado. Fundamento: Aclarar límites en las responsabilidades del PSC.
	TITULO IV DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA	TITULO IV DE LOS CERTIFICADOS ELECTRÓNICOS DE IDENTIDAD Fundamento: Aclarar que se certifica la identidad.
16	Artículo 16.- Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:	Artículo 16.- Los certificados electrónicos de identidad, deberán contener, al menos, las siguientes menciones: Fundamento: Aclarar que se certifica la identidad.
	a) Un código de identificación único del certificado;	

Artículo	Proyecto Original	Indicaciones
	b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, los antecedentes de su acreditación en su caso, y su propia firma electrónica avanzada;	b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, los antecedentes de su acreditación en su caso, y su propia firma electrónica; Fundamento: Eliminar la referencia a la firma electrónica avanzada, sólo existe una firma electrónica.
*	c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y	c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre y su rol único tributario, y Fundamento: Eliminar la obligatoriedad de incluir el e-mail, pueden existir certificados electrónicos de identidad que no sirvan para el correo electrónico, pero que si permitan firmar en otros entornos, como en una página Web.
	d) Su plazo de vigencia.	
	Los certificados de firma electrónica podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente.	Los certificados electrónicos de identidad podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados en virtud de convenio internacional ratificado por Chile y que se encuentre vigente. Fundamento: Un PCS es acreditado por su capacidad para emitir certificados confiables, no por su capacidad para acreditar a otro PSC. Si se le atribuyera esta facultad, entonces también debería poder homologar a un PSC nacional y entonces no tendría sentido la entidad acreditadora estatal. Aclarar que se certifica la identidad.
17	Artículo 17.- Los certificados de firma electrónica quedarán sin efecto, en los siguientes casos:	Artículo 17.- Los certificados electrónicos de identidad quedarán sin efecto, en los siguientes casos: Fundamento: Aclarar que se certifica la identidad.
	1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;	
	2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:	
	a) A solicitud del titular del certificado;	
	b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;	b) Por fallecimiento del titular; Fundamento: No se deben incluir certificados de representante en esta ley.

Artículo	Proyecto Original	Indicaciones
	c) Por resolución judicial ejecutoriada, o	
	d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 27;	
	3) Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados que señala el artículo 19, en razón de lo dispuesto en el artículo 20 o del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) del artículo 13 y d) del artículo 14, y	
	4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 13.	Eliminar. Fundamento: Pretende normar a un PSC no acreditado.
	La revocación de un certificado en las circunstancias de la letra d) del número 2) de este artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador.	
	TITULO V DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN	

Artículo	Proyecto Original	Indicaciones
18	Artículo 18.- La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento, permitiendo su inscripción en el registro que se señala en el artículo 19.	
	Para ser acreditado, el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:	
	a) Demostrar la fiabilidad necesaria de sus servicios;	
	b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;	
	c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;	
	d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;	
*	e) Haber contratado un seguro apropiado en los términos que señala el artículo 15; y,	Eliminar. Fundamento: El seguro debe ser eliminado.
	f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.	

Artículo	Proyecto Original	Indicaciones
19	Artículo 19.- El procedimiento de acreditación se iniciará mediante solicitud ante la Entidad Acreditadora, a la que se deberá acompañar los antecedentes relativos a los requisitos del artículo 18 y que señale el reglamento y el comprobante de pago de los costos de la acreditación. La Entidad Acreditadora deberá resolver fundadamente sobre la solicitud en el plazo de noventa días contados desde la fecha de su presentación. Si no se pronunciare dentro de ese plazo, la solicitud se entenderá aprobada.	
	La Entidad Acreditadora podrá contratar expertos con el fin de verificar el cumplimiento de los requisitos señalados en el artículo 18.	
	Otorgada la acreditación, el prestador será inscrito en un registro público que a tal efecto llevará la Entidad Acreditadora, al que se podrá acceder por medios electrónicos. Durante la vigencia de su inscripción en el registro, el prestador acreditado deberá informar a la Entidad Acreditadora cualquier modificación de las condiciones que permitieron su acreditación.	
20	Artículo 20.- Mediante resolución fundada de la Entidad Acreditadora se podrá dejar sin efecto la acreditación y cancelar la inscripción en el registro señalado en el artículo 19, por alguna de las siguientes causas:	
	a) Solicitud del prestador acreditado;	
	b) Pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o peritos que la Entidad Acreditadora ocupe en la inspección a que se refiere el artículo 21; y,	
	c) Incumplimiento grave o reiterado de las obligaciones que establece esta ley y su reglamento.	

