Aprueban disposiciones complementarias al Reglamento de la Ley de Firmas y Certificados Digitales

RESOLUCION COMISION DE REGLAMENTOS TECNICOS Y COMERCIALES Nº 0103-2003-CRT-INDECOPI

Lima, 23 de octubre de 2003

VISTO:

El Artículo 36 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo Nº 019-2002-JUS modificado por el Decreto Supremo Nº 024-2002-JUS, que designa al Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual como Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Digital; y,

CONSIDERANDO:

Que, de conformidad con el Artículo 36 del Reglamento de la Ley de Firmas y Certificados Digitales el Indecopi como Autoridad Administrativa Competente está a cargo de la acreditación de Entidades de Certificación y de Entidades de Registro/Verificación dentro de la Infraestructura Oficial de Firma Digital, encontrándose facultada para tal efecto a establecer los criterios y requisitos mínimos para la prestación de ambos servicios;

Que, al interior del Indecopi la Comisión de Reglamentos Técnicos y Comerciales ha sido designada como el órgano funcional a cargo de ejercer las funciones de acreditación y demás que confiere el Reglamento de la Ley de Firmas y Certificados Digitales al Indecopi como Autoridad Administrativa Competente;

Que, para efectos de la acreditación de entidades de certificación y de verificación/registro de firmas digitales es necesario establecer mayores precisiones al Régimen de Acreditación previsto en el Capítulo II del Título III del Reglamento de la Ley de Firmas y Certificados Digitales;

Que, asimismo es necesario establecer medidas orientadas a compatibilizar la legislación en materia de micrograbación y las disposiciones sobre el servicio de intermediación digital previsto en el Reglamento de la Ley de Firmas y Certificados Digitales;

Que, el 18 de diciembre de 2002 la Comisión de Reglamentos Técnicos y Comerciales publicó un proyecto de Disposiciones Complementarias al Reglamento de la Ley de Firmas y Certificados

Digitales, a fin de que las empresas e instituciones que a la fecha vienen prestando servicios de certificación y registro puedan alcanzar las observaciones que consideren pertinentes;

Que, luego de revisar las observaciones alcanzadas por las distintas instituciones y profesionales vinculados al tema durante el período de discusión pública, y estando a lo recomendado por la Secretaría Técnica, de conformidad con el Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante Decreto Supremo Nº 019-2002-JUS y con el acuerdo unánime de sus miembros reunidos en sesión del 23 de octubre de 2003

RESUELVE:

Artículo 1.- APROBAR las Disposiciones Complementarias al Reglamento de la Ley de Firmas y Certificados Digitales anexas a la presente Resolución a fin de dar inicio a la acreditación de entidades de certificación y de verificación/registro.

Artículo 2.- En tanto no se incorpore el procedimiento de acreditación de entidades de certificación, y de verificación/registro de firmas digitales en el Texto Único de Procedimientos Administrativos del Indecopi, la cuantía de los derechos de tramitación de estos procedimientos será la prevista para la acreditación de Organismos de Certificación de Productos, sin perjuicio de los costos de auditoria que deben ser asumidos por las entidades solicitantes.

Artículo 3.- Encárguese a la Secretaría Técnica la conformación de un Comité Técnico de Normalización Especializado para la revisión de la NTP 392.030-2: 1997 MICROFORMAS. Requisitos para las Organizaciones que operan sistemas de producción de microformas. Parte 2: Medios de archivo electrónico, a fin de adecuarla al servicio de Intermediación Digital.

Con la intervención de los señores miembros: Fabián Novak, Augusto Ruiloba, Jorge Danós, y José Dajes.

