HANDBOOK

ACREDITACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACION DIGITAL

FIRMAS Y CERTIFICADOS DIGITALES EN EL PERÚ

Handbook N°. 11 I&A: Acreditación de Prestadores de Servicios de Certificación Digital. Firmas y certificados digitales en Perú v.1.0 - 01 de Marzo de 2013

IRIARTE & ASOCIADOS
Jr. Miró Quesada 191 - Of. 510. Lima 01 – Perú.
Telefax (+511) 427 0383
http://www.iriartelaw.com
contacto@iriartelaw.com

HANDBOOK
ACREDITACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACION DIGITAL
FIRMAS Y CERTIFICADOS DIGITALES EN EL PERÚ

Introducción.

I. **Normativa aplicable sobre Firmas y Certificados Digitales**.
   1. Ámbito de aplicación.
   2. Infraestructura Oficial de Firma Electrónica –IOFE. Autoridad Administrativa Competente.
   3. Prestadores de Servicios de Certificación Digital (PSC). Modalidades
      3.1 Entidades de Certificación (EC)
      3.2 Entidades de Registro o Verificación (ER)
      3.3 Prestadores de Servicios de Valor Añadido (SVA)

II. Procedimiento de Acreditación de Prestadores de Servicios de Certificación Digital (PSC)
   1. Acreditación de Entidad de Certificación (EC)
      1.1 Tipos de Procedimiento de Acreditación
      1.2 Solicitud de Acreditación como EC. Documentos sustentatorios
   2. Acreditación de Entidades de Registro o Verificación (ER)
      2.1 Tipos de Procedimiento de Acreditación
      2.2 Solicitud de Acreditación como EC. Documentos sustentatorios
   3. Acreditación de Prestadores de Servicios de Valor Añadido (SVA)
      3.1 Tipos de Procedimiento de Acreditación
      3.2 Solicitud de Acreditación como EC. Documentos sustentatorios
   4. Acreditación de aplicaciones de Software.
      4.1 Solicitud de Acreditación aplicaciones de Software. Documentos sustentatorios.

III. Procedimientos de Acreditación
   1. Procedimiento de Acreditación de Prestadores de Servicios de Certificación Digital (PSC). Fases. Etapas.
   2. Vigencia de la Acreditación
   3. Mantenimiento de la Acreditación
      3.1 Visitas de Supervisión
      3.2 Auditorias Anuales
      3.3 Procedimiento en caso de No conformidades u Observaciones
      3.4 Decisión para el mantenimiento de la acreditación
   4. Renovación de la Acreditación
      4.1 Procedimiento
      4.2 Procedimiento en caso de No conformidades u Observaciones
      4.3 Modificación
   5. Homologación de Acreditación
      5.1 Procedimiento
      5.2 Procedimiento en caso de No conformidades u Observaciones
      5.3 Modificación
   6. Procedimiento de Acreditación de Aplicación de Software

INTRODUCCIÓN

El presente Handbook es un texto elaborado por Iriarte & Asociados que brinda información sobre el trámite y procedimiento para la obtención de acreditación como Prestador de Servicios de Certificación Digital, conforme a la normativa vigente sobre Ley de Firmas y Certificados Digitales en el Perú.

Se han considerado todas las normas sobre la materia referente a firmas y certificados digitales. Entre las principales: Ley N° 27269, Ley de Firmas y Certificados Digitales, y modificatoria por Ley N° 27310, su Reglamento vigente aprobado por Decreto Supremo N° 052-2008-PCM, sus modificatorias el Decreto Supremo N° 070-2011-PCM y Decreto Supremo N° 105-2012-PCM, así como el Texto Único de Procedimiento Administrativo de la Comisión de Normalización y Fiscalización de Barreras No Arancelarias del INDECOPI vigente a la fecha de elaboración del presente manual.

- **Objetivo:**

Brindar información básica y relevante sobre las consideraciones legales respecto a las diferentes modalidades de acreditación de los diferentes participantes de la Infraestructura Oficial de Firmas Electrónicas (IOFE), que se encuentra bajo la supervisión del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), requisitos y características de los procedimientos de acreditación.

Asimismo, las condiciones y requerimientos para la vigencia y mantenimiento de la acreditación otorgada.

- **Alcance:**

A todos las personas naturales y jurídicas, abogados, consultores, administración pública en general y público interesado.

Si tiene alguna consulta o duda respecto del contenido del presente Handbook, no dude en contactarse con nosotros.

IRIARTE & ASOCIADOS

I. NORMATIVA APLICABLE SOBRE FIRMAS Y CERTIFICADOS DIGITALES

La Ley N° 27269 - Ley de Firmas y Certificados Digitales publicada el 28 de mayo de 2000, reguló por primera vez en el Perú la utilización de las firmas electrónicas en general y la firma digital en especial. La Ley N° 27310, publicada el 17 de Julio de 2000, modificó posteriormente su texto original.

