- Zonificación y categorización de circunscripciones político - administrativas.
- Planificación y estudios de prospectiva territorial.
- Gobernanza y Gestión Territorial.
- Gestión Legal y solución de controversias territoriales y Arbitraje Territorial."

Artículo 2.- Refrendo
El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

Dado en la Casa de Gobierno, en Lima, a los veintiocho días del mes de abril del año dos mil dieciséis.

OLLANTA HUMALA TASSO
Presidente de la República

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1374215-1

Aprueban medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado

DECRETO SUPREMO
Nº 026-2016-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, la Ley Nº 27269, Ley de Firmas y Certificados Digitales, tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad;

Que, la precitada Ley es de aplicación a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos, tal como lo dispone en su artículo 2;

Que, mediante el Decreto Supremo Nº 052-2008-PCM, se aprobó el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, a través del cual se regula, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica;

Que, la Única Disposición Complementaria Transitoria del Decreto Supremo N° 105-2012-PCM dispuso que la Secretaria Técnica del Consejo Nacional de la Competitividad convoque a un equipo técnico de trabajo, liderado por la Oficina Nacional de Gobierno Electrónico de la Presidencia del Consejo de Ministros, para diseñar una propuesta para el fortalecimiento de la Infraestructura Oficial de Firma Electrónica y la implementación progresiva de la firma digital en el sector público y privado;

Que, en el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0, aprobado mediante Decreto Supremo Nº 066-2011-PCM, se establece como una de las estrategias del Objetivo 7: Promover una Administración Pública de calidad orientada a la población, la acción de impulsar la interoperabilidad entre las entidades del Estado para la cooperación, el desarrollo, la integración y la prestación de más y mejores servicios públicos para la sociedad, siendo uno de sus componentes el uso de las firmas y certificados digitales;

Que, a través del Decreto Supremo Nº 004-2013-PCM se aprobó la Política Nacional de Modernización de la Gestión Pública y mediante la Resolución Ministerial Nº 048-2013-PCM se aprobó el Plan Nacional de Simplificación Administrativa 2013-2016, cuyo Objetivo Estratégico 2º consiste en promover la incorporación progresiva de las tecnologías de la información y de la comunicación como una estrategia para brindar servicios y trámites de calidad a los ciudadanos y empresas; de esa manera se promueve con dicho fin el uso de herramientas informáticas estandarizadas, procedimientos en línea y el intercambio de información entre entidades públicas para lo cual se establece como acciones la implementación de la firma digital y del expediente electrónico; así como la incorporación de los procedimientos administrativos más demandados en la Plataforma de Interoperabilidad del Estado peruano;

Que, mediante el Decreto Supremo Nº 081-2013-PCM, se aprobó la Política Nacional de Gobierno Electrónico 2013 – 2017, constituyéndose en el principal instrumento para el desarrollo y despliegue del Gobierno Electrónico en el Perú, siendo de alcance nacional y cumplimiento obligatorio por parte de todas las entidades de la Administración Pública a nivel del gobierno nacional, gobiernos regionales y gobiernos locales;

Que, de acuerdo a lo dispuesto en el artículo 5 del Decreto Supremo Nº 081-2013-PCM, la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros - ONGEI-PCM, coordina y supervisa la implementación de la Política Nacional de Gobierno Electrónico en los tres niveles de gobierno: nacional, regional y local; asimismo, la Única Disposición Complementaria Final del citado Decreto Supremo señala que la ONGEI-PCM se encuentra facultada para emitir directivas u otros documentos complementarios en el marco de la Política Nacional de Gobierno Electrónico que coadyuven al cumplimiento de ésta;

Que, en tal sentido, emerge la necesidad de aprobar las medidas para el fortalecimiento de la Infraestructura Oficial de Firma Electrónica - IOFE y la implementación progresiva de la firma digital en el sector público y privado; y,

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; en la Ley Nº 27269, Ley de Firmas y Certificados Digitales; su Reglamento,

aprobado por el Decreto Supremo Nº 052-2008-PCM; el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM;

DECRETA:

Artículo 1.- Objeto

La presente norma tiene por objeto aprobar las medidas para el fortalecimiento de la Infraestructura Oficial de Firma Electrónica - IOFE y la implementación progresiva de la firma digital en el sector público y privado.

