REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES

DECRETO SUPREMO Nº 052-2008-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, mediante la Ley Nº 27269, modificada por la Ley Nº 27310, se aprobó la Ley de Firmas y Certificados Digitales, que regula la utilización de la firma digital otorgándole la misma validez y eficacia jurídica que la firma manuscrita u otra análoga, estableciéndose los lineamientos generales respecto de los Prestadores de Servicios de Certificación Digital y la necesidad de contar con una Autoridad Administrativa Competente encargada de regular de manera más específica esta materia.

Que, mediante el Decreto Supremo Nº 019-2002-JUS, modificado por el Decreto Supremo Nº 024-2002-JUS, se aprobó el Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, el cual finalmente fuera derogado mediante Decreto Supremo Nº 004-2007-PCM, publicado en el Diario Oficial El Peruano con fecha 14 de enero de 2007, que aprobó el Reglamento de la Ley de Firmas y Certificados Digitales.

Que, conforme a la Ley Nº 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, corresponde a esta Entidad 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. Habiéndosele señalado, en la Sétima disposición transitoria del Reglamento de la Ley de Firmas y Certificados Digitales vigente, la responsabilidad de implementar la infraestructura necesaria para la operación de la Entidad de Certificación Nacional del Estado Peruano, a fin de emitir certificados digitales para los DNI electrónicos en tarjetas inteligentes y las entidades de la Administración Pública que operen bajo la modalidad de Entidades de Certificación del Estado Peruano.

Que, ha cobrado gran importancia dentro de la Administración Pública el empleo de las nuevas tecnologías para interactuar con los ciudadanos, como mecanismos de ahorro de tiempo y costos en la tramitación de solicitudes y procedimientos administrativos. En tal sentido, mediante Ley Nº 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. Por su parte, El artículo 20.1.2 de la Ley Nº 27444 - Ley del Procedimiento Administrativo General establece entre las modalidades de notificación, las cursadas a través de medios electrónicos que permitan comprobar de manera fehaciente su acuse de recibo y quien lo recibe; asimismo el artículo 46 de la Ley Nº 27444 permite la cancelación de los derechos de tramitación mediante transferencias electrónicas de fondos; y, el artículo 123.1 de la Ley Nº 27444 señala 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.

Que, a fin de lograr un verdadero desarrollo de las transacciones de gobierno electrónico resulta indispensable establecer un sistema integral que permita acercar de manera efectiva y segura al ciudadano a la realización de transacciones por medios electrónicos, siendo para ello importante que se reconozca a los ciudadanos, al igual

que sucede en la experiencia comparada, el derecho a acceder electrónicamente a las entidades de la Administración Pública de manera sencilla, progresiva y bajo parámetros de seguridad y protección de las transacciones en sí mismas y de los datos personales utilizados en ellas.

Que, el artículo 50 del Decreto Supremo Nº 063-2007-PCM encomienda a la Oficina Nacional de Gobierno Electrónico e Informática, entre otras funciones, proponer la Estrategia Nacional de Gobierno Electrónico y coordinar y supervisar su implementación, así como también aprobar los estándares tecnológicos para asegurar las medidas de seguridad de la información en las entidades de la Administración Pública, lo que resulta indispensable para lograr la materialización del derecho ciudadano de acceso a los servicios públicos electrónicos seguros.

Que, mediante Decreto Legislativo Nº 681 se establecen las normas que regulan el uso de tecnologías avanzadas en materia de documentos e información tanto respecto a la elaborada en forma convencional cuanto a la producida por procedimientos informáticos en computadoras y sus normas técnicas, complementarias y reglamentarias, disponiendo un marco jurídico para la validez y archivo de documentos en formato digital.

Que, en consecuencia, es necesario aprobar un nuevo Reglamento de la Ley Nº 27269 modificada por Ley Nº 27310 - Ley de Firmas y Certificados Digitales.

Que, de conformidad con el Decreto Supremo Nº 066-2003-PCM y el artículo 49 del Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros, actúa como ente rector del Sistema Nacional de Informática;

De conformidad con lo dispuesto en el inciso 8) del artículo 118 de la Constitución Política del Perú, el inciso 3) del artículo 11 de la Ley Nº 29158 - Ley Orgánica del Poder Ejecutivo, la Ley Nº 27269 modificada por Ley Nº 27310 - Ley de Firmas y Certificados Digitales y el Decreto Ley Nº 25868;

DECRETA:

Artículo 1.- Aprobación
Apruébese el Reglamento de la Ley Nº 27269 modificada por Ley Nº 27310 - Ley de Firmas y Certificados Digitales, que consta de tres (3) Títulos, setenta y cinco (75) Artículos y catorce (14) Disposiciones Finales, que en Anexo forma parte del presente Decreto Supremo.

Artículo 2.- Derogación
Deróguese el Decreto Supremo Nº 004-2007-PCM.

Artículo 3.- Refrendo
El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

Dado en la Casa de Gobierno, en Lima, a los dieciocho días del mes de julio del año dos mil ocho.

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.- Del objeto
El objeto de la presente norma es regular, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica, que comprende la acreditación y supervisión de las Entidades de Certificación, las Entidades de Registro o Verificación, y los Prestadores de Servicios de Valor Añadido; de acuerdo a lo establecido en la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310, en adelante la Ley.

Reconociendo la variedad de 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 Infraestructura Oficial de Firma Electrónica no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas, siempre que cumplan los requisitos establecidos en el artículo 2 de la Ley.

Artículo 2.- De la utilización de las firmas digitales
Las disposiciones contenidas en el presente Reglamento no restringen la utilización de las firmas digitales generadas fuera de la Infraestructura Oficial de Firma Electrónica, las cuales serán válidas en consideración a los pactos o convenios que acuerden las partes.

CAPÍTULO I

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

Artículo 3.- De la validez y eficacia de la firma digital
La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica 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 documento electrónico si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica.

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 4.- De los documentos firmados digitalmente como medio de prueba
Los documentos electrónicos firmados digitalmente dentro del marco de la Infraestructura Oficial de Firma Electrónica deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos, siempre y cuando la firma digital haya sido realizada utilizando un certificado emitido por una Entidad de Certificación acreditada en cooperación con una Entidad de Registro o Verificación acreditada, salvo que se tratara de la misma entidad con ambas calidades y con la correspondiente acreditación para brindar ambos servicios, asimismo deberá haberse aplicado un software de firmas digitales acreditado ante la Autoridad Administrativa

Competente. Esto incluye la posibilidad de que a voluntad de las partes pueda haberse utilizado un servicio de intermediación digital.

La firma digital generada en el marco de la Infraestructura Oficial de Firma Electrónica garantiza el no repudio del documento electrónico original. Esta garantía no se extiende a los documentos individuales que conforman un documento compuesto, a menos que cada documento individual sea firmado digitalmente.

La comprobación de la validez de un documento firmado digitalmente se realiza en un ambiente electrónico aplicando el Software de Verificación de la firma digital. En caso de controversia sobre la validez de la firma digital, el Juez podrá solicitar a la Autoridad Administrativa Competente el nombramiento de un perito especializado en firmas digitales, sin perjuicio de lo dispuesto por los artículos 252, 264 y 268 del Código Procesal Civil.

Si el documento firmado digitalmente se ha convertido en una microforma o microarchivo, el notario o fedatario con Diploma de Idoneidad Técnica vigente cumplirá con las normas del Decreto Legislativo Nº 681 y cuidará de cumplir aquellas normas que sean pertinentes de la Ley y de este Reglamento.

Artículo 5.- De la conservación de documentos electrónicos
Cuando los documentos, registros o informaciones requieran de una formalidad para la conservación de documentos electrónicos firmados digitalmente, 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.

Para estos casos, los documentos electrónicos deberán ser conservados mediante microformas o microarchivos, observando para ello lo regulado en el Decreto Legislativo Nº 681 y normas complementarias y reglamentarias; siendo, en tales supuestos, indispensable la participación de un notario o fedatario que cuente con Diploma de Idoneidad Técnica y se encuentre registrado ante su correspondiente Colegio o Asociación Profesional conforme a lo establecido por la legislación de la materia.

CAPÍTULO II

DE LA FIRMA DIGITAL

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, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV 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 74 del presente Reglamento.

c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la Autoridad Administrativa Competente conforme al artículo 72 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 73 del presente Reglamento.

Artículo 7.- De las características de la firma digital
Las características mínimas de la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica son:

a) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado.

b) Es exclusiva del suscriptor y de cada documento electrónico firmado por éste.

c) Es susceptible de ser verificada usando la clave pública del suscriptor.

d) Su generación está bajo el control exclusivo del suscriptor.

e) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado.

Artículo 8.- De las presunciones
Tratándose de documentos electrónicos firmados digitalmente a partir de certificados digitales generados dentro de la Infraestructura Oficial de Firma Electrónica, se aplican las siguientes presunciones:

a) Que el suscriptor del certificado digital tiene el control exclusivo de la clave privada asociada.

b) Que el documento electrónico fue firmado empleando la clave privada del suscriptor del certificado digital.

c) Que el documento electrónico no ha sido alterado con posterioridad al momento de la firma.

Como consecuencia de los literales previos, el suscriptor no podrá repudiar o desconocer un documento electrónico que ha sido firmado digitalmente usando su clave privada, siempre que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.

Artículo 9.- Del suscriptor

Dentro de la Infraestructura Oficial de Firma Electrónica, 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 y suscriptores del certificado digital.

En el caso de personas jurídicas, éstas son titulares del certificado digital. Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización a través agentes automatizados, situación en la cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital.

Artículo 10.- De las obligaciones del suscriptor
Las obligaciones del suscriptor 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 suscriptor debe notificarlo de inmediato a la Entidad de Registro o Verificación o a la Entidad de Certificación que participó en su emisión para que proceda a la cancelación del certificado digital.

Artículo 11.- De la invalidez
Una firma digital generada bajo la Infraestructura Oficial de Firma Electrónica carece de validez, además de los supuestos que prevé la legislación civil, cuando:

a) Es utilizada en fines distintos para los que fue extendido el certificado.

b) El certificado haya sido cancelado conforme a lo establecido en el Capítulo III del presente Título.

CAPÍTULO III

DEL CERTIFICADO DIGITAL

Artículo 12.- De los 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 persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

Artículo 13.- De las 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 el titular la 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 y suscriptor del certificado digital.

Artículo 14.- Del procedimiento para ser titular
Las personas naturales deberán presentar una solicitud a la Entidad de Registro o Verificación; dicha solicitud deberá estar acompañada de toda la información requerida por la Declaración de Prácticas de Registro o Verificación, 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.

