REGLAMENTO A LA LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS


MICIT
Ministerio de
Ciencia y Tecnología

Nº 33018

EL PRESIDENTE DE LA REPÚBLICA

Y EL MINISTRO DE CIENCIA Y TECNOLOGÍA

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, Nº 8454 del 30 de agosto del 2005.

Considerando:

1º—Que la sociedad de la información y del conocimiento se debe construir sobre la base de la confianza de los ciudadanos y sobre la garantía de la utilización de las tecnologías de la información y las comunicaciones en un doble plano: la protección y confidencialidad de los datos de carácter personal y la seguridad de las transacciones electrónicas.

2º—Que la Ley Nº 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, establece el marco jurídico general para la utilización transparente, confiable y segura en nuestro medio de los documentos electrónicos y la firma digital en las entidades públicas y privadas.

3º—Que el artículo 33 de dicha ley establece que el Poder Ejecutivo deberá reglamentarla ley en un plazo de 6 meses, regulación que debe servir para garantizar la disponibilidad de los sistemas e infraestructuras telemáticas, la seguridad y autenticidad de las transacciones, así como la confidencialidad e integridad de la información. Por tanto,

DECRETAN:

Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos

CAPÍTULO PRIMERO

Disposiciones generales

Artículo 1º—Propósito. El presente texto servirá para reglamentar y dar cumplida ejecución a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, número 8454 del 30 de agosto del 2005. Tendrá el carácter y la jerarquía de reglamento general, en los términos del artículo 6.1.d) de la Ley General de la Administración Pública, frente a los demás reglamentos particulares o autónomos en la materia.

Artículo 2º—Definiciones. Para los efectos del presente Reglamento, se entenderá por:

1) AUTENTICACIÓN: Verificación de la identidad de un individuo.

a. En el proceso de registro, es el acto de evaluar las credenciales de la entidad final (por ejemplo, un suscriptor) como evidencia de que realmente es quien dice ser.

b. Durante el uso, es el acto de comparar electrónicamente las credenciales y la identidad enviada (Ej., código de usuario y contraseña, certificado digital, etc.) con valores previamente almacenados para comprobar la identidad.

2) AUTENTICACIÓN MUTUA: Proceso mediante el cual dos entidades verifican su identidad en forma recíproca.

3) AUTENTICIDAD: La veracidad, técnicamente constatable, de la identidad del autor de un documento o comunicación. La autenticidad técnica no excluye el cumplimiento de los requisitos de autenticación o certificación que desde el punto de vista jurídico exija la ley para determinados actos o negocios.

4) AUTORIDAD DE REGISTRO (AR): Entidad delegada por el certificador registrado para la verificación de la identidad de los solicitantes y otras funciones dentro del proceso de expedición y manejo de certificados

digitales. Representa el punto de contacto entre el usuario y el certificador registrado.

5) BITÁCORAS DE AUDITORIA: Registro cronológico de las actividades del sistema, que son suficientes para habilitar la reconstrucción, revisión, y la inspección de la secuencia del entorno y las actividades secundarias o primarias para cada evento en la ruta de una transacción desde su inicio hasta la salida del resultado final.

6) CERTIFICACIÓN: Proceso de creación de un certificado de llave pública para un suscriptor.

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 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.

(Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

8) CERTIFICADO SUSPENDIDO: Cesación temporal o interrupción de la validez de un certificado.

9) CERTIFICADO VÁLIDO: Se refiere a aquel certificado que se encuentra activo, que ha sido emitido por un certificador registrado.

10) CERTIFICADOR: La persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales.

11) CERTIFICADOR RAÍZ: El nodo superior autocertificante de la jerarquía nacional de certificadores registrados.

12) CERTIFICADOR REGISTRADO: El certificador inscrito y autorizado por la Dirección de Certificadores de Firma Digital.

13) CERTIFICADOR PADRE: Certificador registrado que se encuentra en la posición inmediata superior con respecto a otro certificador registrado, en la jerarquía de certificadores.

