LEY DE MENSAJE DE DATOS Y FIRMAS ELECTRONICAS

EXPOSICION DE MOTIVOS

DECRETO CON FUERZA DE LEY N° 1.204 DE FECHA 10 DE FEBRERO DE 2001, DE MENSAJE DE DATOS Y FIRMAS ELECTRONICAS

Venezuela avanza aceleradamente hacia la actualización en materia de tecnologías de información y de las comunicaciones. En los últimos años esta evolución tecnológica ha revolucionado a nivel mundial las diferentes áreas del conocimiento y de las actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicarse y celebrar negocios. Al mismo tiempo ha contribuido a borrar fronteras, disminuir el tiempo y acortar las distancias.

La particularidad de estas tecnologías de información es que utilizan medios electrónicos y redes nacionales e internacionales adecuadas que constituyen una herramienta ideal para realizar intercambios de todo tipo, incluyendo el comercial a través de la transferencia de informaciones de un computador a otro sin necesidad de utilizar documentos escritos en papel, lo que permite ahorro de tiempo y dinero.

El surgimiento de estas formas de interrelación cuenta actualmente con cientos de millones de usuarios a nivel mundial, factor que incidirá en todos los ámbitos del quehacer humano, entre estos, en la economía internacional y en el derecho, los cuales deben estar presente en estas actividades con el fin de proteger, a través de sus normas, los intereses de los usuarios.

En consecuencia, se hace necesaria e inminente la regulación de las modalidades básicas de intercambio de información por medios electrónicos, a partir de las cuales han de desarrollarse las nuevas modalidades de transmisión y recepción de información, conocidas y por conocerse, a los fines de garantizar un marco jurídico mínimo indispensable que permita a los diversos agentes involucrados, desarrollarse y contribuir con el avance de las nuevas tecnologías en Venezuela.

A lo expuesto, cabe agregar que la presentación de un instrumento legal que regule estos mecanismos de intercambio de información, los haga jurídicamente trascendentes a la administración de justicia, y les permita apreciar y valorar estas formas de intercambio y soporte de información, con el objeto de garantizar el cumplimiento de las obligaciones asumidas mediante dichos mecanismos y constituirse en un aporte necesario e indispensable que permita construir la base jurídica para el desarrollo de estas tecnologías.

En esta nueva modalidad de relación hace falta establecer dos elementos principales: 1. identificación de las partes 2. integridad del documento o mensaje. De los cuales se derivan responsabilidades (civil, patrimonial, penal, administrativa, disciplinaria, fiscal, etc.), comunes a los actos y negocios normales previstos en nuestro ordenamiento jurídico actual.

El principal objetivo de este Decreto-Ley es adoptar un marco normativo que avale los desarrollos tecnológicos sobre seguridad en materia de comunicación y negocios

electrónicos, para dar pleno valor jurídico a los mensajes de datos que hagan uso de estas tecnologías.

Nuestra legislación actual establece, que cuando un acto o contrato conste por escrito, bastará como prueba el instrumento privado con las firmas autógrafas de los suscriptores. Dentro de este contexto el Decreto-Ley Sobre Mensaje de Datos y Firmas Electrónicas, pretende crear mecanismos para que la firma electrónica, en adelante, tenga la misma eficacia y valor probatorio de la firma escrita, siempre y cuando cumpla con los requisitos mínimos establecidos en este Decreto-Ley.

En términos generales, la legislación actual no reconoce el uso de los medios electrónicos de manera expresa y en caso de un litigio, el juez o tribunal, tendrá que allegarse de medios de prueba libre y acudir a la sana crítica para determinar que una operación realizada por medios electrónicos es o no válida. Esta situación ha originado que empresas y personas se sientan inseguras de realizar transacciones por medios electrónicos, debido a la incertidumbre legal en caso de controversias.

Por ello se hace indispensable dar valor probatorio al uso de medios electrónicos en los procesos administrativos y judiciales, sin que quede al arbitrio del juez considerar su validez probatoria, en caso de controversia, debido a una ausencia de regulación expresa.

Así tenemos que entre la principales disposiciones contenidas en el Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas, se encuentran disposiciones que regulan:

· El mensaje de datos.
· La firma electrónica.
· Los certificados electrónicos.
· Los proveedores de servicios de certificación.

Como complemento necesario a estas disposiciones se crea la Superintendencia de Servicios de Certificación Electrónica, servicio autónomo con autonomía funcional, financiera y de gestión, adscrito al Ministerio de Ciencia y Tecnología, cuyo objeto es supervisar a los Proveedores de Servicios de Certificación, bien sean estos públicos o privados, a fin de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz y seguro a los usuarios. Estos Proveedores de Servicios de Certificación una vez acreditados, tendrán entre sus funciones emitir un documento contentivo de información "cerciorada" que vincule a una persona natural o jurídica y confirme su identidad, con la finalidad que el receptor pueda asociar inequívocamente la firma electrónica del mensaje a un emisor. El Proveedor de Servicios de Certificación da certeza de la autoría de un mensaje de datos mediante la expedición del certificado electrónico.

Entre los principios que guían al Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas, destacamos los siguientes:

1) Eficacia Probatoria. A los fines de otorgar la seguridad jurídica necesaria para la aplicación del Decreto-Ley, así como la adecuada eficacia probatoria a los mensajes de datos y firmas electrónicas, en el artículo 4° se atribuye a los mismos el valor probatorio que la Ley consagra para los instrumentos escritos, los cuales gozan de tarifa legal y producen plena prueba entre las partes y frente a terceros de acuerdo a

su naturaleza. Asimismo, todo lo concerniente a su incorporación al proceso judicial donde pretendan hacerse valer, se remite a las formas procedimentales reguladas para los medios de pruebas libres, contenidas en el artículo 395 del Código de Procedimiento Civil. De esta forma, ha sido incorporado el principio de equivalencia funcional, adoptado por la mayoría de las legislaciones sobre esta materia y los modelos que organismos multilaterales han desarrollado para la adopción por parte de los países de la comunidad internacional en su legislación interna.

2) Tecnológicamente neutra. No se inclina a una determinada tecnología para las firmas y certificados electrónicos. Incluirá las tecnologías existentes y las que están por existir.

3) Respeto a las formas documentales existentes. Es importante destacar que este Decreto-Ley no obliga a la utilización de la firma electrónica en lugar de la manuscrita, sino que su utilización es voluntaria. Tampoco se pretende alterar las restantes formas de los diversos actos jurídicos, registrales y notariales, sino que se propone que un mensaje de datos firmado electrónicamente, no carezca de validez jurídica únicamente por la naturaleza de su soporte y de su firma.

4) Respeto a las firmas electrónicas preexistentes. Las firmas electrónicas utilizadas en grupos cerrados donde existan relaciones contractuales ya establecidas, pueden ser excluidas del campo de aplicación del Decreto-Ley. En este contexto debe prevalecer la libertad contractual de las partes.

5) Otorgamiento y reconocimiento jurídico de los Mensajes de Datos y las Firmas Electrónicas. Asegura el otorgamiento y reconocimiento jurídico de los mensajes de datos, las firmas electrónicas y los servicios de certificación provistos por los proveedores de servicios de certificación, incluyendo mecanismos de reconocimiento a nivel internacional. Establece las exigencias esenciales que cumplirán dichos proveedores de servicios de certificación, incluida su responsabilidad.

6) Funcionamiento de las firmas electrónicas. El Decreto-Ley busca asegurar el buen funcionamiento de las firmas electrónicas, mediante un marco jurídico homogéneo y adecuado para el uso de estas firmas en el país y definiendo un conjunto de criterios que constituyen los fundamentos de su validez jurídica.

7) No discriminación del mensaje de datos firmado electrónicamente. Garantiza la fuerza ejecutoria, el efecto o la validez jurídica de una firma electrónica que no sea cuestionado por el solo motivo de que se presente bajo la forma de mensaje de datos.

8) Libertad contractual. Permite a las partes convenir la modalidad de sus transacciones, es decir, si aceptan o no las firmas electrónicas.

9) Responsabilidad. Se excluye la responsabilidad siempre que el sujeto pueda demostrar que ha tomado las diligencias necesarias según las circunstancias. Los Proveedores de Servicios de Certificación Electrónica pueden limitar su responsabilidad, incluyendo en los certificados que emitan las restricciones, condiciones y límites establecidas para su utilización.

Otra característica relevante de este Decreto-Ley es el establecimiento de definiciones de índole tecnológica que permiten una adecuada interpretación de sus normas, para así lograr una óptima aplicación de sus disposiciones.

Como elemento de suma importancia, el Decreto-Ley hace especial mención al Estado para que utilice los mecanismos pertinentes previstos en él, es indispensable que éste asuma el liderazgo en la promoción y uso de estas tecnologías. El sector gubernamental, como el resto de los agentes que participan en el desarrollo educativo, económico y social, necesita obtener y consolidar información de manera segura e inmediata, debido a que la realidad nacional y mundial evoluciona a un ritmo cada vez más rápido, por lo que es necesario disponer de información oportuna de la gestión de los distintos organismos gubernamentales. Esto incidirá determinantemente en la automatización de los procesos, la calidad de los servicios públicos, en el ahorro de recursos informáticos y presupuestarios y una mayor transparencia de la gestión de los organismos del Estado; como consecuencia lógica de lo expuesto, el ciudadano percibirá que las acciones del Estado estarán más cerca de sus necesidades y más abierta a sus observaciones.

En virtud de ello, se hace necesario que se consolide "El Gobierno Electrónico", que incluye todas aquellas actividades basadas en las modernas tecnologías de información, en particular Internet, que el Estado desarrollará para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y proveer a las acciones del gobierno de un marco mucho más ágil y transparente que el actual. Mediante la implementación del gobierno electrónico el ciudadano venezolano o extranjero tiene acceso, desde cualquier lugar del mundo, a la información sobre el funcionamiento y gestión de cada uno de los entes estatales y gubernamentales del país, la utilidad de estas tecnologías y de este Decreto-Ley que las hace más seguras, aumenta exponencialmente día a día.

Este marco legal y técnico que adopta el país para el desarrollo de la firma electrónica es compatible con el que ya existe en otros países. La aplicación de criterios legales diferentes a los aplicados en otros países en cuanto a los efectos legales de la firma electrónica y cualquier diferencia en los aspectos técnicos, en virtud de los cuales las firmas electrónicas son consideradas seguras, resultaría perjudicial para el desarrollo futuro de las relaciones y en especial del comercio electrónico que es una modalidad mercantil que está creciendo y englobando transacciones de todo tipo a nivel mundial y, por consiguiente, para el crecimiento económico del país y su incorporación a los mercados globales.

Debido a la evolución acelerada de la tecnología, los países con legislaciones más recientes sobre el tema, han optado al igual que el nuestro, por proyectos simples, tecnológicamente neutros y dinámicos, en los cuales se mantienen los grandes aciertos de modelos anteriores (aplicación indistinta a todo tipo de actos y contratos, tanto en el sector público como en el privado y la homologación con los documentos en formato tradicional). El mecanismo adoptado ha sido la elaboración de normas legales de carácter general, que validan y homologan los actos y contratos celebrados por estos medios, y que contienen provisiones reglamentarias para su implementación. Con los elementos básicos principales contenidos en este Decreto-Ley se brinda seguridad y certeza jurídica a las comunicaciones, transacciones, actos y negocios electrónicos que utilicen los mecanismos previstos en él.

HUGO CHAVEZ FRIAS
Presidente de la República

En ejercicio de la atribución que le confiere el numeral 8 del artículo 236 de la Constitución de la República Bolivariana de Venezuela, en concordancia con el artículo 1, numeral 5, literal b) de la Ley que Autoriza al Presidente de la República para dictar Decretos con Fuerza de Ley en las Materias que se delegan, en Consejo de Ministros,

DICTA

el siguiente

DECRETO CON FUERZA DE LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRONICAS

CAPITULO I
AMBITO DE APLICACION Y DEFINICIONES

Objeto y Aplicabilidad del Decreto-Ley

Artículo 1°: El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas.

La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Definiciones

Artículo 2°: A los efectos del presente Decreto-Ley, se entenderá por:

Persona: Todo sujeto jurídicamente hábil, bien sea natural, jurídica, pública, privada, nacional o extranjera, susceptible de adquirir derechos y contraer obligaciones.
Mensajes de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
Emisor: Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.
Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Signatario: Es la persona titular de una Firma Electrónica o Certificado Electrónico.
Destinatario: Persona a quien va dirigido el Mensaje de Datos.
Proveedor de Servicios de Certificación: Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley.
Acreditación: Es el titulo que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en este Decreto-Ley.
Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.
Sistema de Información: Aquel utilizado para generar, procesar o archivar de cualquier forma Mensajes de Datos.
Usuario: Toda persona que utilice un sistema de información.
Inhabilitación Técnica: Es la incapacidad temporal o permanente del Proveedor de Servicios de Certificación que impida garantizar el cumplimiento de sus servicios, así como, cumplir con los requisitos y condiciones establecidos en este Decreto-Ley para el ejercicio de sus actividades.

El Reglamento del presente Decreto-Ley podrá adaptar las definiciones antes señaladas a los desarrollos tecnológicos que se produzcan en el futuro. Así mismo, podrá establecer otras definiciones que fueren necesarias para la eficaz aplicación de este Decreto-Ley.

Adaptabilidad del Decreto-Ley

Artículo 3°: El Estado adoptará las medidas que fueren necesarias para que los organismos públicos puedan desarrollar sus funciones, utilizando los mecanismos descritos en este Decreto-Ley.

CAPITULO II
DE LOS MENSAJES DE DATOS

Eficacia Probatoria

Artículo 4°: Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Sometimiento a la Constitución y a la Ley

Artículo 5°: Los Mensajes de Datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal.

Cumplimiento De Solemnidades Y Formalidades

Artículo 6°: Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica.

Integridad del Mensaje de Datos

Artículo 7°: Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Constancia por escrito del Mensaje De Datos

Artículo 8°: Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.

Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguientes condiciones:
1. Que la información que contengan pueda ser consultada posteriormente.
2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
3. Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo.

CAPITULO III
DE LA EMISION Y RECEPCION DE LOS MENSAJES DE DATOS

Verificación de la Emisión del Mensaje de Datos

Artículo 9°: Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensajes de Datos proviene del Emisor, cuando éste ha sido enviado por:

1. El propio Emisor.
2. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.
3. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente.

Oportunidad de la Emisión

Artículo 10: Salvo acuerdo en contrario entre las partes, el Mensaje de Datos se tendrá por emitido cuando el sistema de información del Emisor lo remita al Destinatario.

Reglas para la determinación de la Recepción

Artículo 11: Salvo acuerdo en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará conforme a las siguientes reglas:

1. Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.
2. Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de Datos en un sistema de información utilizado regularmente por el Destinatario.

Lugar de Emisión y Recepción

Artículo 12: Salvo prueba en contrario, el Mensaje de Datos se tendrá por emitido en el lugar donde el Emisor tenga su domicilio y por recibido en el lugar donde el Destinatario tenga el suyo.

Del Acuse de Recibo

Artículo 13: El Emisor de un Mensaje de Datos podrá condicionar los efectos de dicho mensaje a la recepción de un acuse de recibo emitido por el Destinatario.

Las partes podrán determinar un plazo para la recepción del acuse de recibo. La no recepción de dicho acuse de recibo dentro del plazo convenido, dará lugar a que se tenga el Mensaje de Datos como no emitido.

Cuando las partes no establezcan un plazo para la recepción del acuse de recibo, el Mensaje de Datos se tendrá por no emitido si el Destinatario no envía su acuse de recibo en un plazo de veinticuatro (24) horas a partir de su emisión.

Cuando el Emisor reciba el acuse de recibo del Destinatario conforme a lo establecido en el presente artículo, el Mensaje de Datos surtirá todos sus efectos.

Mecanismos y Métodos para el Acuse de Recibo

Artículo 14: Las partes podrán acordar los mecanismos y métodos para el acuse de recibo de un Mensaje de Datos. Cuando las partes no hayan acordado que para el acuse de recibo se utilice un método determinado, se considerará que dicho requisito se ha cumplido cabalmente mediante:

1. Toda comunicación del Destinatario, automatizada o no, que señale la recepción del Mensaje de Datos.
2. Todo acto del Destinatario que resulte suficiente a los efectos de evidenciar al Emisor que ha recibido su Mensaje de Datos.

Oferta y Aceptación en los Contratos

Artículo 15: En la formación de los contratos, las partes podrán acordar que la oferta y aceptación se realicen por medio de Mensajes de Datos.

CAPITULO IV
DE LAS FIRMAS ELECTRONICAS

Validez y Eficacia de la Firma Electrónica. Requisitos

Artículo 16: La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:

1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
3. No alterar la integridad del Mensaje de Datos.

A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Efectos Jurídicos. Sana Crítica

Artículo 17: La Firma Electrónica que no cumpla con los requisitos señalados en el artículo anterior no tendrá los efectos jurídicos que se le atribuyen en el presente Capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

La Certificación

Artículo 18: La Firma Electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16.

Obligaciones del Signatario

Artículo 19.:El Signatario de la Firma Electrónica tendrá las siguientes obligaciones:

Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.
Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello.

El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

CAPITULO V
DE LA SUPERINTENDENCIA DE SERVICIOS
DE CERTIFICACION ELECTRONICA

Creación de la Superintendencia

Artículo 20: Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Objeto de la Superintendencia

Artículo 21: La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar, en los términos previstos en este Decreto-Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

Competencias de la Superintendencia

Artículo 22: La Superintendencia de Servicios de Certificación Electrónica tendrá las siguientes competencias:

1. Otorgar la acreditación y la correspondiente renovación a los Proveedores de Servicios de Certificación una vez cumplidas las formalidades y requisitos de este Decreto-Ley, sus reglamentos y demás normas aplicables.
2. Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.
3. Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores

de Servicios de Certificación públicos o privados.
4. Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.
5. Supervisar las actividades de los Proveedores de Servicios de Certificación conforme a este Decreto-Ley, sus reglamentos y las normas y procedimientos que establezca la Superintendencia en el cumplimiento de sus funciones.
6. Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.
7. Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.
8. Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.
9. Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.
10. Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.
11. Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.
12. Requerir de los Proveedores de Servicios de Certificación o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.
13. Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificados y sus usuarios, cuando ello sea solicitado por las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige esta materia.
14. Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.
15. Presentar un informe anual sobre su gestión al Ministerio de adscripción.
16. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.
17. Imponer las sanciones establecidas en este Decreto-Ley.
18. Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.
19. Las demás que establezcan la ley y los reglamentos.

Ingresos de la Superintendencia

Artículo 23: Son ingresos de la Superintendencia de Servicios de Certificación Electrónica:

1. Los recursos que le sean asignados en la Ley de Presupuesto a través del Ministerio de Ciencia y Tecnología.
2. Los provenientes de su gestión conforme a lo establecido en esta Ley.
3. Cualquier otro ingreso permitido por ley.

De las Tasas

Artículo 24: La Superintendencia de Servicios de Certificación Electrónica cobrará las siguientes tasas:

1. Por la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de un mil unidades tributarias (1.000 U.T.).
2. Por la renovación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).
3. Por la cancelación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).
4. Por la autorización que se otorgue a los Proveedores de Servicios de Certificación debidamente acreditados en relación a la garantía de los Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros, conforme a lo establecido en el artículo 44 del presente Decreto-Ley, se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

Los Proveedores de Servicios de Certificación constituidos por entes públicos estarán exentos del pago de las tasas previstas en este artículo.

Mecanismos de Control

Artículo 25: La Contraloría Interna del Ministerio de Ciencia y Tecnología, ejercerá las funciones de control, vigilancia y fiscalización de los ingresos, gastos y bienes públicos sobre este servicio autónomo, de conformidad con la ley que regula la materia.

De la Supervisión

Artículo 26: La Superintendencia de Servicios de Certificación Electrónica supervisará a los Proveedores de Servicios de Certificación con el objeto de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz a sus usuarios. A tal efecto, podrá directamente o a través de expertos, realizar las inspecciones y auditorias que fueren necesarias para comprobar que los Proveedores de Servicios de Certificación cumplen con tales requerimientos.

Medidas para garantizar la Confiabilidad

Artículo 27: La Superintendencia de Servicios de Certificación Electrónica podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los Proveedores de Servicios de Certificación. A tal efecto, podrá ordenar, entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el Proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.

Designación del Superintendente

Artículo 28: La Superintendencia de Servicios de Certificación Electrónica estará a cargo de un Superintendente, será de libre designación y remoción del Ministro de Ciencia y Tecnología.

Requisitos para ser Superintendente

Artículo 29: El Superintendente de Servicios de Certificación Electrónica, debe reunir los siguientes requisitos:

1. Ser venezolano.
2. De reconocida competencia técnica y profesional para el ejercicio de sus funciones.

No podrá ser Superintendente, los miembros directivos, agentes, comisarios, administradores o accionistas de empresas o instituciones sometidas al control de la Superintendencia. Tampoco podrá ejercer tal cargo el que tenga parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad con personas naturales también sometidas al control de la Superintendencia.

Atribuciones del Superintendente

Artículo 30: Son atribuciones del Superintendente:

1. Dirigir el Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.
2. Suscribir los actos y documentos relacionados con las materias especificadas en el artículo 22 de este Decreto-Ley.
3. Administrar los recursos e ingresos del Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.
4. Celebrar previa delegación del Ministro de Ciencia y Tecnología, convenios con organismos públicos o privados, nacionales e internacionales, derivados del cumplimiento de las atribuciones que corresponden a la Superintendencia de Servicios de Certificación Electrónica.
5. Elaborar el proyecto de presupuesto anual, de conformidad con las previsiones legales correspondientes.
6. Proponer escalas especiales de remuneración para el personal de la Superintendencia, de conformidad con las disposiciones legales aplicables.
7. Presentar al Ministro de Ciencia y Tecnología el Proyecto de Reglamento Interno.
8. Celebrar previa delegación del Ministro de Ciencia y Tecnología, los contratos de trabajo y de servicios de personal, que requiera la Superintendencia de Servicios de Certificación Electrónica para su funcionamiento.
9. Elaborar anualmente la memoria y cuenta de la Superintendencia de Servicios de Certificación Electrónica.
10. Las demás que le sean asignadas por el Ministro de Ciencia y Tecnología.

CAPITULO VI
DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACION

Requisito para ser Proveedor

Artículo 31: Podrán ser Proveedores de Servicios de Certificación, las personas, que cumplan y mantengan los siguientes requisitos:

1. La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.
2. La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.
3. Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.
4. Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.
5. Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación .
6. En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.
7. Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.
8. Las demás que señale el reglamento de este Decreto-Ley.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

De la Acreditación

Artículo 32: Los Proveedores de Servicios de Certificación presentarán ante la Superintendencia de Servicios de Certificación Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo 31. La Superintendencia de Servicios de Certificación Electrónica, previa verificación de tales documentos, procederá a recibir y procesar dicha solicitud y deberá pronunciarse sobre la acreditación del Proveedor de Servicios de Certificación, dentro de los veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud.

Una vez aprobada la solicitud del Proveedor de Servicios de Certificación, éste presentará, a los fines de su acreditación, garantías que cumplan con los siguientes requisitos:

1. Ser expedidas por una entidad aseguradora o bancaria autorizada para operar en el país, conforme a las disposiciones que rigen la materia.
2. Cubrir todos los perjuicios contractuales y extracontractuales de los signatarios y terceros de buena fe derivados de actuaciones dolosas, culposas u omisiones atribuibles a los administradores, representantes legales o empleados del Proveedor de Servicios de Certificación.

El Proveedor de Servicios de Certificación deberá mantener vigente la garantía aquí solicitada por el tiempo de vigencia de su acreditación. El incumplimiento de este requisito dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica.

Negativa de la Acreditación

Artículo 33: La Superintendencia de Servicios de Certificación Electrónica podrá negar la solicitud a que se refiere el artículo anterior, en caso que el solicitante no reúna los requisitos señalados en este Decreto-Ley y sus reglamentos.

Actividades de los Proveedores de Servicios de Certificación

Artículo 34: Los Proveedores de Servicios de Certificación realizarán entre otras, las siguientes actividades:

1. Proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos.
2. Ofrecer o facilitar los servicios de creación de Firmas Electrónicas.
3. Ofrecer servicios de archivo cronológicos de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación.
4. Ofrecer los servicios de archivo y conservación de mensajes de datos.
5. Garantizar Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros.
6. Las demás que se establezcan en el presente Decreto-Ley o en sus reglamentos.

Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas Electrónicas que certifiquen, y la titularidad que sobre ellas tengan sus Signatarios.

Obligaciones de los Proveedores

Artículo 35: Los Proveedores de Servicios de Certificación tendrán las siguientes obligaciones:

1. Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.
2. Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.
3. Verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico.
4. Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.
5. Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.
6. Informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su pagina en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.
7. Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.
8. Garantizar la adopción de las medidas necesarias para evitar la falsificación de

Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.
9. Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos.
10. Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su Inhabilitación Técnica.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la suspensión de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones establecidas en el presente Decreto-Ley.

La Contraprestación del Servicio

Artículo 36: La contraprestación por los servicios que los Proveedores de Servicios de Certificación presten, estará sujeta a las reglas de la oferta y la demanda.

Notificación del Cese de Actividades

Artículo 37: Cuando los Proveedores de Servicios de Certificación decidan cesar en sus actividades, lo notificarán a la Superintendencia de Servicios de Certificación Electrónica, al menos con treinta (30) días de anticipación a la fecha de cesación.

En el caso de Inhabilitación Técnica, el Proveedor de Servicios de Certificación notificará inmediatamente a la Superintendencia de Servicios de Certificación Electrónica.

Recibida cualesquiera de las notificaciones señaladas en este artículo, la Superintendencia de Servicios de Certificación Electrónica emitirá un acto por el cual se declare públicamente la cesación de actividades del Proveedor de Servicios de Certificación como prestador de ese servicio, sin perjuicio de las investigaciones que pueda realizar a fin de determinar las causas que originaron el cese de las actividades del Proveedor, y las medidas que fueren necesarias adoptar con el objeto de salvaguardar los derechos de los usuarios. En ese acto la Superintendencia podrá ordenar al Proveedor que realice los trámites que considere necesarios para hacer del conocimiento público la cesación de esas actividades, y para garantizar la conservación de la información que fuere de interés para sus usuarios y el público en general.

En todo caso, el cese de las actividades de un Proveedor de Servicios de Certificación conllevará su retiro del registro llevado por la Superintendencia de Servicios de Certificación Electrónica.

CAPITULO VII
CERTIFICADOS ELECTRONICOS

Garantía de la Autoría de la Firma Electrónica

Artículo 38: El Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

Vigencia del Certificado Electrónico

Artículo 39: El Proveedor de Servicios de Certificación y el Signatario, de mutuo acuerdo, determinarán la vigencia del Certificado Electrónico.

Cancelación

Artículo 40: La cancelación de un Certificado Electrónico procederá cuando el Signatario así lo solicite a su Proveedor de Servicios de Certificación. Dicha cancelación no exime al Signatario de las obligaciones contraídas durante la vigencia del Certificado, conforme a lo previsto en este Decreto-Ley.

El Signatario estará obligado a solicitar la cancelación del Certificado Electrónico cuando tenga conocimiento del uso indebido de su Firma Electrónica. Si el Signatario en conocimiento de tal situación no solicita dicha cancelación, será responsable por los daños y perjuicios sufridos por terceros de buena fe como consecuencia del uso indebido de la Firma Electrónica certificada mediante el correspondiente Certificado Electrónico.

Suspensión Temporal Voluntaria

Artículo 41: El Signatario podrá solicitar la suspensión temporal del Certificado Electrónico, en cuyo caso su Proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el Signatario.

Suspensión o Revocatoria Forzosa

Artículo 42: En los contratos que celebren los Proveedores de Servicios de Certificación con sus usuarios, se deberán establecer como causales de suspensión o revocatoria del Certificado Electrónico de la Firma Electrónica, las siguientes:

1. Sea solicitado por una autoridad competente de conformidad con la ley.
2. Se compruebe que alguno de los datos del Certificado Electrónico proporcionado por el Proveedor de Servicios de Certificación es falso.
3. Se compruebe el incumplimiento de una obligación principal derivada del contrato celebrado entre el Proveedor de Servicios de Certificación y el Signatario.
4. Se produzca una Quiebra Técnica del sistema de seguridad del Proveedor de Servicios de Certificación que afecte la integridad y confiabilidad del certificado contentivo de la Firma Electrónica.

Así mismo, se preverá en los referidos contratos que los Proveedores de Servicios de Certificación podrán dejar sin efecto la suspensión temporal del Certificado Electrónico de una Firma Electrónica al verificar que han cesado las causas que originaron dicha

suspensión, en cuyo caso el Proveedor de Servicios de Certificación correspondiente estará en la obligación de habilitar de inmediato el Certificado Electrónico de que se trate.

La vigencia del Certificado Electrónico cesará cuando se produzca la extinción o incapacidad absoluta del Signatario

Contenido de los Certificados Electrónicos

Artículo 43: Los Certificados Electrónicos deberán contener la siguiente información:

1. Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.
2. El código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica.
3. Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.
4. Las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico.
5. La Firma Electrónica del Signatario.
6. Un serial único de identificación del Certificado Electrónico.
7. Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

Certificados Electrónicos Extranjeros

Artículo 44: Los Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado. Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

CAPITULO VIII
DE LAS SANCIONES

A los Proveedores de Servicios de Certificación

Artículo 45: Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando incumplan las obligaciones que les impone el artículo 35 del presente Decreto-Ley.

Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando dejen de cumplir con alguno de los requisitos establecidos en el artículo 31 del presente Decreto-Ley.

Las sanciones serán impuestas en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes o atenuantes existentes.

Circunstancias Agravantes y Atenuantes

Artículo 46: Son circunstancias agravantes:

1. La reincidencia y la reiteración.
2. La gravedad del perjuicio causado al Usuario.
3. La gravedad de la infracción.
4. La resistencia o reticencia del infractor para esclarecer los hechos.

Son circunstancias atenuantes:

1. No haber tenido la intención de causar el hecho imputado de tanta gravedad.
2. Las que se evidencien de las pruebas aportadas por el infractor en su descargo.

En el proceso se apreciará el grado de la culpa para agravar o atenuar la pena.

Prescripción de las Sanciones

Artículo 47: Las sanciones aplicadas prescriben por el transcurso de tres (3) años, contados a partir de la fecha de notificación al infractor.

Falta de Acreditación

Artículo 48: Serán sancionadas con multa de dos mil (2000) a cinco mil (5000) Unidades Tributarias (U.T.), las personas que presten los servicios de Proveedores de Servicios de Certificación previstos en este Decreto-Ley, sin la acreditación de la Superintendencia de Servicios de Certificación Electrónica, alegando tenerla.

Procedimiento Ordinario

Artículo 49: Para la imposición de las multas previstas en los artículos anteriores, la Superintendencia de Servicios de Certificación Electrónica aplicará el procedimiento administrativo ordinario previsto en la Ley Orgánica de Procedimientos Administrativos.

CAPITULO X
DISPOSICIONES FINALES

Primera: El presente Decreto-Ley entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Segunda: Los procedimientos, trámites y recursos contra los actos emanados de la Superintendencia de Servicios de Certificación Electrónica, se regirán por lo previsto en la Ley Orgánica de Procedimientos Administrativos.

Tercera: Sin limitación de otros que se constituyan, el Estado creará un Proveedor de Servicios de Certificación de carácter público, conforme a las normas del presente Decreto-Ley. El Presidente de la República determinará la forma y adscripción de este Proveedor de Servicios de Certificación.

Cuarta: La Administración Tributaria y Aduanera adoptará las medidas necesarias para ejercer sus funciones utilizando los mecanismos descritos en este Decreto-Ley, así como para que los contribuyentes puedan dar cumplimiento a sus obligaciones tributarias mediante dichos mecanismos.

Dado en Caracas, a los diez días del mes de febrero de dos mil uno. Año 190º de la Independencia y 141º de la Federación.
(L.S.)

HUGO CHAVEZ FRIAS