

REF. Aprueba Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

DECRETO N° 181

_____ /

SANTIAGO, 09 de Julio de 2002

VISTOS:

- a) Lo dispuesto en el artículo 32° N°8 de la Constitución Política de la República;
- b) La Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma;
- c) Lo dispuesto en la resolución N° 520, de 1996, que fija el texto refundido, coordinado y sistematizado de la resolución N° 55, de 1992, ambas de la Contraloría General de la República.

CONSIDERANDO:

Que en fecha 12 de abril de 2002 se publicó en el Diario Oficial la Ley N°19.799 sobre documento electrónico, firma electrónica y la certificación de dicha firma, cuyo artículo 25 autoriza al Presidente de la República a dictar el reglamento correspondiente, en el plazo de 90 días contados desde la referida publicación.

DECRETO:

ARTÍCULO PRIMERO: Apruébase el siguiente Reglamento de la Ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

Artículo 1º. Los documentos electrónicos, la certificación y uso de la firma electrónica por las personas naturales y jurídicas de derecho privado y la administración del Estado, la prestación de los servicios de certificación, la acreditación de los certificadores, y los derechos y obligaciones de los usuarios se regirá por lo dispuesto en la Ley N° 19.799, el presente Reglamento y las normas técnicas que se dicten al efecto.

TÍTULO PRIMERO: De los Prestadores de Servicios de Certificación

Artículo 2º. Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad con la Ley y este Reglamento, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Artículo 3º. El cumplimiento de las normas técnicas fijadas para la aplicación del presente Reglamento es obligatorio para los prestadores acreditados de servicios de certificación.

Artículo 4º. Los actos administrativos que impliquen la modificación de normas técnicas para la prestación del servicio establecerán los plazos en los cuales un prestador acreditado de servicios de certificación deberá adecuarse a las mismas. El incumplimiento en la adecuación a las nuevas normas técnicas será calificado como incumplimiento grave y facultará a la Entidad Acreditadora a dejar sin efecto la acreditación, de conformidad con el artículo 19 de la Ley y el presente Reglamento.

Artículo 5º. A petición de parte o de oficio, y con el objeto de fijar o modificar las normas técnicas establecidas por este Reglamento, la Entidad Acreditadora podrá iniciar el procedimiento para la elaboración y fijación de normas técnicas. De ser necesario, se podrá fijar conjuntos alternativos de normas técnicas para la prestación del servicio con el objeto de permitir el uso de diversas tecnologías y medios electrónicos, en conformidad a la Ley y el presente Reglamento.

Artículo 6º. Es obligación de los prestadores de servicios de certificación contar con reglas sobre prácticas de certificación consistentes en una descripción detallada de las políticas, procedimientos y mecanismos que el certificador se obliga a cumplir en la prestación de sus servicios de certificación y homologación. Las Prácticas de Certificación deben declarar el cumplimiento de los requisitos señalados en el artículo 17 de este Reglamento, con excepción de la póliza de seguro que se acredita por medio de la presentación de la misma.

Las Prácticas de Certificación deben ser objetivas y no discriminatorias, y se deben comunicar a los usuarios de manera sencilla y en idioma castellano.

Dichas prácticas deberán contener al menos:

- a. Una introducción, que deberá contener un resumen de las prácticas de certificación de que se trate, mencionando tanto la entidad que suscribe el documento, como el tipo de usuarios a los que son aplicables.
- b. Consideraciones generales, debiendo contener información sobre obligaciones, responsabilidades, cumplimiento de auditorías, confidencialidad, y derechos de propiedad intelectual, con relación a todas las partes involucradas.
- c. Identificación y autenticación, debiendo describirse tanto los procesos de autenticación aplicados a los solicitantes de certificados, como los procesos para autenticar a los mismos cuando piden suspensión o revocación de certificado.
- d. Requerimientos operacionales, debiendo contener información operacional para los procesos de solicitud de certificado, emisión de certificados, suspensión y revocación de certificados, procesos de auditoría de seguridad, almacenamiento de información relevante, cambio de datos de creación de firma electrónica, superación de situaciones críticas, casos de fuerza mayor y caso fortuito, y procedimiento de término del servicio de certificación.
- e. Controles de procedimiento, personal y físicos, debiendo describir los controles de seguridad no técnicos utilizados por el prestador de servicios de certificación para asegurar las funciones de generación de datos de creación de firma electrónica, autenticación de usuarios, emisión de certificados, suspensión y revocación de certificados, auditoría y almacenamiento de información relevante.
- f. Controles de seguridad técnica, debiendo señalar las medidas de seguridad adoptadas por el prestador de servicios de certificación para proteger los datos de creación de su propia firma electrónica.
- g. Perfiles de certificados y del registro de acceso público, debiendo especificar el formato del certificado y del registro de acceso público.