En el año 2002 se publicó su primer Reglamento, aprobado por el Decreto Supremo N° 019-2002-JUS, que fue sustituido en el año 2007 por el Decreto Supremo N°004-2007-PCM y, finalmente en el año 2008 por el Decreto Supremo N° 052-2008-PCM, que se encuentra actualmente vigente, con las modificaciones efectuadas por Decreto Supremo N° 070-2011-PCM (publicado del 27 de julio de 2011) y Decreto Supremo N° 105-2012-PCM (publicado el 21 de octubre de 2012).

1. AMBITO DE APLICACIÓN DE LA NORMATIVA DE FIRMAS Y CERTIFICADOS DIGITALES

La normativa mencionada establece las características que deben reunir las firmas electrónicas[1] en general, y las firmas digitales[2] en especial, para ser utilizadas con validez legal den el Perú. El Decreto Supremo N° 052-2008-PCM (en adelante el Reglamento) instaura el régimen de la ***Infraestructura Oficial de Firma Electrónica (IOFE),*** que es el sistema que comprende los instrumentos legales y técnicos que permiten e incluyen la generación de firmas digitales en el que participan Prestadores de Servicios de Certificación Digital.

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

Teniendo en cuenta la variedad de firmas electrónicas que puedan existir en el mercado, la Ley N° 27269- Ley de Firmas y Certificados Digitales (en adelante la Ley) limita su ámbito de aplicación a aquellas firmas electrónicas que tengan los siguientes atributos:

- ✓ Estén puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos
- ✓ Puedan vincular e identificar al firmante
- ✓ Puedan garantizar la autenticación e integridad de los documentos electrónicos

Todas las firmas digitales que se generen fuera de la IOFE, serán válidas conforme a los términos y convenios que acuerden las partes.

La normativa es aplicable para el Sector Público y el Sector Privado.

---

[1] La Ley N° 27269- Ley de Firmas y Certificados Digitales define a la **firma electrónica** como cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de la firma manuscrita.

[2] La Ley N° 27269- Ley de Firmas y Certificados Digitales define a la **firma digital** como aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único, asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

2. INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA (IOFE) - AUTORIDAD ADMINISTRATIVA COMPETENTE

La ***Infraestructura Oficial de Firma Electrónica (IOFE)*** 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.

El sistema es regulado y supervisado por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, que es, dentro de régimen de la IOFE, la ***Autoridad Administrativa Competente*** encargada de acreditar a las Entidades Prestadoras de Certificación digital (PSC) y de reconocer los estándares tecnológicos y de seguridad aplicables.

3. PRESTADORES DE SERVICIOS DE CERTIFICACION DIGITAL (PSC). MODALIDADES

Son Prestadores de Servicios de Certificación Digital (PSC) los siguientes:

3.1 Entidades de Certificación (EC)
3.2 Entidades de Registro o Verificación (ER)
3.3 Prestadores de Servicios de Valor Añadido (SVA)

3.1 ENTIDADES DE CERTIFICACIÓN (EC)

La 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.

Sus funciones son:

a) Emitir certificados digitales[3].
b) Cancelar certificados digitales.
c) Reconocer certificados digitales emitidos por entidades de certificación extranjeras que hayan sido incorporadas por reconocimiento a la IOFE.

[3] El 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 (Definición del Reglamento)

3.2 ENTIDADES DE REGISTRO O VERIFICACIÓN (ER)

La Entidad de Registro o Verificación es la persona jurídica, con excepción de los notarios públicos[4], 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.

Sus funciones son:

a) Identificar a los titulares y/o suscriptores del certificado digital mediante el levantamiento de datos y la comprobación de la información brindad por aquel.
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 (EC).

3.3 PRESTADORES DE SERVICIOS DE VALOR AÑADIDO (SVA)

Servicios de Valor Añadido son los servicios complementarios de la firma digital brindados dentro o fuera de la IOFE 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 IOFE es brindado por persona natural o jurídica acreditada ante la AAC.

Sus funciones son:

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 solo 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 IOFE.

   Los usuarios que así lo deseen podrán emplear su propio certificado digital de autenticación.

   Los Prestadores de Servicios de Valor Añadido pueden, a su vez, 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.
      Pueden adoptar a su vez dos modalidades:

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

[4] La figura del Notario público se introdujo con el Reglamento del 2007 y sus funciones se desprendían del Artículo 41°. El Reglamento vigente solo contiene mención a los Notarios con esta competencia en la definición de "Entidad de Registro", sin embargo la consignamos debido a que se mantiene su reglamentación en la Guía de Acreditación para Entidades de Verificación/Registro de Datos vigente.

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

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.
Se refiere al sistema de Sellado de Tiempo, el cual permite consignar la fecha y hora cierta de la existencia de un documento electrónico.

Es factible que una misma Entidad preste sus servicios en más 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 IOFE.