Artículo 2.- Reconocimiento de Entidades de Certificación que cumplan con estándares técnicos internacionales o sellos de confianza internacionales

2.1. Las Entidades de Certificación que cuenten con certificación internacional vigente del cumplimiento de estándares técnicos internacionales reconocidos como ISO 21188, ETSI TS 101 456, ETSI TS 102 042 u otros con las mismas características, o que cuenten con el sello de confianza Webtrust for Certification Authorities o WebTrust for Certification Authorities - Extended Validation vigente, obtenidos luego de haber sido auditados por un Auditor Webtrust autorizado, pueden emitir certificados digitales cumpliendo con el procedimiento que disponga la Autoridad Administrativa Competente - AAC para su ingreso a la IOFE, hasta que una empresa privada se acredite como Entidad de Certificación ante la AAC o se reconozca oficialmente una Entidad Extranjera en virtud de lo establecido en el Capítulo III De los Certificados Emitidos por Entidades Extranjeras del Título III del Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, aprobado mediante el Decreto Supremo Nº 052-2008-PCM.

2.2. Las Entidades de Certificación que cumplan con los estándares técnicos internacionales o sello de confianza internacional indicado en el párrafo anterior deben poner en conocimiento de la AAC, a través de sus representantes en el país, sus operaciones en el ámbito nacional para su incorporación en el Registro Oficial de Prestadores de Servicios de Certificación Digital.

2.3. Una vez que se tenga una Entidad de Certificación privada acreditada o reconocida oficialmente en el país, las entidades de certificación que cumplan con los estándares técnicos internacionales o cuenten con el sello de confianza internacional Web Trust o equivalente y que estén incorporadas en el Registro Oficial de Prestadores de Servicios de Certificación Digital, tienen un (01) año de plazo para iniciar el procedimiento de acreditación, o el reconocimiento oficial de acuerdo a las prácticas y políticas que para tal efecto apruebe la AAC. Los Certificados Digitales que dicha Entidad de Certificación genere surtirán los mismos efectos legales que los emitidos por entidades acreditadas por la AAC, hasta que cumplan su periodo de vigencia o sean revocados.

2.4. Si cumplido aquel plazo la entidad no hubiese iniciado alguno de los procedimientos mencionados, la AAC la retirará del Registro Oficial de Prestadores de Servicios de Certificación Digital.

2.5. Todos los certificados digitales a emitirse por las Entidades de Certificación acreditadas o reconocidas oficialmente deben ser distribuidos a través de Entidades de Registro o Verificación que cuenten con acreditación o reconocimiento vigente.

2.6. Las entidades que hacen las veces de Entidades de Registro o Verificación y que actualmente distribuyen los Certificados de las Entidades de Certificación incorporadas en el Registro Oficial de Prestadores de Servicios de Certificación Digital, tendrán un (01) año de plazo, contado desde la fecha de vigencia del presente Decreto Supremo, para iniciar el procedimiento de acreditación o el procedimiento de reconocimiento oficial ante la AAC de acuerdo a las prácticas y políticas que para tal efecto apruebe dicha autoridad.

2.7. Los certificados digitales a que se refiere el presente artículo también pueden ser utilizados por los administrados, en los trámites, procesos y procedimientos administrativos.

Artículo 3.- Creación del Registro Oficial de Prestadores de Servicios de Certificación Digital

3.1. Créase el Registro Oficial de Prestadores de Servicios de Certificación Digital, en adelante el Registro Oficial, en el marco de lo previsto en el Artículo 15º de la Ley N° 27269 - Ley de Firmas y Certificados Digitales.

3.2. La AAC debe incorporar y mantener a los Prestadores de Servicios de Certificación Digital en el referido Registro, en consonancia con sus funciones previstas en el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, aprobado mediante el Decreto Supremo Nº 052-2008-PCM

3.3. El Registro Oficial brinda información sobre el estado de los Prestadores de Servicios de Certificación Digital acreditados o reconocidos ante la AAC, y se encuentra a disposición para ser consultado en el portal Web institucional de la referida autoridad.

3.4. Las personas naturales y jurídicas pueden consultar el Registro Oficial de acuerdo a sus necesidades y en forma programada, para verificar la información de los Prestadores de Servicios de Certificación Digital acreditados o reconocidas en el marco de la IOFE.