Artículo	Proyecto Original	Indicaciones
	En los casos de letras b) y c), la resolución será adoptada previa audiencia del afectado y se podrá reclamar de ella ante el Ministro de Economía, Fomento y Reconstrucción, dentro del plazo de cinco días contados desde la notificación de dicha resolución. El Ministro tendrá un plazo de treinta días para resolver. Su resolución podrá ser apelada para ante la Corte de Apelaciones de Santiago, dentro de los diez días siguientes a la fecha de su notificación. La apelación deberá ser fundada y para su agregación a la tabla, vista y fallo, se regirá por las normas aplicables al recurso de protección. La resolución de la Corte de Apelaciones no será susceptible de recurso alguno.	En los casos de letras b) y c), la resolución será adoptada previa audiencia del afectado y se podrá reclamar de ella ante el Ministro de Economía, Fomento y Reconstrucción, dentro del plazo de cinco días contados desde la notificación de dicha resolución. El Ministro tendrá un plazo de treinta días para resolver. Su resolución podrá ser apelada ante la Corte de Apelaciones de Santiago, dentro de los diez días siguientes a la fecha de su notificación. La apelación deberá ser fundada y para su agregación a la tabla, vista y fallo, se regirá por las normas aplicables al recurso de protección. La resolución de la Corte de Apelaciones no será susceptible de recurso alguno. Fundamento: Corregir la redacción de "...podrá ser apelada para ante la Corte de Apelaciones de Santiago..."
	Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de firmas electrónicas certificadas por ellos, quedando a partir de ese momento sin efecto los certificados, a menos que sus datos sean transferidos a otro certificador acreditado, en conformidad con lo dispuesto en la letra d) del artículo 14. Los perjuicios que pueda causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador.	Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de certificados electrónicos de identidad firmados por ellos, quedando a partir de ese momento sin efecto los certificados, a menos que sus datos sean transferidos a otro certificador acreditado, en conformidad con lo dispuesto en la letra d) del artículo 14. Los perjuicios que pueda causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador. Fundamento: Aclarar que se certifica la identidad.
21	Artículo 21.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Entidad Acreditadora ejercerá la facultad inspectora sobre los mismos y podrá, a tal efecto, requerir información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados, de conformidad al reglamento.	

Artículo	Proyecto Original	Indicaciones
22	Artículo 22.- La Entidad Acreditadora llevará también un registro especial donde dejará noticia del inicio y cese de la operación comercial de los prestadores de servicios de certificación no acreditados, así como de los precios que informen para dichos servicios y de todas las resoluciones que afecten a los certificadores, en especial las referidas al incumplimiento de las obligaciones establecidas en esta ley y su reglamento. Este registro será público y se podrá acceder a él por medios electrónicos.	Eliminar. Fundamento: Este artículo puede ser eliminado ya que los certificados emitidos por PSC no acreditados no tendrán valor mayor al de cualquier documento electrónico. No tiene sentido que la Entidad Acreditadora se desgaste en mantener esta información, la cual puede llegar a ser enorme, ya que existe mucho software disponible en forma gratuita que permite que cualquier persona genere sus propios certificados. Esta función será impracticable y cara, no tiene sentido que los PSC acreditados paguen los costos de financiamiento requeridos para el ejercicio de esta función.
	Los prestadores que no estén acreditados quedarán sujetos a las facultades inspectivas de la entidad de acreditación, para los efectos de velar por el cumplimiento de las obligaciones correspondientes que establecen esta ley y su reglamento.	Eliminar. Fundamento: El fundamento anterior es para eliminar el artículo entero.
23 24	Artículo 23.- Los prestadores de servicios de certificación podrán ser amonestados por incumplimiento de sus obligaciones, mediante resolución de la Entidad Acreditadora. Dicha resolución se dictará previa audiencia del afectado y deberá dejarse constancia de ella en el correspondiente registro. Artículo 24.- La Entidad Acreditadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los certificadores.	
25	Artículo 25.- Los recursos que perciba la Entidad Acreditadora por parte de los prestadores de servicio de certificación constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.	
	TITULO VI DERECHOS DE LOS USUARIOS DE FIRMAS ELECTRÓNICAS	TITULO VI DERECHOS DE LOS TITULARES DE CERTIFICADOS ELECTRÓNICOS Fundamento:

