LEY DE FIRMA ELECTRÓNICA

LEY N°. 729, aprobada el 01 de julio de 2010

Publicada en La Gaceta, Diario Oficial N°. 165 del 30 de agosto de 2010

El Presidente de la República de Nicaragua

A sus habitantes, Sabed:

Que,

LA ASAMBLEA NACIONAL

Ha ordenado la siguiente:

LEY DE FIRMA ELECTRÓNICA

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1 Objeto de la Ley.
La presente Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica y a los certificados digitales 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.

Art. 2 Ámbito de Aplicación.
Las disposiciones de la presente Ley serán aplicadas dentro del territorio nacional a todos los actos o contratos en que se utilice firma electrónica en el contexto de las actividades no comerciales y comerciales, que garanticen su autenticidad e integridad de los documentos electrónicos.

Art. 3 Definiciones:
Para los fines de la presente Ley se entiende por:

Acreditación voluntaria: Autorización otorgada por el organismo público encargado de su acreditación y supervisión, a petición del proveedor al que se beneficie, y que establece los derechos y obligaciones específicas para la prestación de servicios.

Certificado: Certificación electrónica que vincula unos datos de verificación de firma a

una persona y confirma la identidad de esta.

Certificado de firma electrónica: Es el documento electrónico firmado electrónicamente cuyos datos son vinculados a su titular, y suministrado por un proveedor de servicios de certificación.

Certificado digital: Certificación electrónica que da fe sobre los datos que identifican a quien posee la clave pública de un criptograma.

Certificador: La entidad proveedora de servicios de certificación de firma electrónica.

Clave criptográfica: Aquella que se utiliza en un criptosistema asimétrico para acceder a un documento con firma electrónica.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar electrónicamente y su correspondiente clave pública para verificar dicha firma electrónica.

Datos de creación de firma: Son los datos únicos, códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Dispositivos de creación de firma: Es un mecanismo que sirve para aplicar los datos de creación de firma.

Datos de verificación de firma: Son los datos, códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Dispositivo de verificación de firma: Es un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de firma.

Documento electrónico: Toda información generada, transferida, comunicada o archivada, por medios electrónicos, ópticos u otros análogos.

Encriptar: Es el acto de utilizar una clave única antes de intercambiar información.

Firma electrónica: Son datos electrónicos integrados en un mensaje de datos o lógicamente asociados a otros datos electrónicos, que puedan ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de datos.

Firma electrónica certificada: Es la que permite identificar al titular y ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que vinculada al mismo y a los datos a los que se refiere, permite que sea detectable cualquier modificación ulterior a estos.

Mensaje de datos: Es la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

Producto de firma electrónica certificada: El programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas.

Proveedor de servicios de certificación: Entidades que otorgan, registran, mantienen y publican los certificados de firma electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas que pueden prestar otros servicios relacionados con la firma electrónica.

Titular: Es la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona que representa.

Art. 4 Interpretación de la Ley.
En la interpretación de la presente Ley se tendrá en cuenta los métodos aceptados por el derecho común, así como las recomendaciones de organismos multilaterales en la materia, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Art. 5 Requisitos de Validez de la Firma Electrónica Certificada. Una firma electrónica certificada es válida si cumple los siguientes requisitos:

1. Que los datos de creación de firma correspondan exclusivamente al titular;

2. Que el certificado reconocido en que se base, haya sido expedido por un proveedor de servicios de certificación acreditado; y

3. Cuando el dispositivo seguro de creación de firma provenga de un proveedor de servicios de certificación acreditado.

Art. 6 Efectos Jurídicos de la Firma Electrónica.
La firma electrónica certificada tendrá el mismo valor jurídico que la firma manuscrita. Será admisible como medio de prueba en el proceso judicial o administrativo, valorándose ésta, según los criterios de apreciación establecidos en las leyes de la materia.

Cuando la ley exija la firma manuscrita de una persona, ese requisito quedará cumplido con una firma electrónica certificada. Se exceptúan los casos siguientes:

1. Actos jurídicos del derecho de familia;

2. Actos personalísimos en general;

3. Disposiciones por causa de muerte; y

4. Aquellos actos que deban ser realizados bajo las formalidades exigidas por la Ley de la materia o por aquellos acuerdos entre las partes.

Art. 7 Extinción de la Firma Electrónica.
La firma electrónica se extinguirá por las siguientes circunstancias:

1. A solicitud de su titular;

2. Fallecimiento o incapacidad definitiva de su titular;

3. Por cese de la actividad del proveedor de servicios de certificación, en el caso de la firma electrónica certificada;

4. Disolución o liquidación de la persona jurídica, titular de la firma; y

5. Por causa judicial que así lo declare.

La extinción de la firma electrónica no releva de las obligaciones contraídas en el ámbito civil, administrativo, comercial, laboral y penal.

CAPÍTULO II

DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Art. 8 Requisitos de Validez de los Certificados de Firma Electrónica.
Los certificados de firma electrónica deberán cumplir con los siguientes requisitos de validad mínimos:

1. Indicar que el certificado se expide como certificado electrónico;

2. Identificar al proveedor de servicios de certificación y el país en que se encuentra establecido;

3. Contener el nombre y los apellidos del titular o un seudónimo que conste como tal;

4. Designar un atributo específico del titular, en caso de que fuera significativo en función de la finalidad del certificado;

5. Contener los datos de verificación de firma que correspondan a los datos de

creación de firma bajo control del titular;

6. Estipular una indicación relativa al período de validez del certificado;

7. Contener el código identificativo del certificado;

8. Identificar la firma electrónica certificada del proveedor de servicios de certificación que expide el certificado;

9. Determinar los límites de uso del certificado; y

10. Establecer los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

La consignación en el certificado de cualquier otra información relativa al titular requerirá su consentimiento expreso, siempre y cuando no contravenga la presente Ley.

Art. 9 Mensajes de Datos Firmados Digitalmente.
Se entenderá que un mensaje de datos ha sido firmado digitalmente si el símbolo o la metodología adoptada por la parte cumplen con un procedimiento de autenticación o seguridad establecido por el reglamento de la presente Ley. Cuando una firma electrónica haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Art. 10 Periodo de Vigencia del Certificado de Firma Electrónica.
El certificado de firma electrónica es válido dentro del periodo por el cual fue establecido. Los certificados de firma electrónica quedarán sin efecto por el uso indebido, alteración, sustracción al proveedor autorizado, y además, por el incumplimiento de los requisitos de validez establecidos en la presente Ley.

Art. 11 Reconocimiento de Certificados Extranjeros.
Todo certificado de firma electrónica expedido en el extranjero será reconocido por la instancia rectora de acreditación de firma electrónica, en los mismos términos y condiciones establecidos en la presente Ley, su reglamento o convenios establecidos para tal fin.

El Reglamento a la presente Ley establecerá el procedimiento de reconocimiento.

CAPÍTULO III

USO DE LA FIRMA ELECTRÓNICA EN EL ESTADO

Art. 12 Uso de la Firma Electrónica en el Estado.

Se autoriza el uso de la firma electrónica certificada a las instituciones del Estado, entes desconcentrados, descentralizados y autónomos; para que emitan documentos electrónicos, celebren toda clase de contratos electrónicos en sus relaciones entre sí o con personas naturales o jurídicas.

Se exceptúan aquellos casos mediante el cual la Ley exija la solemnidad que no pueda ser satisfecha por la presente Ley.

Art. 13 Validez de los Actos, Contratos y Documentos Electrónicos.
Los actos, contratos y documentos electrónicos de las instituciones y entes referidos en el artículo anterior, suscritos mediante firma electrónica certificada, serán válidos y producirán los mismos efectos que los expedidos por firma manuscrita.

Art. 14 Notificación Electrónica.
Se autoriza a las Instituciones del Estado a realizar la notificación electrónica a las personas naturales o jurídicas, que sean parte de un proceso judicial o administrativo, en el domicilio del correo electrónico que designen para tal efecto los interesados y bajo su consentimiento.

En el caso de las personas jurídicas, la notificación se hará a su representante legal, abogado, fiscal o procurador designado en las oficinas que estos tuvieren o domicilio del correo electrónico que señalaren. El reglamento a la presente ley establecerá el procedimiento.

CAPÍTULO IV

DE LA ENTIDAD RECTORA

Art. 15 Entidad Rectora de Acreditación de Firma Electrónica.
Se designa a la Dirección General de Tecnología, conocida en adelante como DGTEC, dependencia del Ministerio de Hacienda y Crédito Público, como el ente rector del proceso de acreditación de firma electrónica.

La DGTEC, además de las potestades establecidas en las leyes de la materia, tendrá las siguientes:

1. Autorizar, inspeccionar y evaluar a los proveedores de servicios de certificación;

2. Cancelar o suspender la autorización otorgada a los proveedores de servicios de certificación;

3. Administrar el registro de proveedores de servicios de certificación, que para tal efecto se conformará dentro de la DGTEC;

4. Gestionar, por medio de la Dirección General de Ingresos, los ingresos provenientes

de las tasas y multas establecidas en la presente Ley;

5. Administrar y ejecutar su presupuesto de conformidad con la Ley de la materia;

6. Supervisar la prestación de los servicios que brinden los proveedores de servicios de certificación;

7. Aplicar las sanciones administrativas que correspondan;

8. Seleccionar y contratar al personal técnico administrativo para el desempeño de sus funciones de conformidad con la ley de la materia;

9. Solicitar la información a los proveedores de servicios de certificación;

10. Realizar auditorías técnicas a los proveedores de servicios de certificación; y

11. Velar por el cumplimiento de la presente Ley y su reglamento.

Art. 16 Confidencialidad.
El personal de la DGTEC, está obligado a guardar la confidencialidad de la información y custodia de los documentos que le entreguen los proveedores de servicios de certificación acreditados.

El Reglamento a la presente Ley establecerá las condiciones de confidencialidad.

Art. 17 Presupuesto.
Los ingresos que la DGTEC gestione por los servicios que brinde ante los proveedores acreditados de servicios de certificación o ante cualquier otra persona natural o Jurídica, donaciones y ayudas financieras nacionales e internacionales formarán parte del Tesoro Nacional de conformidad con la Ley No. 550, "Ley de Administración Financiera y del Régimen Presupuestario".

Art. 18 Tasas.
Se establecen las siguientes tasas por los servicios de la DGTEC:

1. Por la acreditación de la prestación de servicios de certificación por un término de cinco años, se cobrará una tasa de Un Mil Dólares de los Estados Unidos de América (US$ 1,000.00) o su equivalente en córdobas;

2. Por la renovación de la prestación de servicios de certificación, se cobrará una tasa de Quinientos Dólares de los Estados Unidos de América (US$ 500.00) o su equivalente en córdobas.

Art. 19 Facultades del Director.
El Director General de la DGTEC tendrá, sin perjuicio de las ya establecidas en el

Decreto Ejecutivo No. 71-98, "Reglamento de la Ley No. 290, Ley de Organización, Competencia y Procedimientos del Poder Ejecutivo", publicado en La Gaceta, Diario Oficial No. 205 del 30 de octubre de 1998, y sus posteriores reformas y adiciones, las siguientes facultades:

1. Representar legalmente a la DGTEC;

2. Suscribir los acuerdos, resoluciones y documentos relacionados con la entidad en mención;

3. Firmar los contratos del personal a su cargo;

4. Elaborar el informe de trabajo en la fecha correspondiente; y

5. Suscribir convenios e instrumentos de colaboración con organismos afines a la entidad públicos o privados, nacionales e internacionales.

CAPÍTULO V

DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Art. 20 Requisitos para ser Proveedor de Servicios de Certificación.
Para ser proveedor de servicios de certificación se requiere:

1. Un establecimiento permanente situado en territorio nicaragüense donde resida de forma continua o habitual, así como de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad;

2. Emplear personal que tenga los conocimientos especializados, la experiencia y las calificaciones necesarias correspondientes a los servicios prestados. En particular, el personal deberá poseer competencia en materia de gestión informática. Conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados. Tal personal deberá poner en práctica los procedimientos administrativos y de gestión adecuada y conformes a normas reconocidas internacionalmente;

3. Contar con sistemas y productos fiables que estén protegidos contra toda alteración a fin de garantizar la seguridad jurídica, técnica y criptográfica de los procedimientos con que trabajan; y la confidencialidad de la información;

4. Ser persona jurídica debidamente constituida e inscrita en el registro público mercantil;

5. Disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Ley, en particular para afrontar el riesgo de responsabilidad

Fuente: http://www.leybook.com/doc/11278

por daños y perjuicios, según valoración de la entidad rectora; y

6. Contratar a uno o varios notarios públicos con cinco años de experiencia profesional, a fin de que puedan dar fe pública sobre el cumplimiento de las obligaciones del proveedor de servicios en el momento del libramiento del certificado al titular.

Art. 21 Obligaciones de los Proveedores de Servicios de Certificación.
Los proveedores de servicios de certificación están obligados a:

1. Garantizar la utilización de un servicio expedito, seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

2. Garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

3. Comprobar, de conformidad con la legislación correspondiente, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;

4. Contratar un seguro apropiado para responder por los daños y perjuicios que ocasione ante el titular de la firma electrónica o ante terceros;

5. Registrar toda la información pertinente relativa a un certificado reconocido durante un periodo de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

6. Antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, ante notario público con cinco años de experiencia profesional. Deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado;

7. Utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

a) Sólo personas autorizadas puedan hacer anotaciones y modificaciones;

b) Pueda comprobarse la autenticidad de la información;

Fuente: http://www.leybook.com/doc/11278

c) Los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado; y

d) El agente pueda detectar todos los cambios que pongan en entredicho los requisitos de seguridad mencionados.

Art. 22 Responsabilidades de los Proveedores de Servicios de Certificación.
Los proveedores de servicios de certificación, son responsables de:

1. Los daños y perjuicios que en el ejercicio de sus funciones ocasionen por la certificación u homologación de certificados de firma electrónica. En todo caso, deberán demostrar que actuaron con la debida diligencia, se exceptúan los daños ocasionados en el uso indebido o fraudulento de un certificado de firma electrónica. En ningún caso la responsabilidad proveniente de una certificación efectuada por un proveedor de servicio acreditado vinculará la responsabilidad pecuniaria del Estado;

2. Tomar medidas de seguridad efectivas contra la falsificación de certificados de firma electrónica y garantizar la confidencialidad de la información y resguardo de los documentos durante el proceso de generación de datos de creación de firma; y

3. No almacenar ni copiar los datos de creación de firma electrónica de la persona a la que el proveedor de servicios de certificación ha brindado servicios de gestión de claves.

Art. 23 Requisitos de los Dispositivos Seguros de Creación de Firma Electrónica.
Los dispositivos seguros de creación de firma electrónica tendrán los siguientes requisitos mínimos:

1. Que los datos utilizados para la generación de firma sólo puedan producirse una vez en la práctica y se garantice razonablemente su secreto;

2. Que exista la seguridad razonable de que los datos utilizados para la generación de firma no puedan ser hallados por deducción y que la firma esté protegida contra la falsificación mediante la tecnología existente en la actualidad; y

3. Que los datos utilizados para la generación de firma puedan ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.

Los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma.

Art. 24 Requisitos para la Verificación Segura de Firma.
Durante el proceso de verificación de firma, se requiere lo siguiente:

1. Que los datos utilizados para verificar la firma correspondan a los datos mostrados al verificador;

2. Que la firma se verifique de forma fiable y el resultado de esa verificación figure correctamente;

3. Que el verificador pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados;

4. Que se verifiquen, de forma fiable, la autenticidad y la validez del certificado exigido al verificarse la firma;

5. Que figuren correctamente el resultado de la verificación y la identidad del firmante;

6. Que conste claramente la utilización de un seudónimo; y

7. Que pueda detectarse cualquier cambio pertinente relativo a la seguridad.

Art. 25 Protección de los Datos Personales.
Los datos personales del titular de la firma electrónica se protegerán en la presente Ley y su reglamento de la siguiente manera:

1. El tratamiento de los datos personales relacionados con los proveedores de servicios de certificación para el desarrollo de su actividad y el que realice el ente regulador que contiene la presente Ley, se sujeta a lo dispuesto en la Ley de la materia;

2. Los proveedores de servicios de certificación que expidan certificados de firma electrónica a los titulares solamente pueden recabar los datos personales de los titulares de los mismos y con su consentimiento expreso, con la exclusiva finalidad de expedir y mantener el certificado. En caso que haya expedido un certificado a un Titular, utilizando un seudónimo, deberán constatar su verdadera identidad y conservar la documentación que la acredite.

CAPÍTULO VI

DE LA ACREDITACIÓN DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Art. 26 De la Acreditación de los Proveedores de Servicios de Certificación.
La acreditación es el acto mediante el cual el proveedor de servicios de certificación es autorizado a funcionar como tal por la DGTEC, habiendo demostrado su capacidad técnica, infraestructura, recursos humanos y económicos, así como programas informáticos necesarios para otorgar los certificados en el plazo establecido en la

presente Ley y en su reglamento, permitiendo su inscripción en el registro que para tal efecto se constituya.

Art. 27 Procedimiento de Acreditación de los Proveedores de Servicios de Certificación.
El procedimiento de acreditación se llevará a cabo por medio de solicitud ante la DGTEC, la que adjuntará los requisitos establecidos en la presente Ley. La DGTEC, resolverá sobre dicha solicitud en un plazo de sesenta días hábiles a partir de la recepción de la solicitud del interesado. Si pasado el término establecido la DGTEC no se pronunciare, la solicitud se entenderá aceptada. En tal caso, el proceso de registro operará de mero derecho conforme a la solicitud con acuse de recibo en manos del interesado.

Otorgada la acreditación, el proveedor de servicios de certificación será inscrito en el Registro que se lleve para tal efecto por la DGTEC. El proveedor de servicios de certificación está obligado a informar a la DGTEC, en un plazo no mayor de tres días hábiles, de cualquier modificación de las condiciones que permitieron su acreditación.

Art. 28 Causas de Cancelación de la Autorización.
La DGTEC, podrá cancelar la autorización del proveedor de servicios de certificación en el registro, por las siguientes causas:

1. A solicitud del proveedor acreditado;

2. Por pérdida de las condiciones que motivaron su acreditación; e

3. Incumplimiento de las obligaciones establecidas en la presente Ley y su reglamento.

CAPÍTULO VII

DERECHOS Y OBLIGACIONES DEL TITULAR DE FIRMA ELECTRÓNICA

Art. 29 Derechos del Titular de Firma Electrónica.
El titular de firma electrónica tendrá los siguientes derechos:

1. A ser informado por el proveedor de servicios de certificación de todo lo relacionado con la creación y verificación de firma electrónica, así como de la prestación del Servicio;

2. A la confidencialidad en la información proporcionada a los proveedores de servicios de certificación;
3. A ser informado de los costos, uso, limitación de uso, procedimientos de reclamos en los servicios de certificación;

4. No transferir sus datos a otro proveedor de servicios de certificación sin su

consentimiento expreso;
5. Acceder al registro de proveedores acreditados que tendrá la DGTEC; y

6. Ser indemnizado y reclamar el seguro comprometido cuando corresponda.

Art. 30 Obligaciones del Titular de Firma Electrónica.
El titular de firma electrónica, tendrá las siguientes obligaciones:

1. Brindar datos exactos y completos;

2. Cuidar de manera responsable el mecanismo de seguridad para el funcionamiento del sistema de certificación que les proporcione el certificador; y

3. Actualizar sus datos o cancelarlos cuando estime conveniente.

CAPÍTULO VIII

INFRACCIONES Y SANCIONES

Art. 31 Infracciones.
Las Infracciones contenidas en la presente Ley y su reglamento, se clasifican en leves y graves.

Art. 32 Infracciones Leves.
Son infracciones leves:

1. La entrega incompleta de la información o fuera del término previsto, solicitada por la entidad rectora;

2. Emitir el certificado de firma electrónica sin llenar los requisitos totales de los datos;

3. Omitir el registro de los certificados expedidos;

4. Omitir la revocación en forma o tiempo de un certificado cuando corresponda hacerlo; e

5. Incumplir las normas dictadas por la entidad rectora.

Art. 33 Infracciones Graves.
Son infracciones graves:

1. La negligencia en la seguridad de los servicios de certificación;

2. No permitir la inspección u obstruir la realización de las mismas o auditorías técnicas por parte de la entidad rectora;

Fuente: http://www.leybook.com/doc/11278

3. Reincidir en la comisión de infracciones que dieran lugar a la sanción de suspensión;

4. Expedir certificados falsos;

5. La comisión de delitos en la prestación de servicio; y

6. Uso indebido del certificado de firma electrónica por omisiones, cuya responsabilidad es del proveedor de Servicios de certificación.

Art. 34 Establecimiento de Sanciones.
Para el establecimiento de las sanciones, se tomará en cuenta lo siguiente:

1. La gravedad de las infracciones cometidas, así como su reincidencia;

2. El daño causado o beneficio reportado al infractor;

3. El efecto social de la infracción.

Art. 35 Sanciones Administrativas.
La DGTEC, sin perjuicio de las responsabilidades civiles y penales que correspondan, impondrá a los proveedores de servicios de certificación, o a sus representantes legales, o administradores, las siguientes sanciones administrativas:

1. Amonestación escrita;

2. Multa de Cien Dólares a Diez Mil Dólares de los Estados Unidos de América o su equivalente en Córdobas;

3. Suspensión temporal de hasta dos años de la autorización de funcionamiento; y

4. Cancelación de la autorización para continuar operando como proveedora de servicios de certificación.

CAPÍTULO IX

DE LOS RECURSOS ADMINISTRATIVOS

Art. 36 De los Recursos Administrativos.
Los recursos administrativos que se interpongan ante la DGTEC, se tramitarán conforme lo establece la Ley No. 290, "Ley de Organización, Competencia y Procedimientos del Poder Ejecutivo", aprobada el 27 de marzo de 1998 y publicada en La Gaceta, Diario Oficial No. 102 del 3 de junio de 1998 y su reglamento.

Fuente: http://www.leybook.com/doc/11278

CAPITULO X

DISPOSICIONES TRANSITORIAS

Art. 37 Plazo para la Implementación de la Ley.
Se autoriza a las instituciones del Estado, entes desconcentrados, descentralizados y autónomos para que implementen la presente Ley dentro del plazo de un año calendario contado a partir de la entrada en vigencia de la misma.

CAPÍTULO XI

DISPOSICIONES FINALES

Art. 38 Reglamentación.
La presente Ley será reglamentada por el Presidente de la República dentro del plazo establecido en el numeral 10 del artículo 150 de la Constitución Política de la República de Nicaragua.

Art. 39 Vigencia.
Esta Ley entrará en vigencia a partir de su publicación en La Gaceta, Diario Oficial.

Dado en la ciudad de Managua, en la Sala de Sesiones de la Asamblea Nacional, el primero de julio del año dos mil diez. **Ing. René Núñez Téllez,** Presidente de la Asamblea Nacional. **Dr. Wilfredo Navarro Moreira,** Secretario de la Asamblea Nacional.

Por tanto. Téngase como Ley de la República. Publíquese y Ejecútese. Managua, diecisiete de Agosto del año dos mil diez. **DANIEL ORTEGA SAAVEDRA,** PRESIDENTE DE LA REPÚBLICA DE NICARAGUA.

Fuente: http://www.leybook.com/doc/11278