Artículo 28°.- Reglamento del Consejo de Usuarios

El Consejo de Usuarios se rige en su funcionamiento por el Reglamento que aprueba el Consejo Directiva del Organismo Regulador, a propuesta del primer Consejo de Usuarios que se instale en virtud de la Primera Disposición Transitoria del presente Decreto Supremo.

El Reglamento del Consejo de Usuarios incorporará disposiciones para la elección del Coordinador.

El Consejo de Usuarios tiene iniciativa para proponer a Consejo Directivo del Organismo Regulador, mediante solicitud debidamente fundamentada, la modificación del reglamento del Consejo de Usuarios."

Artículo 2°.- Del refrendo

El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

Dado en la casa de Gobierno, en Lima, a los doce días del mes de enero del año dos mil siete.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

15539-13

Aprueba Reglamento de la Ley de Firmas y Certificados Digitales

DECRETO SUPREMO
N° 004-2007-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, mediante Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310, se reguló la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga, en especial la utilización de la firma digital y los certificados digitales; se reguló a las entidades de certificación y de registro, y se estableció que el Poder Ejecutivo, por Decreto Supremo, determinaría la autoridad administrativa competente y señalaría sus funciones y facultades;

Que, mediante el Decreto Supremo N° 019-2002-JUS, modificado por el Decreto Supremo N° 024-2002-JUS, se aprobó el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, y se designó al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la Autoridad Administrativa Competente, encargada de administrar la Infraestructura Oficial de Firma Electrónica - IOFE;

Que, mediante Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, se declara al Estado Peruano en proceso de modernización en sus diferentes instancias y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano, siendo necesario impulsar la Infraestructura Oficial de Firma Electrónica - IOFE;

Que conforme a la Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, corresponde al RENIEC planear, dirigir, coordinar y controlar las actividades de registro e identificación de las personas, así como emitir el documento único que acredita la identidad de las personas.

Que, la Ley N° 27444 - Ley del Procedimiento Administrativo General establece entre las modalidades de notificación, las cursadas mediante correo electrónico; asimismo permite la cancelación de los derechos de tramitación mediante transferencias electrónicas de fondos; y, que los administrados puedan solicitar que el envío de información o documentación que les corresponda recibir dentro de un procedimiento, sea realizado por medios de transmisión a distancia, tales como el correo electrónico;

Que, el numeral 28.4 del artículo 28° de la precitada Ley N° 27444, prevé que la constancia documental de la transmisión a distancia por medios electrónicos entre entidades y autoridades, constituye de por sí documentación auténtica y dará plena fe a todos sus efectos dentro del expediente para ambas partes, en cuanto a la existencia del original transmitido y su recepción;

Que, en consecuencia, es pertinente aprobar un nuevo Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, que permitirá poner en práctica y difundir en el más breve plazo el uso de firmas electrónicas y certificados digitales, a través de la adecuada regulación de las entidades de certificación y de las entidades de registro o verificación, tanto en el sector público como en el sector privado, impulsando el desarrollo del Comercio y del Gobierno Electrónico, así como de la Sociedad de la Información;

Que, la Presidencia del Consejo de Ministros es la instancia encargada de coordinar esfuerzos intersectoriales para desarrollar el proceso de modernización de la gestión pública; asimismo, de conformidad con el Decreto Supremo N° 066-2003-PCM y el artículo 34° del Decreto Supremo N° 094-2005-PCM, la Presidencia del Consejo de Ministros, actúa como ente rector del Sistema Nacional de Informática;

Con la opinión favorable de la Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros y de la RENIEC contenida en el Oficio N° 997-2006/SGEN/RENIEC;

De conformidad con lo dispuesto en el inciso 8) del artículo 118° de la Constitución Política del Perú, el inciso 2) del artículo 3° del Decreto Legislativo N° 560, la Ley N° 27269 - Ley de Firmas y Certificados Digitales, la Ley N° 28403 y el Decreto Ley N° 25868;

DECRETA:

Artículo 1°.- Aprobación

Apruébese el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310, que consta de tres (3) Títulos, cincuenta y ocho (58) Artículos y Ocho (8) Disposiciones Finales, que en Anexo forma parte del presente Decreto Supremo.

Artículo 2°.- Derogación

Deróguese el Decreto Supremo N° 019-2002-JUS y el Decreto Supremo N° 024-2002-JUS.

Artículo 3°.- Refrendo

El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

Dado en la Casa de Gobierno, a los doce días del mes de enero del año dos mil siete.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1°.- Objeto

El objeto de la presente norma es regular, para el sector público y privado, la utilización de las firmas electrónicas y el régimen de la Infraestructura Oficial de Firma Electrónica

(IOFE), que comprende la acreditación y supervisión de las entidades de certificación y de las entidades de registro o verificación; de acuerdo a lo establecido en la Ley Nº 27269- Ley de Firmas y Certificados Digitales en adelante la Ley.

Reconociendo la variedad de las modalidades de firmas electrónicas, la diversidad de garantías que ofrecen, los diversos niveles de seguridad y la heterogeneidad de las necesidades de sus potenciales usuarios, la IOFE no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas conforme a los requisitos establecidos en el artículo 2º de la Ley.

Artículo 2º.- Utilización de las Firmas Electrónicas

Las disposiciones contenidas en el presente Reglamento no restringen la utilización de las firmas electrónicas generadas fuera de la IOFE, las cuales serán válidas en consideración a los pactos o convenios que acuerden las partes, así como las políticas que adopte el Estado sobre la validez y eficacia jurídica de la firma electrónica en la Administración Pública, conforme a lo establecido en el artículo 1º de la Ley.

Artículo 3º.- Régimen de servicios de certificación

La prestación de servicios de certificación, así como los de registro o verificación, en el ámbito del sector privado se sustentan en el principio de libre competencia.

CAPÍTULO I

DE LA VALIDEZ Y EFICACIA JURÍDICA DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 4º.- Firma electrónica

Se entenderá por firma electrónica a cualquier símbolo basado en medios electrónicos, generado dentro o fuera de la IOFE, utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y/o garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 5º.- Validez y eficacia de las firmas electrónicas

La firma digital generada dentro de la IOFE tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un mensaje de datos o documento electrónico si se utiliza una firma digital generada en el marco de la IOFE.

A las firmas electrónicas creadas o utilizadas fuera de la IOFE, no se le negarán efectos jurídicos, su validez está sometida a los acuerdos o convenios entre las partes, como también a las disposiciones legales aprobadas por el Estado en el marco de las políticas sobre validez de la firma electrónica en el ámbito de la Administración Pública.

CONSUCODE
Consejo Superior de Contrataciones y Adquisiciones del Estado

RESULTADO DEL PROCESO DE FISCALIZACIÓN POSTERIOR PERÍODO DICIEMBRE - 2006

Nº	CONTRATISTA	Nº REG.	Nº RESOLUCION (*)	SUMILLA DE RESOLUCION
1	ROYJA INGENIEROS S.R.L.	8633	Resolución de Subgerencia Nº 017-2006-CONSUCODE/GRNP/SFP del 18.12.2006	Por no comunicar oportunamente la variación de su plantel técnico, se **cancela** la vigencia de la inscripción otorgada a la empresa mediante Resolución de Subgerencia Nº -1234-2006 de fecha 07.08.2006 y se deja sin efecto legal el Certificado de Inscripción Nº 1440 de fecha 08.08.2006.
2	FODERECA E.I.R.L.	11153	Resolución de Presidencia Nº 518-2006-CONSUCODE/PRE del 17.11.2006.	Disponer el inicio de las acciones legales, vía proceso contencioso administrativo, a fin de que en sede judicial se declarare la nulidad de la Resolución de Gerencia Nº 1262-2005-CONSUCODE/GR de fecha 27.07.2005, que aprobó la Inscripción en el Registro Nacional de Proveedores, poner en conocimiento del Ministerio Público, la presunta comisión de los delitos contra la función jurisdiccional (falsa declaración en procedimiento administrativo y contra la fe pública en agravio de CONSUCODE, poner este hecho en conocimiento del Tribunal de Contrataciones y Adquisiciones del Estado, para iniciar el procedimiento sancionador a que hubiere lugar.
3	ARQUITECTURA CONSTRUCCIONES SERVICIOS ANEXOS S.R.L. (ACSA S.R.L.)	4521	Resolución de Presidencia Nº 528-2006-CONSUCODE/PRE del 24.11.2006.	Disponer el inicio de las acciones legales, vía proceso contencioso administrativo, a fin de que en sede judicial se declarare la nulidad de la Resolución de Gerencia Nº 1736-2005-CONSUCODE/GR de fecha 27.09.2005, que aprobó la Renovación de Inscripción en el Registro Nacional de Proveedores, poner en conocimiento del Ministerio Público, la presunta comisión de los delitos contra la función jurisdiccional (falsa declaración en procedimiento administrativo y contra la fe pública en agravio de CONSUCODE, poner este hecho en conocimiento del Tribunal de Contrataciones y Adquisiciones del Estado, para iniciar el procedimiento sancionador a que hubiere lugar.
4	TYON E.I.R.L.	5469	Resolución de Presidencia Nº 529-2006-CONSUCODE/PRE del 24.11.2006.	Disponer el inicio de las acciones legales, vía proceso contencioso administrativo, a fin de que en sede judicial se declarare la nulidad de la Resolución de Gerencia Nº 1887-2005-CONSUCODE/GR de fecha 17.10.2005, que aprobó la Renovación de Inscripción en el Registro Nacional de Proveedores, disponer el inicio de las acciones legales contra el representante legal de la empresa por la presunta comisión de los delitos contra la función jurisdiccional (falsa declaración en procedimiento administrativo) en agravio de CONSUCODE, poner este hecho en conocimiento del Tribunal de Contrataciones y Adquisiciones del Estado para iniciar el procedimiento sancionador a que hubiere lugar.

Lima, enero de 2006
Gerencia de Registros

Lo establecido en el presente artículo y las demás disposiciones del presente Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 6°.- Documentos Firmados Electrónicamente como medio de prueba

Los mensajes de datos y los documentos firmados electrónicamente deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos. Esto incluye la posibilidad de que a voluntad de las partes puede haberse utilizado un servicio de intermediación electrónica.

El Juez podrá solicitar a la AAC el nombramiento de un perito especializado en firmas electrónicas.

Artículo 7°.- Tecnologías de firmas electrónicas

Las firmas electrónicas podrán basarse en todas las tecnologías disponibles de acuerdo con el principio de neutralidad tecnológica. La Infraestructura Oficial de Firma Electrónica admitirá todas las tecnologías de firma digital acreditadas por la AAC.

Artículo 8°.- Conservación de mensaje de datos o documentos electrónicos

Cuando los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensajes de datos o documentos electrónicos firmados electrónicamente, deberán:

a) Ser accesibles para su posterior consulta.

b) Ser conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico.

c) Ser conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción.

TÍTULO II

DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA

CAPÍTULO I
ASPECTOS GENERALES

Artículo 9°.- Elementos

La Infraestructura Oficial de Firma Electrónica - IOFE - está constituida por:

a) El conjunto de firmas electrónicas, certificados digitales y documentos electrónicos generados bajo la Infraestructura Oficial de Firma Electrónica.

b) Las prácticas de certificación, basadas en estándares internacionales o compatibles a las internacionalmente vigentes, que aseguren la interoperabilidad y las funciones exigidas, conforme a lo establecido por la AAC.

c) El software, el hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los estándares señalados en el inciso b).

d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.

e) La AAC, así como Entidades de Certificación, Entidades de Registro o Verificación, Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), Entidades de Certificación para el Estado Peruano (ECEP) y Entidades de Registro o Verificación para el Estado Peruano (EREP), debidamente acreditadas o reconocidas.

Artículo 10°.- Estándares aplicables

La AAC determinará los estándares compatibles aplicando el principio de neutralidad tecnológica.

CAPÍTULO II
DE LAS ENTIDADES DE CERTIFICACIÓN

Artículo 11°.- Funciones

Las Entidades de Certificación tendrán las siguientes funciones:

a) Emitir certificados digitales manteniendo su numeración correlativa.

b) Cancelar certificados digitales.

c) Reconocer certificados digitales emitidos en el extranjero y responder por ellos.

d) Adicionalmente a las anteriores, las señaladas en el artículo 15° del Reglamento, en caso opten por asumir las funciones de Entidad de Registro o Verificación.

Las Entidades de Certificación podrán brindar otros servicios inherentes a los de certificación, cuyas características y procedimientos estarán contenidos en su declaración de prácticas de certificación.

Artículo 12°.- Obligaciones

Las Entidades de Certificación registradas tienen las siguientes obligaciones:

a) Cumplir con su Declaración de Prácticas de Certificación.

b) Cumplir sus funciones dentro de los plazos señalados en su Declaración de Prácticas de Certificación.

c) Informar a los usuarios de todas las condiciones de emisión y de uso de sus certificados digitales, incluyendo las referidas a la cancelación de éstos.

d) Mantener el control y la reserva de la clave privada que emplea para firmar los certificados digitales que emite. En caso que la clave privada de la entidad de certificación se vea comprometida, de inmediato la entidad de certificación cancelará públicamente todos los certificados que haya emitido, u otra medida que haya sido determinada por la AAC.

e) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia.

f) Publicar permanente e ininterrumpidamente por medios telemáticos la relación de los certificados digitales emitidos y cancelados.

g) Cancelar el certificado digital a solicitud de su titular o, de ser el caso, a solicitud del titular de la firma digital; o cuando advierta que la información contenida en el certificado digital fuera inexacta o hubiera sido modificada, o que el titular incurriera en alguna de las causales previstas en el artículo 30° del Reglamento.

h) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido expreso del titular del certificado digital.

i) Brindar todas las facilidades al personal autorizado por la AAC para efectos de supervisión y auditoría.

j) Mantener la información relativa a los certificados digitales que hubieren sido cancelados, por un período mínimo de diez (10) años a partir de su cancelación.

k) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la AAC conforme a lo establecido en el Reglamento.

l) Informar y solicitar autorización a la AAC para realizar acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.

m) Informar y solicitar autorización a la AAC para efectos del reconocimiento de certificados emitidos por entidades extranjeras.

n) Mantener vigente la contratación de seguros o garantías bancarias que permitan indemnizar al titular por los daños que puedan ocasionar como resultado de las actividades de certificación.

Estas obligaciones podrán ser precisadas por la AAC, a excepción de las que señale expresamente la Ley.

Artículo 13°.- Respaldo financiero
Las Entidades de Certificación acreditadas o reconocidas deberán contar con el respaldo económico suficiente para operar bajo la IOFE, así como para afrontar el riesgo de responsabilidad por daños. La AAC determinará los requisitos y cuantía de las pólizas de seguros o garantías bancarias a exigir y los criterios para evaluar el cumplimiento de este requisito.

Artículo 14°.- Del cese de operaciones
La Entidad de Certificación cesa sus operaciones en el marco de la IOFE, en los siguientes casos:

a) Por decisión unilateral comunicada a la AAC, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sentencia judicial.
e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contemplados en los incisos a) y b) la AAC establecerá el plazo en el cual las Entidades de Certificación notificarán tanto a aquélla como a los titulares de certificados digitales el cese de sus actividades. La AAC deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos d), g) e i) del artículo 12° del Reglamento.
La AAC reglamentará los procedimientos para hacer público el cese de operaciones de las entidades de certificación.
Los certificados digitales emitidos por una Entidad de Certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. El uso de certificados digitales con posterioridad a su cancelación conlleva la inaplicabilidad de los artículos 5° y 6° del presente Reglamento.

CAPÍTULO III
DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 15°.- Funciones
Las Entidades de Registro o Verificación tienen las siguientes funciones:

a) Identificar al solicitante del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquel.
b) Identificar al solicitante de cualquier otra firma electrónica.
c) Aceptar y/o autorizar, según sea el caso, la conformidad de las solicitudes de emisión, modificación o cancelación de certificados digitales, comunicándolo a la Entidad de Certificación.

Artículo 16°.- Obligaciones
Las Entidades de Registro o Verificación registradas tienen las siguientes obligaciones:

a) Cumplir con su Declaración de Prácticas de Registro o Verificación.
b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante del certificado digital, bajo responsabilidad.
c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.
d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
e) Acreditar domicilio en el Perú.
f) Mantener vigente la contratación de seguros o garantías bancarias que permitan indemnizar al titular por los daños que puedan ocasionar como resultado de las actividades de certificación.

Estas obligaciones podrán ser precisadas por la AAC, a excepción de las que señale expresamente la Ley.

Artículo 17°.- Respaldo financiero
Las Entidades de Registro o Verificación acreditadas deberán contar con el respaldo económico suficiente para operar bajo la IOFE, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y en el Reglamento. La AAC determinará los requisitos y cuantía de las pólizas de seguros o garantías bancarias a exigir y los criterios para evaluar el cumplimiento de este requisito.

Artículo 18°.- Cese de operaciones
La Entidad de Registro o Verificación cesa de operar en el marco de la IOFE en los siguientes casos:

a) Por decisión unilateral comunicada a la AAC, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sentencia judicial.
e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

Para los supuestos contenidos en los incisos a) y b) la Entidad de Registro o Verificación debe notificar el cese de sus actividades a la AAC con una anticipación mínima que será establecida por ésta, debiendo dejar constancia ante aquella de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 16° del Reglamento.

CAPÍTULO IV
DE LA FIRMA DIGITAL

Artículo 19°.- Firma digital
Aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al mismo y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior. Tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita.
Las firmas digitales son las generadas a partir de certificados digitales que son:

a) Emitidos conforme a lo dispuesto en el Reglamento por entidades de certificación acreditadas ante la AAC.
b) Incorporados a la IOFE bajo acuerdos de certificación cruzada, conforme al artículo 55° del Reglamento.
c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la AAC conforme al artículo 53° del Reglamento.
d) Emitidos por entidades de certificación extranjeras que hayan sido incorporados por reconocimiento a la IOFE conforme al artículo 54° del Reglamento.

Artículo 20°.- Características
Las características mínimas de la firma digital generada bajo la IOFE son:

a) Se genera al cifrar el código de verificación de un mensaje de datos, usando la clave privada del titular del certificado.
b) Es exclusiva del titular de la firma digital y de cada mensaje de datos firmado por éste.
c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.
d) Su generación está bajo el control exclusivo del titular de la firma digital.
e) Está añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la firma digital o el mensaje de datos fue alterado.

Artículo 21°.- Funciones
Dadas las características señaladas en el artículo anterior, técnicamente la firma digital debe garantizar que:

a) El mensaje de datos fue enviado y firmado con la clave privada del titular de la firma digital.

b) El mensaje de datos no ha sido alterado después que el remitente lo envió.

c) Como consecuencia de los dos literales previos, el titular de la firma digital no podrá repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada dado que ésta se mantiene bajo su control exclusivo.

Artículo 22°.- Del titular de la firma digital

Dentro de la IOFE, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado.

Tratándose de personas naturales, éstas son titulares del certificado digital y de las firmas digitales que se generen a partir de aquél, incluyendo las firmas digitales que se generen a través de agentes automatizados.

En el caso de personas jurídicas, son éstas los titulares del certificado digital, y sus representantes son los titulares de la firma digital, con excepción de las firmas digitales que se generen a través de agentes automatizados, situación en la cual las personas jurídicas son titulares del certificado y de las firmas digitales generadas a partir de éstos.

Artículo 23°.- Obligaciones del titular

Las obligaciones del titular de la firma digital son:

a) Entregar información veraz bajo su responsabilidad.

b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.

c) Mantener el control y la reserva de la clave privada bajo su responsabilidad.

d) Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales.

e) En caso de que la clave privada quede comprometida en su seguridad, el titular debe notificarlo de inmediato a la Entidad de Certificación para que cancele el certificado digital. La Entidad de Certificación será responsable de los daños que pueda ocasionar la demora en dicha cancelación.

Artículo 24°.- Invalidez

Una firma digital generada bajo la IOFE pierde validez si es utilizada:

a) En fines distintos para los que fue extendido el certificado.

b) Cuando el certificado haya sido cancelado o revocado conforme a lo establecido en el Capítulo V del presente Título.

CAPÍTULO V
DEL CERTIFICADO

Artículo 25°.- Requisitos

Para la obtención de un certificado digital, el solicitante deberá acreditar lo siguiente:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la misma y su vigencia mediante los instrumentos públicos o norma legal respectiva.

Artículo 26°.- Especificaciones adicionales para ser titular

Para ser titular de un certificado digital adicionalmente se deberá cumplir con entregar la información solicitada por la Entidad de Registro o Verificación, de acuerdo a lo estipulado por la Entidad de Certificación correspondiente, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.

En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular del certificado digital y de las firmas digitales que se generen.

Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Artículo 27°.- Procedimiento para ser titular

Para el caso de personas naturales, éstas deberán presentar una solicitud a la Entidad de Registro o Verificación, según sea el caso; dicha solicitud deberá estar acompañada de toda la información requerida por la declaración de prácticas de certificación o en los procedimientos declarados. La Entidad de Registro o Verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. La Entidad de Certificación cumplirá lo dispuesto en el presente artículo, en el supuesto previsto en el segundo párrafo del artículo 12° de la Ley.

En el caso de una persona jurídica, la solicitud deberá ser presentada por la persona facultada para tal fin, debiendo acreditar la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante. Asimismo, deberá presentar toda la información requerida por la declaración de prácticas de la entidad correspondiente.

Artículo 28°.- Obligaciones del titular

a) Actualizar permanentemente la información proveída tanto a la Entidad de Certificación como a la Entidad de Registro o Verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.

b) Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.

c) Observar permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado.

Artículo 29°.- Contenido y vigencia

Los certificados emitidos dentro de la IOFE deberán contener como mínimo lo establecido en el artículo 7° de la Ley.

La Entidad de Certificación podrá incluir, a pedido del solicitante del certificado información adicional siempre y cuando la Entidad de Registro o Verificación compruebe fehacientemente la veracidad de ésta.

El período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme al artículo 9° de la Ley. Los certificados digitales tendrán una validez máxima de tres (3) años.

Artículo 30°.- Causales de cancelación

La cancelación del certificado puede darse:

a) A solicitud del titular del certificado digital o del titular de la firma digital sin previa justificación, siendo necesario para tal efecto la aceptación y autorización de la Entidad de Certificación o la Entidad de Registro o Verificación, según sea el caso, la misma que deberá ser aceptada y autorizada como máximo dentro del plazo establecido por la AAC. Si en el plazo indicado la entidad no se pronuncia, se entenderá que el certificado ha sido cancelado, sin perjuicio del tercero de buena fe.

b) Por revocación efectuada por la Entidad de Certificación, con expresión de causa.

c) Por expiración del plazo de vigencia.

d) Por el cese de operaciones de la Entidad de Certificación que lo emitió.

e) Por resolución administrativa o judicial que lo ordene.

f) Por interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta, del titular del certificado.

g) Por extinción de la personería jurídica o declaración judicial de quiebra.

h) Otras causales que establezca la AAC.

i) Por muerte, o por inhabilitacion o incapacidad declarada judicialmente de la persona natural titular del certificado.

Artículo 31°.- Cancelación del certificado a solicitud de su titular

La solicitud de cancelación de un certificado digital puede ser realizada por su titular o a través de un representante debidamente acreditado; pudiendo realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las Entidades de Certificación.

El titular del certificado está obligado, bajo responsabilidad, a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

a) Por exposición, puesta en peligro o uso indebido de la clave privada.

b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

Artículo 32°.- Cancelación por revocación

La revocación supone la cancelación de oficio de los certificados por parte de la Entidad de Certificación, quien debe contar con procedimientos detallados en su declaración de prácticas de certificación.

La revocación también puede ser solicitada por un tercero que informe fehacientemente de alguno de los supuestos de revocación contenidos en los numerales 1) y 2) del artículo 10° de la Ley.

La revocación debe indicar el momento desde el cual se aplica, precisando la fecha, hora, minuto y segundo del mismo. La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La Entidad de Certificación debe inmediatamente incluir la revocación del certificado digital en la relación que corresponda.

CAPÍTULO VI
CERTIFICACION DIGITAL EN EL SECTOR PÚBLICO

Artículo 33°.- Entidades de Certificación y de Registro o Verificación

En el ámbito del Sector Público, las entidades que presten servicios de certificación digital en el marco de la IOFE, son las siguientes:

a) Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), la cual será la encargada de emitir los certificados raíz para las Entidades de Certificación para el Estado Peruano que lo soliciten, además de proponer las políticas y estándares de las ECEP y EREP según lo establecido por el presente reglamento.

b) Entidades de Certificación para el Estado Peruano (ECEP) acreditadas o reconocidas por la AAC, las cuales serán las encargadas de proporcionar, emitir o cancelar los certificados digitales: i) a los administrados, personas naturales y jurídicas, los cuales serán utilizados únicamente en los trámites, procedimientos administrativos y similares; ii) a los funcionarios, empleados y servidores públicos para el ejercicio de sus funciones y la realización de actos de administración interna e interinstitucional, y a las personas expresamente autorizadas por la entidad pública correspondiente. Cualquier otro uso que no forme parte del ejercicio de las funciones, de los procedimientos administrativos o de administración interna del Estado o de los procedimientos y coordinaciones entre entidades públicas carecerá del respaldo legal de la IOFE.

c) Entidades de Registro o Verificación para el Estado Peruano (EREP) acreditadas o reconocidas por la AAC, serán las encargadas de: levantamiento de datos, comprobación de la información de un solicitante, identificación y autenticación del suscriptor, aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales además de su gestión ante las Entidades de Certificación; para los fines previstos en el inciso b) del presente artículo.

Las entidades señaladas en los incisos a), b) y c) podrán brindar servicios de intermediación electrónica, conforme a lo dispuesto en la Ley y el presente reglamento.

La prestación de los servicios de certificación o de registro y verificación por parte de las entidades de la Administración Pública se sustentan en los principios de acceso universal y no discriminación del uso de las tecnologías de la información y de comunicaciones, procurando que los beneficios resultantes contribuyan a la mejora de la calidad de vida de todos los ciudadanos, así como el acceso gratuito de los servicios. En consecuencia, las entidades públicas que presten sus servicios como ECERNEP, ECEP y EREP, con el fin de determinar el valor de los mismos sólo podrán considerar los costos asociados a su prestación.

Artículo 34°.- Designación de las entidades responsables

Se designa al Registro Nacional de Identificación y Estado Civil - RENIEC como ECERNEP, ECEP y EREP. Los servicios a ser prestados en el cumplimiento de los roles señalados estarán a disposición de todas las Entidades Públicas del Estado Peruano y de todas las personas naturales y personas jurídicas que mantengan vínculos con el mismo, no excluyendo ninguna representación del Estado Peruano en el territorio nacional o en el extranjero.

Las entidades a que se refiere el artículo 33° del Reglamento serán acreditadas y reconocidas por la AAC.

Artículo 35°.- El Documento Nacional de Identidad electrónico

El Documento Nacional de Identidad electrónico (DNIe) es el Documento Nacional de Identidad que acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma electrónica de documentos. Este documento se constituye en uno de los medios por los cuales el RENIEC, actuando como ECEP, proveerá los certificados digitales a ser emitidos a los ciudadanos, para los usos en los términos que se señalan en el inciso b) del artículo 33°, del reglamento. A diferencia de los certificados digitales que pudiesen ser provistos por otras ECEP, el que se incorpora en el DNIe cuenta con la facultad adicional de poder ser utilizado para el ejercicio del voto electrónico en los procesos electorales, en la medida que esta alternativa estuviese implementada.

Artículo 36°.- Implementación de otras Entidades de Certificación para el Estado Peruano (ECEP) y Entidades de Registro o Verificación para el Estado Peruano (EREP)

Otras entidades públicas del Estado Peruano, que por sus funciones, facultades o planes estratégicos para la mejora de sus servicios hacia sus usuarios, requieren constituirse en ECEP y/o EREP, deberán acreditarse o ser reconocidas por la AAC, debiendo cumplir con las políticas y estándares propuestos por la ECERNEP para el sector público y que sean compatibles con los estándares establecidos por la AAC.

Artículo 37°.- De la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP)

a) El RENIEC será la única ECERNEP y actuará también como ECEP y EREP.

Todas las ECEP y las EREP deben seguir las políticas y estándares propuestos por la ECERNEP y aprobados

por la AAC, así como aquellos lineamientos definidos por la ONGEI para el Sector Público.

b) A fin de brindar una imagen de plataforma confiable, la ECERNEP deberá, en caso corresponda, realizar las acciones necesarias a fin de registrar su certificado dentro de los principales navegadores de Internet.

c) Deberá soportarse en una estructura funcional y jurídica estable, no cambiante en el mediano plazo, sólo variable en la cantidad de Entidades de Certificación y Registro que pueda tener.

d) La ECERNEP y las ECEP emplearan el grado de seguridad adecuado en la selección del algoritmo, en la longitud de la clave, en el medio de almacenamiento de la clave privada y en la implementación de los algoritmos empleados, así como el contenido de los certificados digitales que permitan interoperabilidad entre las distintas plataformas tecnológicas y sistemas informáticos de firmas digitales, los cuales deberán ser establecidos por la ECERNEP y ser compatibles con las disposiciones establecidas por la AAC.

e) Deberá ser auditada periódicamente por la AAC. Los informes de auditoria deben ser tenidos en cuenta para continuar su operación. Asimismo, en el caso de un proceso de acreditación, la auditoria será previa a la terminación del mismo.

f) Para la acreditación de la ECERNEP ante la AAC, no resultará exigible el requisito de respaldo financiero. Tampoco lo será lo señalado en el inciso n) del artículo 12°.

Artículo 38°.- De las Entidades de Certificación para el Estado Peruano (ECEP)

a) Deberán ofrecer un servicio de directorio y permitir que las aplicaciones accedan a los certificados digitales emitidos y a la Lista de Certificados Digitales Revocados (LCR). Este servicio se debe encontrar actualizado con la frecuencia indicada en las Políticas de Certificación de cada tipo de certificado. Junto al Servicio de Directorio se puede disponer del servicio de consulta en línea del estado de un certificado digital.

b) Una ECEP podrá ofrecer distintos servicios y mecanismos para recibir un requerimiento de certificado digital para otorgar el mismo a su titular. La recepción de solicitudes de revocación y la publicación periódica de la Lista de Certificados Digitales Revocados (LCR) son servicios que debe ofrecer en forma obligatoria. Asimismo, deberá garantizar el acceso permanente a dichos servicios, proponiendo una solución para una eventual contingencia.

c) Deberán ofrecer el servicio de emisión y renovación de certificados digitales.

d) Las ECEP podrán ofrecer y emitir distintos tipos de firmas electrónicas y/o certificados digitales pudiendo soportarse en diversas tecnologías.

e) La estructura de los certificados emitidos por las ECEP deberá ser electrónicamente articulable con todas las aplicaciones y plataformas informáticas que requieran su uso.

f) Se ofrecerá un grado de seguridad adecuado en relación a los equipos informáticos y de comunicación empleados, al personal empleado para operar la ECEP, a los responsables de operar las claves de la ECEP y a los procedimientos utilizados para la autenticación de los datos a ser incluidos en los certificados digitales.

g) La integridad del directorio de certificados digitales y la lista de certificados digitales revocados debe estar permanentemente asegurada. Es responsabilidad de la ECEP garantizar la disponibilidad de este servicio y la calidad de los datos suministrados por éste.

h) Cada titular del certificado deberá ser distinguido unívocamente. Para el caso de los funcionarios, empleados o servidores públicos y de las personas expresamente autorizadas por la entidad pública correspondiente, deberá incluirse en los certificados, el organismo donde desempeñan sus funciones o el organismo por el cual ha sido autorizado. Para los administrados, ciudadanos o empresas deberá incluirse el organismo emisor del certificado.

i) Los campos que indiquen el período de validez o vigencia ("no antes de" y "no después de") deberán detallar la fecha y la hora.

j) Para la acreditación de las ECEP ante la AAC, no resultará exigible el requisito de respaldo financiero. Tampoco lo será lo señalado en el inciso n) del artículo 12°.

Artículo 39°.- Disposiciones generales para el Sector Público

a) Los trámites y procedimientos administrativos ante las entidades de la Administración Pública, la constancia documental de la transmisión a distancia por medios electrónicos entre autoridades administrativas o con sus administrados, o cualquier tramite, procedimiento o proceso por parte de los administrados o ciudadanos ante las Entidades Publicas o entre estas entidades, no excluyendo a las representaciones del Estado Peruano en el exterior, podrán efectuarse utilizando las diversas tecnologías de certificados digitales y firmas electrónicas reconocidas por la AAC, conforme a Ley.

b) Las entidades de la administración pública deberán admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por entidades de certificación acreditadas o reconocidas por la AAC, públicas o privadas, indistintamente.

c) Todas las disposiciones y regulaciones complementarias para la aplicación de las diversas tecnologías de firmas electrónicas y certificados digitales en el sector público para el uso en los sistemas informáticos o aplicativos orientados al desarrollo de la Sociedad de la Información y el Gobierno Electrónico en el Estado Peruano, como el Sistema Electrónico de Contrataciones y Adquisiciones del Estado-SEACE, Voto Electrónico, entre otros, serán definidas y establecidas por Oficina Nacional de Gobierno Electrónico e Informática y aprobadas por la Presidencia del Consejo de Ministros, con el objetivo de garantizar un nivel apropiado de seguridad y confianza acorde con las mejores prácticas y estándares vigentes internacionalmente, así como las orientadas a permitir la interoperabilidad entre las diversas plataformas, sistemas o aplicativos informáticos de las la Administración Pública.

d) Los servicios de intermediación electrónica, pueden ser implementados por una institución pública u organismo independiente, caso contrario serán desarrollados por la misma Entidad.

e) Cuando por primera vez un solicitante requiera ante una EREP que se le emita un certificado digital, deberá acreditarse personalmente para dicho propósito.

f) En concordancia con el artículo 36°, las entidades públicas del Estado Peruano, que por sus funciones, facultades o planes estratégicos para la mejora de sus servicios hacia sus administrados, requieran utilizar funcionalidades de firma digital en sus sistemas o aplicativos informáticos para brindar confianza e interoperabilidad entre otras plataformas del Estado, pudiendo a voluntad constituirse en ECEP, podrán obtener el Certificado Raíz de la ECERNEP, para lo cual deberán seguir las políticas y estándares para el sector público establecidas por la ECERNEP.

g) Todas las disposiciones de la Ley y el Reglamento son aplicables a la ECERNEP, las ECEP y las EREP, en lo que corresponda.

h) Para la acreditación de las EREP ante la AAC, no resultará exigible el requisito de respaldo financiero. Tampoco lo será lo señalado en el inciso f) del artículo 16°.

TÍTULO III

DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

CAPÍTULO I
DE LAS FUNCIONES

Artículo 40°.- Funciones

La Autoridad Administrativa Competente (AAC) tiene las siguientes funciones:

a) Aprobar la política de certificados y las declaraciones de prácticas de certificación.

b) Acreditar Entidades de Certificación nacionales y reconocer a las Entidades de Certificación extranjeras.

c) Acreditar Entidades de Registro o de Verificación.

d) Registrar a las entidades acreditadas señaladas en los incisos b) y c) del presente artículo, en el Registro de Entidades de Certificación y Entidades de Registro o Verificación previsto en el artículo 15° de la Ley.

e) Supervisar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los prestadores de servicios de intermediación electrónica.

f) Cancelar las acreditaciones otorgadas a las Entidades de Certificación y a las Entidades de Registro o Verificación conforme a lo dispuesto en el Reglamento.

g) Publicar, por medios telemáticos, la relación de entidades acreditadas.

h) Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica y determinar la compatibilidad de otros estándares técnicos con los estándares internacionales; cooperar, dentro de su competencia, en la unificación de los sistemas que se manejan en los organismos de la Administración Pública, tendiendo puentes entre todos sus niveles; y en la obtención de la interoperabilidad del mayor número de aplicaciones y plataformas de firmas electrónicas.

i) Formular los criterios para el establecimiento de la idoneidad técnica que deberán cumplir quienes presten servicios en las materias reguladas por la Ley y el Reglamento, así como aquellas relacionadas con la prevención y solución de conflictos.

j) Establecer los requisitos mínimos para la prestación de los servicios de certificación y los servicios de registro o verificación.

k) Impulsar la solución de conflictos por medio de la conciliación y el arbitraje.

l) Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación y las entidades de registro o verificación.

m) Suscribir acuerdos de reconocimiento mutuo con Autoridades Administrativas Extranjeras que cumplen funciones similares a las de la AAC.

n) Autorizar la realización de certificaciones cruzadas con entidades de certificación extranjeras.

o) Fomentar y coordinar el uso y desarrollo de la Infraestructura Oficial de Firma Electrónica en las entidades del sector público nacional en coordinación con la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) que se designe.

p) Aprobar y regular los servicios de valor de intermediación digital al interior de la Infraestructura Oficial de Firma Electrónica.

q) Delegar a terceros bajo sus órdenes y responsabilidad, y a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) designada, las funciones que estime pertinentes conforme a lo previsto en el presente reglamento.

r) Sancionar a las Entidades de Certificación, a las Entidades de Registro o Verificación o a los prestadores de servicios de intermediación electrónica, por el incumplimiento o infracción al presente reglamento y demás disposiciones vinculadas a la Infraestructura Oficial de Firma Electrónica.

s) Las demás que sean necesarias para el buen funcionamiento de la infraestructura Oficial de Firma Electrónica.

CAPÍTULO II

DEL RÉGIMEN DE ACREDITACIÓN DE ENTIDADES DE CERTIFICACION Y DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 41°.- Acreditación de Entidades de Certificación

Las entidades que soliciten su acreditación y registro ante la AAC, como Entidades de Certificación, incluyendo las ECEP, deben contar con los elementos de la IOFE señalados en los incisos b), c) y d) del artículo 9° y someterse al procedimiento de evaluación comprendido en el artículo 45° del reglamento.

Cuando alguno de los elementos señalados en el párrafo precedente sea administrado por un tercero, la entidad solicitante deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones, y la disponibilidad de estos elementos para la evaluación y supervisión que la AAC considere necesarias. La AAC, de ser el caso, precisará los términos bajo los cuales se rigen estos supuestos del servicio de certificación.

Los Notarios Públicos pueden solicitar su acreditación como Entidad de Registro o Verificación en la prestación de los servicios de certificación digital, debiendo cumplir con los requisitos estipulados en el presente reglamento y la Ley.

Artículo 42°.- Presentación de la solicitud de acreditación de la entidad de certificación

La solicitud de acreditación de Entidades de Certificación debe presentarse a la AAC, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:

a) Pago por derecho de solicitud de acreditación por un monto equivalente al 100% de la UIT vigente a la fecha de pago.

b)Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante.

c) Acreditar domicilio en el país.

d) Acreditar contar con la. infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de la visita comprobatoria de la AAC.

e) Declaración de prácticas de certificación y documentación que comprende el sistema de gestión implementado conforme al inciso b) del artículo 9° del Reglamento.

f) Declaración jurada del cumplimiento de los requisitos señalados en los Incisos c) y d) del artículo 9° del Reglamento; información qué será comprobada por parte de la AAC.

g) Documentación que acredite el cumplimiento de lo dispuesto en los artículos 12° y 13° del Reglamento y demás que la AAC señale.

h) Informe favorable de la entidad sectorial correspondiente, cuando lo solicite la AAC, para el caso de personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.

Artículo 43°.- Acreditación de Entidades de Registro o Verificación

Las entidades que soliciten su acreditación y registro ante la AAC, como Entidades de Registro o Verificación, incluyendo las EREP, deben contar con procedimientos para la prestación de sus servicios, los mismos que tendrán que asegurar la verificación presencial de la identidad del solicitante de un nuevo certificado digital.

Artículo 44°.- Presentación de la solicitud de acreditación de Entidades de Registro o Verificación

La solicitud para la acreditación de Entidades de Registro o Verificación debe presentarse a la AAC, observando lo dispuesto en el artículo anterior y adjuntando la información y documentos siguientes:

a) Pago por derecho de solicitud de acreditación por un monto equivalente al 100% de la UIT, vigente.

b) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante. Acreditar domicilio en el país.

c) Acreditar contar con la infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de las visitas comprobatorias de la AAC.

d) Procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.

e) Declaración de prácticas de registro o verificación.

f) Declaración jurada del cumplimiento de los requisitos señalados en los artículos 16° y 17° del Reglamento.

Artículo 45°.- Procedimiento Administrativo de la Acreditación

Admitida la solicitud, la AAC procederá a la evaluación del cumplimiento de los requisitos establecidos en la Ley como en el Reglamento.

La evaluación de los requisitos de competencia técnica de la Entidad de Certificación o de Registro o Verificación solicitante podrá ser realizada directamente por la AAC, o a través de terceros, o reconociendo aquellas realizadas en el extranjero por otras Autoridades Extranjeras que cumplan funciones equivalentes a las de la AAC, y siempre que los requisitos evaluados por ellas sean equivalentes a los requisitos comprendidos en el Reglamento, para lo cual la AAC adoptará los requerimientos, estándares y procedimientos empleados a nivel internacional para la realización de esta función.

Artículo 46°.- Reconocimiento de evaluaciones en el extranjero

La AAC reconocerá las evaluaciones sobre los requisitos de competencia técnica de la Entidad de Certificación solicitante realizadas en el extranjero siempre y cuando se cumplan con las normas establecidas por la AAC en el marco del Reglamento.

Artículo 47°.- Subsanación de observaciones

Dentro del procedimiento podrán subsanarse las deficiencias técnicas observadas durante la evaluación. Las entidades podrán solicitar la suspensión del procedimiento a fin de implementar las medidas necesarias para superar estas dificultades.

Si, culminada la etapa de evaluación, se mantienen observaciones, se denegará el Registro y se archivará el procedimiento.

Artículo 48°.- Costos del Registro y otros procedimientos

Las entidades solicitantes asumirán los costos por la tramitación del procedimiento, y aquellos por evaluación, auditoría y demás previstos por la AAC.

Artículo 49°.- Otorgamiento y vigencia de la acreditación

La acreditación se otorga por un período de tres (3) años, renovable por períodos similares. La Entidad beneficiaria estará sujeta a evaluaciones técnicas anuales para mantener la vigencia de la referida acreditación.

Artículo 50°.- Cancelación de la Acreditación

La cancelación de la acreditación de las Entidades de Certificación o de las Entidades de Registro o Verificación procede:

a) Por decisión unilateral comunicada a la AAC.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sentencia judicial.
e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

CAPÍTULO III

DE LA INTERMEDIACIÓN ELECTRÓNICA

Artículo 51°.- De los servicios de intermediación electrónica

Los servicios de intermediación electrónica a los que acceden voluntariamente y por acuerdo entre las partes en la transmisión de un mensaje de datos o documento electrónicos que utilizan firmas electrónicas, son brindados por prestadores autorizados que deberán estar inscritos y registrados en la AAC.

El prestador de servicios de intermediación electrónica estará habilitado para ejercer sus funciones por un plazo renovable de tres (3) años a partir de su inscripción en la AAC.

Artículo 52°.- De la inscripción para la prestación de servicios de intermediación electrónica:

Los requisitos para la prestación de servicios de intermediación electrónica son:

a) Pago por derecho de solicitud de acreditación por un monto equivalente al 100% de la UIT.
b) Acreditación de la vigencia en el caso de persona jurídica.
c) Acreditar domicilio en el país.
d) Acreditar contar con la infraestructura y capacidad tecnológica para la prestación de los servicios de intermediación electrónica de conformidad con las exigencias previstas en las normas técnicas peruanas vigentes.
e) Declaración jurada de aceptación de auditorías cuando la AAC lo requiera.
f) Cumplir los demás requisitos exigidos por la AAC.

CAPÍTULO IV

DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 53°.- Acuerdos de reconocimiento mutuo

La AAC podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de los certificados digitales otorgados en el extranjero y extender la interoperabilidad de la IOFE. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley y su Reglamento.

Artículo 54°.- Reconocimiento

La AAC podrá reconocer los certificados digitales emitidos por Entidades Extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las que deben velar por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas Entidades de Certificación nacionales que utilicen los servicios de Entidades de Certificación extranjera, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para tal efecto, la entidad extranjera deberá comunicar a la AAC el nombre de aquellas entidades de certificación que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.

La AAC emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así como los mecanismos adecuados de información a los agentes del mercado.

Artículo 55°.- Certificación cruzada

Las Entidades de Certificación acreditadas pueden realizar certificaciones cruzadas con Entidades de Certificación Extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero, incorporándolos como suyos dentro de la IOFE, siempre y cuando obtengan autorización previa de la AAC.

Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.

Las Entidades de Certificación acreditadas que realicen certificaciones cruzadas conforme al primer párrafo del presente artículo, garantizarán ante la AAC que las firmas electrónicas y/o certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la IOFE, y que cumplen las funciones señaladas en el artículo 2° de la Ley.

CAPÍTULO V

DE LA SUPERVISIÓN DE ENTIDADES ACREDITADAS

Artículo 56°.- Facultades de Supervisión

La AAC tiene la facultad de verificar la correcta prestación de los servicios de certificación y/o emisión de

firmas electrónicas así como de los servicios de registro o verificación y el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la IOFE, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, el Reglamento, y en sus Resoluciones.

Artículo 57°.- Aporte por Supervisión y Control Anual

De conformidad con la Ley N° 28403, la AAC recaudará de las entidades privadas de certificación y de verificación o registro acreditadas bajo su ámbito, un aporte por supervisión y control anual, el cual no podrá exceder del 0.8% del valor de la facturación anual, deducido del Impuesto General a las Ventas y el Impuesto de Promoción Municipal.

Artículo 58°.- Fiscalización

La AAC ejercerá su facultad fiscalizadora y sancionadora de conformidad con lo dispuesto en el Decreto Ley N° 25868. Las sanciones a aplicar son determinadas por la AAC en el marco de la Decisión Andina 562 dada la naturaleza de reglamento técnico de la presente norma.

DISPOSICIONES FINALES

Primera.- Cooperación Internacional

Las entidades del Sector Público Nacional pueden suscribir acuerdos de cooperación con sus similares a nivel mundial o con instituciones de cooperación internacional, para recibir apoyo, asesoría y financiamiento para el desarrollo de las firmas electrónicas y transacciones electrónicas en general en la Administración Publica. Encargándose al Consejo Nacional de Ciencia Tecnología e Innovación Tecnológica - CONCYTEC para que en coordinación con la ECERNEP, la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI y la AAC desarrolle las acciones tendientes, dentro del marco de la investigación e innovación tecnológica, a masificar el uso de las firmas electrónicas en las Administración Publica.

Segunda.- Procedimiento administrativo contra decisiones de las Entidades de Certificación

Las Entidades de Certificación deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las mismas que deberán ser atendidas en el más breve plazo. La AAC aprueba o reforma estos procedimientos y regula todo lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante la entidad de certificación, procede recurrir en vía administrativa ante la AAC, con sujeción a la Ley N° 27444 - Ley del Procedimiento Administrativo General. La AAC determinará todos aquellos procedimientos y políticas necesarios para la aplicación del Reglamento. En los casos que proceda la reclamación, adoptará las medidas correctivas pertinentes.

Tercera.- Avances Tecnológicos

Dentro del marco conformado por la Ley y el presente Reglamento, la AAC podrá apoyarse en la Comisión de Reglamentos Técnicos y Comerciales del INDECOPI y en las resoluciones que ésta emita y que sean necesarias para mantener la normativa compatible con la evolución tecnológica de la materia y el desarrollo de las necesidades de los usuarios de la Infraestructura Oficial de Firma Electrónica. Asimismo la AAC, procederá a modificar o sustituir las "Disposiciones Complementarias al Reglamento de la Ley de Firmas y Certificados Digitales" aprobadas por la Resolución Comisión de Reglamentos Técnicos y Comerciales N° 0103-2003/CRT-INDECOPI del 23 de octubre de 2003, para compatibilizarlas dentro del marco de este reglamento.

Cuarta.- Almacenamiento digital

Los notarios y fedatarios públicos o particulares, autorizados de conformidad con el Decreto Legislativo N° 681 y sus normas modificatorias y reglamentarias podrán brindar el servicio almacenamiento digital de documentos.

En el caso de las entidades públicas, las oficinas de informática y sistemas o quien haga sus veces serán responsables del archivo digital de la documentación institucional y de su autenticidad, así como de aquella en la cual interviene el fedatario institucional de conformidad con lo previsto en el artículo 127° de la Ley N° 27444, Ley del Procedimiento Administrativo General. Para estos efectos el titular de las mencionadas oficinas utilizará la firma digital en los términos del artículo 19 del presente Reglamento.

Mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros se podrán establecer criterios para regular el archivo digital de documentos en el ámbito de la Administración Pública.

Quinta.- Disposiciones complementarias de la Ley N° 28403.

Las normas y disposiciones complementarias de la Ley N° 28403 deberán ser dadas por Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

Sexta.- Adecuación del Texto Único de Procedimientos Administrativos del Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (INDECOPI)

En un plazo no mayor de 45 días calendario contados a partir de la vigencia del presente Reglamento, se deberá adecuar de acuerdo a Ley, el Texto Único de Procedimientos Administrativos del Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (INDECOPI), incorporando los procedimientos correspondientes en su calidad de Autoridad Administrativa Competente de la IOFE.

Sétima.- Plazo de Implementación

El RENIEC tendrá un plazo no mayor de 1 (un) año a partir de la vigencia del presente Reglamento, para implementar y poner al servicio de las personas naturales, de las personas jurídicas y de las entidades del Estado, la infraestructura indicada en el artículo 34° del presente Reglamento.

Después de vencido el plazo, la ECERNEP emitirá los certificados raíz correspondientes a las ECEP acreditadas o reconocidas por la AAC, con el fin de garantizar la interoperabilidad y la confianza en el uso de los certificados digitales emitidos por las mismas.

Octava.- Glosario de Términos

De conformidad con lo establecido por la segunda disposición complementaria, transitoria y final de la Ley, se incluye el Glosario de Términos siguiente:

Acreditación.- Acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en el Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Agente Automatizado.- Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.

Autenticación.- Proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente (AAC).- Organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso

de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

Certificación Cruzada.- Acto por el cual una certificadora acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la Autoridad Administrativa Competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

Certificado Digital.- Documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Clave Privada.- Es un sistema de criptografía asimétrica que se emplea para generar una firma electrónica sobre un mensaje de datos y es mantenida en reserva por el titular de la firma electrónica.

Clave Pública.- En un sistema de criptografía asimétrica, que es usada por el destinatario de un mensaje de datos para verificar la firma electrónica puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

Código de verificación.- Secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Criptografía Asimétrica.- Rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el mensaje a su forma original (clave pública). Las claves están matemáticamente relacionadas de tal modo que cualquier de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.

Declaración de Prácticas de Certificación.- Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

Declaración de Prácticas de Registro o Verificación.- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.

Depósito de Certificados.- Sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.

Destinatario.- Persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico, siempre y cuando no actúe a título de intermediario.

Documento.- Cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.

Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.

Entidad de Certificación.- Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Certificación Extranjera.- La que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.

Entidad de Registro o Verificación.-Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificado digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Estándares Técnicos Internacionales.- Requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Estándares Técnicos Nacionales.- Estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales - CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.

Infraestructura Oficial de Firma Electrónica (IOFE).- Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a Ley. El sistema incluye la generación de firmas electrónicas, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).

Integridad.- Característica que indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el iniciador hasta su recepción por el destinatario.

Lista de Certificados Digitales Revocados (LCR).- Es aquella en la que se deberán incorporar todos los certificados cancelados o revocados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.

Mecanismos de Firma Electrónica.- Un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma. Dichos mecanismos varían según el nivel de seguridad que se les aplique.

Medios Telemáticos.- Conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

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

Neutralidad Tecnológica.- Principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, asimismo la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.

Niveles de Seguridad.- Son los diversos niveles de garantía que ofrecen las variedades de firmas electrónicas, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

Par de Claves.- En un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.

Reconocimiento de Servicios de Certificación Prestados en el Extranjero.- Proceso a través del cual la Autoridad Administrativa Competente, acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.

Reglamento.- El presente Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Servicio de Intermediación Electrónica.- Servicios de valor añadido complementarios de la firma digital brindado dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que permiten certificar los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónica dentro de la Infraestructura Oficial de Firma Digital es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

Titular de Certificado Digital.- Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Titular de Firma Electrónica.- Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado electrónicamente utilizando su clave privada. Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado a partir del cual se generan dichas firmas digitales.

15539-14

Encargan el Despacho de la Presidencia de la República a la Segunda Vicepresidenta

RESOLUCIÓN SUPREMA
Nº 008-2007-PCM

Lima, 12 de enero de 2007

CONSIDERANDO:

Que, el señor Presidente Constitucional de la República, doctor Alan García Pérez, viajará a la República del Ecuador, el día 15 de enero del presente año, con la finalidad de participar en las Ceremonias de Transmisión de Mando Presidencial en dicho país;

Que el señor Luis Giampietri Rojas, Primer Vicepresidente de la República, ha solicitado no asumir las funciones del Despacho de la Presidencia de la República, por tener que atender asuntos de índole personal el día 15 de enero de 2007;

Que, en consecuencia, es necesario encargar las funciones del Despacho de la Presidencia de la República a la señora Zoila Lourdes Mendoza del Solar, Segunda Vicepresidenta de la República, en tanto dure la ausencia del señor Presidente de la República;

De conformidad con el Artículo 115º de la Constitución Política del Perú; y,

Estando a lo acordado;

SE RESUELVE:

Artículo 1º.- Encargar el Despacho de la Presidencia de la República a la señora Zoila Lourdes Mendoza del Solar, Segunda Vicepresidenta de la República, a partir del día 15 de enero de 2007 y en tanto dure la ausencia del señor Presidente de la República.

Artículo 2º.- La presente Resolución Suprema será refrendada por el Presidente del Consejo de Ministros.

Regístrese, comuníquese y publíquese.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

15581-1

Ratifican contenido de resoluciones por las que se crearon Comisiones Técnicas encargadas del análisis y revisión de normatividad vigente en materia de incautación y decomiso de bienes muebles a favor del Estado y de la Ley Nº 24973

RESOLUCIÓN MINISTERIAL
Nº 418-2006-PCM

Lima, 22 de noviembre de 2006

Visto el Oficio Nº 2398-2006-JUS/SG de la Secretaría General del Ministerio de Justicia;

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 245-2006-JUS se conformó la Comisión Técnica encargada del análisis y revisión de la normatividad legal y reglamentaria vigente en materia de incautación y decomiso de bienes muebles e inmuebles a favor del Estado, con la finalidad de proponer normas para su sistematización, unificación y ordenación;

Que, de igual modo, mediante Resolución Ministerial Nº 254-2006-JUS se conformó la Comisión Técnica encargada del análisis y revisión de la Ley Nº 24973, que creó el Fondo Indemnizatorio de Errores Judiciales y Detenciones Arbitrarias;

Que, el artículo 5º del Decreto Ley Nº 21292 dispone que las comisiones de carácter multisectorial son conformadas por Resolución del Presidente del Consejo de Ministros;

Que, en salvaguarda de la importante labor que han venido cumpliendo las referidas comisiones técnicas; y a efecto de cumplir con la formalidad establecida por la norma antes citada, es necesario que se ratifique la conformación de las mismas, así como las demás disposiciones que se le vinculan;

De conformidad con lo establecido en el Decreto Legislativo Nº 560 – Ley del Poder Ejecutivo y el Decreto Ley Nº 21292;