II. PROCEDIMIENTO DE ACREDITACION DE PRESTADORES DE SERVICIOS DE CERTIFICACION DIGITAL (PSC)

Para actuar dentro del marco de la IOFE, los Prestadores de Servicios de Certificación Digital (PSC) deben acreditarse según su modalidad, ante la Autoridad Administrativa Competente, conforme al procedimiento regulado por el Reglamento vigente, las Guías de Acreditación y sus respectivos Anexos publicados en el portal web del INDECOPI y el Texto Único de Procedimiento Administrativo – TUPA vigente al año de inicio del procedimiento.

1. ACREDITACION DE ENTIDADES DE CERTIFICACION (EC)

La 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.

1.1 Tipos de Procedimientos de Acreditación de EC:

Pueden solicitarse los siguientes tipos de acreditación de una EC:

A. Acreditación como EC de nivel raíz y como EC de nivel subsiguiente.

Se solicita para Entidades que soliciten funcionar:

a. como EC raíz: emiten certificados digitales para ECs de nivel subsiguiente; y
b. como EC de nivel subsiguiente: emiten certificados digitales para usuarios finales

Este tipo de acreditación deberá ser solicitada por la ECERNEP (y la ECEP respectiva) para efectos de su incorporación en la IOFE.

B. Acreditación como EC de nivel subsiguiente

Se solicita para Entidades que emiten certificados digitales para usuarios finales, personas naturales o jurídicas.

Este tipo de acreditación deberá ser solicitada por las ECEPs para efectos de su incorporación en la IOFE.

C. Autorización para la realización de certificación cruzada con otras ECs

Se solicita cuando una EC acreditada nacional pretende reconocer la validez de un certificado emitido por otra, nacional o extranjera, y asume tal certificado como si fuera de su propia emisión.

D. Renovación de acreditación

La renovación de la acreditación deberá cuando menos realizarse dentro de los 120 días anteriores al vencimiento de la acreditación conferida.

E. Acreditación por homologación

La homologación deberá solicitarse dentro de los 30 días posteriores a la realización de alguna de las auditorías anuales a las que será sometida la EC acreditada.

En caso que la EC solicitante decida realizar servicios adicionales inherentes a la certificación digital, para efecto que los mismos gocen de amparo legal, deberán ser sometidos al procedimiento de acreditación correspondiente en virtud a los lineamientos establecidos para tales efectos para los Prestadores de Servicios de Certificación que brinda servicios de valor añadido (SVA) en el entorno de la IOFE. Asimismo, en el caso que optara por brindar servicios de registro o verificación, deberá someterse al procedimiento establecido para la obtención de acreditación como Entidad de Registro (ER).

1.2 Solicitud de Acreditación como EC. Documentos Sustentatorios

Para solicitar la acreditación de una EC deben cumplirse los requerimientos dispuestos por el Reglamento, la "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas"[5] publicada por la AAC, y el TUPA vigente[6].

Se deberán presentar los siguientes documentos:

(1) Ficha de Solicitud de Acreditación

El formato de la solicitud debe presentarse en el formato de la AAC, que puede descargarse del link http://www.indecopi.gob.pe/RepositorioAPS/0/6/par/GUIAS1/anexo%2010-solicitud%20de%20acreditacion%20como%20ec%20(nov2007).pdf

Deben cumplirse las siguientes especificaciones[7]:

[5] La Guía de acreditación vigente es la Versión 3.3 y cuenta con 13 Anexos. Se puede acceder a los documentos a través del portal web de INDECOPI http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=6&JER=452

[6] TUPA aprobado por D.S. N° 085-2012-PCM publicado el 19 de Agosto de 2012, modificado por D.S. N° 110-2010-PCM de 16 de Diciembre de 2010 y R.M. N° 346-2011-PCM de 22 de Diciembre de 2011.

[7] Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 7) y Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

- Estar dirigida al Secretario Técnico de la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias del INDECOPI.

- Indicar la Modalidad de Acreditación solicitada.

- Indicar Nivel de seguridad al que se postula, según la finalidad para la que se pretenda emitir los certificados digitales.

  Los niveles de seguridad pueden ser MEDIO y MEDIO ALTO. El primero para trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio; información crítica y de seguridad nacional en redes cifradas, acceso a información clasificada o de acceso especial en redes protegidas; y, aplicaciones de valor financiero medio o de comercio electrónico, tales como las planillas, contratos, compra de vehículos, etc. El segundo nivel para todas las aplicaciones para nivel medio; trámites con el Estado en las transacciones económicas de alto monto y alto riesgo, y el intercambio de documentos y transacciones monetarias de alto riesgo; información crítica no clasificada o de seguridad nacional en redes no cifradas; acceso a información clasificada o de acceso especial en redes no protegidas; y aplicaciones de valor financiero de riesgo y monto medio alto o de comercio electrónico.