Artículo 4.- Financiamiento

La implementación de las acciones previstas por el presente Decreto Supremo, se financia con cargo al presupuesto institucional de las entidades involucradas, según corresponda, sin demandar recursos adicionales al Tesoro Público, en el marco de las Leyes Anuales de presupuesto.

Artículo 5.- Refrendo

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

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Asignación de recursos para la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica - IOFE.

El INDECOPI, en su calidad de AAC de la IOFE, asigna al área encargada los recursos humanos y materiales suficientes para el adecuado desempeño de las funciones establecidas en el artículo 57 del Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM; y, en el presente Decreto Supremo. El incumplimiento de este mandato acarrea responsabilidad administrativa.

Segunda.- Certificados digitales y software utilizados en procedimientos relacionados con actividades transfronterizas

Autorícese a los funcionarios públicos que, en el cumplimiento de sus funciones, deban firmar digitalmente documentos electrónicos sobre procedimientos relacionados con actividades transfronterizas, a usar certificados digitales de proveedores privados a los que hace referencia el Artículo 2 del presente Decreto Supremo.

Tercera.- Requerimientos de copias de documentos electrónicos firmados digitalmente

Si un funcionario público requiere copia de un documento electrónico firmado digitalmente a una persona natural o jurídica, pública o privada, se entiende cumplido su mandato con la remisión de las direcciones web necesarias para consultar el archivo electrónico donde conste dicho documento y verificar su autenticidad e integridad, o con la remisión del referido documento por vía electrónica en el que se incorpore dichas direcciones web.

Por excepción, las entidades de la administración pública, a pedido expreso del solicitante, pueden expedir reproducciones impresas de los documentos electrónicos firmados digitalmente en el marco de la IOFE, siempre que incluyan en la impresión las dirección web necesarias que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la administración. El cumplimiento de dicha formalidad otorga la condición de copias auténticas a las reproducciones impresas.

Cuarta.- Uso de firmas electrónicas distintas a la digital

Las entidades de la Administración Pública y sus administrados pueden usar firmas electrónicas distintas a la firma digital, en los trámites, procesos y procedimientos administrativos, cuando dichas entidades estimen que esas firmas son apropiadas según la evaluación de riesgos realizada en función a la naturaleza de cada trámite, proceso o procedimiento administrativo.

Quinta.- Vigencia de los Certificados Digitales a que se refiere la Única Disposición Complementaria Transitoria del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por el Decreto Supremo Nº 052-2008-PCM, incorporada por el Artículo 2º del Decreto Supremo N.° 105-2012-PCM

Los Certificados Digitales que, a la fecha de entrada en vigencia de la presente norma, se emplean bajo las condiciones establecidas en la Única Disposición Complementaria Transitoria del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por el Decreto Supremo Nº 052-2008-PCM, incorporada por el Artículo 2º del Decreto Supremo N.° 105-2012-PCM, surten plenos efectos legales hasta que cumplan su período de vigencia o sean revocados.

Sexta: Registro Oficial de Prestadores de Servicios de Certificación Digital

Cualquier referencia al Registro Oficial de Prestadores de Servicios de Certificación Digital se entiende en el marco de lo establecido por el Artículo 15 de la Ley Nº 27269, Ley de Firmas y Certificados Digitales.

En un plazo no mayor a sesenta (60) días calendario, contados desde el día siguiente de la publicación del presente Decreto Supremo, la AAC, con la asistencia técnica de la ONGEI-PCM, implementa el referido Registro y habilita el acceso a éste a través de su portal web institucional.

Séptima: Vigencia del numeral 3.4. del Artículo 3

Lo dispuesto en el numeral 3.4. del Artículo 3 del presente Decreto Supremo entra en vigencia en el plazo de sesenta (60) días calendario, contados desde el día siguiente de la publicación del presente Decreto Supremo.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

Primera: Modificación del primer párrafo e incisos b), c) y d) del artículo 6; del inciso "m" del artículo 26; de los incisos a), h) y j) del artículo 59; del artículo 61; del artículo 64; del artículo 75; de la Décimo Primera Disposición Complementaria Final y la Décima Cuarta Disposición Complementaria Final del Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado mediante el Decreto Supremo Nº 052-2008-PCM.

Modifícase el primer párrafo y los incisos b), c) y d) del artículo 6; el inciso "m" del artículo 26; los incisos a), h) y j) del artículo 59; el artículo 61; el artículo 64; el artículo 75; la Décimo Primera Disposición Complementaria Final y la Décima Cuarta Disposición Complementaria Final del Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, en los siguientes términos:

"Artículo 6.- De la firma digital

Es 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 signatario 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, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica - IOFE, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.