En el caso de personas jurídicas, la solicitud del certificado digital y el registro o verificación de su identidad deberán realizarse a través de un representante debidamente acreditado. La persona jurídica se constituirá en titular del certificado digital. Conjuntamente con la solicitud, debe indicarse la persona natural que será el suscriptor, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, las facultades de titular y suscriptor de dicho certificado corresponderán a la persona jurídica, quien asumirá la responsabilidad por el uso de dicho certificado digital.

Artículo 15.- De las obligaciones del titular
Las obligaciones del titular son:

a) Entregar información veraz durante la solicitud de emisión de certificados y demás procesos de certificación (cancelación, suspensión, re-emisión y modificación).

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

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

d) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado.

Artículo 16.- Del contenido y vigencia
Los certificados emitidos dentro de la Infraestructura Oficial de Firma Electrónica deberán contener como mínimo, además de lo establecido en el artículo 7 de la Ley, lo siguiente:

a) Para personas naturales:

* Nombres completos
* Número de documento oficial de identidad
* Tipo de documento

* Dirección oficial de correo electrónico

b) Para personas jurídicas:

* Razón social
* Número de RUC
* Nombres completos del suscriptor
* Número de documento oficial de identidad del suscriptor
* Tipo de documento del suscriptor
* Facultades del suscriptor
* Correo electrónico del suscriptor
* Dirección oficial de correo electrónico del suscriptor
* Dirección oficial de correo electrónico de la persona jurídica

La Entidad de Certificación podrá incluir, a pedido del solicitante del certificado, información adicional siempre y cuando la Entidad de Registro o Verificación compruebe de manera fehaciente 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 a lo establecido en el artículo 17 del presente Reglamento.

Artículo 17.- De las causales de cancelación
La cancelación del certificado digital puede darse:

a) A solicitud del titular del certificado digital o del suscriptor 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, dentro del plazo establecido por la Autoridad Administrativa Competente. Si una solicitud de cancelación es aprobada por la Entidad de Registro o Verificación, y luego tal entidad supere el plazo máximo en el cual debe comunicar dicha aprobación a la Entidad de Certificación correspondiente, dicha Entidad de Registro o Verificación será responsable por los daños ocasionados debido a la demora. De otro modo, habiendo sido notificada dentro del plazo establecido, la Entidad de Certificación será responsable de los daños que pueda ocasionar la demora en dicha cancelación. Del mismo modo ocurrirá en el caso que un suscriptor o titular solicite directamente a la Entidad de Certificación la cancelación de su certificado. Compete a la Autoridad Administrativa Competente establecer las sanciones respectivas.

b) Por decisión de la Entidad de Certificación (por revocación, según los supuestos contenidos en el artículo 10 de la Ley), con expresión de causa.

c) Por expiración del plazo de vigencia.

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

e) Por resolución administrativa o judicial que ordene la cancelación del certificado.

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

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

h) Por muerte, o por inhabilitación o incapacidad declarada judicialmente de la persona natural suscriptor del certificado.

i) Por solicitud de un tercero que informe y pruebe de manera fehaciente alguno de los supuestos de revocación contenidos en los incisos 1) y 2) del artículo 10 de la Ley.

j) Otras causales que establezca la Autoridad Administrativa Competente.

Las condiciones bajo las cuales un certificado digital pueda ser cancelado deben ser estipuladas en los contratos de los suscriptores y titulares.

El uso de certificados digitales con posterioridad a su cancelación conlleva la inaplicabilidad de los artículos 3, 4 y 8 del presente Reglamento.

En todos los casos la Entidad de Certificación debe indicar el momento desde el cual se aplica la cancelación, precisando la fecha, hora, minuto y segundo en la que se efectúa. La cancelación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital cuando corresponda. La Entidad de Certificación debe incluir el certificado digital cancelado en la siguiente publicación de la Lista de Certificados Digitales Cancelados.

Artículo 18.- De la cancelación del certificado a solicitud de su titular, suscriptor o representante.
La solicitud de cancelación de un certificado digital puede ser realizada por su titular, suscriptor o a través de un representante debidamente acreditado; tal solicitud podrá realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las Entidades de Certificación o las Entidades de Registro o Verificación.

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la cancelación del certificado al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

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

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

c) Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.

d) Cuando la información contenida en el certificado ya no resulte correcta.

e) Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la Entidad de Certificación.

Artículo 19.- De la cancelación por revocación
La revocación supone la cancelación de oficio de los certificados por parte de la Entidad de Certificación, quien debe contar, para tal efecto, con procedimientos detallados en su Declaración de Prácticas de Certificación.

TÍTULO II

DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA

CAPÍTULO I

ASPECTOS GENERALES

Artículo 20.- De los elementos
La Infraestructura Oficial de Firma Electrónica está constituida por:

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

b) Las políticas y declaraciones de prácticas de los Prestadores de Servicios de Certificación Digital, basadas en estándares internacionales o compatibles con los internacionalmente vigentes, que aseguren la interoperabilidad entre dominios y las funciones exigidas, conforme a lo establecido por la Autoridad Administrativa Competente.

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 literal b).

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

e) La Autoridad Administrativa Competente, así como los Prestadores de Servicios de Certificación Digital acreditados o reconocidos.

Artículo 21.- De los estándares aplicables
La Autoridad Administrativa Competente determinará los estándares compatibles aplicando el principio de neutralidad tecnológica y los criterios que permitan lograr la interoperabilidad entre componentes, aplicaciones e infraestructuras de la firma digital análogas a la Infraestructura Oficial de Firma Electrónica.

Artículo 22.- De los niveles de seguridad
A fin de garantizar el cumplimiento de los requerimientos de seguridad necesarios para la implementación de los componentes y aplicaciones de la Infraestructura Oficial de Firma Electrónica, se establecen tres niveles: Medio, Medio Alto y Alto, cuyas precisiones adicionales a lo establecido en el presente Reglamento serán definidas por la Autoridad Administrativa Competente.

El nivel de seguridad Alto se emplea en aplicaciones militares.

CAPÍTULO II

DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DIGITAL

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.

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 24.- De la acreditación
La acreditación del Prestador de Servicios de Certificación permite su ingreso a la Infraestructura Oficial de Firma Electrónica, gozando de las presunciones legales que rigen para tal supuesto. A tal efecto, el Prestador de Servicios de Certificación será inscrito en el correspondiente Registro de Prestadores de Servicios de Certificación Digital.

De manera general el proceso de acreditación se rige por lo establecido en el presente Reglamento y de manera particular por lo establecido en los Reglamentos Específicos y Guías de Acreditación aprobados para tales efectos por la Autoridad Administrativa Competente.

SECCIÓN I

DE LAS ENTIDADES DE CERTIFICACIÓN

Artículo 25.- De las funciones
Las Entidades de Certificación tendrán las siguientes funciones:

a) Emitir certificados digitales manteniendo una secuencia correlativa en el número de serie.

b) Cancelar certificados digitales.

c) Reconocer certificados digitales emitidos por entidades de certificación extranjeras que hayan sido incorporadas por reconocimiento a la Infraestructura Oficial de Firma Electrónica conforme al artículo 73 del presente Reglamento. Caso contrario, dichos certificados no gozarán del amparo de la Infraestructura Oficial de Firma Electrónica.

d) Adicionalmente a las anteriores funciones, realizará las señaladas en los artículos 29 y 33 del presente Reglamento, en caso opten por asumir las funciones de Entidad de Registro o Verificación, o de Prestador de Servicios de Valor Añadido, respectivamente.

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 el estándar WebTrust for Certification Authorities y la obtención del sello de Webtrust.

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 27.- De la responsabilidad por riesgos
Para operar en el marco de la Infraestructura Oficial de Firma Electrónica y afrontar los riesgos que puedan surgir como resultado de sus actividades de certificación, las Entidades de Certificación acreditadas o reconocidas, de acuerdo a los niveles de

seguridad establecidos, deberán cumplir con mantener vigente la contratación de seguros o garantías bancarias que respalden sus certificados, así como con informar a los usuarios los montos contratados a tal efecto.

La Autoridad Administrativa Competente establecerá la cuantía mínima de las pólizas de seguros o garantías bancarias, así como las medidas tecnológicas correspondientes al nivel de seguridad respectivo.

Asimismo, la Autoridad Administrativa Competente determinará los criterios para evaluar el cumplimiento de este requisito.

Artículo 28.- Del cese de operaciones
La Entidad de Certificación cesa sus operaciones en el marco de la Infraestructura Oficial de Firma Electrónica, en los siguientes casos:

a) Por decisión unilateral comunicada a la Autoridad Administrativa Competente, asumiendo la responsabilidad del caso por dicha decisión.

b) Por extinción de su personería jurídica.

c) Por cancelación 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.

f) Por decisión debidamente sustentada de la Autoridad Administrativa Competente frente al incumplimiento de los requerimientos exigidos en sus Reglamentos Específicos y Guías de Acreditación, observado en el proceso de evaluación técnica anual a que se refiere el artículo 71 del presente Reglamento.

Para los supuestos contemplados en los incisos a) y b) la Entidad de Certificación tiene un plazo de treinta (30) días calendario para notificar el cese de sus operaciones tanto a la Autoridad Administrativa Competente como a los titulares de los certificados digitales que hubiera emitido. En tales supuestos, la Autoridad Administrativa Competente deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos c), g) y h) del artículo 26 del presente Reglamento.

La Autoridad Administrativa Competente establecerá 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.

SECCIÓN II

DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 29.- De las funciones
Las Entidades de Registro o Verificación tienen las siguientes funciones:

a) Identificar a los titulares y/o suscriptores del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquél.

b) Aprobar y/o denegar, según sea el caso, las solicitudes de emisión, modificación, re-emisión, suspensión o cancelación de certificados digitales, comunicándolo a la respectiva Entidad de Certificación, según se encuentre estipulado en la correspondiente Declaración de Prácticas de Certificación.

Artículo 30.- De las obligaciones
Las Entidades de Registro o Verificación acreditadas tienen las siguientes obligaciones:

a) Cumplir con los requerimientos de la Autoridad Administrativa Competente respecto de la Política de Registro o Verificación, Declaración de Prácticas de Registro o Verificación, Política de Seguridad y Política y Plan de Privacidad. Estos documentos deberán ser aprobados por la Autoridad Administrativa Competente dentro del procedimiento de acreditación.

b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por los solicitantes del certificado digital, bajo su responsabilidad.

c) Mantener la confidencialidad de la información relativa a los suscriptores y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de registro o verificación, 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 en la Norma Marco sobre Privacidad.

d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.

e) Acreditar domicilio en el Perú.

f) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 31 del presente Reglamento.

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

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

Artículo 31.- De la responsabilidad por riesgos
Para operar en el marco de la Infraestructura Oficial de Firma Electrónica y afrontar los riesgos que puedan surgir como resultado de sus actividades de registro o verificación, las Entidades de Registro o Verificación acreditadas, de acuerdo a los niveles de seguridad establecidos, deberán cumplir con:

a) Nivel de seguridad Medio: mantener vigente la contratación de seguros o garantías bancarias y emplear para efectos de la verificación de la identidad de los ciudadanos:

* De nacionalidad peruana, la base de datos del Registro Nacional de Identificación y Estado Civil - RENIEC.