FABIAN NOVAK TALAVERA
Presidente de la Comisión de Reglamentos
Técnicos y Comerciales

DISPOSICIONES COMPLEMENTARIAS AL REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES

Primera.- Naturaleza de la Acreditación Otorgada por la AAC. De conformidad con los artículos 1, 2 y 42 del Reglamento, la acreditación de Entidades de Certificación y Entidades de Registro/Verificación, tiene

por finalidad reconocer la confiabilidad de los servicios de certificación digital que se prestan en el mercado, evaluando para tal efecto las políticas y procedimientos de certificación aplicadas, en especial los procedimientos para la verificación y registro de identidad de los solicitantes, a cargo de Entidades de Registro/Verificación, la atención de reclamos y la actualización de mecanismos de seguridad frente al desarrollo de nuevas tecnologías o aplicaciones que puedan afectar los niveles de seguridad que garantizan la autenticación o vinculación del titular de la firma digital con el documento suscrito digitalmente.

Segunda.- Participación de la Comisión de Reglamentos Técnicos y Comerciales en la evaluación de servicios de certificación no acreditados.- La Comisión de Reglamentos Técnicos y Comerciales solo respalda la competencia técnica de las entidades acreditadas, y la confiabilidad de los servicios prestados por ellas en el marco de la Ley y el Reglamento. Excepcionalmente, para efecto de lo dispuesto en los artículos 6 y 7 del Reglamento, la Comisión de Reglamentos Técnicos y Comerciales podrá evaluar firmas digitales emitidas fuera de la Infraestructura Oficial de Firma Digital a solicitud de las autoridades judiciales o administrativas ante las cuales se hayan presentado documentos así firmados como medios de prueba.

Tercera.- Imparcialidad de los servicios de certificación y de verificación/registro acreditados.- En cumplimiento con los literales a) y h) del Artículo 36 del Reglamento, se precisa que los servicios de certificación y de verificación/registro son servicios de tercera parte y deben ser prestados en condiciones de transparencia, guardando imparcialidad con respecto a las partes que solicitan y usan sus servicios.

Los servicios acreditados no pueden ser prestados a personas con las cuales la entidad acreditada mantenga vinculación económica. Para calificar la existencia de dicha vinculación se deben considerar los conceptos de propiedad indirecta, vinculación y grupo económico de la Comisión Nacional de Empresas y Valores - CONASEV.

Cuarta.- Procedimiento de Acreditación.- Para efecto de la aplicación del artículo 41 del Reglamento el procedimiento de acreditación no podrá exceder los 120 días útiles. Los plazos de cada una de las etapas de evaluación previstas a lo largo del procedimiento, son las que a continuación se señalan:

a) Admisión: 10 días útiles.
b) Evaluación documentaria: 20 días útiles
c) Subsanación de observaciones: 30 días útiles
d) Evaluación de campo: 20 días útiles
e) Subsanación de observaciones: 10 días útiles

Quinta.- Solución de Reclamos por parte de las entidades acreditadas.- De conformidad con la segunda Disposición Final del Reglamento, las entidades acreditadas deben contar con procedimientos de atención de reclamos cuyos términos deben ser parte de la información prestada a sus clientes. Estos procedimientos no constituyen instancia administrativa por lo que sus plazos de evaluación deben ser breves y no deben exceder de 10 días útiles para su atención.

Sexta.- Supervisión de Entidades Acreditadas.- De acuerdo a los artículos 46 y 50 del Reglamento, las entidades acreditadas están obligadas a mantener las condiciones que sustentan la acreditación otorgada y a adecuarse a las disposiciones que establezca la Comisión de Reglamentos Técnicos y Comerciales. El incumplimiento de dichas obligaciones puede motivar la suspensión o revocación de la acreditación otorgada. Tratándose de la contravención de las obligaciones de imparcialidad y transparencia procede la revocación de la acreditación.

Considerando que los servicios de certificación acreditados están referidos a aspectos de seguridad en materia de comercio electrónico, con un intenso grado de innovación, la acreditación otorgada está sujeta a auditoria de seguimiento anuales para verificar el mantenimiento de los niveles de seguridad inicialmente acreditados.

Cuando se observen cambios en la estructura o en los procedimientos, así como deficiencias en la infraestructura y recursos inicialmente presentados por las entidades acreditadas, la Comisión de Reglamentos Técnicos y Comerciales podrá disponer la realización de evaluaciones para determinar las implicancias de dichos cambios y en el caso de deficiencias, la suspensión de la acreditación hasta que éstas sean superadas, como una medida preventiva destinada a garantizar la confiabilidad de los servicios acreditado.