Las firmas digitales son las generadas a partir de certificados digitales que son:

a) Emitidos conforme a lo dispuesto en el presente Reglamento por Entidades de Certificación acreditadas ante la Autoridad Administrativa Competente.

b) Incorporados a la Infraestructura Oficial de Firma Electrónica bajo acuerdos de certificación cruzada, conforme al artículo 73 del presente Reglamento.

c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la Autoridad Administrativa Competente conforme al artículo 71 del presente Reglamento.

d) Emitidos por Entidades de Certificación extranjeras que hayan sido incorporados por reconocimiento a la Infraestructura Oficial de Firma Electrónica conforme al artículo 72 del presente Reglamento".

"Artículo 26.- De las obligaciones

Las Entidades de Certificación registradas tienen las siguientes obligaciones:

a) Cumplir con los requerimientos de la Autoridad Administrativa Competente en lo referente a la Política de Certificación, Declaración de Prácticas de Certificación, Política de Seguridad, Política de Privacidad y Plan de Privacidad. Estos documentos deberán ser aprobados por la Autoridad Administrativa Competente dentro del procedimiento de acreditación.

b) 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.

c) Mantener el control y la reserva de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Mantener la debida diligencia y cuidado respecto a la clave privada de la Entidad de Certificación, estando en la obligación de comunicar inmediatamente a la Autoridad Administrativa Competente cualquier potencial o real compromiso de la clave privada.

d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia. No almacenar las claves privadas de los usuarios finales a menos que correspondan a certificados cuyo uso se limite al cifrado de datos.

e) Cancelar el certificado digital al suscitarse alguna de las causales establecidas en el artículo 17 del presente Reglamento. Las causales y condiciones bajo las cuales deba efectuarse la cancelación del certificado deben ser estipuladas en los contratos de los titulares y suscriptores.

f) Mantener la confidencialidad de la información relativa a los titulares y suscriptores de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido del titular o suscriptor del certificado digital (según sea el caso) realizado mediante un mecanismo que garantice el no repudio, debiendo respetar para tales efectos los lineamientos establecidos por la Autoridad Administrativa Competente y contenidos en la Norma Marco sobre Privacidad.

g) Mantener la información relativa a los certificados digitales, por un período mínimo de diez (10) años a partir de su cancelación.

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

i) Informar y solicitar autorización a la Autoridad Administrativa Competente respecto de acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.

j) Informar y solicitar autorización a la Autoridad Administrativa Competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras.

k) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 27 del presente Reglamento.

l) Brindar todas las facilidades al personal autorizado

por la Autoridad Administrativa Competente para efectos de supervisión y auditoría.

m) Demostrar que los controles técnicos que emplea son adecuados y efectivos a través de la verificación independiente del cumplimiento de los requisitos especificados en los estándares técnicos o sellos de confianza vigentes e internacionalmente reconocidos que la AAC haya aprobado en el marco de sus funciones.

n) Acreditar domicilio en el país.

Estas obligaciones podrán ser precisadas por la Autoridad Administrativa Competente, a excepción de las que señale expresamente la Ley."

"Artículo 59.- De la presentación de la solicitud de acreditación de Entidades de Certificación

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

a) El pago por derecho de solicitud de acreditación de Entidades de Certificación, según el monto correspondiente indicado en el TUPA del INDECOPI.

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

c) Los documentos que acrediten contar con un domicilio en el país.

d) Los documentos que acrediten contar con la infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de la visita comprobatoria de la Autoridad Administrativa Competente.

e) Los procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el presente Reglamento.

f) La Política de Certificación, la Declaración de Prácticas de Certificación, la Política de Seguridad, la Política de Privacidad y el Plan de Privacidad, y documentación que comprende el sistema de gestión implementado conforme al inciso d) del artículo 20 del presente Reglamento.

g) La declaración jurada del cumplimiento de los requisitos señalados en los Incisos c) y d) del artículo 20 del presente Reglamento; información que será comprobada por la Autoridad Administrativa Competente.

h) La documentación que acredite el cumplimiento de lo dispuesto en los artículos 26 y 27 del presente Reglamento.