* Extranjeros, carné de extranjería actualizado (residentes) o pasaporte (no residentes); o

b) Nivel de seguridad Medio Alto: mantener vigente la contratación de seguros o garantías bancarias y emplear para efectos de la verificación de la identidad de los ciudadanos:

* De nacionalidad peruana, el sistema de identificación biométrica AFIS del Registro Nacional de Identificación y Estado Civil - RENIEC.

* Extranjeros, carné de extranjería actualizado (residentes) o pasaporte (no residentes).

La Autoridad Administrativa Competente establecerá la cuantía mínima de las pólizas de seguros o garantías bancarias.

Asimismo, la Autoridad Administrativa Competente determinará los criterios para evaluar el cumplimiento de este requisito.

Artículo 32.- Del cese de operaciones
La Entidad de Registro o Verificación cesa de operar en el marco de la Infraestructura Oficial de Firma Electrónica en los siguientes casos:

a) Por decisión unilateral comunicada a la Autoridad Administrativa Competente, asumiendo la responsabilidad del caso por dicha decisión.

b) Por extinción de su personería jurídica.

c) Por cancelación 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.

f) Por decisión debidamente sustentada de la Autoridad Administrativa Competente frente al incumplimiento de los requerimientos exigidos en sus Reglamentos Específicos y Guías de Acreditación, observado en el proceso de evaluación técnica anual a que se refiere el artículo 71 del presente Reglamento.

Para los supuestos contenidos en los incisos a) y b), la Entidad de Registro o Verificación tiene un plazo de treinta (30) días calendario para notificar el cese de sus operaciones a la Autoridad Administrativa Competente debiendo dejar constancia ante aquélla de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 30 del presente Reglamento.

SECCIÓN III

DE LOS PRESTADORES DE SERVICIOS DE VALOR AÑADIDO

Artículo 33.- De las funciones
Los Prestadores de Servicios de Valor Añadido tienen las siguientes funciones:

a) Participar en la transmisión o envío de documentos electrónicos firmados digitalmente, siempre que el usuario lo haya solicitado expresamente.

b) Certificar los documentos electrónicos con fecha y hora cierta (Sellado de Tiempo) o en el almacenamiento de tales documentos, aplicando medios que garanticen la integridad y no repudio de los datos de origen y recepción (Sistema de Intermediación Digital).

c) Generar certificados de autenticación a los usuarios que lo soliciten. Dichos certificados serán utilizados sólo en caso que se requiera la autenticación del usuario para el control de acceso a domicilios electrónicos correspondientes a los servicios vinculados a notificaciones electrónicas. Su uso fuera del servicio, en aplicaciones ajenas al Prestador de Servicios de Valor Añadido que lo emitió, no gozará del amparo de la Infraestructura Oficial de Firma Electrónica.

Los usuarios que así lo deseen podrán emplear su propio certificado digital de autenticación para los usos descritos en el presente inciso.

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.

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 35.- De las modalidades del Prestador de Servicios de Valor Añadido con firma digital del usuario final
Los Prestadores de Servicios de Valor Añadido que realizan procedimientos con firma digital del usuario final, podrán a su vez adoptar dos modalidades:

a) Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo.

b) Sistema de Intermediación Digital cuyo procedimiento no concluye en microforma o microarchivo.

En la modalidad de Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo y se requiera de una formalidad para la conservación de documentos electrónicos firmados digitalmente, se deberá respetar para tales efectos lo establecido en el artículo 5 del presente Reglamento.

Artículo 36.- De la modalidad del Prestador de Servicios de Valor Añadido sin firma digital del usuario final
El Prestador de Servicios de Valor Añadido sin firma digital del usuario final se refiere al sistema de Sellado de Tiempo, el cual permite consignar la fecha y hora cierta de la existencia de un documento electrónico.

Artículo 37.- De las obligaciones
Los Prestadores de Servicios de Valor Añadido tienen las siguientes obligaciones:

a) Cumplir con los requerimientos de la Autoridad Administrativa Competente respecto de la Política de Valor Añadido, Declaración de Prácticas de Servicios de Valor Añadido, Política de Seguridad, Política 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 para la prestación de sus servicios.

c) Mantener la confidencialidad de la información relativa a los usuarios de los servicios, limitando su empleo a las necesidades propias del servicio de valor añadido prestado, salvo orden judicial o pedido del usuario utilizando medios que garanticen el no repudio, debiendo respetar para tales efectos los lineamientos establecidos en la Norma Marco sobre Privacidad.

d) Tener operativo 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.

e) 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 presente Reglamento.

f) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 38 del presente Reglamento.

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

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

Artículo 38.- De la responsabilidad por riesgos
Para operar en el marco de la Infraestructura Oficial de Firma Electrónica y afrontar los riesgos que puedan surgir como resultado de sus actividades de valor añadido, los Prestadores de Servicios de Valor Añadido acreditados, de acuerdo a los niveles de seguridad establecidos, deberán cumplir con:

a) Nivel de seguridad Medio: mantener vigente la contratación de seguros o garantías bancarias; o

b) Nivel de seguridad Medio Alto: acreditar una certificación internacional, según:

* Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo: certificación de acuerdo al Decreto Legislativo Nº 681.

* Sistema de Intermediación Digital cuyo procedimiento no concluye con una microforma o microarchivo: certificación internacional de calidad para la provisión de sus servicios, de acuerdo a lo establecido por la Autoridad Administrativa Competente.

* Sistema de Sellado de Tiempo: certificación internacional de calidad para la provisión de sus servicios, de acuerdo a lo establecido por la Autoridad Administrativa Competente.

La Autoridad Administrativa Competente establecerá la cuantía mínima de las pólizas de seguros o garantías bancarias, las certificaciones de calidad internacional, así como las medidas tecnológicas correspondientes a cada nivel de seguridad.

Asimismo, la Autoridad Administrativa Competente determinará los criterios para evaluar el cumplimiento de este requisito.

Artículo 39.- Del cese de operaciones
El Prestador de Servicios de Valor Añadido cesa de operar en el marco de la Infraestructura Oficial de Firma Electrónica en los siguientes casos:

a) Por decisión unilateral comunicada a la Autoridad Administrativa Competente), asumiendo la responsabilidad del caso por dicha decisión.

b) Por extinción de su personería jurídica.

c) Por cancelación 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) el Prestador de Servicios de Valor Añadido tiene un plazo de treinta (30) días calendario para notificar el cese de sus operaciones a la Autoridad Administrativa Competente.

f) Por decisión debidamente sustentada de la Autoridad Administrativa Competente frente al incumplimiento de los requerimientos exigidos en sus Reglamentos Específicos y Guías de Acreditación.observado en el proceso de evaluación técnica anual a que se refiere el artículo 71 del presente Reglamento;

Para los supuestos contenidos en los incisos a) y b), el Prestador de Servicios de Valor Añadido tiene un plazo de treinta (30) días calendario para notificar el cese de sus operaciones a la Autoridad Administrativa Competente debiendo dejar constancia ante aquélla de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 37 del presente Reglamento.

CAPÍTULO III

DE LA PRESTACIÓN DE SERVICIOS DE GOBIERNO ELECTRÓNICO Y DE LA CERTIFICACIÓN DIGITAL A CARGO DEL ESTADO

SECCIÓN I

ASPECTOS GENERALES

Artículo 40.- Del derecho ciudadano de acceso a servicios públicos electrónicos seguros

El ciudadano tiene derecho al acceso a los servicios públicos a través de medios electrónicos seguros para la realización de transacciones de gobierno electrónico con las entidades de la Administración Pública, como manifestación de su voluntad y en el marco de lo previsto en la Ley del Procedimiento Administrativo General - Ley Nº 27444.

Artículo 41.- De los principios generales de acceso a los servicios públicos electrónicos seguros
La prestación de servicios públicos por medios electrónicos seguros deberá respetar lo establecido para tales efectos por la Ley del Procedimiento Administrativo General - Ley Nº 27444 y en particular deberá ajustarse a los principios siguientes:

41.1. Principio de legalidad, que exige respetar y observar las garantías y normativa vigente que regula las relaciones entre los ciudadanos y las entidades de la Administración Pública, principalmente observando el marco jurídico establecido por la Ley del Procedimiento Administrativo General - Ley Nº 27444.

41.2. Principio de responsabilidad y calidad respecto a la veracidad, autenticidad e integridad de la información y servicios ofrecidos por las entidades de la Administración Pública a través de medios electrónicos.

41.3. Principio de presunción, reconocimiento y validez de los documentos electrónicos y medios de identificación y autenticación empleados en los trámites y procedimientos administrativos, siempre y cuando se respeten los lineamientos y requisitos establecidos por el presente Reglamento.

41.4. Principio de seguridad en la implantación y utilización de medios electrónicos para la prestación de servicios de gobierno electrónico, según el cual se exigirá a las entidades de la Administración Pública el respeto a los estándares de seguridad y requerimientos de acreditación necesarios para poder dotar de respaldo tecnológico y presunción legal suficiente a las operaciones que realicen por medios electrónicos, según lo establecido para tales efectos por la Autoridad Administrativa Competente.

41.5. Principio de protección de datos personales empleados en los trámites y procedimientos ante las entidades de la Administración Pública, así como aquellos mantenidos en sus archivos y sistemas, para lo cual se deberá tener en consideración los lineamientos establecidos por la Norma Marco sobre la Privacidad.

41.6. Principio de cooperación, tanto en la utilización de medios electrónicos, como en el acceso a la información obtenida de los ciudadanos por las entidades de la Administración Pública, a fin de lograr el intercambio seguro de datos entre ellas y garantizar la interoperabilidad de los sistemas y soluciones que adopten para lograr, de manera progresiva y en la medida de lo posible, la prestación integrada de servicios a los ciudadanos.

41.7. Principio de usabilidad en la prestación de los servicios de certificación, brindando la información y los sistemas de ayuda necesarios, de manera que los usuarios puedan acceder a dichos servicios de manera efectiva, eficiente y satisfactoria.

Artículo 42.- De los derechos conexos
El derecho ciudadano de acceso a servicios públicos electrónicos seguros tiene como correlato el reconocimiento de los siguientes derechos:

42.1. A relacionarse con las entidades de la Administración Pública por medios electrónicos seguros para el ejercicio de todos los derechos y prerrogativas que incluye, entre otros, los consagrados en el artículo 55 de la Ley del Procedimiento Administrativo General - Ley Nº 27444. En tal sentido, constituye obligación de la Administración Pública facilitar el ejercicio de estos derechos ciudadanos, debiendo promover la prestación de servicios por medios electrónicos. 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 trámite, procedimiento o proceso por parte de los administrados o ciudadanos ante las Entidades Públicas o entre estas entidades, no excluyendo a las representaciones del Estado Peruano en el exterior, se entenderán efectuadas de manera segura siempre y cuando sean realizados empleando firmas y certificados digitales emitidos por los Prestadores de Servicios de Certificación Digital que se encuentren acreditados y operando dentro de la Infraestructura Oficial de Firma Electrónica.