Artículo	Proyecto Original	Indicaciones
26	Artículo 26.- Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:	Artículo 26.- Los titulares de certificados electrónicos de identidad tendrán los siguientes derechos: Fundamento: Se debe corregir la redacción para aclarar que se trata de titulares de certificados electrónicos de identidad. Los usuarios pueden ser todos aquellos que reciben un documento firmado electrónicamente, por lo tanto se debe eliminar la referencia a los usuarios de los certificados.
	1º. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar;	1º. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de certificados electrónicos de identidad, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar; Fundamento: Se certifica la identidad de los titulares.
	2º. A que el prestador de servicios de certificación emplee alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el usuario y que se le informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos;	
	3º. A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso; de la acreditación del prestador de servicios, si corresponde; y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se convinieren;	
	4º. A que el prestador de servicios o quien homologue sus certificados le proporcionen la información sobre sus domicilios en Chile y sobre todos los medios a los que el usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;	

Artículo	Proyecto Original	Indicaciones
	5º. A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 4º del artículo 17 de la presente ley, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador.	
	6º. A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 3º del artículo 17 de la presente ley, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;	
	7º. A traspasar sus datos a otro prestador de servicios de certificación, especialmente, en los casos descritos en la letra c) del artículo 13 y d) del artículo 14;	
	8º. A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;	
	9º. A acceder, por medios electrónicos, al registro de prestadores acreditados y al registro especial de prestadores no acreditados que mantendrá la Entidad Acreditadora; y,	
	10º. A ser indemnizado y hacer valer los seguros comprometidos, en conformidad con el artículo 15 de la presente ley.	Eliminar. Fundamento: Hace referencia al seguro obligatorio eliminado.

Artículo	Proyecto Original	Indicaciones
	Los usuarios gozarán de estos derechos, sin perjuicio de aquellos que deriven de la Ley Nº 19.628, sobre Protección de la Vida Privada y de la Ley Nº 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10° de este artículo, ejercerlos conforme al procedimiento establecido en esa última normativa.	Eliminar. Fundamento: puede entenderse como "se debe cumplir la ley", lo cual no requiere ser dicho y menos en una ley.
		10.1º. A ser informado por los programas y sistemas computacionales, cuando una firma electrónica recibida por estos sistemas se valide usando un certificado electrónico emitido por un Prestador de Servicios de Certificación no acreditado de acuerdo a la ley Chilena y en el cual el usuario del programa no haya depositado explícitamente su confianza. Los programas nacionales o importados que se comercialicen en el país serán considerados venta ilegal cuando se viole esta disposición. Fundamento: Actualmente, se venden en el país programas que traen pre-configurada la confianza en algunos PSC, por ejemplo, empresas tan desconocidas en Chile como "PTT Post Root CA" (Empresa Holandesa) vienen preinstaladas en Microsoft Internet Explorer y los usuarios no son advertidos al recibir firmas que se validen con certificados emitidos por esta empresa, pero si reciben una advertencia cuando reciben un certificado emitido por Acepta.com y otros PSC Chilenos, a menos que se deposite explícitamente la confianza en estos PSC.
27	Artículo 27.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a solicitar oportunamente la revocación del certificado, custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador y, a actualizar sus datos en la medida que estos vayan cambiando.	Artículo 27.- Los titulares de los certificados electrónicos de identidad quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a solicitar oportunamente la revocación del certificado, custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador y, a actualizar sus datos en la medida que estos vayan cambiando. Fundamento: Aclarar que se certifica la identidad y no la firma.

Artículo	Proyecto Original	Indicaciones
	TITULO VII REGLAMENTO	
28	Artículo 28.- Los reglamentos a que se refieren las disposiciones de esta ley serán dictados en el plazo de noventa días contados desde su publicación, mediante uno o más decretos supremos del Ministerio de Economía, Fomento y Reconstrucción suscritos también por los Ministros de Transportes y Telecomunicaciones y Secretario General de la Presidencia.	
	TITULO VIII DISPOSICIONES TRANSITORIAS	
DT 1	Disposición Primera.- Esta ley comenzará a regir seis meses después de la fecha en que se publique en el Diario Oficial.	
DT 2	Disposición Segunda.- Los certificadores que hayan iniciado la prestación de sus servicios con anterioridad a la entrada en vigencia de la presente ley, deberán adecuar su actividad de certificación a ella, dentro del plazo de sesenta días.	
DT 3	Disposición Tercera.- El mayor gasto que irrogue a la Subsecretaría de Economía, Fomento y Reconstrucción las funciones que le asigna esta ley, durante el año 2001, se financiará con los recursos consultados en su presupuesto.".	