- h. Especificaciones de administración de la política de certificación, debiendo señalar la forma en que la misma está contenida en la Práctica, los procedimientos para cambiar, publicar y notificar la política.

Artículo 7º. El prestador de servicios de certificación deberá mantener un registro de certificados de acceso público, en el que se garantice la disponibilidad de la información contenida en él de manera regular y continua.

A dicho registro se podrá acceder por medios electrónicos y en él deberán constar los certificados emitidos por el certificador, indicando si los mismos se encuentran vigentes, revocados, suspendidos, traspasados de otro prestador de servicios de certificación u homologados.

Artículo 8º. En caso que un prestador de servicios de certificación cese en la prestación del servicio, deberá comunicar tal situación a los titulares de los certificados por ella emitidos en la siguiente forma:

- a) Si el cese es voluntario, con una antelación de a lo menos dos meses y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, deberá traspasar los certificados, necesariamente, a un certificador acreditado.
- b) Si el cese no es voluntario, la cancelación de la acreditación, deberá comunicarse inmediatamente a los titulares. En caso que el prestador de servicios de certificación este en situación traspasar los certificados a otro prestador acreditado, deberá informar tal situación en la forma y plazo señalado en la letra a).

Si el titular del certificado se opone a la transferencia, el certificado quedará sin efecto sin más trámite, sin perjuicio de lo dispuesto en el artículo 11 de este Reglamento.

Artículo 9º. En caso que el cese en la prestación del servicio sea por voluntad del prestador acreditado de servicios de certificación, deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en el registro público a que hace referencia el artículo 16 de este Reglamento, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda.

Artículo 10. El cese de la actividad del prestador acreditado de servicios de certificación será registrado como nota de cancelación de la inscripción de la acreditación por la Entidad Acreditadora en el registro público a que se refiere el artículo 16 de este Reglamento.

Artículo 11. Los datos proporcionados por el titular del certificado deberán ser conservados por el prestador de servicios de certificación a lo menos durante seis años desde la emisión inicial de los certificados, cualquiera sea estado en que se encuentre el certificado.

En caso que el prestador de servicios de certificación cese en su actividad, deberá transferir dichos datos a un prestador de servicios de certificación, que deberá estar acreditado si aquel lo fuera, o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los 6 años desde la emisión de cada certificado. Esta situación deberá verse reflejada en el registro público que señala el artículo 16 de este Reglamento.

Artículo 12. Los prestadores de servicios de certificación acreditados deberán contratar y mantener vigente un seguro de responsabilidad civil, que cubra los daños y perjuicios que ocasionen, con motivo de la certificación y homologación de firmas electrónicas, el que deberá contener las siguientes estipulaciones mínimas:

- a) Una suma asegurada de al menos el equivalente de cinco mil unidades de fomento;
- b) La ausencia de deducibles o franquicias, en la parte de la indemnización que no exceda el equivalente de cinco mil unidades de fomento;
- c) La responsabilidad civil asegurada, que comprenderá la originada en hechos acontecidos durante la vigencia de la póliza, no obstante sea reclamada con posterioridad a ella.

TÍTULO SEGUNDO: De la Acreditación de los Prestadores de Servicios de Certificación

Artículo 13. 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 la ley y en este reglamento, permitiendo su inscripción en el registro que se señala en el artículo 16.