42.2. A optar por relacionarse con las entidades de la Administración Pública ya sea empleando los centros de acceso ciudadano o a través de canales seguros para la realización de transacciones de gobierno electrónico que éstas deberán poner a su disposición.

42.3. A conocer por medios electrónicos el plazo y los requisitos necesarios para el inicio de cualquier procedimiento o tramitación ante una entidad de la Administración Pública. Teniendo asimismo derecho a conocer por medios electrónicos el estado en el que tales procedimientos o trámites se encuentran y solicitar la emisión de copias y constancias electrónicas. Esto no resulta aplicable para los casos de procedimientos o trámites que pudieran afectar a la intimidad personal, las vinculadas a la seguridad nacional o las que expresamente sean excluidas por Ley.

42.4. A obtener y utilizar firmas y certificados digitales emitidos por Prestadores de Servicios de Certificación Digital acreditados y que se encuentren dentro de la Infraestructura Oficial de Firma Electrónica como medio de identificación en todo tipo de trámite y actuación ante cualquier entidad de la Administración Pública.

42.5. A presentar solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro (24) horas, para tal efecto las entidades de la Administración Pública deberán contar con un archivo electrónico detallado de recepción de solicitudes. Corresponde a la Oficina Nacional de Gobierno Electrónico e Informática, el establecimiento de los lineamientos para el cómputo de plazos en los casos de solicitudes, escritos y comunicaciones recibidas bajo estas condiciones.

42.6. A obtener servicios de gobierno electrónico de calidad, en estricta observancia de los lineamientos y requisitos establecidos para tales efectos por el presente Reglamento y por la Autoridad Administrativa Competente.

Artículo 43.- De las garantías para el acceso de los ciudadanos a los servicios públicos electrónicos seguros

Las diferentes entidades y dependencias de la Administración Pública deberán garantizar el acceso a los ciudadanos para la realización de transacciones de gobierno electrónico, debiendo para tales efectos:

a) Adecuar sus trámites y procedimientos aplicados en sus comunicaciones tanto con los ciudadanos como con las distintas entidades de la Administración Pública, a fin de llevarlos a cabo por medios electrónicos; debiendo asegurar en todo momento la disponibilidad de acceso, la integridad, la autenticidad, el no repudio y la

confidencialidad de las transacciones realizadas por estos medios, empleando para tales fines los certificados y firmas digitales emitidos dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo al artículo 4 del presente Reglamento, así como canales seguros.

b) Proveer a su personal competente de certificados digitales y sistemas basados en firma digital reconocidos por la Infraestructura Oficial de Firma Electrónica de acuerdo al artículo 4 del presente Reglamento. Asimismo, cada Administración Pública deberá brindar a sus empleados la capacitación en la utilización de las firmas y certificados digitales, y demás medios electrónicos requeridos en las actividades propias de dicha entidad. Además, deberán ser capacitados en los temas de seguridad y privacidad respecto de los documentos de carácter personal que les competen según la función o cargo que ocupen.

c) Poner a disposición de los interesados, por vía electrónica, la información actualizada acerca de los trámites y procedimientos a su cargo, con especial indicación de aquellos que resulten factibles de ser iniciados por vía electrónica.

d) Informar a los ciudadanos de las condiciones tecnológicas necesarias para el acceso a servicios públicos electrónicos seguros y, de ser el caso, el modo de obtención de los implementos o dispositivos requeridos para tal efecto.

e) El equipo informático constituido por los servidores empleados por las instituciones para la prestación y realización de transacciones de gobierno electrónico, deberá brindar las garantías necesarias para una comunicación segura, debiendo obtener los correspondientes certificados de dispositivo seguro emitidos por una Entidad de Certificación debidamente acreditada ante la Autoridad Administrativa Competente.

f) Las entidades de la Administración Pública deberán admitir la recepción de documentos firmados digitalmente de acuerdo al artículo 4 del presente Reglamento, siempre que hayan sido emitidos por Entidades de Certificación y Entidades de Registro o Verificación que se encuentren acreditadas y operen dentro de la Infraestructura Oficial de Firma Electrónica.

g) Contar con personal capacitado para brindar información a los usuarios sobre el manejo y uso de la tecnología requerida (implementos y dispositivos) para la realización de transacciones de gobierno electrónico. Esta información podrá ser proporcionada por el mencionado personal y deberá necesariamente estar incorporada en el mismo medio o instrumento requerido para la realización del trámite o solicitud correspondiente.

h) Contar con una red de puntos de acceso a nivel nacional a través de centros de acceso ciudadano que por medio de canales seguros permitan la interacción con otras dependencias de la Administración Pública. Estos centros de acceso ciudadano deberán estar dotados de personal capacitado para brindar la información y facilidades necesarias para que el ciudadano pueda realizar transacciones seguras de gobierno electrónico, debiendo igualmente contar con un servicio integral de atención de reclamos y solicitudes de información respecto al empleo de los mecanismos necesarios para la interacción con el Estado a través de medios electrónicos.

i) Implementar los procedimientos necesarios para que en los casos de ciudadanos que no cuenten con el conocimiento y la tecnología necesaria para poder realizar transacciones electrónicas, su identificación y autenticación a efectos de poder acceder a los mismos podrá ser realizada por un notario que cuente con Diploma de

Idoneidad Técnica inscrito en su correspondiente Colegio profesional. En este caso, el ciudadano deberá identificarse ante el depositario de la fe pública y prestar su consentimiento expreso, dejando constancia de ello para los casos de discrepancia o litigio.

j) Aplicar los criterios de usabilidad establecidos por la Autoridad Administrativa Competente.

Artículo 44.- De la implementación de los procedimientos y trámites administrativos por medios electrónicos seguros
A fin de lograr una correcta implementación de la prestación de servicios de gobierno electrónico a través del empleo de canales seguros, certificados y firmas digitales reconocidos por la Infraestructura Oficial de Firma Electrónica, de acuerdo con el artículo 4 del presente Reglamento, para el intercambio seguro de datos, resulta indispensable la elaboración de un análisis de rediseño funcional y simplificación de los procedimientos, trámites y servicios administrativos, debiéndose poner principal énfasis en los aspectos siguientes:

a) La creación y mantenimiento de archivos electrónicos para el almacenamiento y gestión de los documentos electrónicos generados durante los trámites y procedimientos públicos: recepción y envío de solicitudes, escritos y comunicaciones.

Las entidades de la Administración Pública, mediante convenios de colaboración, podrán habilitar sus respectivos archivos electrónicos para la recepción de solicitudes, escritos y comunicaciones de competencia de otra entidad, según lo establecido en el convenio.

Los sistemas informáticos encargados de la gestión de los archivos electrónicos emitirán automáticamente un acuse de recibo o cargo electrónico consistente en una copia autenticada del escrito, solicitud o comunicación, incluyendo la fecha y la hora de presentación y el número de ingreso al archivo.

b) El establecimiento de convenios que hagan factible el intercambio electrónico seguro de información y documentos obtenidos de los ciudadanos, entre las entidades encargadas de su archivo y las entidades interesadas, con el propósito de suprimir su reiterada solicitud.

c) La puesta a disposición de los ciudadanos de sus servicios empleando firmas digitales, certificados digitales y canales seguros que se encuentren dentro del ámbito de la Infraestructura Oficial de Firma Electrónica.

d) La protección del derecho a la intimidad y a la confidencialidad de las comunicaciones dentro de lo establecido para tales efectos por la Norma Marco sobre Privacidad.

e) El empleo de la dirección oficial de correo electrónico cuando dicho servicio sea implementado.

En cumplimiento de lo establecido en el presente artículo, las entidades de la Administración Pública que brinden el servicio de Sistema de Intermediación Digital deberán acreditarse ante la Autoridad Administrativa Competente como Prestador de Servicios de Valor Añadido para el Estado Peruano.

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.

SECCIÓN II

DE LAS TRANSACCIONES DE GOBIERNO ELECTRÓNICO EN LAS QUE INTERVIENEN PRESTADORES DE SERVICIOS DE CERTIFICACION DIGITAL PÚBLICOS

Artículo 46.- De la Estructura Jerárquica de Certificación del Estado Peruano
Las entidades que presten servicios de certificación digital en el marco de la Infraestructura Oficial de Firma Electrónica son las entidades de la administración pública o personas jurídicas de derecho público siguientes:

a) Entidad de Certificación Nacional para el Estado Peruano, 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 a la Autoridad Administrativa Competente, las políticas y estándares de las Entidades de Certificación para el Estado Peruano y Entidades de Registro o Verificación para el Estado Peruano, según los requerimientos de la Autoridad Administrativa Competente y lo establecido por el presente Reglamento.

b) Entidades de Certificación para el Estado Peruano acreditadas por la Autoridad Administrativa Competente, 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 prioritariamente 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.

c) Entidades de Registro o Verificación para el Estado Peruano acreditadas por la Autoridad Administrativa Competente, las cuales serán las encargadas del: levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los titulares y suscriptores, aceptación y autorización de solicitudes de emisión, cancelación, modificación, re-emisión y suspensión, si fuera el caso, de certificados digitales además de su gestión ante las Entidades de Certificación; para los fines previstos en el inciso b) del presente artículo.

d) Prestador de Servicios de Valor Añadido para el Estado Peruano acreditados por la Autoridad Administrativa Competente, quienes se encargarán de intervenir en la transmisión o envío de documentos electrónicos, pudiendo participar grabando, almacenando o conservando cualquier información enviada por medios electrónicos que permitan certificar los datos de envío y recepción, fecha y hora y no repudio de origen y recepción, concernientes a alguna tramitación o procedimiento realizado ante una entidad de la Administración Pública.

Las entidades señaladas en los incisos a) y b) podrán brindar servicios de valor añadido en condición de Prestador de Servicios de Valor Añadido para el Estado Peruano conforme a lo dispuesto en la Ley y el presente Reglamento, siempre y cuando cuenten con la correspondiente acreditación.

Cualquier entidad pública que cumpla con lo requerido para su acreditación ante la Autoridad Administrativa Competente puede operar bajo la modalidad de Entidad de Certificación para el Estado Peruano, Entidad de Registro o Verificación para el Estado Peruano y/o Prestador de Servicios de Valor Añadido para el Estado Peruano.

En ningún caso se admitirá la existencia de sistemas de certificación digital fuera de la Infraestructura Oficial de Firma Electrónica por parte de las entidades de la Administración Pública.

Los servicios brindados por los Prestadores de Servicios de Certificación Digital públicos 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. En consecuencia, las entidades públicas que presten servicios como Entidad de Certificación Nacional para el Estado Peruano, Entidades de Certificación para el Estado Peruano, Entidades de Registro o Verificación para el Estado Peruano y Prestador de Servicios de Valor Añadido para el Estado Peruano, sólo podrán considerar los costos asociados a la prestación del servicio al momento de determinar su valor.

Artículo 47.- De la designación de las entidades responsables
Se designa al Registro Nacional de Identificación y Estado Civil - RENIEC como Entidad de Certificación Nacional para el Estado Peruano, Entidad de Certificación para el Estado Peruano y Entidad de Registro o Verificación para el Estado Peruano. Los servicios a ser prestados en cumplimiento de los roles señalados estarán a disposición de todas las Entidades Públicas del Estado Peruano y de todas las personas naturales y jurídicas que mantengan vínculos con él, no excluyendo ninguna representación del Estado Peruano en el territorio nacional o en el extranjero.

A fin de viabilizar la prestación segura de los servicios públicos a los ciudadanos, el Registro Nacional de Identificación y Estado Civil - RENIEC deberá realizar los trámites correspondientes para su acreditación ante la Autoridad Administrativa Competente a fin de ingresar a la Infraestructura Oficial de Firma Electrónica.

Las demás entidades de la Administración Pública que opten por constituirse como Entidad de Certificación para el Estado Peruano y/o Entidad de Registro o Verificación para el Estado Peruano deberán cumplir con las políticas y estándares que sean propuestos por la Entidad de Certificación Nacional para el Estado Peruano y aprobadas por la Autoridad Administrativa Competente, y solicitar su acreditación correspondiente a fin de ingresar a la Infraestructura Oficial de Firma Electrónica.

Artículo 48.- De la Entidad de Certificación Nacional para el Estado Peruano

a) El Registro Nacional de Identificación y Estado Civil - RENIEC será la única Entidad de Certificación Nacional para el Estado Peruano y actuará también como Entidad de Certificación para el Estado Peruano y Entidad de Registro o Verificación para el Estado Peruano. Todas las Entidades de Certificación para el Estado Peruano y las Entidades de Registro o Verificación para el Estado Peruano deben seguir las políticas y estándares propuestos por la Entidad de Certificación Nacional para el Estado Peruano y aprobados por la Autoridad Administrativa Competente.

b) La Entidad de Certificación Nacional para el Estado Peruano contará con una estructura funcional y jurídica estable, no cambiante en el mediano plazo, sólo variable en la cantidad de Entidades de Certificación para el Estado Peruano y Entidades de Registro o Verificación para el Estado Peruano que pueda tener.

c) La Entidad de Certificación Nacional para el Estado Peruano y las Entidades de Certificación para el Estado Peruano observarán los lineamientos establecidos por la Autoridad Administrativa Competente en relación al 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 la interoperabilidad entre los distintos componentes tecnológicos, aplicaciones informáticas e infraestructuras de firmas digitales.

d) La Entidad de Certificación Nacional para el Estado Peruano será auditada periódicamente por la Autoridad Administrativa Competente, de conformidad con lo establecido para tales efectos en el presente Reglamento y en las correspondientes Guías de Acreditación. Los informes de auditoria deben ser tenidos en cuenta para continuar su operación.

Artículo 49.- De las Entidades de Certificación para el Estado Peruano y las Entidades de Registro o Verificación para el Estado Peruano

a) Las Entidades de Certificación para el Estado Peruano deberán ofrecer un servicio de directorio y permitir que las aplicaciones accedan a los certificados digitales emitidos y a la Lista de Certificados Digitales Cancelados, de conformidad con los lineamientos establecidos para tales efectos por la Autoridad Administrativa Competente en las correspondientes Guías de Acreditación, debiendo encontrarse actualizado dicho servicio con la frecuencia indicada en las Guías de Acreditación. Junto al Servicio de Directorio se puede disponer del servicio de consulta en línea del estado de un certificado digital.

b) Una Entidad de Certificación para el Estado Peruano podrá ofrecer distintos servicios y mecanismos para recibir un requerimiento de certificado digital, siendo necesario que en todos los casos de primera emisión de un certificado digital, el solicitante comparezca de manera personal ante la correspondiente Entidad. Además, deberá ofrecer en forma obligatoria los servicios de recepción de solicitudes de cancelación y la publicación periódica de la Lista de Certificados Digitales Cancelados. Asimismo, deberá garantizar el acceso permanente a dichos servicios, proponiendo una solución para una eventual contingencia, todo lo cual deberá encontrarse en estricta observancia de lo establecido para tales efectos por la Autoridad Administrativa Competente en sus correspondientes Guías de Acreditación.

c) Las Entidades de Certificación para el Estado Peruano deberán ofrecer el servicio de emisión y cancelación de certificados digitales, conforme a los lineamientos

establecidos por la Autoridad Administrativa Competente. Podrán ofrecer servicios de re-emisión, modificación o suspensión de certificados digitales.

d) Las Entidades de Certificación para el Estado Peruano deberán brindar el nivel de seguridad adecuado en relación a los equipos informáticos y de comunicación utilizados, el personal empleado para operar la Entidad de Certificación para el Estado Peruano, así como los responsables de operar las claves de la Entidad de Certificación para el Estado Peruano y los procedimientos utilizados para la autenticación de los datos a ser incluidos en los certificados digitales, serán establecidos de conformidad con lo señalado para tales efectos en las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.

e) Las Entidades de Certificación para el Estado Peruano y Entidades de Registro o Verificación para el Estado Peruano serán auditadas periódicamente por la Autoridad Administrativa Competente, de conformidad con lo establecido para tales efectos en el presente Reglamento y en las correspondientes Guías de Acreditación. Los informes de auditoria deben ser tenidos en cuenta para continuar su operación.

f) La integridad del Directorio de Certificados Digitales y la Lista de Certificados Digitales Cancelados debe estar permanentemente asegurada. Es responsabilidad de la Entidad de Certificación para el Estado Peruano garantizar la disponibilidad de este servicio y la calidad de los datos suministrados por éste.

g) Respecto a los elementos que componen el nombre diferenciado de un certificado digital, los nombres correspondientes al titular y suscriptor del certificado deberán ser distinguidos 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 digitales, el organismo en el cual desempeñan sus funciones o el organismo por el cual ha sido autorizada la emisión de los certificados digitales.

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

Artículo 50.- De los Prestadores de Servicios de Valor Añadido para el Estado Peruano

a) Los Prestadores de Servicios de Valor Añadido para el Estado Peruano podrán adoptar cualquiera de las dos modalidades de prestación de servicios de valor añadido a que se refiere el artículo 34 del presente Reglamento.

b) En todos los casos, los Prestadores de Servicios de Valor Añadido para el Estado Peruano que realicen procedimientos que incluyan la firma digital del usuario final, y cuyo procedimiento concluya con una microforma o microarchivo, será indispensable emplear los servicios de un notario o fedatario que cuente con Diploma de Idoneidad Técnica y se encuentre registrado ante su correspondiente Colegio o Asociación Profesional, conforme a lo establecido por el Decreto Legislativo Normas que regulan el uso de Tecnología Avanzada en materia de documentos e información - Decreto Legislativo Nº 681.

c) Los Prestadores de Servicios de Valor Añadido para el Estado Peruano serán auditados periódicamente por la Autoridad Administrativa Competente, de conformidad con lo establecido para tales efectos en el presente Reglamento y en las correspondientes Guías de Acreditación. Los informes de auditoria deben ser tenidos en cuenta para continuar su operación.

SECCIÓN III

DE LOS CENTROS DE ACCESO CIUDADANO

Artículo 51.- De los modos de acceso del ciudadano
Los ciudadanos titulares y suscriptores de certificados digitales emitidos por un Prestador de Servicios de Certificación Digital dentro de la Infraestructura Oficial de Firma Electrónica pueden realizar transacciones electrónicas a través de cualquier computador o punto de acceso que cuente con la tecnología necesaria para tales efectos, no están limitados a ningún modo en particular.

Artículo 52.- De los Centros de Acceso Ciudadano
Se entiende por Centros de Servicios Ciudadanos a los locales, instituciones o puntos que sirven para el acceso ciudadano a la realización de transacciones de gobierno electrónico prioritariamente, a fin que a través de tales Centros los ciudadanos puedan materializar los derechos a que se refieren los artículos 40, 41 y 42 del presente Reglamento.

Artículo 53.- De los elementos de los Centros de Acceso Ciudadanos
A fin de poder dotar al ciudadano de todas las facilidades necesarias para una óptima interacción con el Estado, resulta indispensable que un Centro de Acceso Ciudadano ponga a disposición de los usuarios, como mínimo, los siguientes elementos:

a) Equipos de cómputo que cuenten con lectoras de tarjetas inteligentes, incluyendo sus respectivos controladores de dispositivo (drivers), a fin de permitir a los usuarios su autenticación y empleo de firma digital para las transacciones en que ésta sea requerida.

b) Infraestructura tecnológica adecuada (computadores, equipos de red, etc.).

c) Sistemas que garanticen la seguridad en las transacciones que realizan, confidencialidad, privacidad y no almacenamiento de información personal.

d) Personal capacitado para la asistencia en el empleo de los mecanismos y dispositivos necesarios para la realización de transacciones de gobierno electrónico

e) Terminales equipados con los componentes de software necesarios para la realización de transacciones públicas a través de medios electrónicos, incluyendo los componentes de firma digital y verificación de firma digital.

Adicionalmente, los Centros de Acceso Ciudadano podrán también encargarse de la prestación de los servicios siguientes:

* Línea de producción de microformas digitales a partir de documentos en formato papel, debiendo respetar para tal efecto lo establecido por el Decreto Legislativo Nº 681.

* Archivo y almacenamiento de documentos electrónicos, debiendo para tales efectos respetar igualmente lo establecido por el Decreto Legislativo Nº 681.

* Prestación de servicios de registro o verificación, para tales efectos deberán contar con la acreditación correspondiente por parte de la Autoridad Administrativa Competente.

* Prestación de servicios de valor añadido, para tal efecto deberán contar con la acreditación correspondiente por parte de la Autoridad Administrativa Competente.

Corresponde a la Oficina Nacional de Gobierno Electrónico e Informática verificar el cumplimiento de los requisitos necesarios para operar un Centro de Acceso Ciudadano, de acuerdo a lo establecido en el presente artículo, debiendo asimismo llevar un Registro Nacional de los Centros de Acceso Ciudadano autorizados para la prestación de este tipo de servicios.

SECCIÓN IV

DEL INTERCAMBIO DE INFORMACIÓN Y COOPERACIÓN ENTRE ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

Artículo 54.- Del intercambio de documentos electrónicos por medios seguros

a) Todas las entidades de la Administración Pública contarán con facultades suficientes para la emisión válida de comunicaciones y resoluciones por medios electrónicos de todo tipo de documento administrativo, siempre que se respete para tales efectos los lineamientos establecidos por el presente Reglamento y normas complementarias.

b) El intercambio de documentos electrónicos tanto al interior de las entidades de la Administración Pública, como aquellos realizados entre entidades, requerirá para su validez y a efecto de gozar del principio de equivalencia funcional, del empleo de firmas y certificados digitales.

c) Los certificados digitales a que alude el inciso anterior, necesariamente deberán haber sido emitidos por una Entidad de Certificación para el Estado Peruano que cuente con la correspondiente acreditación por parte de la Autoridad Administrativa Competente. Las firmas digitales deben ser generadas por programas de software o componentes acreditados por la Autoridad Administrativa Competente según su Guía de Acreditación de Software.

Artículo 55.- De la cooperación de información entre las entidades de la Administración Pública

Cada entidad de la Administración Pública deberá facilitar, mediante convenios, el acceso de las demás entidades a los documentos de los ciudadanos que obren en su poder y que se encuentren en archivo electrónico, especificando las condiciones y criterios para el acceso a dicha información. La disponibilidad de dichos documentos estará limitada estrictamente a aquellos que son requeridos por las entidades de la Administración Pública para la tramitación y resolución de los procedimientos de su competencia. El acceso a los documentos con información de carácter personal estará condicionado al cumplimiento de lo establecido en la Norma Marco sobre Privacidad.

Artículo 56.- De la interoperabilidad de los sistemas para la prestación de servicios de gobierno electrónico

Las entidades de la Administración Pública utilizarán las tecnologías y sistemas para la prestación de sus servicios a los ciudadanos y para sus relaciones con las demás entidades y dependencias del Estado, aplicando medidas informáticas, tecnológicas, organizativas y de seguridad que garanticen la interoperabilidad, en estricta observancia de lo establecido para tales efectos por la Autoridad Administrativa Competente.

TÍTULO III

DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

CAPÍTULO I

DE LAS FUNCIONES

Artículo 57.- De las funciones
La Autoridad Administrativa Competente tiene las siguientes funciones:

a) Aprobar 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 de las Entidades de Certificación, de Registro o Verificación y de Valor Añadido, de los Prestadores de Servicios de Certificación tanto públicos como privados.

b) Acreditar Entidades de Certificación nacionales tanto públicas como privadas y establecer acuerdos de reconocimiento mutuo con otras Infraestructuras compatibles con la Infraestructura Oficial de Firmas Electrónicas.

c) Acreditar Entidades de Registro o de Verificación tanto públicas como privadas.

d) Acreditar a los Prestadores de Servicios de Valor Añadido tanto públicos como privados y el software que emplean en la prestación de sus servicios en los casos del artículo 34 inciso a).

e) Registrar a las entidades acreditadas señaladas en los incisos c), d) y e) del presente artículo en el Registro de Prestadores de Servicios de Certificación Digital, previsto en el artículo 15 de la Ley.

f) Supervisar a los Prestadores de Servicios de Certificación Digital.

g) Cancelar las acreditaciones otorgadas a los Prestadores de Servicios de Certificación Digital conforme a lo dispuesto en el presente Reglamento.

h) Publicar, por medios telemáticos, la relación de Prestadores de Servicios de Certificación Digital acreditados.

i) Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica, así como de otros estándares técnicos determinando su compatibilidad 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, componentes e infraestructuras de firmas digitales (análogos a la Infraestructura Oficial de Firma Electrónica en otros países).

j) Formular los criterios para el establecimiento de la idoneidad técnica de los Prestadores de Servicios de Certificación Digital, así como aquellas relacionadas con la prevención y solución de conflictos.

k) Establecer los requisitos mínimos para la prestación de los diferentes servicios a cargo de los Prestadores de Servicios de Certificación Digital.

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

m) Definir los criterios para evaluar el cumplimiento del requisito relativo al riesgo por los daños que los Prestadores de Servicios de Certificación Digital puedan ocasionar como resultado de sus actividades de certificación.

n) Suscribir acuerdos de reconocimiento mutuo con Autoridades Administrativas Extranjeras que cumplan funciones similares a las de la Autoridad Administrativa Competente.

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

p) 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.

q) Delegar a terceros, bajo sus órdenes y responsabilidad, las funciones que estime pertinentes conforme a lo previsto en el presente Reglamento.

r) Elaborar el Reglamento de infracciones y sanciones a los usuarios finales y los procedimientos correspondientes en caso de incumplimiento por parte de los Prestadores de Servicios de Certificación Digital de lo establecido en la Ley, el presente Reglamento y en los Reglamentos y Guías de Acreditación de la Autoridad Administrativa Competente.

s) Sancionar a los Prestadores de Servicios de Certificación Digital, por el incumplimiento o infracción al presente Reglamento y demás disposiciones vinculadas a la Infraestructura Oficial de Firma Electrónica, de acuerdo al Reglamento de infracciones y sanciones a que se refiere el inciso anterior.

t) Definir las precisiones adicionales a lo establecido en el presente Reglamento, correspondientes a cada uno de los niveles de seguridad contemplados en el artículo 22 del referido Reglamento, bajo los cuales podrán operar los Prestadores de Servicios de Certificación acreditados.

u) Definir los criterios para evaluar el cumplimiento de la responsabilidad por riesgos por parte de los Prestadores de Servicios de Certificación acreditados, considerando los niveles de seguridad establecidos.

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

Se designa al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI como Autoridad Administrativa Competente.

CAPÍTULO II

DEL RÉGIMEN DE ACREDITACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DIGITAL

Artículo 58.- De la acreditación de Entidades de Certificación
Las entidades que soliciten su acreditación y registro ante la Autoridad Administrativa Competente, como Entidades de Certificación, incluyendo las Entidades de Certificación para el Estado Peruano, deben contar con los elementos de la Infraestructura Oficial de Firmas Electrónicas señalados en los incisos b), c) y d) del

artículo 20 del presente Reglamento y someterse al procedimiento de evaluación comprendido en el artículo 70 del presente 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 Autoridad Administrativa Competente considere necesarias. La Autoridad Administrativa Competente, de ser el caso, precisará los términos bajo los cuales se regirán los supuestos del servicio de certificación.

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 por un monto equivalente al 100% de la UIT, vigente a la fecha de pago.

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 y demás requisitos que la Autoridad Administrativa Competente señale.

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) Otros documentos o requisitos establecidos por la Autoridad Administrativa Competente.

Artículo 60.- De la acreditación de Entidades de Registro o Verificación

Las entidades que soliciten su acreditación y registro ante la Autoridad Administrativa Competente, como Entidades de Registro o Verificación, incluyendo las Entidades de Registro o Verificación para el Estado Peruano, deben contar con los requerimientos establecidos por la Autoridad Administrativa Competente para la prestación de sus servicios, los que tendrán que asegurar la verificación presencial de la identidad del solicitante de un nuevo certificado digital.

Artículo 61.- 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 por un monto equivalente al cien por ciento (100%) de la UIT, vigente a la fecha de pago.

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 documento 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 30 y 31 del presente Reglamento.

h) Otros documentos o requisitos establecidos por la Autoridad Administrativa Competente.

Artículo 62.- De la acreditación de los Prestadores de Servicios de Valor Añadido
Las entidades públicas y privadas que soliciten su acreditación y registro ante la Autoridad Administrativa Competente como Prestadores de Servicios de Valor Añadido, deben contar con procedimientos idóneos para la prestación de sus servicios, los cuales se encontrarán recogidos en su correspondiente Declaración de Prácticas de Valor Añadido. En el caso de los Prestadores de Servicios de Valor Añadido con modalidad de Servicios de Valor Añadido con firma digital del usuario, y cuyo procedimiento concluya con una microforma o microarchivo, sus procedimientos tendrán que asegurar la presencia de un notario o fedatario que cuente con Diploma de Idoneidad Técnica y se encuentre inscrito en su correspondiente Colegio o Asociación Profesional, conforme a lo establecido por el Decreto Legislativo Nº 681.

Artículo 63.- De la acreditación del Software de los Prestadores de Servicios de Valor Añadido que realizan procedimientos con firma digital del usuario final
A fin de garantizar la seguridad de la prestación de los servicios de los Prestadores de Servicios de Valor Añadido que involucran la realización de procesos de firma digital por parte de los usuarios, resulta indispensable la acreditación del software a ser

empleado en la prestación de los servicios, conforme a los lineamientos y parámetros establecidos por la Autoridad Administrativa Competente.

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 por un monto equivalente al cien por ciento (100%) de la UIT vigente a la fecha de pago.

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) Las Políticas de Registro, la Declaración de Prácticas de Valor Añadido, la Política de Seguridad, 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.

h) Otros documentos o requisitos establecidos por la Autoridad Administrativa Competente.

Artículo 65.- Del procedimiento Administrativo de la Acreditación
Admitida la solicitud, la Autoridad Administrativa Competente procederá a la evaluación del cumplimiento de los requisitos establecidos en la Ley, el Reglamento y las respectivas Guías de Acreditación.

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

En todos los casos, el procedimiento de acreditación se regirá en particular por lo establecido para tales efectos por la Autoridad Administrativa Competente en los correspondientes Reglamentos y Guías de Acreditación, y en todos los casos de respuesta favorable a la acreditación, implicará el ingreso de la entidad solicitante a la

Infraestructura Oficial de Firmas Electrónicas a través de su Registro como Prestador de Servicios de Certificación Digital acreditado.

Artículo 66.- Del reconocimiento de evaluaciones en el extranjero
La Autoridad Administrativa Competente reconocerá las evaluaciones sobre los requisitos de competencia técnica de la Entidad de Certificación solicitante realizadas en el extranjero siempre y cuando se cumpla con las normas establecidas por la Autoridad Administrativa Competente en el marco del Reglamento, en especial si dichas evaluaciones consisten en certificaciones de cumplimiento de estándares internacionales que sean estipuladas por la Autoridad Administrativa Competente.

Artículo 67.- De la subsanación de observaciones
Dentro del procedimiento y en el plazo máximo de seis (6) meses, 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, subsisten observaciones, se denegará el Registro y se archivará el procedimiento.

Artículo 68.- Del Costo del Registro y otros procedimientos
Las entidades solicitantes asumirán los costos por la tramitación del procedimiento, y aquellos por evaluación, auditoria y demás previstos por la Autoridad Administrativa Competente.

Artículo 69.- Del otorgamiento y vigencia de la acreditación
La acreditación se otorga por un período de cinco (5) años, renovable por períodos similares. La Entidad beneficiaria estará sujeta a evaluaciones técnicas anuales para mantener la vigencia de la referida acreditación.

Artículo 70.- De la cancelación de la acreditación
La cancelación de la acreditación de los Prestadores de Servicios de Certificación Digital procede:

a) Por decisión unilateral comunicada a la Autoridad Administrativa Competente.

b) Por extinción de su personería jurídica.

c) Por cancelación 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.

f) Por determinación de la Autoridad Administrativa Competente frente al incumplimiento observado en los procesos de evaluación técnica anual, de los requerimientos exigidos en sus Reglamentos Específicos y Guías de Acreditación.

CAPÍTULO III

DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 71.- De los acuerdos de reconocimiento mutuo

La Autoridad Administrativa Competente podrá suscribir acuerdos de reconocimiento mutuo con entidades extranjeras que cumplan funciones similares, a fin de reconocer la validez de los certificados digitales otorgados en el extranjero y extender la interoperabilidad de la Infraestructura Oficial de Firmas Electrónicas. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley y su Reglamento.

Artículo 72.- Del reconocimiento
La Autoridad Administrativa Competente 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 presente Reglamento u otra norma posterior.

Asimismo, podrá autorizar la operación de aquellas Entidades de Certificación nacionales que utilicen los servicios de Entidades de Certificación extranjeras, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para tal efecto, la entidad extranjera deberá comunicar a la Autoridad Administrativa Competente los nombres de aquellas Entidades de Certificación que autorizarán las solicitudes de emisión de certificados digitales y que asumirán la gestión de tales certificados.

La Autoridad Administrativa Competente 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 73.- De la 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 Infraestructura Oficial de Firmas Electrónicas, siempre y cuando obtengan autorización previa de la Autoridad Administrativa Competente.

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 Autoridad Administrativa Competente que las firmas digitales y/o certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la Infraestructura Oficial de Firmas Electrónicas, y que cumplen las funciones señaladas en el artículo 2 de la Ley.

El incumplimiento de lo estipulado en el párrafo anterior ameritará las sanciones correspondientes, de acuerdo a lo establecido en el Reglamento de infracciones y sanciones a que se refiere el inciso r) del artículo 57 del presente Reglamento.

CAPÍTULO IV

DE LA SUPERVISIÓN DE ENTIDADES ACREDITADAS

Artículo 74.- De las facultades de supervisión

La Autoridad Administrativa Competente tiene la facultad de verificar la correcta prestación de los servicios de certificación y/o emisión de firmas digitales, así como de los servicios de registro o verificación y de los servicios de valor añadido, el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la Infraestructura Oficial de Firmas Electrónicas, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, el Reglamento, y en sus Resoluciones.

Artículo 75.- De la fiscalización
La Autoridad Administrativa Competente ejercerá su facultad fiscalizadora y sancionadora de conformidad con lo dispuesto en el Decreto Ley de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Decreto Ley Nº 25868. 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 deberá aplicar el Reglamento de infracciones y sanciones a que se refiere el inciso r) del artículo 58 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

Primera.- De la 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 empleo de la tecnología relativa a las firmas digitales y transacciones electrónicas en general en la Administración Pública, en el marco de la Ley. Encárguese al Consejo Nacional de Ciencia Tecnología e Innovación Tecnológica - CONCYTEC para que en coordinación con la Entidad de Certificación Nacional para el Estado Peruano, la Oficina Nacional de Gobierno Electrónico e Informática y la Autoridad Administrativa Competente desarrolle las acciones tendientes a masificar el uso de las firmas digitales en la Administración Pública, dentro del marco de la investigación e innovación tecnológica.

Segunda.- Del procedimiento administrativo contra decisiones de las Entidades de Certificación
Los Prestadores de Servicios de Certificación Digital deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las cuales deberán ser atendidas en el más breve plazo. La Autoridad Administrativa Competente aprobará o reformará estos procedimientos y regulará lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante el Prestador de Servicios de Certificación Digital, procederá recurrir en vía administrativa ante la Autoridad Administrativa Competente, con sujeción a la Ley Nº 27444 - Ley del Procedimiento Administrativo General. La Autoridad Administrativa Competente determinará todos aquellos procedimientos y políticas necesarios para la aplicación del presente Reglamento. En los casos que proceda la reclamación, la Autoridad Administrativa Competente adoptará las medidas correctivas pertinentes.

Tercera.- De la compatibilidad de la normativa con los avances tecnológicos
Dentro del marco conformado por la Ley y el presente Reglamento, la Autoridad Administrativa Competente se encargará de emitir las resoluciones que sean necesarias para mantener la presente normativa compatible con la evolución tecnológica de la materia y el desarrollo de las necesidades de los usuarios de la Infraestructura Oficial de Firmas Electrónicas.

Cuarta.- Del plan de implementación de los procedimientos y trámites administrativos por medios electrónicos seguros en las entidades de la Administración Pública
En el plazo de seis (6) meses a partir de la vigencia del presente Reglamento, las entidades de la Administración Pública deberán elaborar y presentar a la Oficina Nacional de Gobierno Electrónico e Informática un plan para el cumplimiento de lo estipulado en los artículos 40, 41, 42, 43, 44 y 45 del presente Reglamento, asimismo deberán proponer las normas complementarias necesarias para tal fin. La Oficina Nacional de Gobierno Electrónico e Informática evaluará y aprobará dichas propuestas.

Considerando que las entidades de la Administración Pública que brinden el servicio de Sistema de Intermediación Digital deberán acreditarse como Prestadores de Servicios de Valor Añadido ante la Autoridad Administrativa Competente, el mencionado plan deberá incorporar las estimaciones de los recursos económicos, técnicos y humanos, así como los plazos necesarios para su implantación. El plazo máximo para la implementación de lo descrito en dicho plan es de veinticuatro (24) meses a partir de su aprobación por la Oficina Nacional de Gobierno Electrónico e Informática.

Durante la implementación progresiva de los servicios de Gobierno Electrónico por parte de las entidades de la Administración Pública, éstas deberán incentivar la utilización de los medios electrónicos para la realización de sus trámites y procedimientos, considerando aquellos casos donde los ciudadanos se vean imposibilitados debido a que no cuentan con la tecnología, conocimientos necesarios para poder acceder a la prestación de los servicios electrónicos, ni con centros de acceso ciudadano disponibles en su respectiva provincia.

Quinta.- De la capacitación de empleados públicos
Cada entidad de la Administración Pública deberá garantizar de manera gradual la capacitación de sus empleados en los temas competentes a su función, que impliquen el uso de certificados y firmas digitales, así como los requerimientos de seguridad en la utilización de los medios electrónicos, la protección de la información personal de los ciudadanos y el respeto a la propiedad intelectual.

Sexta.- De la implementación del Registro Nacional de Centros de Acceso Ciudadano
En un plazo no mayor de ciento veinte (120) días calendario contados a partir de la vigencia del presente Reglamento, la Oficina Nacional de Gobierno Electrónico e Informática deberá tomar las medidas necesarias a fin de implementar el Registro Nacional de los Centros de Acceso Ciudadano a que hace referencia el artículo 53 de este Reglamento.

Séptima.- De la importación de computadoras personales con lectoras de tarjetas inteligentes para uso en el sector público y en aquéllas que se vinculen a éste
A partir de los ciento veinte (120) días calendario de vigencia del presente Reglamento, las Entidades del Sector Público adquirirán, preferentemente, computadoras personales que deberán incorporar lectoras de tarjetas inteligentes, incluyendo sus respectivos controladores de dispositivo (drivers), según los estándares correspondientes.

Octava.- Del plazo de Implementación de la Entidad de Certificación Nacional para el Estado Peruano
El Registro Nacional de Identificación y Estado Civil -RENIEC, en su calidad de Entidad de Certificación Nacional para el Estado Peruano, tendrá un plazo de diez (10) meses a partir de la vigencia del presente Reglamento, para implementar y poner al servicio de las personas naturales y jurídicas, así como de las entidades de la Administración Pública, la infraestructura indicada en el artículo 48 del presente Reglamento. Dicho plazo podrá ser prorrogado si por motivo de fuerza mayor debidamente acreditado, el Registro Nacional de Identificación y Estado Civil - RENIEC se viera imposibilitado de cumplir con lo señalado.

Después de vencido el plazo, la Entidad de Certificación Nacional para el Estado Peruano emitirá los certificados raíz correspondientes a las Entidades de Certificación para el Estado Peruano acreditadas por la Autoridad Administrativa Competente, con el fin de garantizar la interoperabilidad y la confianza en el uso de los certificados digitales emitidos por las referidas entidades.

Novena.- Del plazo para la habilitación del Registro de Prestadores de Servicios de Certificación Digital
La Autoridad Administrativa Competente se encargará de la aprobación de las Guías de Acreditación de los Prestadores de Servicios de Certificación Digital y realizar las gestiones, procedimientos legales y técnicos necesarios para iniciar los procesos de acreditación, a fin de habilitar el Registro de Prestadores de Servicios de Certificación Digital señalado en el Artículo 15 de la Ley.

Corresponde a la Oficina Nacional de Gobierno Electrónico e Informática supervisar la efectiva implementación de la Infraestructura Oficial de Firma Electrónica y el cumplimiento del plazo establecido en la presente Disposición Final.

En caso de incumplimiento del plazo establecido, la Oficina Nacional de Gobierno Electrónico e Informática asumirá la responsabilidad de aprobar las mencionadas Guías de Acreditación en un plazo adicional no mayor de quince (15) días calendario. Corresponderá a la Autoridad Administrativa Competente la ejecución de los procesos de acreditación aprobados.

Décima.- De la reutilización de aplicaciones de software de propiedad de la Administración Pública
Las entidades de la Administración Pública que sean titulares de derechos de propiedad intelectual de aplicaciones de software desarrolladas para la prestación de sus servicios o cuyo desarrollo haya sido objeto de contratación, deberán ponerlas a disposición de cualquier otra entidad de la Administración Pública sin necesidad de pago de contraprestación alguna.

Corresponde a la Oficina Nacional de Gobierno Electrónico e Informática, llevar un registro actualizado de las diferentes aplicaciones de software desarrolladas por las entidades de la Administración Pública o las contrataciones que pudieran haberse realizado para tales efectos, debiendo poner dicha información a disposición de todas las entidades de la Administración Pública, a efectos de lograr un efectivo intercambio tecnológico y reutilización de las citadas aplicaciones.