i) El informe favorable de la entidad sectorial correspondiente, cuando lo solicite la Autoridad Administrativa Competente, para el caso de personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.

j) Tratándose de servicios de certificación digital prestados por Entidades de Certificación de empresas no domiciliadas en el país, deberán acreditar:

1. Poder que la empresa extranjera no domiciliada otorga al representante legal en el Perú.
2. Copia del instrumento correspondiente que evidencie la constitución formal de la empresa así como la inscripción en la entidad o autoridad competente en el lugar de origen del proveedor; a fin de verificar si el objeto social de la empresa coincide con las actividades de Prestador de Servicios de Certificación Digital.
3. Acreditar establecimiento en el territorio nacional.
4. Contar con los seguros o garantías bancarias que respalden sus certificados según lo indicado en artículo 27 del presente reglamento.
5. Documentos que acrediten vinculación con una o más Entidades de Registro o Verificación acreditadas.

Los documentos que se acompañen deberán encontrarse en idioma español. Si las fuentes originales provinieran de otro idioma, éstas deberán ser traducidas de manera oficial."

"Artículo 61º.- De la 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 Autoridad Administrativa Competente, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:

a) El pago por derecho de solicitud de acreditación de Entidades de Certificación, según el monto correspondiente indicado en el TUPA del INDECOPI.

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

c) Los documentos que acrediten contar con domicilio en el país.

d) Los documentos que acrediten contar con la infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de las visitas comprobatorias de la Autoridad Administrativa Competente.

e) Los procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el presente Reglamento.

f) Las Políticas de Registro, la Declaración de Prácticas de Registro o Verificación, la Política de Seguridad, la Política y el Plan de Privacidad.

g) La declaración jurada del cumplimiento de las obligaciones y los requisitos señalados en los artículos 30º y 31º del presente Reglamento."

"Artículo 64.- De la presentación de la solicitud de acreditación de los Prestadores de Servicios de Valor Añadido

La solicitud para la acreditación de Prestadores de Servicios de Valor Añadido debe presentarse a la Autoridad Administrativa Competente, observando lo señalado en los artículos anteriores y adjuntando lo siguiente:

a) El pago por derecho de solicitud de acreditación de Entidades de Certificación, según el monto correspondiente indicado en el TUPA del INDECOPI.

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

c) Los documentos que acrediten contar con domicilio en el país.

d) Los documentos que acrediten contar con la infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de la visita comprobatoria de la Autoridad Administrativa Competente.

e) La Declaración de Prácticas de Valor Añadido, la Política de Seguridad, y la Política y el Plan de Privacidad.

f) La declaración jurada de tener operativo el software, hardware y demás componentes adecuados para la prestación de servicios de valor añadido y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren la interoperabilidad y las condiciones exigidas por la Autoridad Administrativa Competente.

g) La declaración jurada del cumplimiento de las obligaciones y los requisitos señalados en los artículos 37 y 38 del presente Reglamento."

"Artículo 75.- De la fiscalización

La Autoridad Administrativa Competente ejercerá su facultad fiscalizadora y sancionadora de conformidad con lo dispuesto en el **Decreto Legislativo Nº 1033 – Decreto Legislativo que aprueba la Ley de Organización y**

Funciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI. Las sanciones a aplicar son determinadas por la Autoridad Administrativa Competente en el marco de la Decisión Andina 562 dada la naturaleza de reglamento técnico de la presente norma.

La Autoridad Administrativa Competente debe aplicar el Reglamento de infracciones y sanciones a que se refiere el inciso r) del artículo 57 de este Reglamento a efectos de regular el procedimiento administrativo sancionador a ser seguido en caso de incumplimiento o infracción al presente Reglamento, las Guías de Acreditación de los Prestadores de Servicios de Certificación Digital y demás disposiciones vinculadas a la Infraestructura Oficial de Firma Electrónica; asimismo, debe fiscalizar el cumplimiento de lo establecido en las Políticas de Certificación, de Registro o Verificación y de Valor Añadido, las Declaraciones de Prácticas de Certificación, de Registro o Verificación y de Valor Añadido, las Políticas de Seguridad y las Políticas y Planes de Privacidad"

"DISPOSICIONES COMPLEMENTARIAS FINALES

(…)

Décimo Primera.- De la contratación de seguros o garantías bancarias

A fin de fomentar el registro de los Prestadores de Servicios de Certificación Digital ante la Autoridad Administrativa Competente, como presupuesto indispensable para la efectiva operación de la infraestructura Oficial de Firma Electrónica y el desarrollo de las transacciones de Gobierno y Comercio electrónico seguras, exonérese a los Prestadores de Servicios de Certificación Digital, hasta el 31 de diciembre de 2016, de la contratación de seguros o garantías bancarias previstas en los artículos 27, 31 y 38 del presente Reglamento; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos."