  Según el nivel de seguridad y el tipo de transacciones objeto de los procesos de la EC, se deberá especificar la siguiente información:

  - Los dispositivos criptográficos físicos, hardware y firmware (sistema operativo), que almacenan las claves privadas de la entidad final (usuarios) deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.
  - La longitud de clave privada mínima debe ser de 1024 bits y el certificado debe ser renovado como máximo anualmente para el Nivel Medio y de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años para el Nivel Medio Alto.
  - Los certificados a nivel de entidad final (usuarios) deben ser generados de manera individual y separados para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.
  - Adicionalmente, la EC que otorgue certificados digitales para transacciones de nivel de seguridad medio alto, deberá contar con certificación ISO 27001 para los procesos inherentes a su función y la infraestructura tecnológica respectiva.

- Adicionalmente, como parte del formato de acreditación, deberá consignarse la Declaración Jurada del solicitante de tener conocimiento respecto a los criterios, requisitos y condiciones de acreditación establecidos por la Comisión; así como las obligaciones y derechos que involucra obtener la correspondiente acreditación, la veracidad de la información acompañada al mencionado formato, de ser el caso, el contar con la infraestructura e instalaciones necesarias para prestar los servicios de certificación digital cuya acreditación se solicita; el tener operativo software, hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren interoperabilidad y las condiciones exigidas por Comisión, así como aceptar la visita comprobatoria que efectuará la Comisión o las personas o institución que ésta designe para tales efectos, y brindar las facilidades necesarias en todas las instalaciones en donde se lleven a cabo las evaluaciones a efecto de poder verificar el cumplimento de los requisitos necesarios para la acreditación.

- La solicitud deberá estar suscrita por el representante legal de la EC solicitante y deberán incluirse sus datos de contacto.

(2) Copia simple del documento de identidad del solicitante[8].

En el caso que el solicitante sea un nacional deberá acompañar su Documento Nacional de Identidad con la correspondiente constancia de sufragio en las últimas elecciones. En el caso de solicitantes extranjeros, deberán acompañar su Carné de Extranjería o Pasaporte con el visado correspondiente.

(3) 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[9].

Respecto de la existencia y vigencia de la persona jurídica, deberá acreditarse con:

a. Documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente.
b. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por autoridad competente en su país de origen.
c. En el caso de las instituciones del Estado, deberán acreditar la existencia de una Oficina, Gerencia o dependencia interna a la cual se le otorgan funciones como prestador de servicios de certificación digital.

Respecto a la acreditación de poderes de los representantes legales:

a. En el caso de personas jurídicas constituidas en el país: en el documento que acredite la representación, deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia del poder respectivo.
b. En el caso de personas jurídicas constituidas en el extranjero: los correspondientes poderes deberán ser legalizados por un funcionario consular peruano y de encontrarse redactados en idioma extranjero, será necesario que sean traducidos, debiendo el responsable de la traducción suscribir el correspondiente documento.
c. En el caso de instituciones del Estado, deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la certificación digital. Debiéndose asimismo acreditar las facultades de este funcionario.

(4) Documentos que acrediten contar con un domicilio en el país[10].

Para acreditar la condición de domiciliada de una EC solicitante, debe presentarse el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), donde debe constar la condición de “habida”. Cualquier otra documentación será evaluada por la Comisión.

8 Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

9 Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 7) y Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

10 Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

(5) 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 AAC[11].

La Guía no especifica los documentos que pueden utilizar el solicitante para acreditar que cuenta con la infraestructura e instalaciones necesarias para la prestación del servicio[12], requisito solicitado por el TUPA vigente.

Para acreditar la aceptación de la visita comprobatoria de la AAC es suficiente presentar la Declaración Jurada, que forma parte integrante de la Ficha de Solicitud de Acreditación como EC, por lo que bastará la suscripción de este documento para que se entienda efectuada. Sin perjuicio de ello, la EC solicitante podrá elaborar las mencionadas Declaraciones Juradas en documentos independientes, los mismos que se deberán acompañar a la solicitud de acreditación.

(6) Memoria Descriptiva que contenga los procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento[13]

La Memoria descriptiva y el Organigrama Estructural y Funcional deberán ser realizados conforme al Formato denominado: Memoria Descriptiva y Organigrama Estructural y Funcional – Entidad de Certificación (EC), descritos en el Anexo 9 de la Guía de Acreditación.

(7) Política de Certificación (CP), Declaración de Prácticas de Certificación (CPS), la Política de Seguridad, la Política y el Plan de Privacidad y documentación que comprende el Sistema de Gestión Implementado conforme al inciso d) del Artículo 20° del Reglamento.

La "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" [14] define las Políticas de Certificación como el documento que describe de manera general las políticas y procedimientos que aplica la EC para la prestación de sus servicios. Por su parte, define la Declaración de Prácticas de Certificación como el documento en el que constan de manera detallada las políticas y procedimientos que aplica la EC para la prestación de sus servicios.

Ambos documentos deben observar los Lineamientos para Infraestructura de clave pública (PKI) del APEC, según el documento Marco de la Política de emisión de certificados digitales, así como de la Norma Marco sobre Privacidad.

