REPUBLICA ORIENTAL DEL URUGUAY

CÁMARA DE REPRESENTANTES

SECRETARÍA

COMISIÓN DE CONSTITUCIÓN, CÓDIGOS, LEGISLACIÓN GENERAL Y ADMINISTRACIÓN

ANEXO I AL
REPARTIDO Nº 1516
JUNIO DE 2009

CARPETA Nº 3132 DE 2009

DOCUMENTO ELECTRÓNICO Y FIRMA ELECTRÓNICA

Se reconocen su validez y eficacia jurídica

I n f o r m e

XLVIa. Legislatura

COMISIÓN DE CONSTITUCIÓN, CÓDIGOS,
LEGISLACIÓN GENERAL Y ADMINISTRACIÓN

I N F O R M E

Señoras y señores Representantes:

La Comisión de Constitución, Códigos, Legislación General y Administración, ha considerado el proyecto de ley relativo a documento electrónico y firma electrónica.

Las tecnologías de la información, las comunicaciones y el conocimiento han venido consolidándose como motor integrador de desarrollo socio-económico de las presentes generaciones y, sin lugar a dudas, serán un soporte cultural de generaciones venideras. Las redes de información y comunicaciones electrónicas son cada vez más cruciales para elevar la productividad, modernizar el Estado, mejorar la calidad de vida de los ciudadanos y profundizar la democracia. Ante esta realidad, el avance hacia la sociedad de la información y el conocimiento que ha encarado decididamente el Uruguay, no sólo constituye un desafío tecnológico, sino que plantea a su vez desafíos desde el punto de vista institucional y legal que paulatinamente se han venido encarando, particularmente desde la creación de la AGESIC creada en la órbita del Poder Ejecutivo, y del trabajo parlamentario de esta temática.

El proyecto de ley de "Documento electrónico y firma electrónica", cuya aprobación recomienda este informe, consagra un marco normativo actualizado y ordenado de medidas que amparen y garanticen tanto la seguridad como la confianza en los documentos electrónicos y la firma electrónica que sirven de sustento a las transacciones electrónicas que tienen lugar en ámbitos como el gobierno electrónico y el comercio electrónico, posibilitando así un desarrollo que consideramos de importancia estratégica para el país tanto a nivel interno como en sus relaciones con el mundo hacia el futuro.

En ese sentido se promueve la aplicación de servicios conexos como ser la creación de una Autoridad Certificadora Raíz Nacional, que permita alcanzar niveles óptimos de seguridad en la aplicación de la firma referida, a través de la emisión de certificados digitales emitidos por prestadores formalmente acreditados, con el objeto de que los usuarios de tales servicios tengan garantías con respecto a sus efectos jurídicos. Asimismo, se incorpora a nuestro derecho positivo el concepto de Firma Electrónica Avanzada, la cual asegura fehacientemente la identidad

del autor, el no repudio del documento y la integridad de su contenido, a través de determinados requisitos.

Autenticidad, integridad y no repudio, son requisitos sine qua non para que nuestra sociedad integrada a un mundo globalizado pueda participar con confianza en todo tipo de transacciones electrónicas, protegiendo los medios de pago, los datos personales, a los consumidores en internet y a la propiedad intelectual entre muchos otros. Esta perspectiva global fundamenta también la aprobación de este proyecto que permitirá corregir las asimetrías existentes con los marcos jurídicos extranjeros y articular nuestro ordenamiento interno con los estándares internacionales en la materia, promoviendo con ello un entendimiento tecnológico con sus respectivas estructuras legales.

Todo el marco normativo propuesto se articula en torno a cinco principios generales que sin tener carácter taxativo son esenciales en el desarrollo de las nuevas tecnologías de la información y las comunicaciones aplicadas al derecho:

- Equivalencia funcional, que considera a los actos jurídicos que se realicen por medios electrónicos con idéntica validez y eficacia jurídica a los que se ejecutan habitualmente en forma escrita y autógrafa, alcanzando los mismos niveles de seguridad y confianza requeridos por la sociedad y evitando la discriminación entre las declaraciones de voluntad expresadas en forma electrónica con respecto a las expresadas en forma escrita tradicional.