14) CERTIFICADOR SUBORDINADO: Certificador registrado que se encuentra en la posición inmediata inferior con respecto a otro certificador registrado, en la jerarquía de certificadores.

15) COMPROMISO: Violación de la seguridad de un sistema, por haber ocurrido una divulgación no autorizada de información sensible.

16) CONTROL MÚLTIPLE: Condición mediante la cual dos o más partes, separada y confidencialmente, tienen la custodia de los componentes de una llave particular, pero que individualmente no tienen conocimiento de la llave resultante.

17) DATOS DE ACTIVACIÓN: Valores de datos (que no son las llaves), que son requeridos para operar los módulos criptográficos y que necesitan ser protegidos (ejemplo: PINs, frase clave, biométricos o llaves distribuidas manualmente).

18) DECLARACIÓN DE LAS PRÁCTICAS DE CERTIFICACIÓN (DPC): Declaración de las prácticas que utiliza el certificador para la emisión de los certificados (define el equipo, las políticas y los procedimientos que el certificador utiliza para satisfacer los requerimientos especificados en las políticas del certificado que son soportados por él).

19) DIRECCIÓN DE CERTIFICADORES DE FIRMA DIGITAL (DCFD): Dependencia del Ministerio de Ciencia y Tecnología, encargada de la administración y supervisión del sistema de certificación digital.

20) DISPOSITIVO O MODULO SEGURO DE CREACION DE FIRMAS (MSCF): Dispositivo que resguarda las claves y el certificado de un suscriptor, utilizado para generar su firma digital y que, al menos, garantiza:

a. Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;

b. Que existe una expectativa razonable de que los datos utilizados para la generación de la firma no pueden ser descubiertos por deducción y la firma está protegida contra falsificación por medio de la tecnología disponible a la fecha, siendo posible detectar cualquier alteración posterior; y,

c. Que los datos empleados en la generación de la firma pueden ser protegidos de modo fiable por el firmante legítimo, contra su utilización por cualesquiera terceros.

21) DOCUMENTO ELECTRÓNICO: Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático.

22) ENTE COSTARRICENSE DE ACREDITACIÓN (ECA): La dependencia pública a que se refiere la "Ley del Sistema Nacional para la Calidad", número 8279 de 2 de mayo del 2002.

23) ENTIDAD FINAL: Suscriptor del certificado.

24) FIRMA DIGITAL: Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

25) FIRMA DIGITAL CERTIFICADA: Una firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado.

26) INFRAESTRUCTURA DE LLAVE PÚBLICA (PKI por sus siglas en inglés): Se refiere a una estructura de hardware, software, personas, procesos y políticas que emplean tecnología de firma digital para proveer una asociación verificable entre una llave pública y un suscriptor específico que posee la llave privada correspondiente.

27) INTEGRIDAD: Propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión, o bien que -habiendo sido alterados posteriormente- lo fueron con el consentimiento de todas las partes legitimadas.

28) LEY: La Ley de Certificados, Firmas Digitales y Documentos electrónicos, Ley número 8454 del 30 de agosto del 2005.

29) LGAP: La Ley General de la Administración Pública.

30) LINEAMIENTOS TÉCNICOS: El conjunto de definiciones, requisitos y regulaciones de carácter técnico-informático, contenido en la Norma INTE /ISO 21188 versión vigente y en las políticas que al efecto emita la DCFD.

(Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

31) LRC: Lista de revocación de certificados.

32) MECANISMO EN LÍNEA PARA VERIFICAR EL ESTADO DEL CERTIFICADO: Mecanismo mediante el cual se permite a las partes que confían, consultar y obtener, la información del estado de un certificado sin requerir para ello el uso de una LRC.

33) OFICINA DE TARJETAS (card bureau): Agente del certificador registrado o de la autoridad de registro que personaliza la tarjeta de circuito integrado (o tarjeta inteligente), que contiene la llave privada del suscriptor (como mínimo).