Sétima.- Clase de Certificados comprendidos en la IOFD.- De acuerdo al artículo 16 del Reglamento, los certificados digitales comprendidos dentro de la Infraestructura Oficial de Firmas Digitales son aquellos que permiten la generación de firmas para la identificación de una persona natural, previa verificación presencial de su identidad, o en su defecto para personas jurídicas a través de agentes automatizados.

Las entidades acreditadas deben garantizar el nivel de seguridad requerido al interior de IOFD frente al desarrollo de nuevas tecnologías o aplicaciones que puedan afectar los niveles de seguridad que garantizan la autenticación o vinculación del titular de la firma digital con el documento suscrito digitalmente.

Octava.- Requisitos de orden técnico que deben observar las Entidades de Certificación.- Para efectos del cumplimiento de los requisitos previstos en el artículo 11 del Reglamento, las entidades de certificación deben contar o tener acceso al uso de soluciones e infraestructura que soporten las políticas técnicas futuras, que defina la Comisión de Reglamentos Técnicos y Comerciales, así como los requisitos que se detallan a continuación que deben ser implementados en el país:

a) Dominios de confianza en el país, que permitan verificar los sistemas en que se soporta la prestación de los servicios de certificación digital.

b) Política de Confidencialidad, que asegure a los clientes del servicio de certificación que la información alcanzada para obtención de un certificado Digital no será empleada por la entidad de certificación para otros fines, ni divulgada sin que medie requerimiento de una autoridad judicial o administrativa debidamente motivada.

c) Políticas de Integridad, Autenticación y No repudio, para ello deberán contar con los procedimientos y mecanismos necesarios fijados en la Ley y el Reglamento.

d) Políticas y Normas de Monitoreo, Reporte y Auditoria de los servicios de PKI, deberán contar con un documento detallado sobre sus políticas de Seguridad y Disponibilidad de los servicios brindados.

e) Contar con un repositorio que contenga los certificados emitidos garantizando su conservación por un período mínimo de 10 años.

1. Requisitos de Funcionalidad. Las entidades de certificación deben adoptar el estándar ISO X 509 en su versión actualizada u otro estándar compatible a éste como base de los servicios de certificación digital. Asimismo deben contar con los siguientes requisitos:

1.1. Políticas y procedimientos para la administración del ciclo de vida de las claves, las mismas que deberán involucrar:

a) Políticas y Normas de recuperación de las claves.

b) Políticas y Normas de generación de las claves.

c) Políticas y Normas de distribución, revocación, suspensión, repudio y archivo (almacenamiento) de las claves. Tratándose de revocación de certificados estas políticas deben propiciar que la cancelación del certificado se realice en forma automática.

1.2. Estructura de Manejo de los Certificados sujeta a mecanismos de auditoria periódicos, entendiendo por dicha estructura un sistema que involucra políticas, procedimientos, personal y el soporte técnico para:

a) La administración y control de claves (creación y mantenimiento, habilidad para enlazar las claves con un nombre, habilidad para preguntar que claves se enlazan a un nombre). Estas políticas no deben estar basadas en la identidad individual. La certificación del enlace entre una llave pública y un nombre del directorio será obligatorio. La certificación del enlace entre los atributos adicionales y un nombre del directorio serán discrecionales.

b) Dotar de capacidad al certificado para interactuar en diferentes sectores, tales como el financiero y tributario, considerando las restricciones que cada uno de estos impone.

c) El Intercambio entre certificados (interoperabilidad técnica)

d) Permitir la transferencia de certificados de una entidad de certificación a otra (en el caso de inoperatividad de la entidad que los emitió inicialmente), a fin de garantizar la continuidad del servicio.

e) Permitir la certificación cruzada entre distintos organismos de certificación

f) Superar los problemas de interoperabilidad que se presenten - en caso de que los caminos de la certificación sean contradictorios o múltiples - a través de arbitrajes técnicos para permitir la aceptabilidad de certificados mediante los dispositivos correspondientes, en función a la plataforma de generación utilizada.

