

EC/ 1157

*Presidencia de la República Oriental del Uruguay*

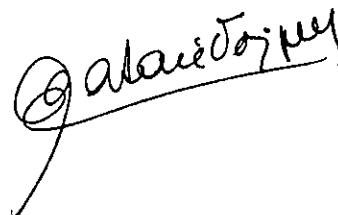
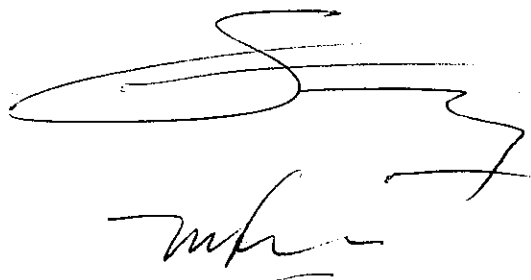
MINISTERIO DE EDUCACION Y CULTURA  
MINISTERIO DEL INTERIOR  
MINISTERIO DE RELACIONES EXTERIORES  
MINISTERIO DE ECONOMIA Y FINANZAS  
MINISTERIO DE DEFENSA NACIONAL  
MINISTERIO DE TRANSPORTE Y OBRAS PUBLICAS  
MINISTERIO DE INDUSTRIA, ENERGIA Y MINERIA  
MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL  
MINISTERIO DE SALUD PUBLICA  
MINISTERIO DE GANADERIA, AGRICULTURA Y PESCA  
MINISTERIO DE TURISMO Y DEPORTE  
MINISTERIO DE VIVIENDA, ORDENAMIENTO TERRITORIAL Y MEDIO  
AMBIENTE  
MINISTERIO DE DESARROLLO SOCIAL

Montevideo, - 2 MAR. 2009

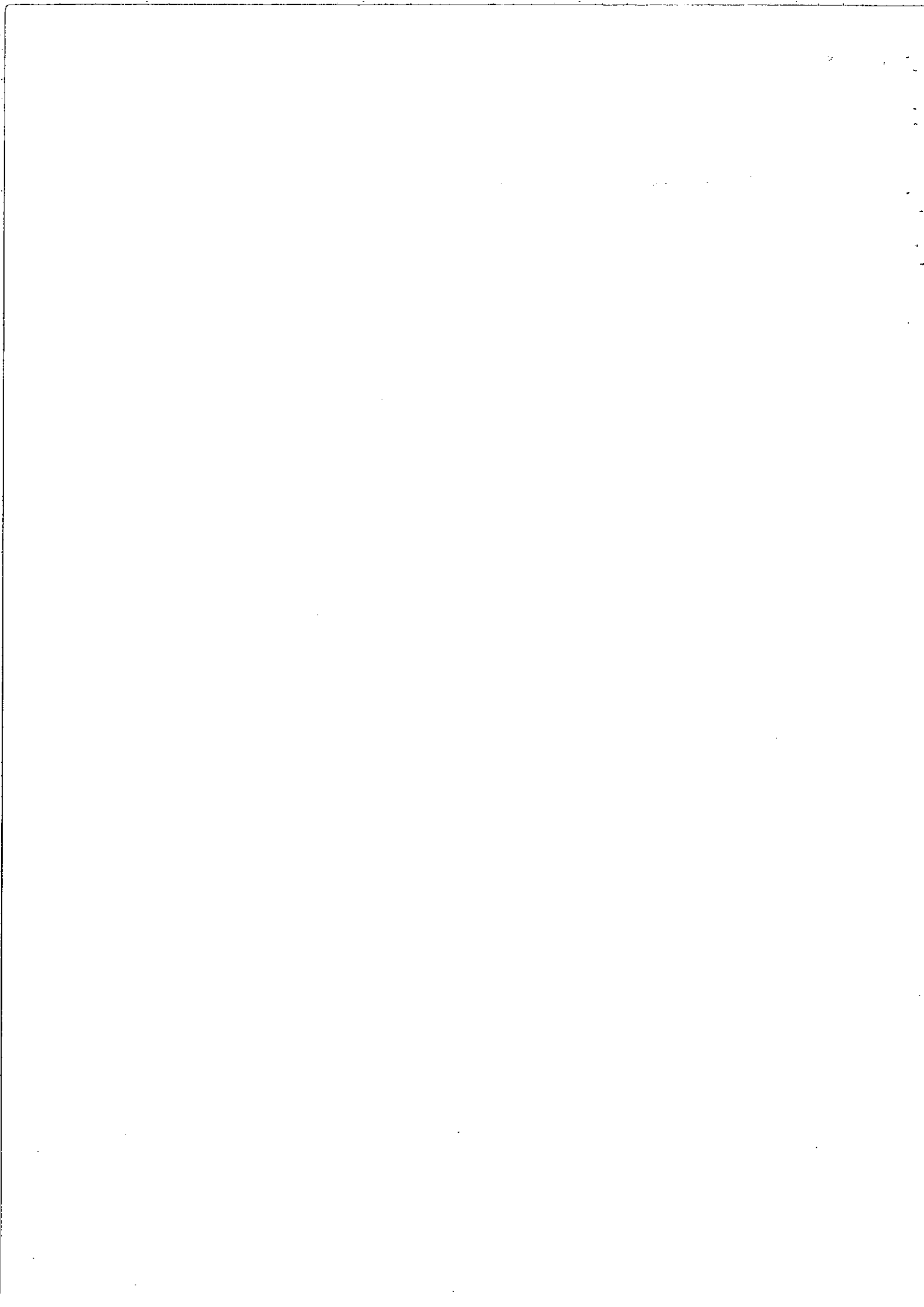
Señor Presidente de la  
Asamblea General

El Poder Ejecutivo tiene el honor de dirigirse a ese  
Cuerpo a efectos de remitir el proyecto de ley sobre Documento Electrónico y  
firma electrónica que se adjunta.

Saluda al señor Presidente con la mayor consideración,



2009 10 10 10 00





## *Presidencia de la República Oriental del Uruguay*

### **EXPOSICIÓN DE MOTIVOS**

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.

Es por ello que el proyecto de ley que se acompaña, busca medidas que amparen y garanticen, la seguridad y 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.

Siendo así, es que en el texto de la misma 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.

La motivación del presente, persigue también el corregir las asimetrías con los marcos jurídicos extranjeros y así poder adaptar nuestro ordenamiento a los estándares internacionales en la materia, promoviendo con ello un entendimiento tecnológico con sus respectivas estructuras legales.

#### **1. Antecedentes normativos nacionales y regionales**

a) A nivel regional encontramos el Acuerdo del MERCOSUR/GMC EXT./RES. N° 37/06, que lleva por título: "Reconocimiento de la Eficacia Jurídica del Documento Electrónico, la Firma Electrónica y la Firma Electrónica Avanzada en el Ámbito del MERCOSUR", lo que impone la adecuación de nuestro régimen jurídico a los efectos de armonizar internacionalmente en la región.

b) A nivel nacional tenemos en primer término, la Ley N° 16.002 del 25 de Noviembre de 1988 que con su artículo 129, fue la primera innovación en materia telemática disponiendo que: "... la transmisión a distancia por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido."

c) Continuó la promulgación de la Ley N° 16.736 del 5 de Enero de 1996 donde en su Sección VIII referente a Normas de Desregulación y Reforma Administrativa, Capítulo I, Normas Generales, en los artículos 694 al 698, insta a la Administración a emplear medios informáticos y telemáticos para el desarrollo de

sus actividades y el ejercicio de sus competencias, reconociendo a las actuaciones que se realicen por medios informáticos o telemáticos validez y valor probatorio "idénticos" a los que se tramiten por medios convencionales y regulando aspectos esenciales de la documentación electrónica.

d) El Decreto del Poder Ejecutivo N° 65/998 del 10 de Marzo de 1998 reglamentó los citados artículos de la Ley N° 16.736 del 5 de Enero de 1998 definiendo en dicha instancia a la "firma electrónica" y la "firma digital".

e) Posteriormente la Ley N° 17.243 del 29 de Junio de 2000, en la Sección 3ra. sobre el "Sistema informático del Estado", obligó a los entes públicos a "implantar el expediente electrónico para la sustanciación de todas las actuaciones administrativas." En el Artículo 25 del mismo capítulo estableció que: "*Autorízase en todo caso la firma electrónica y la firma digital, las que tendrán idéntica validez y eficacia a la firma autógrafa siempre que estén autenticadas por claves u otros procedimientos seguros, de acuerdo a la tecnología informática.*", trascendiendo de esta forma el ámbito de la actividad administrativa y haciéndolas aplicables a todo acto jurídico como lo ha sostenido mayoritariamente la más calificada doctrina nacional.

El segundo inciso del Artículo 25 dispuso que: "*La prestación de servicios de certificación no estará sujeta a autorización previa y se realizará en régimen de libre competencia...*", situación que el presente proyecto amplía creando la categoría de prestadores de servicios de certificación acreditados, los cuales estarán sujetos a supervisión, regulación y control por parte del Estado.

f) El Decreto del Poder Ejecutivo N°. 382/003 de 17 de setiembre de 2003, reglamentó las normas sobre el uso de la firma digital y el reconocimiento de su eficacia jurídica y valor probatorio, invocando el Art. 25 de la Ley N° 17.243, que el actual proyecto deroga expresamente. Además, explicitó la definición de firma digital y caracterizó al prestador de servicios de certificación.

g) Por último encontramos los Arts. 329 y 330 de la Ley N° 18.172 de 31 de agosto de 2007 la cual creó al Registro de Prestadores de Servicios de Certificación a cargo de la Unidad Reguladora de Servicios de Comunicaciones (URSEC) atribuyéndole cometidos especiales en la materia, situación que es también modificada por este proyecto.

## **2. Principios Generales**

El presente Proyecto tiene su pilar fundamental en cinco Principios Generales del derecho, los cuales sin tener carácter taxativo, son los protagonistas principales de las nuevas tecnologías de la información y las comunicaciones aplicadas al derecho. El mismo, recoge los cinco esenciales, que en breve reseña se pueden resumir de la siguiente forma:

**I.- Equivalencia funcional**, en el sentido de que los actos jurídicos que se realicen por medios electrónicos tienen 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



## *Presidencia de la República Oriental del Uruguay*

discriminación entre las declaraciones de voluntad expresadas en forma electrónica con respecto a las expresadas en forma escrita tradicional.

**II.- Neutralidad tecnológica**, apunta a que el marco normativo general que se aplique a todas las actividades que se puedan desarrollar informática y/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.

**III.- Libre competencia**, significa que los operadores del mercado de prestación de servicios de certificación de Firma Electrónica no estarán sujetos a autorización previa y actuarán bajo el denunciado régimen.

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

**V.- Buena Fe**, 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, sobretodo en lo que refiere al intercambio nacional e internacional de bienes y servicios a través de transacciones electrónicas, el cual utiliza soportes tecnológicos que deben proteger esa confianza entre las partes.

### **3. Estructura del Proyecto de Ley**

- Capítulo I - Disposiciones generales (arts. 1 a 9)
- Capítulo II - Infraestructura Nacional de Certificación Electrónica (arts. 10 a 14)
- Capítulo III – Prestadores de Servicios de Certificación Acreditados (arts. 15 a 21)
- Capítulo IV – Certificados Reconocidos (arts. 20 a 22)
- Capítulo V – Firmante o Signatario (arts. 23 a 25)
- Capítulo VI -Disposiciones Finales (arts. 26 a 28)

### **4.- Documento y Firma Electrónica**

De conformidad a la definición que se expresa en el Proyecto en su Artículo 2, literal h) por Documento electrónico y documento digital se entiende la

*"representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo."*

Es pacíficamente aceptado que todo documento tiene que tener un soporte material, perseguir una finalidad informativa y tener carácter probatorio.

En sentido corriente, de conformidad a lo expresado por el Dr. Eduardo J. Couture, se entiende por Firma el: *"trazado gráfico, conteniendo habitualmente el nombre, apellido y rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y obligarse con lo que en ellos se dice"*; la misma puede tener distintas formas como por ejemplo: nombre y apellido, rúbrica, un simple trazado gráfico, sus iniciales o grafías ilegibles.

La particularidad, es que deben tener el carácter de "habitualidad" en relación con su autor, dando la nota de autoría y su voluntad de obligarse. La firma por sí misma, no resulta ser un elemento fundamental del documento, pero se vincula con su eficacia y valor probatorio.

Hoy, las tecnologías informáticas permiten cumplir con estos dos últimos requisitos utilizando herramientas como claves, códigos o signos. Esto lleva a distinguir la "Firma Electrónica" como *"cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita"*. Esta conceptualización permite aplicar el ya nombrado principio de "equivalencia funcional" que se encuentra ínsito en la Ley Modelo sobre Comercio Electrónico creada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), la cual en su art. 7 dispone que: *"Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente"*

Este Proyecto, propone incorporar 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 los siguientes requisitos:

- Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca
- Ser creada por medios que el firmante pueda mantener bajo su exclusivo control.
- Ser susceptible de verificación por terceros.



## Presidencia de la República Oriental del Uruguay

- Estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente del mismo sea detectable
- 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.

La utilización de los términos firma electrónica y firma electrónica avanzada se sustenta, en primer lugar, en una interpretación de equivalencia semántica entre firma electrónica y firma digital de carácter estrictamente tecnológico, así como por compatibilidad internacional en base a estudios de derecho comparado.

### 5. Conveniencia de la aprobación del Proyecto Adjunto y breve explicación de su contenido

Este Proyecto, tiene dentro de sus objetivos el de extender el uso de las Firmas Electrónicas a toda la sociedad, tanto en los ámbitos públicos y privados, como académicos, apuntando hacia horizontes de mejores y más seguras comunicaciones electrónicas con el fin de brindar mayor confianza a los usuarios en las transacciones que por este medio deseen realizar.

Para alcanzar este objetivo se propone un sistema de "Infraestructura Nacional de Certificación Electrónica" que tal como se expresa en el Artículo 10 del Proyecto 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.", para ello se crea la Unidad de Certificación Electrónica (UCE) como órgano desconcentrado de la AGESIC la que será asistida por un Consejo Consultivo.

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.

El conocimiento, hace al crecimiento de una nación dentro un marco jurídico seguro, permitiendo a los ciudadanos acceder democráticamente a las redes de la información y las comunicaciones electrónicas, y por ende a la modernización y riqueza del estado de derecho, permitiéndoles su participación no como simples espectadores sino como protagonistas en el quehacer nacional.

Dr. TABARE VAZQUEZ  
Presidente de la República

~~Handwritten signature~~  
Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature



# *Presidencia de la República Oriental del Uruguay*

## DOCUMENTO ELECTRONICO Y FIRMA ELECTRONICA

### CAPITULO I

#### DISPOSICIONES GENERALES

##### **Artículo 1. 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 la presente 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 la presente ley no alteran el Derecho preexistente respecto a la celebración, perfeccionamiento, validez y eficacia de los actos y negocios jurídicos.

##### **Artículo 2. Definiciones.**

A los efectos de la presente 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 la presente 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) "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.

j) "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; y

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.

k) "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.

l) "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.

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

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

### **Artículo 3. 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;



## *Presidencia de la República Oriental del Uruguay*

- b) neutralidad tecnológica;
- c) libre competencia;
- d) compatibilidad internacional; y
- 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 4. Efectos legales de los documentos electrónicos.**

Los documentos electrónicos satisfacen el requerimiento de escritura y tendrán los mismos efectos jurídicos que los documentos escritos, salvo las excepciones contempladas en la presente ley.

La documentación emergente de la transmisión por medios electrónicos constituirá de por sí documentación auténtica y hará plena fe, a todos sus efectos, en cuanto a la existencia del original transmitido.

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 5. 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 6. Efectos legales de la firma electrónica avanzada.**

La firma electrónica avanzada tendrá idéntica validez y eficacia a la firma autógrafa consignada en documento público, 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; y

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 suscrito con firma electrónica avanzada tendrá idéntico valor probatorio al documento público en soporte papel

#### **Artículo 7. 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 8. 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 9. 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.

## **CAPITULO II**

### **INFRAESTRUCTURA NACIONAL DE CERTIFICACION ELECTRÓNICA**

#### **Artículo 10. 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.



## *Presidencia de la República Oriental del Uruguay*

### **Artículo 11. 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 12. 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 13. Competencia.**

La Unidad de Certificación Electrónica deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente 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 la presente 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 la presente 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:



## *Presidencia de la República Oriental del Uruguay*

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 la presente ley o de las normas que resulten aplicables al servicio que presta, las sanciones que se graduarán en atención a la gravedad y/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 la presente ley, constituyen título ejecutivo a todos sus efectos.

### **Artículo 14. 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.

## **CAPITULO III**

### **PRESTADORES DE SERVICIOS DE CERTIFICACION ACREDITADOS**

#### **Artículo 15. 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 16. 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 17. 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.



## *Presidencia de la República Oriental del Uruguay*

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 18. 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, con su consentimiento expreso, su gestión 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 vaya a dar 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 a lo previsto en el numeral tercero del artículo precedente.

## **Artículo 19. 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 la presente ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios de certificación acreditados 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 sobre 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.

## **CAPITULO IV**

### **CERTIFICADOS RECONOCIDOS**

#### **Artículo 20. 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 e identificación fiscal



## *Presidencia de la República Oriental del Uruguay*

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 21. 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 22. 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 23. 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 que se encuentre vigente.

## **CAPITULO V**

### **FIRMANTE O SIGNATARIO**

#### **Artículo 24. 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 artículo 17 numeral 2.



## *Presidencia de la República Oriental del Uruguay*

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 25. 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 26. Responsabilidad de los representantes y/o administradores de las personas jurídicas.** Para el caso en que el titular del certificado reconocido sea una persona jurídica serán responsables sus representantes y/o administradores de acuerdo a lo establecido en la presente ley y en las normas generales en la materia.

## **CAPITULO VI**

### **DISPOSICIONES FINALES**

**Artículo 27. Derogaciones.** Deróganse los artículos: 129 y 130 de la Ley Nº 16.002 de fecha 25 de noviembre de 1988; 697 de la Ley Nº 16.736 de fecha 5 de enero de 1996; 25 de la Ley Nº 17.243 de fecha 29 de junio de 2000; 329 y 330 de la Ley Nº 18.172 de fecha 31 de agosto de 2007; y demás normas que se opongan a la presente ley.

**Artículo 28. Traslado del Registro de Prestadores de Servicios de Certificación.**

Se establece un plazo de 90 días para realizar el traslado del Registro de Prestadores de Servicios de Certificación, a cargo de la URSEC, al Registro de Prestadores de Servicios de Certificación Acreditados creado por la presente ley en la Unidad de Certificación Electrónica.

**Artículo 29. Reglamentación.** El Poder Ejecutivo deberá reglamentar la presente ley dentro de los 180 días de su promulgación.

A collection of approximately 12 handwritten signatures in black ink, arranged vertically and horizontally on the page. The signatures vary in style, with some being highly stylized and others more legible. They are located in the lower half of the page, below the text of the articles.