"Décima Cuarta Disposición Complementaria Final.- Glosario de Términos

(…)

Declaración de Prácticas de Valor Añadido.-

Documento oficialmente presentado por un Prestador de Servicios de Valor Añadido a la Autoridad Administrativa Competente, mediante el cual define las prácticas y procedimientos que emplea en la prestación de sus servicios."

Segunda: Incorporación de un segundo párrafo en el artículo 23; del inciso "o" en el artículo 26; de un segundo párrafo en el artículo 34; del tercer párrafo en el artículo 45 y el artículo 58-A al Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM.

Incorpórese el segundo párrafo en el artículo 23; el inciso "o" en el artículo 26; un segundo párrafo en el artículo 34; un tercer párrafo en el artículo 45 y el artículo 58-A en el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, conforme a los siguientes textos:

"Artículo 23.- De las modalidades

Los Prestadores de Servicios de Certificación Digital (PSC) pueden adoptar cualquiera de las modalidades siguientes:

a) Entidad de Certificación.
b) Entidad de Registro o Verificación.
c) Prestador de Servicios de Valor Añadido.

Cuando la evolución tecnológica lo haga necesario, la AAC puede proponer las modificaciones que corresponda al Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, a fin de establecer modalidades adicionales para los Prestadores de Servicios de Certificación Digital, en base a estándares técnicos internacionales; servicios que contarán con la presunción de no repudio para las transacciones realizadas por los usuarios de dichos servicios.

De conformidad con lo establecido en la Ley, resulta factible que una misma Entidad preste sus servicios en más de una de las modalidades establecidas anteriormente. No obstante, deberá contar con una acreditación independiente y particular para cada una de las modalidades de prestación de servicios de certificación que decida adoptar, a efectos de formar parte de la Infraestructura Oficial de Firma Electrónica."

"Artículo 26.- De las obligaciones

Las Entidades de Certificación registradas tienen las siguientes obligaciones:

a) Cumplir con los requerimientos de la Autoridad Administrativa Competente en lo referente a la Política de Certificación, Declaración de Prácticas de Certificación, Política de Seguridad, Política de Privacidad y Plan de Privacidad. Estos documentos deberán ser aprobados por la Autoridad Administrativa Competente dentro del procedimiento de acreditación.

b) 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.

c) Mantener el control y la reserva de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Mantener la debida diligencia y cuidado respecto a la clave privada de la Entidad de Certificación, estando en la obligación de comunicar inmediatamente a la Autoridad Administrativa Competente cualquier potencial o real compromiso de la clave privada.

d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia. No almacenar las claves privadas de los usuarios finales a menos que correspondan a certificados cuyo uso se limite al cifrado de datos.

e) Cancelar el certificado digital al suscitarse alguna de las causales establecidas en el artículo 17 del presente Reglamento. Las causales y condiciones bajo las cuales deba efectuarse la cancelación del certificado deben ser estipuladas en los contratos de los titulares y suscriptores.

f) Mantener la confidencialidad de la información relativa a los titulares y suscriptores de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido del titular o suscriptor del certificado digital (según sea el caso) realizado mediante un mecanismo que garantice el no repudio, debiendo respetar para tales efectos los lineamientos establecidos por la Autoridad Administrativa Competente y contenidos en la Norma Marco sobre Privacidad.

g) Mantener la información relativa a los certificados digitales, por un período mínimo de diez (10) años a partir de su cancelación.

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

i) Informar y solicitar autorización a la Autoridad Administrativa Competente respecto de acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.

j) Informar y solicitar autorización a la Autoridad Administrativa Competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras.

k) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 27 del presente Reglamento.

l) Brindar todas las facilidades al personal autorizado por la Autoridad Administrativa Competente para efectos de supervisión y auditoría.

m) Demostrar que los controles técnicos que emplea son adecuados y efectivos a través de la verificación independiente del cumplimiento de los requisitos especificados en los estándares técnicos o sellos de confianza vigentes e internacionalmente reconocidos que

la AAC haya aprobado en el marco de sus funciones.

n) Acreditar domicilio en el país.

o) Cumplir lo dispuesto en las normas que regulan la protección de datos personales.