g) Separar los servicios de certificación de los sistemas de almacenamiento de los datos obtenidos en la prestación del servicio, sin que ello perjudique la posibilidad de controlar el flujo de información desde el repositorio de datos hacia el sistema de certificación (requerimiento transaccional)

1.3. Una Infraestructura de Seguridad entendiendo por ella a un sistema que involucra políticas, procedimientos, personal y soporte técnico con el objeto de:

a) Proteger la confidencialidad, integridad y disponibilidad de los servicios de certificación.

b) Garantizar servicios de no repudio tecnológico1 para mantener la operatividad del certificado,

c) Impedir que el sistema de certificación implementado permita revocar sus propias acciones

d) Evitar que los usuarios del servicio de certificación puedan revocar tecnológicamente sus propias acciones

1.4. En caso de incorporar servicios de valor añadido de fechado y hora (time stamping), deben contar con un proveedor para tal servicio, el mismo que debe estar disponible dentro de una red abierta, accesible desde cualquier plataforma tecnológica. En todo caso el certificador es responsable por la aptitud de los servicios subcontratados.

1.5. Procedimientos estructurados sobre la base de estándares internacionales para la integración de los servicios de certificación prestados dentro de la Infraestructura Oficial de Firma Digital, con Certificados y datos asociados provenientes de Infraestructuras Oficiales extranjeras o infraestructuras nacionales no oficiales, que presenten diferencias culturales tales como las barreras idiomáticas;

2. Requisitos de Arquitectura. Las entidades de certificación deben estructurar sus servicios de certificación digital, involucrando los siguientes componentes:

2.1. Componentes Criptográficos Básicos2. Estos componentes deben contar con soportes de hardware (como smartcards o módulos criptográficos) o software. Los Protocolos requeridos en este tipo de componentes deben observar los parámetros del estándar X 509 u otro compatible a éste.

Las Interfaces requeridas están publicadas en la página web del Indecopi y se actualizan periódicamente.

Los módulos criptográficos deben proveer soporte para distintos tipos de plataformas. Si alguno de los módulos criptográficos utilizado tuviese restricciones en su desarrollo por razones de afectación de la propiedad intelectual u otro motivo, deben ser especificados por la entidad de certificación al momento de solicitar la acreditación.

Para efecto del establecimiento de paridad entre aplicaciones del sistema de certificación debe primar el de mayor nivel de seguridad.

2.2. Componentes de servicios criptográficos3. Los Protocolos requeridos en este tipo de componentes deben observar los parámetros del estándar X 509 u otro compatible a éste.

Las Interfaces requeridas están publicadas en la página web del Indecopi y se actualizan periódicamente.

Los módulos criptográficos deben proveer soporte para distintos tipos de plataformas. Si alguno de los módulos criptográficos utilizados tuviese restricciones en su desarrollo por razones de afectación de la propiedad intelectual u otros motivos, deben ser especificados por la entidad de certificación al momento de solicitar la acreditación.

Para efecto del establecimiento de comparación entre aplicaciones del sistema de certificación debe primar el de mayor nivel de seguridad. La interfaz de los servicios criptográficos debe permitir la selección y vinculación de los mismos, así como entre las aplicaciones disponibles de un solo servicio criptográfico.

2.3. Componentes de Clave de Servicios a largo plazo, que deben elaborarse sobre la base del estándar X.509 y sus ampliaciones, y deben involucrar:

a) La administración del ciclo de vida de las claves (Key Lifecycle Management)4.

b) La Recuperación de Claves (Key Recovery)5.

c) El Servicio Virtual de Tarjetas Inteligentes (Virtual Smartcard Service)6. De acuerdo a la plataforma, las Interfaces requeridas están publicadas en la página web del Indecopi y se actualizan periódicamente.

d) Administración de Certificados (Certifícate Management)7. Las interfaces requeridas están publicadas en la página web del Indecopi y se actualizan periódicamente

e) Servicio de Entrega y verificación de las claves públicas (Public Key Delivery and Verification)8. Las interfaces requeridas están publicadas en la página web del Indecopi y se actualizan periódicamente.