Artículo 14. Las funciones correspondientes a la Entidad Acreditadora serán desarrolladas por la Subsecretaría de Economía, Fomento y Reconstrucción, la que, a efectos de su cumplimiento, podrá contratar expertos, a cuyos contratos se incorporarán normas sobre probidad administrativa.

Artículo 15. La Entidad Acreditadora ejercerá la facultad inspectora sobre los prestadores acreditados de servicios de certificación y, a tal efecto, velará porque los requisitos que se observaron al momento de otorgarse la acreditación y las obligaciones que impone la Ley y este Reglamento se cumplan durante la vigencia de la acreditación.

La facultad inspectora comprende tanto inspección ordinaria como la extraordinaria. La inspección ordinaria consiste en la facultad de practicar una visita anual a las instalaciones del prestador acreditado de servicios de certificación, como asimismo requerir, en forma semestral, información sobre el desarrollo de la actividad. La inspección extraordinaria será practicada de oficio o por denuncia motivada sobre la prestación del servicio, ordenada por el Subsecretario mediante resolución fundada.

Las inspecciones podrán ser practicadas por medio de funcionarios o peritos especialmente contratados y habilitados para estos fines, los que en el ejercicio de sus funciones podrán requerir al certificador información adicional a la proporcionada por él.

La información solicitada por la Entidad Acreditadora deberá ser proporcionada dentro del plazo de 5° día, contado desde la fecha de la solicitud, sin perjuicio del otorgamiento de plazos especiales atendida la información requerida.

Artículo 16. La Entidad Acreditadora mantendrá un registro público de prestadores acreditados de servicios de certificación, el que deberá contener el número de la resolución que concede la acreditación, el nombre o razón social del certificador, la dirección social, el nombre de su Representante Legal, el número de su teléfono, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros que exige el artículo 14 de la Ley.

El referido registro público deberá permitir su acceso por medios electrónicos, sin perjuicio, de la mantención del mismo en soporte de papel en la Entidad Acreditadora. Este Registro deberá ser actualizado permanentemente, manteniendo un acceso regular y continuo.

Artículo 17. La acreditación es voluntaria, sin perjuicio de lo cual para obtenerla 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 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 12 de este Reglamento, y
- f. Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

El cumplimiento de dichas condiciones será evaluado por la Entidad Acreditadora de conformidad con las normas técnicas aplicables a la prestación del servicio, durante el procedimiento de acreditación.

Artículo 18. El procedimiento de acreditación de los prestadores de servicios de certificación se iniciará por medio de una solicitud presentada a la Entidad Acreditadora, acompañada del comprobante de pago de los costos de la acreditación y de los antecedentes que permitan verificar el cumplimiento de los requisitos de acreditación, con excepción de la póliza de seguro a que hace referencia el artículo 14 de la Ley.

En la solicitud que presente el interesado deberá individualizarse debidamente y para ello señalará su nombre o razón social, su RUT, el nombre y RUT del Representante Legal, su domicilio social y dirección de correo electrónico, aceptando expresamente dicho medio electrónico como forma de comunicación.

Artículo 19. Recibida la solicitud, la Entidad Acreditadora procederá a verificar la admisibilidad de la misma mediante la verificación de los antecedentes requeridos, dentro de 5° día hábil.

De ser inadmisibile la solicitud, dentro de 3° día hábil se procederá a comunicar al interesado tal situación el que podrá, completar los antecedentes dentro del plazo de 15 días, bajo apercibimiento de ser rechazada la solicitud.

Admitida a trámite la solicitud, la Entidad Acreditadora procederá a un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la Ley y este Reglamento para obtener la acreditación, certificando dentro del plazo de 90 días

contados desde la fecha de la admisibilidad de la solicitud, prorrogables por una vez e igual período y por motivos fundados, que el interesado cumple los requisitos y obligaciones para ser acreditado y que dispone de un plazo de 20 días para presentar la póliza de seguros que exige el artículo 14 de la ley, bajo apercibimiento de ser rechazada la solicitud.