34) PARTE CONFIANTE: Se refiere a las personas físicas, equipos, servicios o cualquier otro ente que confía en la validez de un certificado emitido por un certificador específico.

35) POLÍTICAS DEL CERTIFICADO (PC): Conjunto de reglas que indican la aplicabilidad del certificado a una comunidad particular y/o clase de aplicaciones con los requerimientos comunes de seguridad.

36) PROTOCOLO EN LÍNEA PARA DETERMINAR EL ESTADO DEL CERTIFICADO (OCSP POR SUS SIGLAS EN INGLÉS): Protocolo suplementario para determinar el estado actual de un certificado.

37) RECUPERACIÓN DE LLAVES: Capacidad de restaurar la llave privada de una entidad a partir de un almacenamiento seguro, en el caso de que se pierda, corrompa o que por cualquier otra razón se convierta en no utilizable.

38) RE-EMISIÓN DE LLAVES DEL CERTIFICADO: Proceso por medio del cual una entidad con un par de llaves y un certificado previamente emitidos, luego de la generación de un nuevo par de llaves, recibe un nuevo certificado y una nueva llave pública.

39) REGLAMENTO: Este Reglamento.

40) RENOVACIÓN DEL CERTIFICADO: Proceso donde una entidad emite una nueva instancia de un certificado existente, con un nuevo período de validez.

41) REPOSITORIO: Sistema de almacenamiento y distribución de certificados e información relacionada (Ej., almacenamiento y distribución de certificados, almacenamiento y recuperación de políticas de certificación, estado del certificado, etc.).

42) ROL DE CONFIANZA: Función de trabajo que permite ejecutar labores críticas. Si dichas labores se ejecutan de una forma insatisfactoria puede ocurrir un impacto adverso, que dará como resultado una degradación en la confianza que provee el certificador.

43) SELLO DE GARANTÍA (tamper evident): Características de un dispositivo que proveen evidencia de que existió un intento de ataque sobre él.

44) SERVICIOS DE VALIDACIÓN DE CERTIFICADOS: Servicios provistos por el certificador registrado o sus agentes que ejecutan la tarea de confirmar la validez del certificado a una tercera parte que confía.

45) SUSCRIPTOR: La persona física a cuyo favor se emite un certificado digital y que lo emplea para los propósitos señalados en el inciso 7) anterior, en conjunto con las claves, contraseñas y/o dispositivos necesarios al efecto y de cuya custodia es responsable.

46) VERIFICACIÓN DE FIRMA: Con relación a la firma digital, significa determinar con precisión: (1) que la firma ha sido creada durante el período operacional de un certificado válido, utilizando la llave pública listada en el certificado; y, (2) que el mensaje no ha sido alterado desde que la firma fue creada.

Artículo 3º—Aplicación al Estado. A los efectos del párrafo segundo del artículo 1º de la Ley, los Supremos Poderes, el Tribunal Supremo de Elecciones, los demás órganos constitucionales y todas las entidades públicas podrán adoptar separadamente las disposiciones particulares que requiera su ámbito específico de competencia o la prestación del servicio público, incluyendo la posibilidad de fungir como certificador respecto de sus funcionarios.

Artículo 4º—Incentivo de los mecanismos de gobierno electrónico. Con excepción de aquellos trámites que necesariamente requieran la presencia física del ciudadano, o que éste opte por realizarlos de ese modo, el Estado y todas las dependencias públicas incentivarán el uso de documentos electrónicos, certificados y firmas digitales para la prestación directa de servicios a los administrados, así como para facilitar la recepción, tramitación y resolución electrónica de sus gestiones y la comunicación del resultado correspondiente.

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 e interoperatividad. 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.

En lo relativo a la conservación de los documentos electrónicos, así como la migración de documentos de soporte físico a electrónico, se aplicará lo dispuesto en el artículo 6º de la Ley.

CAPÍTULO SEGUNDO

Certificados Digitales

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 y las políticas que al efecto emita la DCFD.

(Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 6°—Tipos de certificados. La DCFD establecerá los tipos de certificados que podrán emitir los certificadores, con estricto apego a las normas técnicas y estándares internacionales aplicables que promuevan la interoperabilidad con otros sistemas.

En el caso de los certificados digitales que vayan a ser utilizados en procesos de firma digital y de autenticación de la identidad, los certificadores necesariamente deberán:

1) Utilizar al menos un proceso de verificación y registro presencial (cara a cara) de sus suscriptores.

(Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

2) Guardar copia de la documentación utilizada para verificar la identidad de la persona.

3) Registrar de forma biométrica (fotografía, huellas digitales, etc.) al suscriptor a quién le será emitido un certificado.

4) Requerir el uso de módulos seguros de creación de firma, con certificación de seguridad que se indique conforme a las normas internacionales y a las Políticas establecidas por la DCFD.

(Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

5) Establecer un contrato de suscripción detallando el nivel de servicio que ofrece y los deberes y responsabilidades de las partes.

6) La DCFD podrá establecer cualquier otro requisito que considere pertinente, en tanto emisor y gestor de políticas del sistema de firma digital.

Artículo 7º—Obligaciones de los usuarios. Para los efectos de los artículos 14, inciso d) y 15 de la Ley, todos los suscriptores del sistema de certificados y firmas digitales estarán obligados a:

1) Suministrar a los certificadores la información veraz, completa y actualizada que éstos requieran para la prestación de sus servicios.

2) Resguardar estrictamente la confidencialidad de la clave, contraseña o mecanismo de identificación que se les haya asignado con ese carácter, informando inmediatamente al certificador en caso de que dicha confidencialidad se vea o se sospeche que haya sido comprometida.

3) Acatar las recomendaciones técnicas y de seguridad que le señale el correspondiente certificador.

Artículo 8°—Plazo de suspensión de certificados. Cuando un certificado digital deba ser suspendido por incurrir en alguna de las causales establecidas en el artículo 14 de la Ley , éste será revocado y, una vez desaparecido el motivo de suspensión, se procederá a la emisión de un nuevo certificado.

(Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 9º—Revocación por cese de actividades. Para los efectos del artículo 16 de la Ley, en el caso del cese de actividades de un certificador, éste mismo –o la DCFD en su defecto– gestionarán el traslado de la cartera de suscriptores

que así lo hayan consentido a otro certificador, que expedirá los nuevos certificados.

CAPÍTULO TERCERO

Certificadores

Artículo 10.—Reconocimiento jurídico. Solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital.

Las firmas y certificados emitidos dentro o fuera del país que no cumplan con esa exigencia no surtirán efectos por sí solos, pero podrán ser empleados como elemento de convicción complementario para establecer la existencia y alcances de un determinado acto o negocio.

Artículo 11.—Comprobación de idoneidad técnica y administrativa. Para obtener la condición de certificador registrado, se requiere poseer idoneidad técnica y administrativa, que serán valoradas por el ECA, de conformidad con los lineamientos técnicos establecidos en las Normas INTE-ISO/IEC 17021 e INTE/ISO 21188 versión vigente, las políticas fijadas por la DCFD y los restantes requisitos que esa dependencia establezca, de acuerdo con su normativa específica.

A fin de cumplir con lo establecido en el párrafo anterior, el certificador contará con el plazo de un año contado a partir de la fecha en que se le otorgó el registro por parte de la DCFD , con el propósito de lograr la acreditación respectiva por parte del ECA. Si en el plazo señalado no lograra obtener la acreditación, se le cancelará su registro por parte de la DCFD y no podrá ser registrado nuevamente hasta tanto no presente la acreditación del ECA.

(Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 12.—Formalidades de la solicitud. La solicitud de inscripción del certificador se presentará debidamente autenticada ante la DCFD y deberá incluir la siguiente información:

1) Nombre o razón social de la solicitante, número de cédula de persona jurídica, domicilio y dirección postal, así como los

correspondientes números telefónicos y de fax (si lo tuviera), su sitio Web en Internet y al menos una dirección de correo electrónico para la recepción de comunicaciones de la DCFD. En el caso de los sujetos privados, deberá adjuntar además una certificación de personería jurídica con no menos de un mes de expedida, o el acuerdo de nombramiento debidamente certificado, en el caso de los funcionarios públicos. Dicho documento deberá acreditar, en el primer supuesto, que la persona jurídica se encuentra debidamente constituida de acuerdo con la ley y en pleno goce y ejercicio de su capacidad jurídica.

(Así reformado el inciso el anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

2) Identificación completa de la persona o personas que fungirán como responsables administrativos del certificador ante la DCFD. Ésta o éstas necesariamente serán los firmantes de la gestión y ostentarán la representación legal u oficial de la solicitante.

(Así reformado el inciso el anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

3) Identificación completa de la persona o personas que fungirán como responsables técnicos del certificador, si no fueren las mismas del punto anterior. Se entenderá por tales a la persona o personas que recibirán y custodiarán las claves, contraseñas y/o mecanismos de identificación asignados al certificador y que podrán firmar digitalmente en su nombre.

4) La dirección física precisa del establecimiento o local desde el cual se realizará la actividad de certificación digital.

5) Documentación en la cual se demuestre a juicio de la DCFD , que cuenta con los requisitos para brindar el servicio de certificación digital (con 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, todo acorde a los requerimientos de las normas INTE/ISO 21188 versión vigente, INTE-ISO/IEC 17021 versión vigente, así como a las políticas dictadas por la DCFD).

(Así reformado el inciso el anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

6) Certificación de composición y propiedad del capital social, si la solicitante fuera una sociedad mercantil.

7) (Derogado este inciso por el artículo 3° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 13.—Caución. Los sujetos privados deberán rendir una caución que será utilizada para responder por las eventuales consecuencias civiles, contractuales y extracontractuales de su actividad. Esta caución será rendida preferiblemente por medio de una póliza de fidelidad expedida por el Instituto Nacional de Seguros. El monto –de acuerdo con la Ley- será fijado por la DCFD en consulta con el Instituto Nacional de Seguros, tomando en consideración los riesgos y responsabilidades inherentes en la labor de certificación digital.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Cuando la caución 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:

1) Apercibir al interesado en un plazo no mayor de diez días hábiles y por una única vez sobre cualquier falta u omisión que deba ser subsanada, así como la necesidad de ampliar la documentación que se indica en el inciso 5 de artículo 12 de este reglamento, para dar inicio a su trámite. Al efecto, se aplicará lo dispuesto en la “Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos”, número 8220 de 4 de marzo del 2002; y -en cuanto fuere necesario- lo dispuesto en el artículo 340 de la LGAP.

2) Posteriormente, la DCFD estará facultada para que en caso necesario proceda a realizar una visita al domicilio 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 caución señalada en el artículo 13 anterior.

(Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 15.—Oposiciones. Tramitada la solicitud ante la DCFD , ésta le entregará un resumen al solicitante, el cual deberá ser publicado en el Diario Oficial La Gaceta , sin perjuicio de que la DCFD lo haga también en los medios electrónicos establecidos en la Ley y este Reglamento.

Dentro de los cinco días hábiles siguientes a la publicación, quien se sintiere legítimamente perjudicado por la solicitud planteada, deberá comunicarlo a la DCFD, presentando todas las pruebas pertinentes. En tal caso, la DCFD conferirá audiencia al interesado por un plazo de cinco días hábiles para que se refiera a los hechos planteados.

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 caución indicada en el artículo 13 de este Reglamento.

No se aplicará lo dispuesto en este artículo cuando la gestión corresponda a una dependencia pública.

(Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 16.—Resolución. Cumplido lo dispuesto en el artículo anterior, la DCFD resolverá lo que corresponda –incluyendo las oposiciones formuladas, si las hubiere– en un plazo no mayor de quince días, por medio de resolución fundada que notificará a los interesados. Si el acuerdo fuera favorable, se publicará a través de los medios electrónicos previstos en la Ley y este Reglamento.