En todos los casos los perfiles deben ser definidos de acuerdo a la funcionalidad del sector en el que se implementen.

2.4. Servicios y Componentes del Protocolo de Seguridad9. Estos componentes deben:

a) Proveer mecanismos de seguridad y protección de calidad de los protocolos que permitan la interoperación entre aplicaciones del sistema, empleados por los usuarios de los servicios de certificación.

b) Administrar y controlar el nivel de seguridad de la información definido por la Entidad de Certificación.

c) Encapsular los datos, autenticar el origen, proteger los datos y definir credenciales y privilegios de transporte dentro de un servicio simple de certificación digital10.

d) Aplicar mecanismos de seguridad basados en políticas administrativas de información de la Entidad de Certificación.

2.5. Componentes del Protocolo de Seguridad11. Los protocolos reconocidos se encuentran publicados en la página web del Indecopi y se actualizan periódicamente. La Entidad de certificación deberá establecer un perfil para cada protocolo.

2.6. Componentes de Servicio de la Política de seguridad.12

Los protocolos reconocidos se encuentran publicados en la página web del Indecopi y se actualizan periódicamente.

Novena.- Reconocimiento de servicios de certificación prestados en el extranjero.- De acuerdo a lo dispuesto en el Artículo 48 del Reglamento, el reconocimiento de certificaciones emitidas por entidades de certificación que operan en el extranjero requiere la acreditación previa de dichas entidades para lo cual deben seguir el procedimiento de acreditación regular poniendo a disposición de la Comisión de Reglamentos Técnicos y Comerciales, la documentación prevista en el artículo 38 del Reglamento, a través de una empresa que represente sus servicios en el país.

De contar con la acreditación en su país de origen u otros mecanismos de auditoria con respecto a sus servicios, la entidad de certificación debe presentar documentación que acredite tal situación así como las condiciones acreditadas o auditadas, ello a fin de acogerse al reconocimiento de evaluaciones previsto en los artículos 41 y 42 del Reglamento.

Las entidades de certificación extranjeras que operen a través de representantes nacionales deben mantener las mismas políticas y niveles de seguridad previstos en sus países de origen para la clase de certificados comprendida en la IOFD, así como las mismas condiciones y

coberturas de seguros para cubrir los daños que eventualmente se generen por la prestación de sus servicios.

Décima.- Equivalencia de niveles de seguridad.- Las entidades de certificación que utilicen servicios de entidades extranjeras, deben garantizar que dichos servicios mantengan los niveles de seguridad previstos en el país de origen para la clase de certificados comprendida en la IOFD.

Décimo Primera.- Certificados Digitales de uso limitado.- Los Certificados Digitales emitidos en el marco de la Infraestructura Oficial de Firma Digital para su empleo en ámbitos cerrados pueden ser empleados para la generación de firmas digitales en otros ámbitos bastando para ello la aceptación de los destinatarios.

Décimo Segunda.- Entidades de registro/verificación.- Conforme al artículo 20 del Reglamento, el proceso de certificación se inicia con la participación de entidades de registro/verificación, en tal sentido para efectos de su acreditación las entidades de registro/verificación deben declarar la relación existente con una Entidad de Certificación acreditada o reconocida en el país, documentando la vigencia de dicha relación por un período no menor a la acreditación solicitada. Asimismo las entidades de registro/verificación deben contar con mecanismos que permitan una comunicación ininterrumpida con la Entidad de Certificación, para garantizar la atención oportuna de solicitudes de certificación, así como la actualización de información o la cancelación de la certificación.

Décimo Tercera.- Procedimientos y requisitos que deben observar las Entidades de Verificación/Registro.- De acuerdo a los artículos 32 y 33 las entidades de verificación acreditadas deben contar con registros que demuestren la presencia de la persona natural o el representante de la persona jurídica solicitante de la certificación.

No es admisible, tomando en cuenta la naturaleza de los certificados digitales previstos en la Ley y el Reglamento, la atención de solicitudes de certificación por medio de correos electrónicos u otros medios que no garanticen la identidad del solicitante.

Asimismo las entidades de verificación/registro deben contar con ambientes de trabajo seguros para custodiarla información proporcionada por los solicitantes o titulares de la certificación, y con medidas de seguridad que eviten su reproducción por parte del personal que tenga acceso a dicha información.

La entidad de registro o verificación debe contar con Procedimientos que le permitan:

a) Atender las solicitudes de certificación verificando la veracidad de la información proporcionada por el solicitante de la certificación digital incluyendo la verificación de la capacidad de ejercicio de derechos civiles tratándose de las personas naturales, o la existencia de la persona jurídica y la vigencia de poderes de ser el caso. Para ello debe mantenerse contacto con las bases de datos nacionales de identificación y registro civil y de registros públicos tratándose de personas jurídicas.

b) Informar a los solicitantes el procedimiento a través del cual se genera la clave privada así como las condiciones establecidas para la utilización del certificado digital y la generación de firmas digitales, precisando que el incumplimiento de estas condiciones puede motivar la invalidez de las firmas digitales generadas. Los procedimientos deben incluir el tratamiento o condiciones para la generación de firmas a través de agentes automatizados, de ser el caso.

c) Remitir las solicitudes aprobadas a la Entidad de Certificación, informando al usuario de dicha aprobación así como la oportunidad en que se le emitirá el certificado digital.

d) Actualizar la información proveída a la entidad de certificación respecto a los titulares del certificado y las firmas digitales.

e) Asegurar que la información proporcionada por los solicitantes no se emplee para fines distintos de la certificación.

f) Contar con personal que posea la educación necesaria, adiestramiento actualizado así como el perfil y la experiencia para las funciones que les son asignadas.

Décimo Cuarta.- Respaldo Económico y Financiero.- Las entidades de certificación, y de verificación/registro deben contar con recursos propios para la prestación de sus servicios, o estar en condiciones de garantizar la continuidad de los mismos. Asimismo, deben contar con una cobertura de seguros para cubrir los daños que eventualmente se generen por la prestación de sus servicios, ya sean en sus clientes directos o terceros. Dicha información debe ser comunicada a los usuarios en forma previa a la prestación de los servicios.

La Comisión de Reglamentos Técnicos y Comerciales establecerá en función al desarrollo del mercado, valores y porcentajes mínimos asegurables, los mismos que podrán ser reajustados semestralmente. Los servicios de valor añadido requieren en cada caso coberturas de seguros adicionales:

Décimo Quinta.- Sistemas de gestión.- Las entidades de certificación y de verificación/registro deben contar sistemas de gestión de calidad aplicadas a sus servicios.

Específicamente en el caso de Entidades de certificación, su estructura debe ser tal que proporcione confianza con respecto a sus certificaciones, para tal efecto conjuntamente con su Manual de Procedimiento deben presentar su Organigrama estructural y funcional.

Asimismo, la Entidad de Certificación debe ser responsable de todas las decisiones relacionadas con el otorgamiento, mantenimiento y cancelación de la certificación. Para tal efecto debe contar con procedimientos para la subcontratación de los servicios de registro/verificación.

Tratándose de Entidades de Verificación/Registro éstas deben contar con procedimientos para el registro o verificación, la Atención de quejas y el Manejo y archivo de los registros. La entidad de registro o verificación debe tener el personal suficiente para llevar a cabo el trabajo para el cual declara ser competente.

Décimo Sexta.- Servicios de valor añadido.- Las entidades de certificación o de verificación/registro que deseen prestar servicios de valor añadido deben garantizar que los mismos no afectarán los servicios principales de verificación o certificación así como la transmisión de los mensajes de datos firmados digitalmente. La calificación de estos servicios se realizará dentro del proceso de acreditación, para tal efecto deberán presentarse los manuales de procedimientos previstos para su prestación, así como una declaración de la infraestructura con la que cuentan para tal efecto, cuando dichos servicios sean subcontratados la entidad acreditada asumirá la responsabilidad por los mismos.