- Neutralidad tecnológica, que implica que el marco normativo general que se aplique a todas las actividades que se puedan desarrollar informática o telemáticamente, no adopte un tipo de tecnología en particular, ya que esto implicaría la pérdida de vigencia de la legislación en el corto o mediano plazo, en razón de que la tecnología informática cambia constantemente.

- Libre competencia, que determina que los operadores del mercado de prestación de servicios de certificación de Firma Electrónica actuarán bajo las condiciones y el régimen establecido por la ley, no sujetos a autorización previa.

- Compatibilidad internacional, en relación a la participación en las redes globales de comunicaciones, que exigen que las partes se ciñan a estándares internacionales para garantizar la compatibilidad e interoperabilidad de las transacciones electrónicas. Y,

- Buena fe, que es un principio general de confianza que participa a todo nivel del derecho, por lo tanto se debe hacer extensiva su aplicación a los entornos electrónicos que deben proteger la confianza entre las partes.

Finalmente corresponde destacar que el texto resultante del trabajo en Comisión resultó enriquecido en relación al remitido por el Poder Ejecutivo, y es resultado del intercambio entre distintos actores institucionales, académicos y políticos. El mismo recoge el aporte de la Suprema Corte de Justicia que acompañó la propuesta que fuera incorporada, con una nota valorando positivamente la iniciativa legislativa y su importancia para el Poder Judicial que "… en cuanto habilita a la Suprema Corte de Justicia a constituirse en prestador de servicios de certificación acreditado para Abogados, Escribanos y Procuradores, se inscribe en la línea de aplicación de las más modernas y mejores técnicas de gestión púbica". A su vez el texto final contiene respuestas jurídicas a planteos u observaciones realizados por la Asociación de Escribanos del Uruguay, así como por parte de legisladoras y legisladores -tanto de integrantes de la Comisión como de otros parlamentarios que participaron en el tratamiento del mismo- que lo enriquecieron y permitieron clarificar las redacciones sobre aspectos como la fecha cierta de los documentos, los efectos legales de los documentos electrónicos establecidos en el artículo 4º, y despejar la preocupación acerca de la eventual modificación del concepto de documento público, al consignar que "la firma electrónica avanzada tendrá idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas".

Sala de la Comisión, 20 de mayo de 2009.

EDGARDO ORTUÑO
Miembro Informante
GUSTAVO BERNINI
DIEGO GUADALUPE BRENNA
ÁLVARO F. LORENZO
JAVIER SALSAMENDI
JORGE ZÁS FERNÁNDEZ

PROYECTO DE LEY

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1º. (Ámbito de aplicación).- Queda reconocida la admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica.

Los servicios de certificación deberán ajustarse a lo previsto en esta ley, su actividad no estará sujeta a autorización previa y se realizará en régimen de libre competencia, sin que ello implique sustituir o modificar las normas que regulan las funciones que corresponde realizar a quienes están facultados legalmente para dar fe pública.

Las disposiciones de esta ley no alteran el Derecho preexistente respecto a la celebración, perfeccionamiento, validez y eficacia de los actos y negocios jurídicos.

Artículo 2º. (Definiciones).- A los efectos de esta ley se entenderá por:

A) "Acreditación"; el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Unidad de Certificación Electrónica que cumple con esta ley y su respectiva reglamentación.

B) "Certificado electrónico": documento electrónico firmado electrónicamente que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica.

C) "Certificado reconocido": certificado electrónico emitido por un prestador de servicios de certificación acreditado.

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

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

F) "Dispositivo de creación de firma": componente informático que sirve para aplicar los datos de creación de firma.

G) "Dispositivo de verificación de firma": componente informático que sirve para aplicar los datos de verificación de firma.

H) "Documento electrónico o documento digital": representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.