Artículo 20. En caso que la Entidad Acreditadora determine que el prestador de servicios de certificación no cumple con las normas técnicas fijadas para el desarrollo de la actividad, señalará si los incumplimientos son subsanables, y si no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica avanzada.

En caso que los incumplimientos no sean subsanables, la Entidad Acreditadora procederá a dictar una resolución en la que rechaza la solicitud de acreditación.

Si los incumplimientos son subsanables y no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica avanzada, la Entidad Acreditadora podrá acreditar al interesado, previa autorización de un plan de medidas correctivas.

Artículo 21. Una vez completados los requisitos exigidos, la Entidad Acreditadora procederá a acreditar al interesado en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse.

Artículo 22. Durante todo el proceso de acreditación, la Entidad Acreditadora podrá solicitar documentación adicional y/o realizar visitas a las instalaciones del interesado, por intermedio de sus funcionarios o por expertos especialmente contratados para dichos fines.

Artículo 23. La acreditación del prestador de servicios de certificación producirá los siguientes efectos:

- a. La incorporación al registro público de prestadores acreditados que mantiene la Entidad Acreditadora.
- b. Habilitará al certificador a emitir certificados de firma electrónica avanzada.
- c. Someterá al certificador a la inspección de la Entidad Acreditadora.
- d. Los demás que establecen la ley y este Reglamento.

Artículo 24. La Entidad Acreditadora por medio de resolución fijará dentro del primer trimestre de cada año el arancel de los costos de la acreditación y el arancel de supervisión.

Los costos de acreditación serán pagados por el prestador de servicios de certificación que solicite acreditarse, los que no serán restituidos en el evento que la acreditación no se conceda por incumplimiento de los requisitos y obligaciones legales y reglamentarias exigidos para el desarrollo de la actividad de certificación como acreditado.

El arancel de supervisión comprenderá los costos correspondientes a las inspecciones, ordinarias y extraordinarias, y del sistema de acreditación. El arancel deberá ser pagado por los prestadores acreditados de servicios de certificación dentro de los 90 días siguientes a la fecha de la resolución que los fija.

Artículo 25. La Entidad Acreditadora podrá dejar sin efecto la acreditación mediante resolución fundada, por las causales previstas en el artículo siguiente. Dicha resolución deberá ordenar la cancelación de la inscripción del certificador del registro público que lleve la Entidad Acreditadora.

Artículo 26. La acreditación de los certificadores se dejará sin efecto por las siguientes causas:

- a) Por solicitud del prestador acreditado de servicios de certificación, ante la Entidad acreditadora con una antelación de a lo menos un mes a la fecha del término previsto por el prestador acreditado de servicios de certificación para que se haga efectiva, indicando el destino que dará a los certificados y a los datos de ellos, para lo cual deberá cumplir con lo dispuesto en el artículo 8 letra a) de este Reglamento, y garantizar el pago del aviso que deberá ser publicado de conformidad con lo dispuesto en el artículo siguiente.
- b) Por pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o expertos que la Entidad Acreditadora ocupe para el cumplimiento de la facultad inspectora.
- c) Por incumplimiento grave o reiterado de las obligaciones que establece la Ley y este Reglamento.

En los casos de las letras b) y c), la resolución deberá ser adoptada previo traslado de cargos y audiencia del afectado, para lo cual la Entidad Acreditadora dará un plazo de 5 días hábiles para que éste evacue sus descargos. Recibidos éstos la Entidad Acreditadora deberá resolver fundadamente dentro del plazo de 15 días, prorrogables por el mismo período, por motivos fundados.

Artículo 27. Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de las firmas certificadas por

ellos. Sin perjuicio de ello, la Entidad Acreditadora publicará, a costa del certificador, un aviso dando cuenta de la cancelación.

Dicho aviso deberá ser publicado en un medio de prensa escrito de circulación nacional, sin perjuicio de la publicación de la resolución en el registro público que señala el artículo 16 de este Reglamento. El aviso deberá señalar que desde esta publicación los certificados quedarán sin efecto, a menos que hayan sido transferidos a otro certificador acreditado.

TÍTULO TERCERO: De los Certificados de Firma Electrónica

Artículo 28. El certificado de firma electrónica es la certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de firma electrónica.

Los certificados de firma electrónica deben contener, al menos, las siguientes menciones:

- a. Un código de identificación único del certificado.
- b. Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada.
- c. Los datos de la identidad del titular, entre los cuales deben incluir su nombre, dirección de correo electrónico y su rol único tributario.
- d. Su plazo de vigencia.

Artículo 29. Los prestadores de servicios de certificación deberán introducir en los certificados de firma electrónica que emitan, las menciones señaladas en el artículo 15 de la Ley, de acuerdo con las normas fijadas por este Reglamento para el desarrollo de la actividad.

Los atributos adicionales que los prestadores de servicios de certificación introduzcan con la finalidad de incorporar límites al uso del certificado, no deberán dificultar o impedir la lectura de las menciones señaladas en el inciso anterior ni su reconocimiento por terceros.

Artículo 30. Tratándose de un certificado de firma electrónica avanzada deberá el prestador de servicios de certificación comprobar fehacientemente la identidad del solicitante antes de la emisión del mismo, de conformidad con las normas técnicas.

Dicha comprobación la hará el prestador de servicios de certificación, ante sí o ante notario u oficial del Registro Civil, requiriendo la comparecencia personal y

directa del solicitante o de su representante legal si se tratare de una persona jurídica.

Artículo 31. Los datos de creación de firma cuando sean generados por el prestador de servicios de certificación deben ser entregados al usuario o titular del certificado de manera de garantizar la recepción de los mismos en forma personal.

Queda prohibido al prestador de servicios de certificación mantener copia de los datos de creación de firma electrónica una vez que éstos hayan sido entregados a su titular, momento desde el cual éste comenzará a ser responsable de mantenerlos bajo su exclusivo control.

Artículo 32. El certificado de firma electrónica podrá ser usado por su titular de conformidad con las operaciones que han sido autorizadas a realizar en las prácticas de certificación del prestador de servicios de certificación con quien se ha contratado.

El certificado de firma electrónica avanzada deberá permitir a quien lo reciba verificar, en forma directa o mediante consulta electrónica, que ha sido emitido por un prestador acreditado de servicios de certificación, con la finalidad de comprobar la validez del mismo.

Artículo 33. Procederá la suspensión de la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias:

- a. Solicitud del titular del certificado.
- b. Decisión del prestador de servicios de certificación en virtud de razones técnicas.

El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular.

La suspensión del certificado terminará por cualquiera de las siguientes causas:

- a. Por la decisión del prestador de servicios de certificación de revocar el certificado, en los casos previstos en la Ley.
- b. Por la decisión del prestador de servicios de certificación de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.
- c. Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste.

Artículo 34. Los certificados de firma electrónica quedarán sin efecto por la revocación practicada por el prestador de servicios de certificación.

La revocación tendrá lugar cuando el prestador de servicios de certificación constatare alguna de las siguientes circunstancias:

- a) Solicitud del titular del certificado.
- b) Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.
- c) Resolución judicial ejecutoriada.
- d) Que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.
- e) Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.
- f) Que el titular del certificado no ha actualizado sus datos al cambiar éstos.
- g) Las demás causas que convengan al prestador de servicios de certificación con el titular del certificado.

El efecto de la revocación del certificado es el cese permanente de los efectos jurídicos de éste conforme a los usos que le son propios e impide el uso legítimo del mismo.

Artículo 35. Los prestadores acreditados de servicios de certificación podrán homologar los certificados de firma electrónica avanzada emitidos por certificadores no establecidos en Chile, bajo su responsabilidad.

Para ello el prestador acreditado de servicios de certificación deberá demostrar a la Entidad Acreditadora que los certificados por ella homologados han sido emitidos por un prestador de servicios de certificación no establecido en Chile que cumple con normas técnicas equivalentes a las establecidos en este Reglamento para el desarrollo de la actividad.

Una vez practicada la homologación de un certificado o de un grupo de certificados de firma electrónica avanzada el prestador acreditado de servicios de certificación deberá, dentro del plazo de tercero día, comunicar tal situación a la Entidad Acreditadora y se deberá publicar, inmediatamente, en el registro de acceso público señalado en el artículo 7 de este Reglamento.

Las prácticas de homologación deberán estar declaradas en las Prácticas de Certificación.



Artículo 36. La revocación de un certificado de firma electrónica podrá producirse de oficio o a petición de su titular por la concurrencia de algunas de las causales previstas en la Ley o en este Reglamento.

La solicitud de suspensión o revocación, según corresponda, se podrá dirigir al prestador de servicios de certificación en cualquiera de las formas que prevean sus prácticas de certificación.

La suspensión o revocación del certificado deberá ser comunicada inmediatamente a su titular, sin perjuicio que deba publicarse en el registro de acceso público que señala el artículo 7 de este Reglamento.

Tratándose de la suspensión por razones técnicas o revocación del certificado de firma electrónica por las causales de las letras d), e) o f) del artículo 34, dicha decisión deberá ser comunicada al titular con anterioridad a su puesta en práctica, indicando la causa que la provoca y el momento en que se hará efectiva.

El término de la vigencia del certificado será oponible a terceros desde el momento de la publicación de ésta en el registro de acceso público que señala el artículo 7 de este Reglamento.

TÍTULO CUARTO: Protección de los derechos de los usuarios

Artículo 37. De acuerdo con el artículo 13 de la ley el cumplimiento por parte de los prestadores no acreditados de servicios de certificación de las obligaciones que impone la ley, en la forma que lo hacen los prestadores acreditados, servirá como antecedente para determinar la debida diligencia en la prestación del servicio, para los efectos de hacer efectiva la responsabilidad del artículo 14 de la Ley.

Artículo 38. De acuerdo con el artículo 23 de la ley los usuarios podrán ejercer los derechos señalados en dicho artículo 23 de conformidad con el procedimiento establecido en la Ley 19.496 sobre protección de los derechos de los consumidores, salvo en lo que diga relación con el derecho a ser indemnizado y hacer valer los seguros comprometidos, situación en la cual se regirá por el derecho común.

TÍTULO QUINTO

Sobre la utilización de la firma electrónica por los órganos de la Administración del Estado

Párrafo 1º: Reglas comunes

Artículo 39. Los órganos de la Administración del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. Para tal efecto, los actos administrativos, formalizados por medio de documentos electrónicos y que consten en decretos o resoluciones, en acuerdos de órganos colegiados, así como la celebración de contratos, la emisión de cualquier otro documento que exprese la voluntad de un órgano o servicio público de la Administración del Estado en ejercicio de sus potestades legales y, en general, todo documento que revista la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de éstos, deberán suscribirse mediante firma electrónica avanzada.

Artículo 40. La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos y servicios públicos de la Administración del Estado se realizará por los respectivos ministros de fe. En aquellos órganos en que el ministro de fe no se encuentre expresamente establecido, el jefe superior del servicio deberá designar un funcionario público de planta, por resolución, para que actúe como certificador.

Artículo 41. Los órganos de la Administración del Estado podrán contratar, de acuerdo con las normas que rigen la contratación administrativa, los servicios de certificación de firma electrónica con un prestador acreditado de servicios de certificación, cuando mediante resolución fundada constaten su conveniencia técnica y económica. La estimación de dicha conveniencia estará basada en criterios de calidad de servicio y precio de éste.

Artículo 42. Los órganos de la Administración del Estado que utilicen documentos electrónicos deberán contar con un Repositorio o archivo electrónico a los efectos de su archivo una vez que haya finalizado su tramitación, de conformidad con las normas que regulan a su respectiva oficina de partes.

El Repositorio será responsabilidad del respectivo funcionario a cargo del archivo, sin perjuicio de la celebración de convenios de cooperación entre diferentes órganos o de la contratación de una empresa privada para que preste el servicio.

El Repositorio deberá garantizar que se respeten las normas sobre publicidad de los documentos, contenidas en la Ley 18.575 sobre Bases de la Administración del Estado y otras leyes especiales.

Artículo 43. El Repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida.

Para ello la información deberá ser respaldada en copias de seguridad, bajo las siguientes características:

- a. La información deberá ser respaldada con cada proceso de actualización de documentos.
- b. Se deberá mantener una copia de seguridad en el lugar de operación de los sistemas de información y otra en un centro de almacenamiento de datos electrónicos especializado. Este centro de almacenamiento de datos electrónicos, que puede ser propio o provisto por terceros, deberá cumplir con condiciones tales como un estricto control de acceso, un completo y detallado registro de entrada y salida de respaldos, resguardo de la humedad, temperatura adecuada, control del riesgo de incendio y otras.
- c. El esquema de respaldo deberá ser simple, basado en generación de copias acumulativas, con el objeto de mantener la historia de la información en el mínimo de versiones posibles.

La seguridad, integridad y disponibilidad del repositorio deberán estar caracterizadas por:

- a. Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios.
- b. Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de eventuales fallas de las medidas de seguridad al acceso,
- c. La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella.
- d. La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso que el repositorio deje de operar por razones no programadas.

Artículo 44. Para los efectos de garantizar la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, los certificadores de los órganos y servicios públicos de la Administración del Estado deberán cumplir con normas técnicas equivalentes a aquellas fijadas para los prestadores de servicios de certificación acreditados para el desarrollo de la actividad.

Artículo 45. Los documentos electrónicos suscritos por medio de firma electrónica avanzada deberán contener un mecanismo que permita verificar la integridad y autenticidad de los mismos al ser impresos.

Artículo 46. La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos y servicios públicos de la Administración del Estado deberá contener, además de las menciones propias de todo certificado, la fecha y hora de emisión del documento.

Artículo 47. Créase el Comité de Normas para el Documento Electrónico, cuya función principal será asesorar al Presidente de la República con respecto a la fijación de normas técnicas que deberán seguir los órganos de la Administración del Estado para garantizar la compatibilidad de los distintos tipos de documentos electrónicos.

Artículo 48. El Comité estará integrado por:

- a. El Ministro Secretaría General de la Presidencia, quien deberá presidirlo.
- b. El Subsecretario de Economía, Fomento y Reconstrucción.
- c. El Subsecretario de Telecomunicaciones.
- d. El Subsecretario de Hacienda.

Las labores de Secretaría Ejecutiva del Comité de quedarán radicadas en el Subsecretario de Economía en su condición de titular de la Entidad Acreditadora.

Artículo 49. El Comité funcionará, en forma ordinaria, a lo menos dos veces al año, en los días y horas que acuerde. Su Presidente podrá citarlo a sesión extraordinaria cuando las necesidades del cumplimiento de su función así lo ameriten.

El Comité funcionará con la mayoría de sus integrantes y tomará los acuerdos por los dos tercios de sus miembros presentes.

Artículo 50. En el cumplimiento de su función, el Comité de Normas para el Documento Electrónico servirá de instancia de coordinación las acciones de los Ministerios señalados en el artículo 48 de este decreto en el ámbito establecido en el artículo 47 y para ello estará facultado, si lo estima conveniente, para solicitar la asistencia de otros Ministros e invitar a otras autoridades.

Párrafo 2º: Sobre el uso de firmas electrónicas en la relación con los particulares

Artículo 51. Las personas podrán relacionarse con los órganos de la administración del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito en la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos. Con la finalidad de garantizar dicha compatibilidad se estará a las normas técnicas fijadas a instancia del Comité creado en el artículo 47 del presente Reglamento.

Artículo 52. Las personas que se relacionen con la Administración del Estado por medios electrónicos, podrán utilizar firma electrónica, sin perjuicio de aquellos casos en que se haga necesaria la comprobación fehaciente de su identidad, en los cuales deberán emplear firma electrónica avanzada.

Artículo 53. Los órganos de la Administración del Estado podrán relacionarse por medios electrónicos con los particulares, cuando estos hayan consentido expresamente en esta forma de comunicación.

Artículo 54. El Comité creado en el artículo 47, dentro del plazo de 90 días contados desde la fecha de entrada en vigencia del presente Reglamento, elaborará la norma técnica que permita que las comunicaciones por medios electrónicos efectuadas entre los órganos de la Administración del Estado y de éstos con los ciudadanos operen de manera efectiva y eficiente.

Artículo 55. Lo dispuesto en este Título no se aplicará a las empresas públicas creadas por Ley, las que se registrarán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares.

DISPOSICIONES TRANSITORIAS

Primera En tanto no sea aprobadas las normas chilenas aplicables, se fijan como normas técnicas para todos los fines previstos en este Reglamento las siguientes:

Prácticas de Certificación:

- ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates".

- RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Marzo 1999

Seguridad:

- ISO/IEC 17799:2000 Information Technology – Code of Practice for information Security Management (2000).
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 2.1 (2000)
- FIPS PUB 140-1: Security Requirements for Cryptographic Modules, (Mayo 2001)

Estructura de Certificados

- ISO/IEC 9594-8:2001 “Information technology – Open Systems Interconnection – The Directory attributr certificate framework”
- ITU-T Rec. X.690 (1997) / ISO/IEC 8825-1:1998. ASN.1 Basic Encoding Rules

Repositorio de Información.

- [RFC 2559] Boeyen, S. et al., "Internet X.509 Public Key Infrastructure. Operational Protocols - LDAPv2", Abril 1999.

Segunda Se define la siguiente gramática para incluir el RUT de empresas o personas en las extensiones ISSUER_ALT_NAME Y SUBJECT_ALT_NAME. Según aparece en el documento de la IETF RFC 2594 la extensión Subject Alternative Name tiene la siguiente estructura (en formato ASN.1)

```
id-ce-subjectAltName OBJECT IDENTIFIER ::= { id-ce 17 }
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
    otherName          [0]  OtherName,
/* otherName será el campo usado */
    rfc822Name         [1]  IA5String,
    dNSName            [2]  IA5String,
    x400Address        [3]  ORAddress,
    directoryName      [4]  Name,
    ediPartyName       [5]  EDIPartyName,
    uniformResourceIdentifier [6] IA5String,
    iPAddress          [7]  OCTET STRING,
    registeredID       [8]  OBJECT IDENTIFIER}
```

```
OtherName ::= SEQUENCE {
    type-id OBJECT IDENTIFIER,
    value [0] EXPLICIT ANY DEFINED BY type-id }
```

En este mismo documento se menciona que la opción "otherName", es el lugar donde se deben especificar otro tipo de identificadores. Esta es la opción que se utilizará para almacenar el Rut.

Por lo tanto la información a almacenar será la siguiente:

SubjectAltName.otherName.Type-id = "<Definición de la OID>"

SubjectAltName.otherName.Value = "99999999-D" (2 tipos de string : IA5String o PrintableString).

Tercera La OID a usar por los prestadores de servicios de certificación será la siguiente:

Prefijo para PRIVATE ENTERPRISE NUMBERS: 1.3.6.1.4.1

Número asignado a la Entidad Acreditadora: 8321

Sufijos:

RUT del titular del certificado : 1

RUT de la certificadora emisora : 2

Por lo tanto, el OID completo para cada uno de estos items quedaría:

RUT del titular del certificado : 1.3.6.1.4.1.8321.1

RUT de la certificadora emisora : 1.3.6.1.4.1.8321.2

ARTÍCULO SEGUNDO Derógase el Decreto N°81, de 1999, del Ministerio Secretaría General de la Presidencia.

ANÓTESE, TÓMESE RAZÓN, COMUNÍQUESE Y PUBLÍQUESE

RICARDO LAGOS ESCOBAR
PRESIDENTE DE LA REPÚBLICA

JORGE RODRÍGUEZ GROSSI
MINISTRO DE ECONOMÍA, FOMENTO Y RECONSTRUCCIÓN

MARIO FERNANDEZ BAEZA
MINISTRO SECRETARIO GENERAL DE LA PRESIDENCIA

JAVIER ETCHEBERRY CELHAY
MINISTRO DE TRANSPORTES Y TELECOMUNICACIONES