La "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" comprende dos documentos instructivos en materia de seguridad:

- Documento Estándar de una Política de Seguridad (Anexo 4 de la Guía) que contiene los parámetros para la elaboración de la Política de Seguridad de la EC.

11 Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

12 El Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8) se limita a requerir que se suscriba la Ficha de Solicitud de Acreditación que contiene la Declaración Jurada de contar con tales elementos.

13 Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

14 Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8)

- Requisitos de Seguridad para la Acreditación (Anexo 2 de la Guía) que resume los requerimientos técnicos y su correspondencia con Normas Técnicas Internacionales.

Igualmente, la "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" establece una Norma Marco sobre Privacidad APEC (Anexo 6 de la Guía) que contiene los parámetros para la elaboración de la Política y el Plan de Privacidad de la EC. [15]

Respecto del Sistema de Gestión Implementado conforme al inciso d) del Artículo 20° del Reglamento, este apartado hace referencia el sistema de gestión que permita el mantenimiento de las condiciones que aseguren a la generación de firmas digitales, certificados digitales y documentos electrónicos bajo la IOFE; las políticas y declaraciones de prácticas de las EC basadas en estándares internacionales o compatibles con los internacionalmente vigentes, que aseguren la interoperabilidad entre dominios y las funciones exigidas por la AAC; el software, el hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los estándares señalados; así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.

(8) Declaración Jurada del cumplimiento de los requisitos señalados en los incisos c) y d) del Artículo 20 del Reglamento, información que será comprobada por la AAC.

En la Ficha de Solicitud de Acreditación como Entidad de Certificación (EC) se integran varias declaraciones, que no abarcan completamente el alcance de los artículos, por lo que se recomienda elaborar la mencionada Declaración Jurada en documento independiente, el mismo que deberá ser acompañado a la solicitud de acreditación

La declaración jurada debe comprender el siguiente texto:

- El software, el hardware y demás componentes son adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los 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.
- El sistema de gestión permite el mantenimiento de las condiciones señaladas en el Artículo 20° del Reglamento de la Ley de Firmas Digitales, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de servicios.

(9) Documentación que acredite el cumplimiento de los artículos 26 y 27 del Reglamento, y demás requisitos que la AAC señale.

En consecuencia se debe acreditar que la EC cumple con sus obligaciones y responsabilidades, que son las siguientes:

a) Cumplir los requerimientos referentes 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 AAC dentro del procedimiento de acreditación.

[15] La Política y el Plan de Privacidad deberán dar cumplimiento a la Ley de N° 29733 – Ley de Protección de Datos Personales, en sus términos vigentes.

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 EC, estando en la obligación de comunicar inmediatamente a la AAC 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 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 AAC 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 AAC conforme a lo establecido en el Reglamento.
i) Informar y solicitar autorización a la AAC 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 AAC para efectos del reconocimiento de certificados emitidos por entidades extranjeras.
k) Cumplir con las disposiciones de la AAC a que se refiere el artículo 27 del Reglamento.
l) Brindar todas las facilidades al personal autorizado por la AAC 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.

   Nota[16]:
   La obtención del sello de Web Trust al que hace referencia este inciso es de cumplimiento obligatorio para las EC que acrediten en el nivel de seguridad Medio Alto.
   Las EC están exoneradas del cumplimiento de este requisito hasta el 31 de Diciembre de 2012; sin perjuicio de aquellas que opten voluntariamente por el cumplimiento de dichos requerimientos.

n) Acreditar domicilio en el país.

En cuanto a la responsabilidad por riesgo, para operar en el marco de la IOFE y afrontar los riesgos que puedan surgir como resultado de sus actividades de certificación, la EC acreditada o reconocida, de acuerdo a los niveles de seguridad establecidos, deberá 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. Corresponde a la AAC establecer la cuantía

16 Disposición Décimo Segunda del Reglamento, modificada por D.S. N° 105-2012-PCM.

mínima de las pólizas de seguros o garantías bancarias, las medidas tecnológicas correspondientes al nivel de seguridad respectivo, así como los criterios para evaluar el cumplimiento de este requisito.

Este requisito no será exigible para la ECERNEP ni ECEPs.

Para efectos del procedimiento de acreditación, bastará suscribir la Ficha de solicitud en la cual en la parte correspondiente a la Declaración Jurada la EC solicitante se compromete a la contratación de los seguros o garantías bancarias en caso obtener la acreditación, como requisito indispensable para poder ingresar a la IOFE.

Los Prestadores de Servicios de Certificación Digital están exonerados hasta el 31 de Diciembre de 2013[17] de la contratación de seguros o garantías bancarias; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

(10) Informe favorable de la entidad sectorial correspondiente, en caso sea necesario, para el caso de personas Jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de las actividades de certificación[18].

Este requisito es exigible solo para entidades supervisadas.

(11) Otros documentos o requisitos establecidos por la AAC.