Estas obligaciones podrán ser precisadas por la Autoridad Administrativa Competente, a excepción de las que señale expresamente la Ley."

"Artículo 34.- De las modalidades del Prestador de Servicios de Valor Añadido

Los Prestadores de Servicios de Valor Añadido pueden adoptar cualquiera de las modalidades siguientes:

a) Prestador de Servicios de Valor Añadido con firma digital del usuario final. En este caso, se requiere en determinada etapa del servicio de valor añadido la firma digital del usuario final en el documento.

b) Prestador de Servicios de Valor Añadido sin firma digital del usuario final. En ninguna parte del servicio de valor añadido se requiere la firma digital del usuario final.

Sin perjuicio de los sistemas o modalidades señalados en los artículos 35 y 36, la Autoridad Administrativa Competente podrá proponer las modificaciones que corresponda al Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, a fin de reconocer y admitir en la IOFE otras modalidades de servicios o sistemas de valor añadido, sustentados en estándares técnicos internacionales.

En cualquiera de los casos, el Prestador de Servicios de Valor Añadido puede contar con los servicios de un notario o fedatario con diploma de idoneidad técnica registrado ante su correspondiente colegio o asociación profesional, de conformidad con lo establecido en el Decreto Legislativo Nº 681, para los casos de prestación de servicios al amparo de lo señalado en el artículo 35 inciso a) del presente Reglamento."

"Artículo 45.- Del Documento Nacional de Identidad Electrónico - DNIe

El Documento Nacional de Identidad electrónico (DNIe) es un Documento Nacional de Identidad, emitido por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos y el ejercicio del voto electrónico presencial. A diferencia de los certificados digitales que pudiesen ser provistos por otras Entidades de Certificación públicas o privadas, el que se incorpora en el Documento Nacional de Identidad electrónico (DNIe) cuenta con la facultad adicional de poder ser utilizado para el ejercicio del voto electrónico primordialmente no presencial en los procesos electorales.

El voto electrónico presencial o no presencial se dará en la medida que la Oficina Nacional de Procesos Electorales - ONPE reglamente e implante dichas alternativas de conformidad con lo dispuesto por la Ley que establece normas que regirán para las Elecciones Generales del año 2006 - Ley Nº 28581.

Tratándose del DNIe para los menores de edad, personas con discapacidad y adulto mayor, el RENIEC dispondrá las características y condiciones técnicas especiales de dicho documento."

"Artículo 58 A.- De la presentación de la solicitud para la acreditación de software de firma digital

La solicitud para la acreditación de software de firma digital debe presentarse a la Autoridad Administrativa Competente adjuntando lo siguiente:

a) El pago por derecho de solicitud de acreditación de Entidades de Certificación, según el monto correspondiente indicado en el TUPA del INDECOPI.

b) En el caso de las personas jurídicas, los documentos que acrediten su existencia y vigencia, así como las facultades vigentes del representante.

c) Acreditar establecimiento en el territorio nacional.

d) Documento en el que consten los derechos de propiedad sobre el software o la autorización para su uso.

e) Dos (02) dispositivos electrónicos que contengan el software a evaluar en un (01) original y una (01) copia de respaldo.

La acreditación del software tendrá una vigencia de cinco (05) años."

Dado en la Casa de Gobierno, en Lima, a los veintiocho días del mes de abril del año dos mil dieciséis.

OLLANTA HUMALA TASSO
Presidente de la República

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1374214-1

Aprueban Texto Único de Procedimientos Administrativos - TUPA del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - CENEPRED

DECRETO SUPREMO
N° 027-2016-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, mediante Ley Nº 29664 se crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), como sistema interinstitucional, sinérgico, descentralizado, transversal y participativo; con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y la preparación y atención ante situaciones de desastre, a través del establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres. El Reglamento de la citada Ley fue aprobado por el Decreto Supremo N° 048-2011-PCM;

Que, el artículo 12 de la referida Ley Nº 29664, define al Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (CENEPRED), como un organismo público ejecutor con calidad de Pliego Presupuestal, adscrito a la Presidencia del Consejo de Ministros;