I) "Fecha electrónica": conjunto de datos en forma electrónica utilizados como medio para determinar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que está asociado.

J) "Firma electrónica": los datos en forma electrónica anexos a un documento electrónico o asociados de manera lógica con el mismo, utilizados por el firmante como medio de identificación.

K) "Firma electrónica avanzada": la firma electrónica que cumple los siguientes requisitos:

1) Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca.

2) Ser creada por medios que el firmante pueda mantener bajo su exclusivo control.

3) Ser susceptible de verificación por terceros.

4) Estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable.

5) Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma.

L) "Firmante o signatario": persona que utiliza bajo su exclusivo control un certificado electrónico o un certificado reconocido para efectuar operaciones de firma electrónica o firma electrónica avanzada.

M) "Prestador de servicios de certificación": persona física o jurídica, pública o privada, nacional o extranjera, que expida certificados electrónicos o preste otros servicios de certificación en relación con la firma electrónica.

N) "Prestador de servicios de certificación acreditado": aquel prestador de servicios de certificación acreditado ante la Unidad de Certificación Electrónica.

Ñ) "Titular del certificado": persona que utiliza bajo su exclusivo control un certificado electrónico.

Artículo 3º. (Principios generales).- Sin que la enumeración tenga carácter taxativo, los actos y negocios jurídicos realizados electrónicamente, las firmas electrónicas o firmas electrónicas avanzadas y la prestación de los servicios de certificación, se ajustarán a los siguientes principios generales:

A) Equivalencia funcional.

B) Neutralidad tecnológica.

C) Libre competencia.

D) Compatibilidad internacional.

E) Buena fe.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

Artículo 4º. (Efectos legales de los documentos electrónicos).- Los documentos electrónicos satisfacen el requerimiento de escritura y tendrán el mismo valor y efectos jurídicos que los documentos escritos, salvo las excepciones legalmente consagradas.

El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del Código Penal, según corresponda.

Artículo 5º. (Efectos legales de la firma electrónica).- La firma electrónica tendrá eficacia jurídica cuando fuese admitida como válida por las partes que la utilizan, o haya sido aceptada por la persona ante quien se oponga el documento firmado electrónicamente.

Se respetará la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas, conforme a la presente normativa.

En caso de ser desconocida la firma electrónica por una de las partes, corresponde a la otra parte probar su validez.

Artículo 6º. (Efectos legales de la firma electrónica avanzada).- La firma electrónica avanzada tendrá idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas, siempre que esté debidamente autenticada por claves u otros procedimientos seguros que:

A) Garanticen que la firma electrónica avanzada se corresponde con el certificado reconocido emitido por un prestador de servicios de certificación acreditado, que lo asocia con la identificación del signatario.

B) Aseguren que la firma electrónica avanzada se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado.

C) Garanticen que la firma electrónica avanzada ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado reconocido.

El documento electrónico suscripto con firma electrónica avanzada tendrá idéntico valor probatorio al documento público o al documento privado con firmas certificadas en soporte papel. El documento electrónico no hará fe

respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador de servicios de certificación acreditado.

Artículo 7º. (Uso de la firma electrónica avanzada en la función notarial).- Autorízase el uso de documentos electrónicos y firma electrónica avanzada en la función notarial, de conformidad con la reglamentación que establezca la Suprema Corte de Justicia.

Artículo 8º. (Empleo de la firma electrónica o firma electrónica avanzada en los órganos del Estado).- El Estado, los Gobiernos Departamentales, los Entes Autónomos, los Servicios Descentralizados y, en general, todos los órganos 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 o firma electrónica avanzada.

Se exceptúan aquellas actuaciones para las cuales la Constitución de la República o la ley exijan una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

Artículo 9º. (Régimen específico de uso de la firma electrónica o firma electrónica avanzada en la Administración Pública).- La Unidad de Certificación Electrónica podrá determinar por vía reglamentaria el uso de la firma electrónica o firma electrónica avanzada en el seno de la Administración Pública y en las relaciones que con ella mantengan los particulares, a los efectos de adoptar las condiciones adicionales que se estimen necesarias, para salvaguardar las garantías de cada procedimiento.

Artículo 10. (Régimen de uso de la firma electrónica o firma electrónica avanzada en las profesiones de Abogado, Escribano y Procurador).- La Suprema Corte de Justicia expedirá, en forma exclusiva, los certificados reconocidos para ser utilizados en el ejercicio de las profesiones de Abogado, Escribano y Procurador, si se constituye como prestador de servicios de certificación acreditado bajo las condiciones que establece esta ley.

En caso de que la Suprema Corte de Justicia no se constituya como prestador de servicios de certificación acreditado, tendrán plena validez y eficacia para ser utilizados en el ejercicio de las profesiones de Abogado, Escribano y Procurador, los certificados reconocidos expedidos por otro prestador de servicios de certificación acreditado.

CAPÍTULO II

INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA

Artículo 11. (Infraestructura Nacional de Certificación Electrónica).- La infraestructura nacional de certificación electrónica es el conjunto de equipos y programas informáticos, dispositivos criptográficos, políticas, normas y

procedimientos, dispuestos para la generación, almacenamiento y publicación de los certificados reconocidos, así como también para la publicación de información y consulta del estado de vigencia y validez de dichos certificados.

Artículo 12. (Unidad de Certificación Electrónica).- Créase la Unidad de Certificación Electrónica como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotada de la más amplia autonomía técnica.

La Unidad de Certificación Electrónica estará dirigida por un Consejo Ejecutivo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que, por sus antecedentes personales, profesionales y de conocimiento en la materia, aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de su cargo.

Dichos miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de su sucesor o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso.

La Presidencia de la Unidad de Certificación Electrónica será ejercida en forma rotativa por períodos anuales entre los integrantes del Consejo Ejecutivo -a excepción del Director Ejecutivo de la AGESIC- y tendrá a su cargo la representación de la misma y la ejecución de las actividades necesarias para el cumplimiento de sus resoluciones.

Artículo 13. (Consejo Consultivo).- El Consejo Ejecutivo de la Unidad de Certificación Electrónica funcionará asistido por un Consejo Consultivo, que estará integrado por el Presidente de la Unidad de Certificación Electrónica, que lo presidirá, el Presidente de la Suprema Corte de Justicia, el Presidente del Banco Central del Uruguay, el Rector de la Universidad de la República, el Presidente de la Unidad Reguladora de Servicios de Comunicaciones (URSEC) y el Presidente de la Cámara Nacional de Comercio y Servicios del Uruguay, o quienes ellos designen como sus representantes.

Sesionará a convocatoria del Presidente de la Unidad de Certificación Electrónica o de la mayoría absoluta de los miembros del Consejo Consultivo.

Podrá ser consultado por el Consejo Ejecutivo sobre cualquier aspecto de su competencia y lo será preceptivamente por éste cuando ejerza potestades de reglamentación, sin que sus pronunciamientos tengan carácter vinculante.

Artículo 14. (Competencia).- La Unidad de Certificación Electrónica deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de esta ley. A tales efectos tendrá las siguientes funciones y atribuciones:

1) De acreditación:
   A) Recibir, tramitar y resolver las solicitudes de acreditación de los prestadores de servicios de certificación.
   B) Inscribir a los prestadores de servicios de certificación en el Registro de Prestadores de Servicios de Certificación Acreditados, que a tal efecto se crea en esta ley, una vez otorgada la acreditación.
   C) Suspender o revocar la inscripción de los prestadores de servicios de certificación acreditados.
   D) Mantener en el sitio web de la Unidad de Certificación Electrónica la información relativa al Registro de Prestadores de Servicios de Certificación Acreditados, tales como altas, bajas, sanciones y revocaciones.
2) De control:
   A) Controlar la calidad y confiabilidad de los servicios brindados por los prestadores de servicios de certificación acreditados, así como los procedimientos de auditoría que se establezcan en la reglamentación.
   B) Realizar auditorías a los prestadores de servicios de certificación acreditados de conformidad con los criterios que la reglamentación establezca para verificar todos los aspectos relacionados con el ciclo de vida de los certificados reconocidos y de sus claves criptográficas.
   C) Determinar las medidas que estime necesarias para proteger la confidencialidad de los titulares de certificados reconocidos.
   D) Efectuar inspecciones y requerir en cualquier momento a los prestadores de servicios de certificación acreditados toda la información necesaria para garantizar el cumplimiento de la función en los términos definidos en esta ley y su reglamento.
3) De instrucción: recibir y evaluar reclamos de titulares de certificados reconocidos relativos a la prestación de servicios de certificación, sin perjuicio de la responsabilidad directa que el prestador de servicios de certificación acreditado tiene ante el titular.

4) De regulación:

   A) Definir los estándares técnicos y operativos que deberán cumplir los prestadores de servicios de certificación acreditados, así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.

   B) Fijar reglas y patrones industriales que aseguren la compatibilidad, interconexión e interoperabilidad, así como el correcto y seguro funcionamiento de los dispositivos de creación y verificación de firma, controlando su aplicación.

5) De sanción: La Unidad de Certificación Electrónica podrá imponer al prestador de servicios de certificación acreditado que infringiere total o parcialmente cualesquiera de las obligaciones derivadas de esta ley o de las normas que resulten aplicables al servicio que presta, las sanciones que se graduarán en atención a la gravedad o reiteración de la infracción, que se detallan a continuación:

   A) Apercibimiento.

   B) Multa entre 100.000 UI (cien mil unidades indexadas) y 4.000.000 UI (cuatro millones de unidades indexadas).

   C) Suspensión hasta por un año de la acreditación.

   D) Revocación de la acreditación.

Las sanciones podrán aplicarse independiente o conjuntamente, según resulte de las circunstancias del caso.

Las resoluciones que impongan sanciones pecuniarias de acuerdo a lo previsto en esta ley, constituyen título ejecutivo a todos sus efectos.

Artículo 15. (Autoridad Certificadora Raíz Nacional).- La Autoridad Certificadora Raíz Nacional es la primera autoridad de la cadena de certificación a la cual le compete emitir, distribuir, revocar y administrar los certificados de los prestadores de servicios de certificación acreditados.

Desígnase a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) como Autoridad Certificadora Raíz Nacional.

CAPÍTULO III

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN ACREDITADOS

Artículo 16. (Registro de Prestadores de Servicios de Certificación Acreditados).- Créase el Registro de Prestadores de Servicios de Certificación Acreditados que estará a cargo de la Unidad de Certificación Electrónica.

Artículo 17. (Requisitos para ser Prestador de Servicios de Certificación Acreditado).- Son condiciones indispensables para ser Prestador de Servicios de Certificación Acreditado, las siguientes:

1) Ser persona física o jurídica constituida en el país, dar garantía económica y solvencia suficiente para prestar los servicios.
2) Contar con personal calificado con conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica avanzada.
3) Utilizar estándares y herramientas adecuadas según lo establecido por la Unidad de Certificación Electrónica.
4) Estar domiciliado en el territorio de la República Oriental del Uruguay, entendiéndose que cumple con este requisito, cuando su infraestructura tecnológica y demás recursos materiales y humanos se encuentren situados en territorio uruguayo.

Artículo 18. (Obligaciones de los Prestadores de Servicios de Certificación Acreditados).- Todos los prestadores de servicios de certificación acreditados deben cumplir las siguientes obligaciones:

1) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma electrónica avanzada de los titulares de los certificados reconocidos por él emitidos.
2) Proporcionar al solicitante antes de la expedición del certificado reconocido la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:
    A) Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica avanzada que sean compatibles con los datos de firma y con el certificado reconocido expedido.
    B) Los mecanismos para garantizar la fiabilidad de la firma electrónica avanzada de un documento a lo largo del tiempo.
    C) El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado reconocido.
    D) Las condiciones precisas de utilización del certificado reconocido, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

E) Las acreditaciones que haya obtenido el prestador de servicios de certificación.

F) Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados reconocidos deberá estar disponible a instancia de éstos.

3) Mantener un registro actualizado de certificados reconocidos en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del registro se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

4) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados reconocidos.

5) Informar a la Unidad de Certificación Electrónica cualquier modificación de las condiciones que permitieron su acreditación durante la vigencia de su inscripción en el Registro de Prestadores de Servicios de Certificación Acreditados.

Artículo 19. (Cese de la actividad de un Prestador de Servicios de Certificación Acreditado).- El prestador de servicios de certificación acreditado que vaya a cesar en su actividad deberá comunicarlo a los titulares de certificados reconocidos que hubiere expedido y podrá transferir su gestión, con su consentimiento expreso, a otro prestador de servicios de certificación acreditado o, en caso contrario, extinguir su vigencia.

La referida comunicación deberá efectuarse con una antelación mínima de sesenta días al cese efectivo de su actividad, e informará, en su caso, sobre las características del prestador al que se propone la transferencia. La comunicación deberá realizarse perentoriamente dentro de los primeros veinte días y los titulares de los certificados contarán con un plazo de veinte días a partir de la recepción de la comunicación para dar su consentimiento.

El prestador cesante deberá comunicarlo a la Unidad de Certificación Electrónica con una antelación de veinte días al cese efectivo de su actividad y deberá indicar el destino que dará a los certificados reconocidos, especificando si los va a transferir y a quién, o si los dejará sin efecto.

La inscripción del prestador de servicios de certificación en el Registro de Prestadores de Servicios de Certificación Acreditados será cancelada de oficio, por la Unidad de Certificación Electrónica, cuando aquél cese en su actividad.

La Unidad de Certificación Electrónica se hará cargo de la información relativa a los certificados reconocidos que se hubieren dejado sin efecto por

el prestador de servicios de certificación, de conformidad con lo previsto en el numeral 3) del artículo 18.

Artículo 20. (Responsabilidad de los Prestadores de Servicios de Certificación Acreditados).- Los prestadores de servicios de certificación acreditados responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad, cuando incumplan las obligaciones que se estipulan en esta ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios de certificación acreditado demostrar que actuó con la debida diligencia.

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

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

Lo dispuesto en este artículo se entiende sin perjuicio de lo establecido en la Ley Nº 17.250, de 11 de agosto de 2000, relativa a las relaciones de consumo.

En ningún caso la responsabilidad que pueda emanar de la certificación efectuada por un prestador de servicios de certificación acreditado no estatal comprometerá la responsabilidad pecuniaria del Estado.

CAPÍTULO IV

CERTIFICADOS RECONOCIDOS

Artículo 21. (Contenido de los certificados reconocidos).- Los certificados reconocidos tendrán el siguiente contenido:

A) La indicación de que se expiden como tales.

B) El código identificativo único del certificado.

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

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

E) La identificación del firmante a través de sus nombres, apellidos y documento de identidad para las personas físicas o la razón social y número de identificación fiscal para las personas jurídicas. Se podrá consignar en el certificado cualquier otra circunstancia del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.

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

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

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

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

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

Artículo 22. (Comprobación de la identidad de los solicitantes).- La identificación de la persona física que solicite un certificado reconocido exigirá su comparecencia física ante los encargados de verificarla y se acreditará mediante el documento de identidad, pasaporte u otros medios legalmente admitidos.

En el caso de certificados reconocidos de personas jurídicas, se exigirá la comparecencia física del representante, que deberá acreditar mediante certificado notarial la representación invocada, la personería jurídica y su vigencia.

Artículo 23. (Vigencia de los certificados reconocidos).- Los certificados reconocidos quedarán sin efecto si concurre alguna de las siguientes circunstancias:

A) Expiración del período de validez del certificado.