- Los siguientes son documentos solicitados por la AAC en la "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" [19] para su presentación, según el caso, en el proceso de acreditación:

- Documentos que se deben acompañar en caso que alguno de los elementos relativos al sistema de gestión o software, hardware y demás componentes sean administrados 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 evaluación y supervisión que la AAC considere necesarias. La vinculación a que se alude en el punto anterior puede ser demostrada a través de un contrato, acuerdo, convenio de outsourcing u otro tipo de documentación permitida bajo el ordenamiento peruano, según los términos requeridos por la AAC.

- Documentos que acrediten vinculación con una o más ERs.

Esta vinculación deberá ser por un periodo no menor al de la acreditación solicitada.
Este requisito no será necesario en el caso que la EC a su vez realice funciones de ER, en cuyo supuesto deberá solicitar la acreditación correspondiente como ER. En este caso, su acreditación como EC quedará condicionada a la obtención de la correspondiente acreditación como ER.

17 Disposición Décimo Primera del Reglamento, modificada por D.S. N° 105-2012-PCM.

18 TUPA aprobado por D.S. N° 085-2012-PCM publicado el 19 de Agosto de 2012, modificado por D.S. N° 110-2010-PCM de 16 de Diciembre de 2010 y R.M. N° 346-2011-PCM de 22 de Diciembre de 2011.

19 Reglamento Específico de Acreditación Entidad de Certificación – EC (Anexo 8 de la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas)

- Documentación que acredite la contratación de seguros o garantías bancarias para salvaguardar las actividades de certificación.

Para efectos de la presentación de la solicitud de acreditación bastará adjuntar Declaración Jurada en la cual se señale que en caso se obtenga la acreditación por parte del INDECOPI, se procederá a la contratación del seguro o garantía bancaria correspondiente[20].
Este requisito no será exigible para la ECERNEP ni ECEPs.

- Documentación que acredite contar con respaldo económico.

En el caso de EC particulares, deberán presentar estados financieros (balance general, estado de ganancias y pérdidas y notas contables), con una antigüedad no mayor a dos meses del cierre contable del mes anterior a la presentación de la solicitud, acreditando solvencia económica. Estos estados financieros deberán ser individuales (no consolidados) y encontrarse auditados.
Si una empresa presentara estados financieros con pérdidas acumuladas de ejercicios anteriores, para acreditar solvencia económica deberá capitalizar dicha pérdida o realizar nuevos aportes en cuantía que compense el desmedro y mostrar el nuevo capital suscrito y pagado e inscrito en Registros Públicos.
Este requisito no será exigible para la ECERNEP ni ECEPs.

- Documento donde conste el mapeo correspondiente: CP, CPS – APEC.

Este documento será requerido en el supuesto que no se hayan elaborado la Política de Certificación y la Declaración de Prácticas de Certificación siguiendo el esquema establecido en el anexo 1 de Guía de Acreditación de Entidad de Certificación (EC), para el caso de los países miembros del APEC que no hubieran participado en el mapeo que dio origen a los Lineamientos antes señalados y que no hubieran homologado en sus legislaciones los lineamientos antes señalados, así como para el caso del resto de países. En este supuesto, el documento versará en un mapeo que deberá realizarse entre la CP y CPS de la solicitante y el documento del APEC

En el caso que la EC solicitante, pertenezca a Australia, Canadá, China Hong Kong, Singapur y Estados Unidos, que son los países que participaron en el mapeo efectuado con las provisiones del IETF RFC 3647 contenidas en los “Lineamientos para el marco de la política de emisión de certificados que pueden ser usados en comercio electrónico transnacional” del APEC, la documentación que se deberá acompañar es la siguiente: Documentos que acredite la condición de economía miembro del APEC.

- Documento en el que conste el mapeo entre la CP y CPS del solicitante y el documento del APEC.

En el caso que la EC solicitante, pertenezca a un país miembro del APEC que no hubiera participado en el mapeo a que se alude en el inciso anterior y que no hubiera homologado en su legislación los lineamientos antes señalados o pertenezca a cualquier otro país, la documentación a acompañar es la siguiente:

- CP y CPS elaboradas de acuerdo a la estructura establecida, en el documento “Marco de la Política de emisión de certificados digitales” (anexo 1 de la Guía de Acreditación de Entidad de Certificación – EC); o
- Documento donde conste el mapeo entre la CP y CPS del solicitante y el documento “Marco de la Política de emisión de certificados digitales”.

[20] Los Prestadores de Servicios de Certificación Digital están exonerados hasta el 31 de Diciembre de 2013[20] de la contratación de seguros o garantías bancarias; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

En el caso de países con los cuales la AAC hubiera celebrado un acuerdo de reconocimiento mutuo, se deberá acompañar la documentación siguiente:

- Acreditación otorgada en el país de origen de la solicitante.
- Hacer referencia a la fecha de celebración del acuerdo de reconocimiento mutuo entre la institución competente del país de la solicitante y la AAC.

En el caso que se solicite la acreditación como EC de nivel subsiguiente, la documentación a acompañar es la siguiente:
- Únicamente se acompañará la Resolución de acreditación de la EC Raíz, siempre y cuando la gestión de los certificados digitales sea realizada en la misma infraestructura montada para la EC Raíz acreditada.

Deberá encontrarse especificado en la CP y CPS de la solicitante las condiciones de gestión de certificados digitales conforme a lo establecido en el punto anterior.

- Acreditación otorgada en el país de origen de la solicitante

Esto opera en el caso que exista un acuerdo de reconocimiento mutuo entre la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias (antes Comisión de Reglamentos Técnicos y Comerciales) con entidades similares a nivel mundial. En este caso, bastará que la solicitante acompañe la autorización o acreditación otorgada en su país de origen, debiendo hacer referencia a la fecha de celebración del acuerdo de reconocimiento mutuo antes señalado.

- Resolución de acreditación de la Entidad de Certificación Raíz

Se presentará en el caso que se solicite la acreditación como EC de nivel subsiguiente siempre y cuando la gestión de los certificados sea realizada en la misma infraestructura montada para la Entidad de Certificación raíz acreditada. Para tales efectos bastará que este hecho se encuentre detallado en la CP y CPS de la solicitante y se acompañe la resolución de acreditación de la EC raíz.

(12) Constancia de pago de los derechos administrativos.

Los derechos administrativos que deben cancelarse para efectos del procedimiento de acreditación como EC ascienden al 100% del valor de la UIT.

(13) Certificaciones sobre declaraciones informadas en los Datos técnicos[21].

Las certificaciones que deben presentarse corresponden a la información declarada sobre aspectos técnicos de la solicitud.

En el caso de acreditación de EC, se deberá acreditar:
a. Certificación Módulo Criptográfico
b. Certificación Tarjetas inteligentes

Respecto al cumplimiento de requisitos de Seguridad para la acreditación, incluyéndose Políticas de Seguridad, Capacidad Tecnológica, Seguridad Física y Ambiental, Requerimientos de Personal, se

[21] Este requisito no se encuentra en el TUPA, sin embargo se desprende del texto de la Ficha de Solicitud elaborada por el INDECOPI.

debe revisar en extenso los Requisitos exigidos por la AAC, en los Anexos 2, 4, 5, 11 y demás pertinentes de la Guía de Acreditación.

La Guía de Acreditación de Entidades de Certificación (EC) comprende la evaluación de la confiabilidad de los sistemas PKI respecto del manejo de claves, la gestión del ciclo de vida de los certificados digitales, así como la evaluación de la gestión de los controles de seguridad física, informática y de personal basados en la NTP/ISO 17799 y el ISO 27001 de las plantas de certificación digital; la evaluación de los sistemas informáticos (controles de seguridad en redes, control de acceso, criptografía), finalmente se evaluará el cumplimiento en requerimientos de Usabilidad.

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

La relación de documentos antes señalada no es taxativa. En tal sentido, la Comisión podrá considerar y solicitar cualquier documentación adicional que sea necesaria a efectos de poder tomar una decisión informada sobre la acreditación o no del solicitante.

2. ACREDITACION DE ENTIDAD DE REGISTRO O VERIFICACION (ER)

La Entidad de Registro o Verificación es la persona jurídica, con excepción de los notarios públicos[22], 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.

2.1 Tipos de Procedimientos de Acreditación de ER:

Pueden solicitarse los siguientes tipos de acreditación de una ER:

A. Acreditación como ER – persona jurídica

Se solicita por personas jurídicas, públicas o privadas.
Este tipo de acreditación deberá seguirse para el caso de las EREP.

B. Acreditación como ER – persona natural

Este tipo de acreditación sólo podrá ser solicitada por los Notarios en ejercicio de sus funciones.

C. Renovación de la acreditación

La renovación de la acreditación deberá cuando menos realizarse dentro de los 120 días anteriores al vencimiento de la acreditación conferida.

[22] La figura del Notario público se introdujo con el Reglamento del 2007 y sus funciones se desprendían del Artículo 41°. El Reglamento vigente solo contiene mención a los Notarios con esta competencia en la definición de "Entidad de Registro", sin embargo la consignamos debido a que se mantiene su reglamentación en la Guía de Acreditación para Entidades de Verificación/Registro de Datos vigente.

2.2 Solicitud de Acreditación como ER. Documentos Sustentatorios

Para solicitar la acreditación de una Entidad de Registro (ER) deben cumplirse los requerimientos dispuestos por el Reglamento, la "Guía de Acreditación para Entidades de Verificación/Registro de Datos"[23] publicada por la AAC, y el TUPA vigente[24].

Se deberán presentar los siguientes documentos:

(1) Ficha de Solicitud de Acreditación

El formato de la solicitud debe presentarse en el formato de la AAC, que puede descargarse del link http://www.indecopi.gob.pe/RepositorioAPS/0/6/par/GUIAS2/anexo%209-sol.acreditacion%20como%20er%20(nov2007).pdf

Deben cumplirse las siguientes especificaciones[25]:

- Estar dirigida al Secretario Técnico de la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias del INDECOPI.
- Indicar el tipo de procedimiento solicitado.
- Indicar el Tipo de Nivel de seguridad al que se postula y que será empleado en la prestación de servicios de certificación digital.