Que, en concordancia con la precitada Ley, el artículo 2 del Reglamento de Organización y Funciones del CENEPRED aprobado por Decreto Supremo N° 104-2012-PCM, establece entre otros, que la referida entidad es responsable técnico de coordinar, facilitar y supervisar la formulación e implementación de la Política Nacional y el Plan Nacional de Gestión del Riesgo de Desastres en los procesos de estimación, prevención y reducción del riesgo y reconstrucción;

Que, de acuerdo con establecido por el artículo 37 de la Ley N° 27444, Ley del Procedimiento Administrativo General, todas las entidades de la Administración Pública deben elaborar y aprobar o gestionar, según sea el caso, su Texto Único de Procedimientos Administrativos – TUPA, el cual debe comprender lo dispuesto por el referido artículo;

Que, a través del Decreto Supremo Nº 079-2007-PCM, se aprueban los Lineamientos para elaboración y aprobación del Texto Único de Procedimientos Administrativos - TUPA y se establecen disposiciones para el cumplimiento de la Ley del Silencio Administrativo;

Que, por Decreto Supremo Nº 062-2009-PCM, se aprueba el Formato del Texto Único de Procedimientos Administrativos - TUPA y se establecen precisiones para su aplicación;

Que, así también, por Decreto Supremo Nº 064-2010-PCM, se aprueba la metodología de determinación de costos de los procedimientos administrativos y servicios prestados en exclusividad, comprendidos en los Textos Únicos de Procedimientos Administrativos de las entidades públicas, en cumplimiento del numeral 44.6 del artículo 44 de la Ley Nº 27444;

Que, conforme al ámbito de su competencia y en observancia de lo establecido por el numeral 11.2 del artículo 11 de los Lineamientos para elaboración y aprobación del TUPA y disposiciones para el cumplimiento de la Ley del Silencio Administrativo, aprobados por el Decreto Supremo Nº 079- 2007-PCM, la Oficina General de Planeamiento y Presupuesto de la Presidencia del Consejo de Ministros ha emitido opinión técnica favorable sobre el TUPA del CENEPRED;

Que, en atención a lo expuesto y en el marco de lo preceptuado por el artículo 15 de la norma referida precedentemente, el cual faculta a la Presidencia del Consejo de Ministros aprobar el TUPA del CENEPRED mediante Decreto Supremo refrendado por el Titular del Sector; resulta necesario aprobar el TUPA de la citada entidad lo que le permitirá ordenar los procedimientos administrativos y servicios exclusivos que presta en favor de la ciudadanía;

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 27444, Ley del Procedimiento Administrativo General; el Decreto Supremo Nº 079-2007-PCM que aprueba los Lineamientos para elaboración y aprobación del TUPA y disposiciones para el cumplimiento de la Ley del Silencio Administrativo; el Decreto Supremo Nº 062-2009-PCM que aprueba el Formato del TUPA; y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM;

DECRETA:

Artículo 1º.- Aprobación del Texto Único de Procedimientos Administrativos

Apruébese el Texto Único de Procedimientos Administrativos - TUPA del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - CENEPRED, y los Formularios N° FO-01 "Solicitud de Acceso a la Información Pública" y N° FO-02 "Solicitud de Duplicado de Credencial de Inspector Técnico de Seguridad en Edificaciones", que en Anexo forman parte integrante del presente Decreto Supremo.

Artículo 2º.- Publicación

El presente Decreto Supremo y el TUPA del CENEPRED aprobado por el Artículo 1°, son publicados en el Diario Oficial El Peruano.

Asimismo, el TUPA del CENEPRED y los Formularios aprobados por el Artículo 1° se publican en el Portal del Estado Peruano (www.peru.gob.pe), en el Portal Institucional del CENEPRED (www.cenepred.gob.pe) y en el Portal de Servicios al Ciudadano y Empresas – PSCE (www.serviciosalciudadano.gob.pe), el mismo día de la publicación del presente Decreto Supremo en el Diario Oficial.

Artículo 3°.- Vigencia

El presente Decreto Supremo entra en vigencia al día siguiente de su publicación en el Diario Oficial El Peruano.

Artículo 4º.- Refrendo

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

Dado en la Casa de Gobierno, en Lima, a los veintiocho días del mes de abril del año dos mil dieciséis.

OLLANTA HUMALA TASSO
Presidente de la República

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros