



Ministerio de Justicia

PREPUBLICACIÓN

**Reglamento de la Ley de Firmas
y Certificados Digitales
Ley N° 27269**

Las opiniones y sugerencias podrán ser remitidas por escrito a la Dirección Nacional de Asuntos Jurídicos del Ministerio de Justicia, sito en la Sede del Ministerio de Justicia, (módulo 14), Jr. Scipión Llona N° 350 Miraflores, Lima 18 - Perú,
Central Telefónica: 440-4310, o vía **Correo Electrónico** a: jespinoz@minjus.gob.pe, hasta el 4 de julio de 2001.

SEPARATA ESPECIAL

**PROYECTO DE REGLAMENTO DE LA LEY DE FIRMAS
Y CERTIFICADOS DIGITALES. LEY. N° 27269**

**TÍTULO I
NORMAS GENERALES**

CAPÍTULO I

Artículo 1°.- Objeto

El presente Reglamento regula la utilización de firmas electrónicas en mensaje de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica comprendiendo el régimen de acreditación y supervisión de las entidades de certificación, así como de las entidades de registro o verificación, establecidas en la Ley N° 27269 -Ley de Firmas y Certificados Digitales-, modificada en su Artículo 11° por la Ley N° 27310, en adelante se denominará "la Ley".

Cualquier otra firma electrónica podrá tener los mismos efectos que los de las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, siempre que la autoridad administrativa competente apruebe su utilización conforme a lo establecido en el presente Reglamento.

Artículo 2°.- Principio de la autonomía de la voluntad

Las disposiciones contenidas en el presente Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial de Firmas Electrónicas.

Artículo 3°.- Régimen de servicios de certificación

La prestación de servicios de certificación así como los de registro o verificación se realiza en el régimen de libre competencia.

Artículo 4°.- Definiciones

Para efectos del presente Reglamento, entiéndase por:

Registro.- Incorporación de una entidad de certificación o de una entidad de registro o verificación, a la Infraestructura Oficial de Firma Electrónica como resultado del proceso de acreditación.

Acreditación.- Proceso a través del cual la autoridad administrativa competente, previo cumplimiento de las exigencias establecidas en la Ley, 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.

Documento Electrónico.- Conjunto de datos basados en bits o impulsos electromagnéticos, elaborados, generados, transmitidos, comunicados y archivados a través de medios electrónicos, ópticos o cualquier otro análogo.

Mensaje de datos.- Es la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el Intercambio Electrónico de Datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el télex, el telefax, entre otros.

Firma electrónica.- Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita. Se incluye dentro de esta definición a la firma o signatura informática.

Infraestructura Oficial de Firma Electrónica.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente constituido por programas, equipos, estándares, políticas, procesos, procedimientos u otros recursos que permiten la generación de firmas electrónicas y que garantizan la autenticación e integridad de los documentos electrónicos.

Criptografía asimétrica.- Es una técnica basada en el uso de un par de claves únicas; una clave privada y una clave pública relacionadas matemáticamente en-

tre sí de tal manera que una no pueda operar sin la otra y de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Autenticación.- Proceso técnico que permite determinar la identidad de la persona que emite un mensaje de datos firmado electrónicamente, vinculándolo con dicho mensaje; este proceso no otorga certificación notarial ni fe pública.

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

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

Firma digital.- Aquella firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido.

Titular de firma digital.- Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada.

Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado digital a partir del cual se generan dichas firmas digitales.

Agente automatizado.- Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana.

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

Clave pública.- En un sistema de criptografía asimétrica, es aquella usada por el receptor de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.

Clave privada.- En un sistema de criptografía asimétrica, es aquella que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

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

Bit.- (Binary Digit) Dígito simple del sistema binario, que representa una unidad mínima de almacenamiento de datos o información en un sistema informático o de cómputo.

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

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

Infraestructura Oficial de Firma Digital.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente en el marco de la Infraestructura Oficial de Firma Electrónica mediante el uso de tecnología de firma digital, en la que partici-

pan entidades de certificación y entidades de registro o verificación acreditadas ante la autoridad administrativa competente.

Autoridad Administrativa Competente.- Organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, así como la reglamentación y prestación de servicios de valor añadido relacionados con la misma y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones.

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

Entidad de Registro o Verificación.- Persona jurídica encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la identificación y autenticación del suscriptor de una firma digital, la aceptación y autorización de las solicitudes para la emisión de certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Declaración de Prácticas de Certificación.- Conjunto de políticas y procedimientos que sigue una entidad de certificación para la prestación de sus servicios.

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

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

Neutralidad Tecnológica.- Principio que fomenta la creación y uso de diversas tecnologías, sin preferir, restringir, ni discriminar a ninguna de ellas.

Tiempo Universal Coordinado (UTC).- Hora relacionada con el Meridiano de Greenwich.

Servicio de Valor Añadido.- Servicio complementario a las funciones de certificación, verificación o registro al interior de la Infraestructura Oficial de Firma Electrónica.

CAPÍTULO II VALIDEZ Y EFECTOS JURÍDICOS DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 5º.- Validez de las firmas electrónicas
Para efectos de la manifestación de voluntad, las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos tienen la misma validez y eficacia jurídica que las firmas manuscritas, siempre que vinculen e identifiquen al firmante y garanticen la autenticación e integridad de los documentos electrónicos.

Artículo 6º.- Firmas en la Infraestructura Oficial de Firma Electrónica
Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos y generada bajo la Infraestructura Oficial de Firma Electrónica, cumple con lo dispuesto en el Artículo 5º del presente Reglamento.

Artículo 7º.- Documentos Firmados Electrónicamente como medio de prueba
Los documentos firmados electrónicamente podrán ser ofrecidos como prueba en toda clase de procesos o procedimientos.

Artículo 8º.- Presunciones acerca de las firmas electrónicas bajo la Infraestructura Oficial de Firma Electrónica
Las disposiciones y presunciones del presente Reglamento no excluyen el cumplimiento de las formalidades

específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Tratándose de documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume, salvo prueba en contrario, que el documento fue firmado por su titular.

Artículo 9º.- Conservación de documentos electrónicos

Cuando el usuario lo requiera o la legislación exija que los documentos, registros o informaciones sean conservados, este requisito tratándose de mensajes de datos o documentos firmados electrónicamente, queda satisfecho cuando se cumplan las siguientes condiciones:

- a) Que sean accesibles para su posterior consulta.
- b) Que sean conservados con su formato original de generación, transmisión, recepción u otro formato que reproduzca en forma demostrable la autenticación e integridad del documento electrónico, en concordancia con la legislación de la materia.
- c) Que sea conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción, en concordancia con la legislación de la materia.

TÍTULO II DE LA INFRAESTRUCTURA OFICIAL DE FIRMA DIGITAL

CAPÍTULO I ASPECTOS GENERALES

Artículo 10º.- Tecnologías de firmas electrónicas al interior de la Infraestructura Oficial de Firma Electrónica

La Infraestructura Oficial de Firma Electrónica se puede basar en las siguientes tecnologías de firmas electrónicas:

- a) Tecnologías de firmas digitales, sobre la cual se basa la Infraestructura Oficial de Firma Digital.
- b) Otras tecnologías de firmas electrónicas que sean aprobadas por la autoridad administrativa competente de acuerdo con el principio de neutralidad tecnológica.

Artículo 11º.- Elementos de la Infraestructura Oficial de Firma Digital

La Infraestructura Oficial de Firma Digital está constituida por:

- a) Procedimientos de certificación basados en estándares internacionales o compatibles a los empleados internacionalmente, de acuerdo con lo establecido por la autoridad administrativa competente.
- b) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados a los procedimientos de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal a).
- c) Personal competente para la conducción de los procedimientos de certificación y el mantenimiento de la Infraestructura Oficial de Firma Digital.
- d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios.
- e) Autoridad Administrativa Competente, así como entidades de certificación y entidades de registro o verificación debidamente acreditadas.

Artículo 12º.- Estándares aplicables bajo la Infraestructura Oficial de Firma Digital

Los procedimientos de certificación comprendidos en la Infraestructura Oficial de Firma Digital deben estar basados sobre los estándares técnicos internacionales vigentes que aseguren las funciones exigidas en el Artículo 2º de la Ley y la interoperabilidad.

La autoridad administrativa competente determinará los estándares compatibles aplicando el principio de neutralidad tecnológica con la necesidad de cumplir los requisitos mencionados en el párrafo anterior.

CAPÍTULO II DE LA FIRMA DIGITAL

Artículo 13°.- Firmas digitales generadas bajo la Infraestructura Oficial

Las Firmas digitales que gozan de las presunciones establecidas en los Artículos 6° y 7° del presente Reglamento son las generadas a partir de certificados digitales:

- Emitidos conforme a lo dispuesto en el presente Reglamento por entidades de certificación acreditadas ante la autoridad administrativa competente.
- Incorporados a la Infraestructura Oficial de Firma Digital bajo acuerdos de certificación cruzada, conforme al Artículo 48° del presente Reglamento.
- Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la autoridad administrativa competente conforme al Artículo 46° del presente Reglamento.
- Emitidos por entidades de certificación extranjeras que hayan sido incorporados a la Infraestructura Oficial de Firma Digital conforme al Artículo 47° del presente Reglamento.

Artículo 14°.- Características de la firma digital

Las características mínimas de la firma digital generadas bajo la Infraestructura Oficial de Firma Digital son:

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

Artículo 15°.- Funciones de la firma digital

Dadas las características señaladas en el Artículo anterior, técnicamente la firma digital debe garantizar:

- Que el mensaje de datos fuera firmado con la clave privada del titular de la firma digital.
- La integridad del mensaje de datos firmado digitalmente, dado que cualquier alteración en el mensaje de datos o en la firma digital puede ser detectada.
- Que el titular de la firma digital no pueda repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada, dado que ésta se mantiene bajo su control exclusivo.

Artículo 16°.- Del titular de la firma digital

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

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

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

Artículo 17°.- Obligaciones del titular de la firma digital

Las obligaciones del titular de la firma digital son:

- Entregar información veraz bajo su responsabilidad.
- Mantener el control y la reserva de la clave privada bajo su responsabilidad.
- Observar las condiciones establecidas por la entidad de certificación para la utilización del certificado digital y la generación de firmas digitales.

Artículo 18°.- Invalidez de la firma digital

Una firma digital generada bajo la Infraestructura Oficial de Firma Digital pierde validez si es utilizada:

- En fines distintos para el que fue extendido el certificado digital.
- En operaciones que superen el valor para el cual fue autorizado.
- Cuando el certificado haya sido cancelado conforme a lo establecido en el Capítulo IV del presente Título.

CAPÍTULO III DEL CERTIFICADO DIGITAL

Artículo 19°.- Requisitos para obtener un certificado digital

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

- Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
- Tratándose de personas jurídicas, estar inscritas en el registro correspondiente, solicitado por la autoridad administrativa competente.

Artículo 20°.- Especificaciones adicionales para ser titular de un certificado digital

Para ser titular de un certificado digital adicionalmente se deberá cumplir con:

Entregar la información solicitada por la entidad de certificación o la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.

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

Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales.

Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado digital y de las firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica.

Artículo 21°.- Procedimiento para ser titular de un certificado digital

Para el caso de personas naturales, éstas deberán presentar una solicitud a la entidad de certificación o a la entidad de registro o verificación, según sea el caso; dicha solicitud deberá estar acompañada de toda la información requerida por la declaración de prácticas de certificación o en la declaración de prácticas de registro. La entidad de registro o verificación deberá comprobar la identidad del solicitante a través de su documento nacional de identidad, su pasaporte o su carné de extranjería.

En el caso de una persona jurídica, la solicitud deberá ser presentada por la persona facultada para tal fin, debiendo demostrar que la persona jurídica se encuentra debidamente inscrita en el registro correspondiente, acreditando la veracidad de la información comprendida en su solicitud. Asimismo, deberá presentar toda la información requerida por la declaración de prácticas de certificación de la entidad de certificación.

Artículo 22°.- Obligaciones del titular de certificado digital

- Actualizar permanentemente la información proveída tanto a la entidad de certificación como a la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.

- b) Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
- c) Observar permanentemente las condiciones establecidas por la entidad de certificación para la utilización del certificado digital.

Artículo 23°.- Contenido del certificado digital

Los certificados digitales emitidos dentro de la Infraestructura Oficial de Firma Digital deberán contener como mínimo lo establecido en el Artículo 7° de la Ley.

La entidad de certificación podrá incluir, a pedido del solicitante del certificado digital, información adicional siempre y cuando la entidad de registro o verificación compruebe fehacientemente la veracidad de ésta.

Artículo 24°.- Período de vigencia

El período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme al Artículo 9° de la Ley.

CAPÍTULO IV DE LA CANCELACIÓN DE CERTIFICADOS DIGITALES

Artículo 25°.- Causales de cancelación del certificado digital

- a) Por solicitud del titular sin previa justificación, siendo necesaria para tal efecto la aceptación y autorización de la entidad de certificación o la entidad de registro o verificación. La misma que deberá ser aceptada y autorizada como máximo dentro de las 36 horas siguientes a su presentación, si en el plazo indicado la entidad no se pronuncia, se entenderá la cancelación del certificado.
- c) Por revocación.
- d) Por expiración del plazo de vigencia.
- e) Por el cese de operaciones de la entidad de certificación que lo emitió.
- f) Por resolución judicial que lo ordene.
- g) Por muerte, interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta.

Artículo 26°.- Cancelación del certificado digital a solicitud de su titular

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

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

- a) Por exposición, puesta en peligro o uso indebido de la clave privada.
- b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

Si en estos casos el titular no solicita la cancelación, será responsable por los daños o perjuicios generados a terceros de buena fe que confiaron en el contenido del certificado.

Artículo 27°.- Cancelación por revocación

Para efectos de la cancelación de oficio o revocación de certificados digitales, la entidad de certificación debe contar con procedimientos detallados en su declaración de prácticas de certificación.

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

La revocación debe indicar el momento desde el cual se aplica precisando como mínimo: minutos y segundos. La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La entidad de certificación debe inmediatamente incluir la

revocación del certificado en la relación de certificados digitales cancelados firmada digitalmente por ella.

CAPÍTULO V DE LA ENTIDAD DE CERTIFICACIÓN

Artículo 28°.- De las funciones de la Entidad de Certificación

Las entidades de certificación tienen las siguientes funciones:

- a) Emitir certificados digitales manteniendo su numeración correlativa.
- b) Cancelar certificados digitales.
- c) Gestionar certificados digitales emitidos en el extranjero.
- d) Las señaladas en el Artículo 32° del presente Reglamento, en caso opten por asumir las funciones de entidad de registro o verificación.

Adicionalmente las entidades de certificación podrán brindar otros servicios inherentes a los de certificación, cuyas características y procedimientos estarán contenidos en su declaración de prácticas de certificación.

Artículo 29°.- De las obligaciones de la Entidad de Certificación

Las entidades de certificación tienen las siguientes obligaciones:

- a) Cumplir con su declaración de prácticas de certificación.
- b) Informar a los usuarios 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 los certificados digitales que emite, bajo responsabilidad.
- d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia.
- e) Publicar permanente e ininterrumpidamente por medios telemáticos la relación de los certificados digitales emitidos y cancelados.
- f) Cancelar el certificado digital a solicitud de su titular o, de ser el caso, a solicitud del titular de la firma digital; o cuando advierta que la información contenida en el certificado digital fuera inexacta o hubiera sido modificada, o que el titular incurriera en alguna de las causales previstas en el Artículo 25° del presente Reglamento.
- g) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido expreso del titular del certificado digital.
- h) Brindar todas las facilidades al personal autorizado por la autoridad administrativa competente para efectos de supervisión y auditoría.
- i) Mantener la información relativa a los certificados digitales que hubieren sido cancelados, por un período mínimo de diez (10) años a partir de su cancelación.
- j) 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.
- k) Informar y solicitar autorización a la autoridad administrativa competente para realizara acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.
- l) Informar y solicitar autorización a la autoridad administrativa competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras.
- m) Cumplir sus funciones dentro de los plazos señalados en su declaración de prácticas de certificación.
- n) Contratar los seguros o garantías bancarias necesarias que permitan indemnizar al titular por los daños que pueda ocasionar como resultado de las actividades de certificación.

Artículo 30°.- Respaldo financiero

Las entidades de certificación acreditadas deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y el presente Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 31°.- Del cese de operaciones de la Entidad de Certificación

La entidad de certificación cesa sus operaciones en el marco de la Infraestructura Oficial de Firma Digital, en los siguientes casos:

- Por decisión unilateral comunicada ante la autoridad administrativa competente.
- Por extinción de su personería jurídica.
- Por revocación de su registro.
- Por disposición de la autoridad administrativa competente.
- Por orden judicial.
- Por declaración de insolvencia, siempre que en el plazo fijado por ley, no se levante dicho estado.

Para los supuestos contemplados en los incisos a) y b) la autoridad administrativa competente establecerá el plazo en el cual las entidades de certificación notificarán tanto a aquélla como a los titulares de certificados digitales el cese de sus actividades. La autoridad administrativa competente deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos d), g) e i) del Artículo 29° del presente Reglamento.

La autoridad administrativa competente reglamentará los procedimientos para hacer público el cese de operaciones de las entidades de certificación.

Los certificados digitales emitidos por una entidad de certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. El uso de certificados digitales con posterioridad a su cancelación implica la pérdida de las presunciones descritas en los Artículos 6° y 7° del presente Reglamento.

CAPÍTULO VI DE LA ENTIDAD DE REGISTRO O VERIFICACIÓN

Artículo 32°.- De las funciones de la Entidad de Registro o Verificación

Las entidades de registro o verificación tienen las siguientes funciones:

- Identificar al solicitante del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquél.
- Aceptar, autorizar según sea el caso, la conformidad de las solicitudes de emisión, modificación o cancelación de certificados digitales, comunicándolo a la entidad de certificación bajo responsabilidad.

Artículo 33°.- De las obligaciones de la Entidad de Registro o Verificación

Las entidades de registro o verificación acreditadas tienen las siguientes obligaciones:

- Cumplir los procedimientos declarados para la prestación del servicio.
- Determinar objetivamente la veracidad de la información proporcionada por el solicitante de certificado digital bajo responsabilidad.
- Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.
- Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
- Informar y solicitar autorización a la autoridad administrativa, especialmente en el supuesto previsto en el Artículo 47° del presente Reglamento.

- Acreditar domicilio en el Perú.
- Contratar los seguros necesarios que le permitan indemnizar por los daños que puedan ocasionar como resultado de las actividades de registro o verificación.

Artículo 34°.- Respaldo financiero

Las entidades de registro o verificación acreditada deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital; así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y por el presente Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 35°.- Del cese de operaciones de la entidad de registro o verificación

La entidad de registro o verificación cesa de operar en el marco de la Infraestructura Oficial de Firma Digital:

- Por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión.
- Por extinción de su personería jurídica.
- Por revocación de su registro.
- Por sanción dispuesta por la autoridad administrativa competente.
- Por orden judicial.
- Por declaración de insolvencia, siempre que en el plazo fijado por ley no se levante dicho estado.

Para los supuestos contenidos en los incisos a) y b), la entidad de registro o verificación debe notificar el cese de sus actividades a la autoridad administrativa competente con una anticipación mínima que será establecida por ésta, debiendo dejar constancia ante aquélla de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del Artículo 33° del presente Reglamento.

TÍTULO III DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

CAPÍTULO I FUNCIONES DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

Artículo 36°.- Funciones

La autoridad administrativa competente tiene las siguientes funciones:

- Acreditar entidades de certificación.
- Acreditar entidades de registro o verificación.
- Supervisar a las entidades de certificación y a las entidades de registro o verificación, estableciendo de ser el caso las sanciones correspondientes.
- Cancelar las acreditaciones otorgadas a las entidades de certificación y a las entidades de registro o verificación conforme a lo dispuesto en el presente Reglamento.
- Publicar ininterrumpidamente la relación de entidades acreditadas.
- Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica y determinar la compatibilidad de otros estándares técnicos con los estándares internacionales.
- Establecer los requisitos mínimos para la prestación de los servicios de certificación y los servicios de registro o verificación.
- Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación y las entidades de registro o verificación.
- Aprobar la utilización de otras tecnologías de firmas electrónicas distintas a las firmas digitales, previa verificación del cumplimiento de los requisitos establecidos en el Artículo 2° de la Ley y regular su utilización al interior de la Infraestructura Oficial de Firma Electrónica.
- Suscribir acuerdos de reconocimiento mutuo con autoridades administrativas extranjeras que cum-

- plan funciones similares a las de la autoridad administrativa competente.
- k) Dictar medidas cautelares.
 - l) Autorizar la realización de certificaciones cruzadas con entidades de certificación extranjeras.
 - m) Delegar a terceros bajo sus órdenes y responsabilidad las funciones que determine.
 - n) Fomentar y coordinar el uso y desarrollo de la Infraestructura oficial de firma electrónica al interior de las entidades del sector público nacional.
 - o) Aprobar y regular los servicios de valor añadido al interior de la Infraestructura Oficial de Firma Electrónica.

CAPÍTULO II RÉGIMEN DE ACREDITACIÓN DE ENTIDADES DE CERTIFICACIÓN Y DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 37°.- Acreditación de Entidades de Certificación

Las entidades que soliciten su acreditación como entidades de certificación ante la autoridad administrativa competente deben contar con los elementos de la Infraestructura Oficial de Firma Digital señalados en los incisos a), b), c) y d) del Artículo 11°, y someterse al procedimiento de evaluación comprendido en el Artículo 41° 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 rigen estos supuestos del servicio de certificación.

Artículo 38°.- Presentación de la solicitud de acreditación de Entidad de Certificación

La solicitud de acreditación de entidades de certificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el Artículo anterior y adjuntando lo siguiente:

- a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.
- b) Acreditar domicilio en el país.
- c) Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
- d) Declaración de prácticas de certificación y documentación que comprenda el sistema de gestión implementado conforme a los incisos a) y d) del Artículo 11° del presente Reglamento.
- e) Declaración jurada del cumplimiento de los requisitos señalados en los incisos b) y c) del Artículo 11° del presente Reglamento; información que será comprobada por la autoridad administrativa competente.
- f) Documentación que acredite el cumplimiento de lo dispuesto en el Artículo 29° y 30° del presente Reglamento y demás que la autoridad administrativa competente señale.

Artículo 39°.- Acreditación de Entidades de Registro o Verificación

Las entidades que soliciten su acreditación como entidades de registro o verificación ante la autoridad administrativa competente deben contar con procedimientos para la prestación de sus servicios.

Artículo 40°.- 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 la información y documentos siguientes:

- a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.
- b) Acreditar domicilio en el país.
- c) Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
- d) Declaración de prácticas de verificación o registro.
- e) Declaración jurada del cumplimiento de los requisitos señalados en los Artículos 33° y 34° del presente Reglamento.

Artículo 41°.- 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 como en el presente Reglamento.

La evaluación de los requisitos de competencia técnica de la entidad de certificación 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 presente Reglamento.

Artículo 42°.- 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 cumplan con las normas establecidas por la autoridad administrativa competente en el marco del presente Reglamento.

Artículo 43°.- Subsanación de observaciones

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

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

Artículo 44°.- Costos del Registro

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

Artículo 45°.- Cancelación de la Acreditación

La cancelación de la acreditación procede por:

- a) Solicitud de la entidad de certificación o de la entidad de verificación o registro.
- b) Extinción de su personería jurídica.
- c) Sanción impuesta por la autoridad administrativa competente o por decisión judicial.
- d) Por declaración de insolvencia, siempre que en el plazo fijado por ley no se levante dicho estado.

CAPÍTULO III DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 46°.- Acuerdos de reconocimiento mutuo

La autoridad administrativa competente podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de certificados digitales otorgados en el extranjero y extender la validez de la Infraestructura Oficial de Firma Digital. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley como en el presente Reglamento.

Artículo 47°.- Reconocimiento de certificados emitidos por entidades extranjeras

La autoridad administrativa competente podrá reconocer certificados digitales emitidos por entidades extranjeras, siempre y cuando se garantice el cumplimiento de las obligaciones y responsabilidades establecidas en el presente Reglamento y en las normas de la Infraestructura Oficial de Firma Digital u otro mecanismo que apruebe la autoridad administrativa competente.

Para los efectos de lo dispuesto en el párrafo precedente, la entidad extranjera deberá comunicar a la autoridad administrativa competente el nombre de aquellas entidades que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.

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 48°.- 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 Firma Digital de conformidad con el Artículo 11° de la Ley, 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 los certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la Infraestructura Oficial de Firma Digital, y que cumplen las funciones señaladas en el Artículo 2° de la Ley.

CAPÍTULO IV**SUPERVISIÓN DE ENTIDADES ACREDITADAS****Artículo 49° - Facultades de supervisión**

La autoridad administrativa competente tiene la facultad de verificar la correcta prestación de los servicios de certificación así como de los servicios de registro o verificación y el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la Infraestructura Oficial de Firma Electrónica, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, en el presente Reglamento, y en las resoluciones emitidas por la autoridad administrativa competente.

Artículo 50° - Facultad sancionadora

La autoridad administrativa competente tiene la facultad de tipificar los hechos u omisiones que configuran infracciones administrativas dentro de la Infraestructura Oficial de Firma Electrónica, y tiene la facultad de imponer las sanciones que correspondan, dentro de su ámbito de competencia y con las limitaciones contenidas en la Ley y en el presente Reglamento.

Artículo 51° - Infracciones aplicables

Las infracciones administrativas se clasifican en leves, graves y muy graves.

Dependiendo de su gravedad, las infracciones administrativas son pasibles de las siguientes sanciones:

- Faltas leves: amonestación escrita o multa de hasta 25 Unidades Impositivas Tributarias.
- Faltas graves: multa de más de 25 hasta 100 Unidades Impositivas Tributarias.
- Faltas muy graves: multa de más de 100 hasta 200 Unidades Impositivas Tributarias.

La determinación de una falta muy grave podrá implicar además la cancelación de la acreditación otorgada. En estos casos, la entidad cuya acreditación haya sido

cancelada sólo podrá obtenerla luego de transcurridos tres años desde su la cancelación.

Las sanciones previstas en el presente Artículo serán establecidas e impuestas por la autoridad administrativa competente mediante resolución motivada, pudiendo disponer la publicación de la misma.

Artículo 52° - Gradación de la sanción

La autoridad administrativa competente determinará la gradación de la sanción a imponerse, aplicando los siguientes criterios:

- Naturaleza y gravedad de la infracción.
- El daño causado o grado de afectación generado por la infracción en los usuarios.
- El beneficio obtenido con la infracción, a fin de evitar, en lo posible, que dicho beneficio sea superior al monto de la sanción.
- La reincidencia y la reiterancia.
- La conducta de la entidad acreditada infractora a lo largo del procedimiento de imposición de sanción, que comprende la continuación de la práctica materia del procedimiento de infracciones y especialmente la disposición para reparar el daño o mitigar sus efectos.
- La intencionalidad del infractor.
- Necesidad de dictar medidas cautelares.
- Cualquier otro que la autoridad administrativa competente deba imponer.

Disposiciones Finales

Artículo Primero.- Designada la autoridad administrativa competente, conforme a lo establecido en el Artículo 15° de la Ley, esta deberá contar con la asesoría permanente de una Comisión Multisectorial integrada por representantes de instituciones públicas y privadas. La Comisión antes indicada que estará bajo la presidencia de un representante de la autoridad administrativa competente, actuará como órgano asesor y consultivo de dicha autoridad administrativa.

Artículo Segundo.- Las entidades del Sector Público Nacional pueden suscribir acuerdos de cooperación con sus similares a nivel mundial o con instituciones de cooperación, para recibir apoyo, asesoría y financiamiento para el desarrollo del comercio electrónico en general, las firmas electrónicas, las firmas y certificados digitales en particular.

Artículo Tercero.- Las entidades de certificación deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las mismas que deberán ser atendidas en el más breve plazo. La autoridad administrativa competente aprueba o reforma estos procedimientos y regula todo lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante la entidad de certificación, procede recurrir en vía administrativa ante la autoridad administrativa competente, con sujeción a la Ley N° 27444 - Ley del Procedimiento Administrativo General.

La autoridad administrativa competente determinará todos aquellos procedimientos necesarios para la aplicación del presente Reglamento. En los casos que proceda la reclamación, adoptará las medidas correctivas pertinentes y sancionará a la empresa.

Artículo Cuarto.- Los mensajes de datos y los documentos transmitidos electrónicamente cuyo emisor se identifica mediante firmas electrónicas pueden ser convertidos a microformas a solicitud de parte interesada de acuerdo al Decreto Legislativo N° 681 y demás normas respectivas. Se incluyen las comunicaciones, mensajes y documentos con cualquier tipo de firma electrónica; así como los certificados digitales, reportes de envío y recepción de mensajes, y aquellos documentos usados en actividades de certificación, verificación o registro.

Los notarios y fedatarios con Certificado de Idoneidad Técnica expiden testimonios, copias fieles, legalizan y autentican documentos y mensajes de datos de acuerdo a la Ley de la materia.