Artículo 17.—Silencio positivo. La gestión que no haya sido resuelta dentro del plazo que señala el artículo precedente se entenderá aprobada.

Artículo 18.—Recursos. Contra lo resuelto por la DCFD, se admitirá el recurso de reposición, aplicándose al efecto lo dispuesto en los artículos 346, siguientes y concordantes, de la LGAP.

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

1) Expedir las claves, contraseñas o dispositivos de identificación a sus suscriptores, en condiciones seguras y previa verificación fehaciente de su identidad. Lo mismo hará respecto de sus certificadores subordinados cuando los hubiere, los cuales también deberán registrarse ante la DCFD.

El certificador no podrá copiar o conservar información relativa a la clave privada de firma digital de un suscriptor y deberá abstenerse de tomar conocimiento o acceder a ella bajo ninguna circunstancia.

2) Llevar un registro completo y actualizado de todos sus suscriptores, para lo cual les requerirá la información necesaria. En el caso de los certificadores, comerciales, no se solicitará de sus clientes más información personal que la que sea estrictamente necesaria, quedando obligados a mantenerla bajo estricta confidencialidad, con la salvedad prevista en el inciso último de este artículo.

3) Expedir el certificado digital que respalde la firma digital de los suscriptores de sus servicios y de sus certificadores subordinados, así como suspenderlo o revocarlo bajo las condiciones previstas en la Ley y este Reglamento.

4) Prestar los servicios ofrecidos a sus suscriptores, en estricta conformidad con las políticas de certificación que haya comunicado al público y que hayan sido aprobados por la DFCD.

5) Conservar la información y registros relativos a los certificados que emitan, durante no menos de diez años contados a partir de su expiración o revocación. En caso de cese de actividades, la información y registros respectivos deberán ser remitidos a la DCFD, quien dispondrá lo relativo a su adecuada conservación y consulta.

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 la Norma INTE /ISO 21188 versión vigente y en los lineamientos que sobre el particular dicte la DCFD.

(Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

7) Suministrar, con arreglo a las disposiciones constitucionales y legales pertinentes, la información que las autoridades competentes soliciten con relación a sus suscriptores y a los certificados que les hayan sido expedidos.

8) Impartir lineamientos técnicos y de seguridad a los suscriptores y certificadores subordinados, con base en los que a su vez dicte la DCFD.

9) Acatar las instrucciones y directrices que emita la DCFD para una mayor seguridad o confiabilidad del sistema de firma digital.

(Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

10) Rendir a la DCFD los informes y datos que ésta requiera para el adecuado desempeño de sus funciones y comunicarle a la mayor brevedad cualquier otra circunstancia relevante que pueda impedir o comprometer su actividad.

Artículo 20.—Divulgación de datos. En adición al repositorio en línea a que se refiere el artículo previo, todo certificador registrado deberá mantener un sitio o página electrónica en Internet, de alta disponibilidad y protegida con esquemas de seguridad razonables para impedir su subplantación, por medio del cual suministre permanentemente al público al menos los datos siguientes, empleando un lenguaje fácilmente comprensible y en idioma español:

1) Su nombre, dirección física y postal, número(s) telefónico(s) y de fax (si lo tuviera), así como un mecanismo de contacto por medio de correo electrónico.

2) Los datos de inscripción ante la DCFD y su estado actual (activo o suspendido).

3) Las políticas de certificación que aplica y que son respaldados y aprobados por la DCFD

4) El resultado final más reciente de evaluación o auditoría de sus servicios, efectuada por el Ente Costarricense de Acreditación.

5) Cualesquiera restricciones establecidas por la DCFD.

6) Cualquier otro dato de interés general que disponga la Ley, este Reglamento o la DCFD.

Artículo 21.—Corresponsalías. Al informar a la DCFD sobre el establecimiento de relaciones de corresponsalía conforme al artículo 20 de la Ley, se deberá especificar si la homologación de certificados expedidos por certificadores extranjeros está o no sujeta a alguna clase de restricción o salvedad y, caso afirmativo, en qué consiste. Lo mismo se hará al momento de ofrecer este servicio al público.