Décima 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, por un período de un (1) año, a partir de la vigencia del presente Reglamento, de la contratación de seguros o garantías bancarias, sea cual fuera la modalidad bajo la que decidan operar; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

Décima Segunda.- Del cumplimiento de los criterios WebTrust
A fin de fomentar el registro de los Entidades de Certificación ante la Autoridad Administrativa Competente, como presupuesto indispensable para la efectiva operación de la Infraestructura Oficial de Firmas Electrónicas y el desarrollo de las transacciones de gobierno y comercio electrónico seguras, exonérese a las Entidades de Certificación, por un período de tres (3) años a partir de la vigencia del presente Reglamento, del cumplimiento de los requisitos especificados en el estándar WebTrust for Certification Authorities y la obtención del sello de WebTrust; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

Décima Tercera.- Del voto electrónico
En tanto no se implemente el Documento Nacional de Identidad electrónico (DNIe), los ciudadanos podrán utilizar los certificados de persona natural emitidos por cualquier Entidad de Certificación para el Estado Peruano a efectos del ejercicio del voto electrónico en los procesos electorales, en la medida que la Oficina Nacional de Procesos Electorales (ONPE) implemente dicha alternativa.

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

Acuse de Recibo.- Son los procedimientos que registran la recepción y validación de la Notificación Electrónica Personal recibida en el domicilio electrónico, de modo tal que impide rechazar el envío y da certeza al remitente de que el envío y la recepción han tenido lugar en una fecha y hora determinada a través del sello de tiempo electrónico.

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

Ancho de banda.- Especifica la cantidad de información que se puede enviar a través de una conexión de red en un período de tiempo dado (generalmente un segundo). El ancho de banda se indica generalmente en bites por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

Cuánto más elevado el ancho de la banda de una red, mayor es su aptitud para transmitir un mayor caudal de información.

Archivo.- Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fin, y que están destinados al servicio.

Archivo Electrónico.- Es el conjunto de registros que guardan relación. También es la organización de dichos registros.

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

Autoridad Administrativa Competente.- Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente 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.

Canal seguro.- Es el conducto virtual o físicamente independiente a través del cual se pueden transferir datos garantizando una transmisión confidencial y confiable, protegiéndolos de ser interceptados o manipulados por terceros.

Certificación Cruzada.- Es el acto por el cual una Entidad de Certificación 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.- Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender:

La suspensión consiste en inhabilitar la validez de un certificado digital por un período de tiempo establecido en el momento de la solicitud de suspensión, dicho período no puede superar la fecha de expiración del certificado digital.

La modificación de la información contenida en un certificado sin la re-emisión de sus claves.

La re-emisión consiste en generar un nuevo par de claves y un nuevo certificado, correspondiente a una nueva clave pública pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar.

Clave privada.- Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

Clave pública.- Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

Código de verificación o resumen (hash).- Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:

(1) El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.

(2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.

(3) Sea improbable por medios técnicos, se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

Controlador de dispositivo (driver).- Es el programa informático que permite a un Sistema Operativo entender y manejar diversos dispositivos electrónicos físicos que se conectan o forman parte de la computadora.

Criptografía Asimétrica.- Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos 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 documento electrónico a su forma original (clave pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera 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.- Es el 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.

Declaración de Prácticas de Valor Añadido.- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define las prácticas y procedimientos que emplea en la prestación de sus servicios.

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

Destinatario.- Es la persona designada por el iniciador para recibir un documento electrónico, siempre y cuando no actúe a título de intermediario.

Dirección de correo electrónico.- Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

Dirección oficial de correo electrónico.- Es la dirección de correo electrónico del ciudadano, reconocido por el Gobierno Peruano para la realización confiable y segura de las notificaciones electrónicas personales requeridas en los procesos públicos.

Esta dirección recibirá los mensajes de correo electrónico que sirvan para informar al usuario acerca de cada notificación o acuse de recibo que haya sido remitida a cualquiera de sus domicilios electrónicos. A diferencia del domicilio electrónico, esta

dirección centraliza todas las comunicaciones que sirven para informar al usuario que se ha realizado una actualización de los documentos almacenados en sus domicilios electrónicos. Su lectura es de uso obligatorio.

Documento.- Es 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.

Documento electrónico.- Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.

Documento oficial de identidad.- Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:

a) Documento Nacional de Identidad (DNI);

b) Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,

c) Pasaporte, si se trata de personas naturales extranjeras no residentes.

Domicilio electrónico.- Está conformado por la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital, para la tramitación confiable y segura de las notificaciones, acuses de recibo y demás documentos requeridos en sus procedimientos. En el caso de una persona jurídica el domicilio electrónico se asocia a sus integrantes.

Para estos efectos, se empleará el domicilio electrónico como equivalente funcional del domicilio habitual de las personas naturales o jurídicas.

En este domicilio se almacenarán los documentos y expedientes electrónicos correspondientes a los procedimientos y trámites realizados en el respectivo Sistema de Intermediación Digital. El acceso a este domicilio se realiza empleando un certificado digital de autenticación.

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

Entidades de la Administración Pública.- Es el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales de los ciudadanos y la industria.

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

Entidad final.- Es el suscriptor de un certificado digital.

Estándares Técnicos Internacionales.- Son los requisitos de orden técnico y de uso internacional que deben observarse en la emisión de certificados digitales y en las prácticas de certificación.

Estándares Técnicos Nacionales.- Son los 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.

Equivalencia funcional.- Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

Expediente electrónico.- El expediente electrónico se constituye en los trámites o procedimientos administrativos en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan los usuarios internos o externos a la entidad que tengan los perfiles de accesos o permisos autorizados.

Gobierno Electrónico.- Es el uso de las Tecnologías de Información y Comunicación para redefinir la relación del gobierno con los ciudadanos y la industria, mejorar la gestión y los servicios, garantizar la transparencia y la participación, y facilitar el acceso seguro a la información pública, apoyando la integración y el desarrollo de los distintos sectores.

Identificador de objeto OID.- Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 | ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).

Infraestructura Oficial de Firma Electrónica.- Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:

1) La integridad de los documentos electrónicos;
2) La identidad de su autor, lo que es regulado conforme a Ley.

El sistema incluye la generación de firmas digitales, 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, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

Integridad.- Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Interoperabilidad.- Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas:

* Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI.

* Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí.

* Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.

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

Lista de Certificados Digitales Cancelados.- Es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.

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

Medios electrónicos.- Son los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar de documentos electrónicos.

Medios electrónicos seguros.- Son los medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de Certificación Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.

Medios telemáticos.- Es el 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.

Neutralidad tecnológica.- Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica 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 digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos.

No repudio.- Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

En el ámbito del artículo 2 de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

Nombre Diferenciado (X.501).- Es un sistema estándar diseñado para consignar en el campo sujeto de un certificado digital los datos de identificación del titular del certificado, de manera que éstos se asocien de forma inequívoca con ese titular dentro del conjunto de todos los certificados en vigor que ha emitido la Entidad de Certificación. En inglés se denomina “Distinguished Name”.

Norma Marco sobre Privacidad.- Es la norma basada en la normativa aprobada en la 16 Reunión Ministerial del APEC, que fuera llevada a cabo en Santiago de Chile el 17 y 18 de noviembre de 2004, la cual forma parte integrante de las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.

Notificación electrónica personal.- En virtud del principio de equivalencia funcional, la notificación electrónica personal de los actos administrativos se realizará en el domicilio electrónico o en la dirección oficial de correo electrónico de las personas por cualquier medio electrónico, siempre que permita confirmar la recepción, integridad, fecha y hora en que se produce. Si la notificación fuera recibida en día u hora inhábil, ésta surtirá efectos al primer día hábil siguiente a dicha recepción.

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

Políticas de Certificación.- Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas.

Práctica.- Es el modo o método que particularmente observa alguien en sus operaciones.

Prácticas de Certificación.- Son las prácticas utilizadas para aplicar las directrices de la política establecida en la Política de Certificación respectiva.

Prácticas específicas de Certificación.- Son las prácticas que completan todos los aspectos específicos para un tipo de certificado que no están definidos en la Declaración de Prácticas de Certificación respectiva.

Prácticas de Registro o Verificación.- Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.

Prestador de Servicios de Certificación.- Es toda entidad pública o privada que indistintamente brinda servicios en la modalidad de Entidad de Certificación, Entidad de Registro o Verificación o Prestador de Servicios de Valor Añadido.

Prestador de Servicios de Valor Añadido.- Es la entidad pública o privada que brinda servicios que incluyen la firma digital y el uso de los certificados digitales. El presente Reglamento presenta dos modalidades:

a. Prestadores de Servicio de Valor Añadido que realizan procedimientos sin firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido, como Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.

b. Prestadores de Servicio de Valor Añadido que realizan procedimientos con firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido como el sistema de intermediación electrónico, en donde se requiere en determinada etapa de operación del procedimiento la firma digital por parte del usuario final en algún tipo de documento.

Prestador de Servicios de Valor Añadido para el Estado Peruano.- Es la Entidad pública que brinda servicios de valor añadido, con el fin de permitir la realización de las transacciones públicas de los ciudadanos a través de medios electrónicos que garantizan la integridad y el no repudio de la información (Sistema de Intermediación Digital) y/o registran la fecha y hora cierta (Sello de Tiempo).

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

Registro.- En términos informáticos, es un conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos.

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

Servicio de Valor Añadido.- Son los servicios complementarios de la firma digital brindados dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que certifican los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónico dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

Servicio OCSP (Protocolo del estado en línea del certificado, por sus siglas en inglés).- Es el servicio que permite utilizar un protocolo estándar para realizar consultas en línea (on line) al servidor de la Autoridad de Certificación sobre el estado de un certificado.

Sistema de Intermediación Digital.- Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

Sistema de Intermediación Electrónico.- Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e

integridad de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

Sistema WEB ("World Wide Web").- Sistema de documentos electrónicos enlazados y accesibles a través de Internet. Mediante un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

Suscriptor.- Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

Tercero que confía o tercer usuario.- Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

Titular.- Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Usabilidad.- En el contexto de la certificación digital, el término Usabilidad se aplica a todos los documentos, información y sistemas de ayuda necesarios que deben ponerse a disposición de los usuarios para asegurar la aceptación y comprensión de las tecnologías, aplicaciones informáticas, sistemas y servicios de certificación digital de manera efectiva, eficiente y satisfactoria.

Usuario final.- En líneas generales, es toda persona que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado.

Voto electrónico.- Sistema de votación que utiliza una combinación de procedimientos, componentes de hardware y software, y red de comunicaciones que permiten automatizar los procesos de identificación del elector, emisión del voto, conteo de votos, emisión de reportes y/o presentación de resultados de un proceso electoral, referéndum y otras consultas populares. El voto electrónico se puede clasificar en:

a) Presencial: cuando los procesos de votación se dan en ambientes o lugares debidamente supervisados por las autoridades electorales; y

b) No presencial: cuando los procesos de identificación del elector y emisión del voto se dan desde cualquier ubicación geográfica o ambiente que el elector elija y disponga de los accesos apropiados.

WebTrust.- Certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades Certificadoras - EC, que de manera consistente cumplen con estándares establecidos por el Instituto Canadiense de Contadores Colegiados (CICA por sus siglas en inglés - ver Cica.ca) y el Instituto Americano de Contadores Públicos Colegiados (AICPA). Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.