Reforma Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Decreto Ejecutivo N° 33018-MICIT, del 20 de marzo de 2006 publicado en el Diario Oficial La Gaceta Nº 77 del 21 de abril de 2006

Nº 34890-MICIT

EL PRESIDENTE DE LA REPÚBLICA

Y EL MINISTRO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Con fundamento en lo dispuesto en los artículos 140, incisos 3) y 18) y 146 de la Constitución Política; y el artículo 33 de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, N° 8454 del 30 de agosto del 2005.

Considerando:

I.-Que el Decreto Ejecutivo N° 33018-MICIT, del 20 de marzo del 2006, que es el Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, tiene por objeto reglamentar y dar cumplida ejecución a la Ley número 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos.

II.-Que el artículo 19 de la Ley N° 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, establece que la Dirección de Certificadores de Firma Digital será la encargada de establecer, vía reglamento, todos los requisitos, el trámite y las funciones de las personas que soliciten su registro ante la misma, fijando los requerimientos técnicos para el estudio, de acuerdo con la Ley N° 8279, de 2 de mayo de 2002, y las prácticas y los estándares internacionales.

III.-Que es necesario modificar algunas de las disposiciones contenidas en el Decreto Ejecutivo N° 33018-MICIT del 20 de marzo del 2006, con el propósito de actualizar los lineamientos y estándares establecidos de acuerdo con las buenas prácticas internacionales.

IV.-Que los ajustes propuestos se hacen con el fin de facilitar el avance y desarrollo de toda clase de transacciones y actos jurídicos, públicos o privados, así como ofrecer un trámite expedito y efectivo en la emisión de los certificados digitales y los documentos electrónicos. Por tanto;

EL PRESIDENTE DE LA REPÚBLICA

Y EL MINISTRO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES, DECRETAN

Reforma al Reglamento a la Ley de Certificados,

Firmas Digitales y Documentos Electrónicos,

Decreto Ejecutivo N° 33018-MICIT, del 20

de marzo de 2006, publicado en el

Diario Oficial La Gaceta Nº 77

del 21 de abril de 2006

Artículo 1º-Modifíquense los artículos 2 inciso 7), 30) y eliminar el inciso 39), 4 párrafo 2°, 5, 6 inciso 1), 11, 12 inciso 5), 13, 14 inciso 2) y 3), 15 párrafo 2° y eliminar párrafo 3°, 19 inciso 6), 20 inciso 4), 23, 24 párrafo 2°, 26 e inciso 2), 28 párrafo 2°, 29 inciso 5), 32 párrafo 2° y 36 del Decreto Ejecutivo N° 33018-MICIT, de 20 de marzo del 2006, que es el Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, para que en adelante se lean:

"Artículo 2°-**Definiciones.** Para los efectos del presente Reglamento, se entenderá por:

.

7)CERTIFICADO DIGITAL: Una estructura de datos creada y firmada digitalmente por un certificador, del modo y con las características que señalan este Reglamento, la Norma INTE /ISO 21188 versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities versión vigente – Webtrust, y las políticas que al efecto emita la DCFD, cuyo propósito primordial es posibilitar a sus suscriptores la creación de firmas digitales, así como la identificación personal en transacciones electrónicas. Sin perjuicio del concepto anterior, la DCFD podrá autorizar a los certificadores registrados la generación de certificados con propósitos diferentes o adicionales a los indicados.

30) LINEAMIENTOS TÉCNICOS: El conjunto de definiciones, requisitos y regulaciones de carácter técnico-informático, contenido en la Norma INTE /ISO 21188 versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities versión vigente – Webtrust y en las políticas que al efecto emita la DCFD.”

“Artículo 4º—**Incentivo de los mecanismos de gobierno electrónico.**

.

En la emisión de los reglamentos particulares a que se refieren los artículos 2º, inciso c) y 33 de la Ley, todas las dependencias públicas procurarán ajustar sus disposiciones a los principios de neutralidad tecnológica, accesibilidad, usabilidad y experiencia de usuario, seguridad tecnológica e interoperabilidad. En ningún caso se impondrán exigencias técnicas o jurídicas que impidan o dificulten injustificadamente la interacción con las oficinas públicas por medio de firmas o certificados digitales emitidos por un certificador registrado.”

“Artículo 5°—**Contenido y características.** El contenido, condiciones de emisión, suspensión, revocación y expiración de los certificados digitales, serán los que se señalan en la Norma INTE /ISO 21188 versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities versión vigente – Webtrust y las políticas que al efecto emita la DCFD.”

“Artículo 6°—**Tipos de certificados.**

.

1) Utilizar al menos un proceso de verificación y registro presencial (cara a cara) de sus suscriptores o mediante una autorización electrónica firmada digitalmente con un certificado de firma digital certificada vigente y emitido de acuerdo con la normativa.”

“Artículo 11. **Comprobación de idoneidad técnica y administrativa.** Para obtener la condición de certificador registrado, se requiere poseer idoneidad técnica y administrativa, certificada por un ente acreditado ante el ECA, de conformidad con el esquema de certificación para Autoridades Certificadoras del Sistema Nacional de Certificación Digital versión vigente, las políticas fijadas por la DCFD y los restantes requisitos que esa dependencia establezca, de acuerdo con su normativa específica.”

“Artículo 12.—**Formalidades de la solicitud.**

.

5) Declaración jurada que indique que cuenta con los requisitos para brindar el servicio de certificación digital acorde a los requerimientos de las normas INTE/ISO 21188 versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities versión vigente – Webtrust, INTE-ISO/IEC 17021 versión vigente, así como a las políticas dictadas por la DCFD (por ejemplo: personal calificado, con los conocimientos y experiencia necesarios para las labores que realizan, procedimientos de seguridad y de gestión apropiados, así como la infraestructura adecuada para realizar las actividades de certificación digital).”

“Artículo 13.— **Póliza de fidelidad.** La persona jurídica pública o privada, nacional o extranjera, deberán rendir una caución póliza de fidelidad que será utilizada para responder por las eventuales consecuencias civiles, contractuales y extracontractuales de su actividad. Esta póliza de fidelidad será expedida por una aseguradora que opere y se encuentre oficialmente registrada en el país. El monto –de acuerdo con la Ley- será fijado por la DCFD en consulta con una aseguradora que opere y se encuentre oficialmente registrada en el país el Instituto Nacional de Seguros, tomando en consideración los riesgos y responsabilidades inherentes en la labor de certificación digital.

Cuando la póliza de fidelidad esté sujeta a vencimiento, necesariamente deberá ser renovada por el interesado al menos dos meses antes de la fecha de expiración.”

“Artículo 14.—**Tramite de la solicitud.** Recibida la solicitud de inscripción, la DCFD procederá a:

.

2) Posteriormente, la DCFD estará facultada para que en caso necesario proceda a realizar una visita al domicilio, ya sea de manera presencial o virtual, donde se realizará la actividad de certificación digital, con el fin de constatar la veracidad de lo indicado en los documentos aportados por el solicitante.

3) En caso de resultar favorable la solicitud y resueltas las oposiciones que se indican en el artículo 15 de este Reglamento a favor del solicitante, se le prevendrá para que en el plazo de cinco días hábiles presente el comprobante de pago de la póliza de fidelidad señalada en el artículo 13 anterior.”

“Artículo 15.—**Oposiciones.**

.

Una vez vencido el plazo indicado y resueltas las posibles oposiciones, se le prevendrá al solicitante a fin de que aporte el pago respectivo de la póliza de fidelidad indicada en el artículo 13 de este Reglamento.”

“Artículo 20.—**Divulgación de datos.**

.

4) El resultado final más reciente de evaluación o auditoría de sus servicios.”

“Artículo 19.—**Funciones.** Los certificadores registrados tendrán las siguientes atribuciones y responsabilidades:

.

6) Mantener un repositorio electrónico, permanentemente accesible en línea y publicado en internet para posibilitar la consulta de la información pública relativa a los certificados digitales que haya expedido y de su estado actual, de la manera que se indique en los lineamientos técnicos.”

“Artículo 23.—**Responsabilidad.** La Dirección de Certificadores de Firma Digital -perteneciente al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones- será el órgano administrador y supervisor del sistema nacional de certificación digital. Tendrá el carácter de órgano de desconcentración máxima y las resoluciones dictadas en los asuntos de su competencia agotarán la vía administrativa.

La DCFD tendrá, de pleno derecho, el carácter de certificador raíz. No obstante, para garantizar una óptima efectividad en el cumplimiento de esta función, podrá gestionar el apoyo de otro órgano, entidad o empresa del Estado, a los efectos de que supla la infraestructura material y el personal idóneo necesarios para operar la raíz, debiendo acreditar un sistema de calidad para este proceso ante el ECA, para lo cual tendrá un plazo no mayor a tres años a partir de que la misma entre en operación completa.”

“Artículo 24.—**Funciones.**

.

La DCFD tendrá la responsabilidad de definir políticas y requerimientos para el uso de certificados digitales que deberán ser especificados en una Política de Certificados o acuerdos complementarios; en especial la DCFD será el emisor y el gestor de las políticas para el Sistema de Certificadores de Firma Digital, las cuales serán de acatamiento obligatorio.”

“Artículo 26.—**Jefatura.** El superior administrativo de la DCFD será el Director, quien será nombrado por el Ministro de Ciencia, Innovación, Tecnología y Telecomunicaciones y será un funcionario de confianza, de conformidad con el inciso g) del artículo 4, del Estatuto de Servicio Civil. El Director deberá declarar sus bienes oportunamente, de conformidad con lo establecido en la Ley Contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública.

.

2) Tener experiencia profesional en temas afines a la rama tecnológica.”

“Artículo 28.—**Comité Asesor de Políticas.**

.

Cada una de esas dependencias designará a un representante propietario y otro suplente, por períodos de dos años, reelegibles automáticamente y en forma indefinida salvo manifestación en contrario de la respectiva dependencia. Deberá tratarse en todos los casos de profesionales, graduados en materias afines y con experiencia demostrable en el tema, en el caso de las personas designadas por el Colegio de Abogados y Abogadas su perfil es para la colaboración en aspectos legales y notariales. El cargo será desempeñado en forma ad honórem.”

“Artículo 29.—**Funciones del Comité Asesor de Políticas.**

.

5) Funcionar como Comité para la preservación de la imparcialidad, conforme a los parámetros señalados en la norma INTE-ISO/IEC 17021 versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities versión vigente – Webtrust.”

“Artículo 32.—**Suspensión.**

.

En los casos del inciso a) del referido artículo, si al cabo del plazo de suspensión el certificador persiste en no renovar debidamente la póliza de fidelidad a pesar de la prevención que en ese sentido se le hará, se procederá conforme al artículo 30, inciso c) de la Ley, a efectos de declarar la revocatoria de la inscripción.”

“Artículo 36.—**Medios de ejecución.** Si el certificador sancionado no realiza oportunamente el pago a que estuviere obligado, se procederá a ejecutar la caución póliza de fidelidad por el monto respectivo. En tal caso (así como para el reclamo de cualquier saldo en descubierto que pudiera subsistir) se aplicará en lo pertinente lo dispuesto en los artículos 149 y 150 de la LGAP. La DCFD será el órgano competente para realizar las intimaciones de ley, así como para expedir el título ejecutivo, si corresponde.”

Artículo 2º-Adiciónense en los artículos 2 el inciso 1) y 43) y actualícese la numeración de los demás incisos; 7 inciso 4), 28 inciso 7) y 8) del Decreto Ejecutivo N° 33018-MICIT, de 20 de marzo del 2006, que es el Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, para que se lean de la siguiente manera:

"Artículo 2°-**Definiciones.** Para los efectos del presente Reglamento, se entenderá por:

1) AGENTE ELECTRONICO: Certificado de autenticación de persona jurídica; se suelen utilizar como parte de un proceso automático de autenticación (prueba de identidad) entre sistemas automatizados, en donde el dispositivo criptográfico que contiene las llaves asociadas al certificado está activo para que pueda trabajar en forma desatendida y de esta manera no requiera de intervención humana cada vez que se requiere de su uso.

43) SELLO ELECTRONICO: Firma digital certificada generada a partir de un certificado digital de sello electrónico de persona jurídica; se utilizan como parte de procesos automáticos de firma digital en donde, el dispositivo criptográfico que contiene las llaves asociadas al certificado está activado para que pueda trabajar en forma desatendida y de esta manera no requiera de intervención humana a la hora de realizar cada firma digital.”

“Artículo 7º—**Obligaciones de los usuarios**

**.**

4)Cumplir los procedimientos técnicos establecidos en la normativa vigente para el uso de los certificados digitales.”

“Artículo 28.—**Comité Asesor de Políticas.**

.

7) Dirección General de Archivo Nacional (DGAN)

8) Colegio de Abogados y Abogadas de Costa Rica”

Artículo 3º-Rige a partir de su publicación

Dado en la Presidencia de la República. -San José, a los once días del mes de febrero del dos mil veintidós