Artículo 22.—Actualización permanente de datos. Los certificadores deberán mantener permanentemente actualizada la información que requieran la DCFD y el ECA para el cumplimiento de sus funciones. Cualquier cambio de domicilio físico o electrónico, o de cualquier otro dato relevante, deberá ser comunicado de inmediato a ambas instituciones.

(Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

CAPÍTULO CUARTO

Dirección de Certificadores de Firma Digital

Artículo 23.—Responsabilidad. La Dirección de Certificadores de Firma Digital -perteneciente al Ministerio de Ciencia y Tecnología- 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 la operación técnica de la misma ante el ECA, para lo cual tendrá un plazo de un año a partir de que la misma entre en operación completa.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 24.—Funciones. La Dirección de Certificadores de Firma Digital (DCFD tendrá las funciones que señala la Ley. El registro de certificados digitales a que se refiere el inciso b) del artículo 24 de la Ley tendrá un contenido y propósitos puramente cuantitativos y estadísticos.

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.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Dentro de sus actividades, la DCFD procurará realizar programas de difusión en materia de Firma Digital, así como en la media de sus posibilidades establecer enlaces de cooperación con organismos o programas internacionales relacionados con esta materia.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Artículo 25.—Cooperación interinstitucional. Se autoriza a las instituciones del Estado para presupuestar y girar recursos, en la medida de sus posibilidades jurídicas y materiales, a fin de contribuir a lograr los objetivos de la DCFD.

Artículo 26.—Jefatura. El superior administrativo de la DCFD será el Director, quien será nombrado por el Ministro de Ciencia y Tecnología 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.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

Quien sea designado Director deberá reunir los siguientes requisitos:

1) Poseer un título universitario pertinente al cargo, con grado mínimo de licenciatura.

2) Tener experiencia profesional demostrable en el tema.

3) Estar incorporado al respectivo colegio profesional y al día en sus obligaciones con éste.

4) Los demás que establezca el manual de clasificación y puestos del Ministerio de Ciencia y Tecnología.

Artículo 27.—Régimen interior. El régimen de servicio al que estará sujeto el personal de la DCFD será el establecido en el reglamento autónomo de servicio del Ministerio de Ciencia y Tecnología, que se aplicará también al Director en lo que legalmente sea procedente.

Artículo 28.—Comité Asesor de Políticas. El Director de la DCFD contará con la asesoría de un comité de políticas, integrado por representantes de los siguientes órganos y entidades:

1) Banco Central de Costa Rica;

2) Tribunal Supremo de Elecciones;

3) Poder Ejecutivo;

4) Poder Judicial;

5) Consejo Nacional de Rectores (CONARE), en representación del sector académico; y,

6) Asociación Cámara Costarricense de Tecnologías de la Información y Comunicaciones (CAMTIC), en representación del sector privado.

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 con grado mínimo de licenciatura, graduados en materias afines y con experiencia demostrable en el tema. El cargo será desempeñado en forma ad honórem.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

El Comité Asesor será presidido por el Director de la DCFD. Se reunirá ordinariamente al menos una vez cada seis meses y extraordinariamente cada vez que lo convoque el Director de la DCFD o lo soliciten por escrito al menos cuatro de sus integrantes.

(Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008)

En lo demás, el Comité ajustará su funcionamiento al régimen de los órganos colegiados previsto en la LGAP.

Artículo 29.—Funciones del Comité Asesor de Políticas. El Comité Asesor tendrá las siguientes funciones:

1) Recomendar a la DCFD las políticas generales de operación del sistema nacional de certificación digital, observando los estándares y buenas prácticas internacionales de la materia;

2) Interpretar, aclarar o adicionar esas políticas ante las dudas o consultas de cualquier operador del sistema;

3) Evaluar y actualizar periódicamente las políticas de operación, formulando -en caso necesario- las recomendaciones pertinentes a la DCFD; y,

4) Aconsejar a la DCFD en cualquier otro aspecto que ésta someta a su consideración.

5) Funcionar como Comité para la preservación de la imparcialidad, conforme a los parámetros señalados en la norma INTE-ISO/IEC 17021 versión vigente.

(Así adicionado el inciso anterior por el artículo 2° del decreto ejecutivo N ° 34890 del 27 de octubre de 2008)

Salvo caso de urgencia, la adopción o modificación de políticas que afecten la operación del sistema nacional de certificación digital se hará previa consulta pública, en la que se invitará a las entidades públicas y privadas, organizaciones representativas y público en general a ofrecer comentarios y sugerencias pertinentes; todo conforme a los artículos 361 y 362 de la LGAP.

CAPÍTULO QUINTO

Sanciones

Artículo 30.—Aplicación de mecanismos alternativos de solución de conflictos. Tanto antes como durante la tramitación de los procedimientos disciplinarios por quejas o denuncias planteadas contra un certificador, la DCFD procurará aplicar mecanismos alternativos de resolución de conflictos para encontrar salidas que permitan tutelar los derechos legítimos de las partes, así como la continuidad y confiabilidad del sistema, todo conforme a la legislación aplicable.

Artículo 31.—Multas. El pago de las multas impuestas conforme al artículo 28 de la Ley se realizará por medio de Entero de Gobierno, dentro de los diez días hábiles siguientes a la firmeza de la resolución que las imponga.

El cobro de multas no canceladas oportunamente se realizará conforme a lo dispuesto en el artículo 36 siguiente.

Artículo 32.—Suspensión. La suspensión que se aplique de acuerdo con el artículo 29 de la Ley implicará la imposibilidad para el certificador sancionado de expedir nuevos certificados digitales o de renovar los que expiren durante el plazo de la suspensión. No afectará en nada los emitidos previamente.

En los casos del inciso a) del referido artículo, si al cabo del plazo de suspensión el certificador persiste en no renovar debidamente la caución 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 33.—Revocatoria de la inscripción. Para los efectos del artículo 30, inciso a) de la Ley, se entenderá por "certificado falso" aquel que no esté respaldado por una solicitud previa demostrable del correspondiente suscriptor o cuyo trámite no haya seguido los procedimientos de seguridad establecidos para la clase de certificado de que se trate.

Artículo 34.—Publicidad de las sanciones. Para los propósitos del artículo 32 párrafo segundo de la Ley, la publicación electrónica de las sanciones impuestas se mantendrá:

1) En el caso de multa, por todo el lapso en que ésta permanezca sin cancelar y posteriormente por dos años a partir del pago.

2) En el caso de suspensión o revocatoria de la inscripción, durante cinco años desde la firmeza de la resolución sancionatoria.

Artículo 35.—Determinación de responsabilidades adicionales. Si corresponde, lo relativo a la responsabilidad civil en que pueda haber incurrido un certificador se examinará y resolverá en el mismo procedimiento en que se discuta la responsabilidad disciplinaria. Caso de estimarse que ha lugar al pago de una indemnización, el acto final prevendrá al certificador su oportuno pago, dentro del plazo que al efecto se señalará y que no excederá de un mes.

De llegarse a considerar además que los hechos investigados suponen la posible comisión de un ilícito penal, la Dirección ordenará testimoniar las piezas correspondientes y pondrá los hechos en conocimiento del Ministerio Público.

Artículo 36.—Medios de ejecución. Si el certificador sancionado no realiza oportunamente el pago a que estuviere obligado, se procederá a ejecutar la caución 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.

CAPÍTULO SEXTO

Disposiciones finales

Artículo 37.—Vigencia. Rige a partir de su publicación.

Dado en la Presidencia de la República.—San José, a los veinte días del mes de marzo del dos mil seis.

ANEXO ÚNICO

(Derogado este Anexo por el artículo 3° del decreto ejecutivo N° 34890 del 27 de octubre de 2008).