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

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

D) Utilización indebida por un tercero.

E) Resolución judicial o administrativa que lo ordene.

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

G) Cese en su actividad del prestador de servicios de certificación acreditado salvo que, previo consentimiento expreso del firmante,

los certificados reconocidos expedidos por aquél sean transferidos a otro prestador de servicios acreditado.

H) Inexactitudes graves en los datos aportados por el firmante para la obtención del certificado reconocido.

La pérdida de eficacia de los certificados reconocidos, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios de certificación acreditados, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado reconocido surtirá efectos desde la fecha en que el prestador de servicios de certificación acreditado tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su registro actualizado de certificados reconocidos.

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

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

Artículo 24. (Equivalencia de certificados).- Los certificados reconocidos podrán ser emitidos por entidades no establecidas en el territorio nacional y serán equivalentes a los otorgados por prestadores de servicios de certificación acreditados, cuando exista un convenio internacional ratificado por la República Oriental del Uruguay y se encuentre vigente.

CAPÍTULO V

FIRMANTE O SIGNATARIO

Artículo 25. (Derechos del firmante o signatario).- El firmante o signatario tiene los siguientes derechos:

A) A ser informado por el prestador de servicios de certificación acreditado, con carácter previo a la emisión del certificado reconocido, de acuerdo a lo establecido en el numeral 2) del artículo 18.

B) A que el prestador de servicios de certificación acreditado emplee los elementos técnicos disponibles para brindar seguridad y

confidencialidad a la información proporcionada por él y a ser informado sobre ello.

C) A que el prestador de servicios de certificación acreditado le informe sobre su domicilio en la República Oriental del Uruguay y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

Artículo 26. (Obligaciones del firmante o signatario).- Son obligaciones del firmante o signatario:

A) Brindar declaraciones exactas y completas en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación.

B) Mantener el control exclusivo de sus datos de creación de firma electrónica avanzada, no compartirlos e impedir su divulgación.

C) Utilizar un dispositivo de creación de firma electrónica avanzada técnicamente confiable.

D) Solicitar la revocación de su certificado reconocido al prestador de servicios acreditado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma.

E) Informar sin demora al prestador de servicios acreditado el cambio de alguno de los datos contenidos en el certificado reconocido que hubiera sido objeto de verificación.

Artículo 27. (Responsabilidad de los representantes o administradores de las personas jurídicas).- Para el caso en que el titular del certificado reconocido sea una persona jurídica serán responsables sus representantes o administradores de acuerdo a lo establecido en esta ley y en las normas generales en la materia.

CAPÍTULO VI

DISPOSICIONES FINALES

Artículo 28. (Derogaciones).- Deróganse los artículos 129 y 130 de la Ley Nº 16.002, de 25 de noviembre de 1988; 697 de la Ley Nº 16.736, de 5 de enero de 1996; 25 de la Ley Nº 17.243, de 29 de junio de 2000; 329 y 330 de la Ley Nº 18.172, de 31 de agosto de 2007; y demás normas que se opongan a esta ley.

Artículo 29. (Traslado del Registro de Prestadores de Servicios de Certificación).- Se establece un plazo de noventa días para realizar el traslado del Registro de Prestadores de Servicios de Certificación, a cargo de la Unidad Reguladora de Servicios de Comunicaciones (URSEC), al Registro

de Prestadores de Servicios de Certificación Acreditados creado por esta ley en la Unidad de Certificación Electrónica.

Artículo 30. (Reglamentación).- El Poder Ejecutivo deberá reglamentar esta ley dentro de los ciento ochenta días de su promulgación.

Sala de la Comisión, 20 de mayo de 2009.

EDGARDO ORTUÑO
Miembro Informante
GUSTAVO BERNINI
DIEGO GUADALUPE BRENNA
ÁLVARO F. LORENZO
JAVIER SALSAMENDI
JORGE ZÁS FERNÁNDEZ

=