  Los niveles de seguridad pueden ser MEDIO y MEDIO ALTO. El primero para trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio; información crítica y de seguridad nacional en redes cifradas, acceso a información clasificada o de acceso especial en redes protegidas; y, aplicaciones de valor financiero medio o de comercio electrónico, tales como las planillas, contratos, compra de vehículos, etc. El segundo nivel para todas las aplicaciones para nivel medio; trámites con el Estado en las transacciones económicas de alto monto y alto riesgo, y el intercambio de documentos y transacciones monetarias de alto riesgo; información crítica no clasificada o de seguridad nacional en redes no cifradas; acceso a información clasificada o de acceso especial en redes no protegidas; y aplicaciones de valor financiero de riesgo y monto medio alto o de comercio electrónico.

  Según el nivel de seguridad y el tipo de transacciones objeto de los procesos de la ER, se debe tener en consideración lo siguiente:

  - Los dispositivos criptográficos físicos, hardware y firmware (sistema operativo), que almacenan las claves privadas de la entidad final (usuarios) deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.

[23] La Guía de acreditación vigente es la Versión 3.3 y cuenta con 11 Anexos. Se puede acceder a los documentos a través del portal web de INDECOPI http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=6&JER=453

[24] TUPA aprobado por D.S. N° 085-2012-PCM publicado el 19 de Agosto de 2012, modificado por D.S. N° 110-2010-PCM de 16 de Diciembre de 2010 y R.M. N° 346-2011-PCM de 22 de Diciembre de 2011.

[25] Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 5)

- La longitud de clave privada mínima debe ser de 1024 bits y el certificado debe ser renovado como máximo anualmente para el Nivel Medio y de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años para el Nivel Medio Alto.
- Los certificados a nivel de entidad final (usuarios) deben ser generados de manera individual y separados para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.
- Adicionalmente, para el caso de transacciones de nivel de seguridad medio alto, la ER deberá contar con certificación ISO 9001:2000 para todos los procesos inherentes a su función.

- Adicionalmente, como parte del formato de acreditación, deberá consignarse la Declaración Jurada del solicitante de tener conocimiento respecto a los criterios, requisitos y condiciones de acreditación establecidos por la Comisión; así como las obligaciones y derechos que involucra obtener la correspondiente acreditación, la veracidad de la información acompañada al mencionado formato, de ser el caso, el contar con la infraestructura e instalaciones necesarias para prestar los servicios de certificación digital cuya acreditación se solicita; el tener operativo software, hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren interoperabilidad y las condiciones exigidas por Comisión, así como aceptar la visita comprobatoria que efectuará la Comisión o las personas o institución que ésta designe para tales efectos, y brindar las facilidades necesarias en todas las instalaciones en donde se lleven a cabo las evaluaciones a efecto de poder verificar el cumplimento de los requisitos necesarios para la acreditación.

- La acreditación de una ER implica la acreditación de sus agencias (sucursales), las cuales deben de cumplir con lo establecido en la RPS y demás documentos relevantes de la ER. Debe entregarse un documento donde se especifique la localización de las agencias, así como los nombres de los responsables de los procesos de registro en cada una de las mismas.

- La solicitud deberá estar suscrita por el representante legal de la ER solicitante y deberán incluirse sus datos de contacto.

(2) Copia simple del documento de identidad del solicitante[26].

En el caso que el solicitante sea un nacional deberá acompañar su Documento Nacional de Identidad con la correspondiente constancia de sufragio en las últimas elecciones. En el caso de solicitantes extranjeros, deberán acompañar su Carné de Extranjería o Pasaporte con el visado correspondiente.

(3) 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[27].

[26] Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

[27] Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

Respecto de la existencia y vigencia de la persona jurídica, deberá acreditarse con:

a. Documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente.
b. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por autoridad competente en su país de origen.
c. En el caso de las instituciones del Estado, deberán acreditar la existencia de una Oficina, Gerencia o dependencia interna a la cual se le otorgan funciones como prestador de servicios de una ER.
d. En el caso de los Notarios, se acreditará este hecho con una constancia de habilitación expedida para tales efectos por su Colegio Profesional, así como con su correspondiente Resolución Ministerial de nombramiento en el cargo.

Respecto a la acreditación de poderes de los representantes legales:

a. En el caso de personas jurídicas constituidas en el país: en el documento que acredite la representación, deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia del poder respectivo.
b. En el caso de personas jurídicas constituidas en el extranjero: los correspondientes poderes deberán ser legalizados por un funcionario consular peruano y de encontrarse redactados en idioma extranjero, será necesario que sean traducidos, debiendo el responsable de la traducción suscribir el correspondiente documento.
c. En el caso de instituciones del Estado, deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la certificación digital. Debiéndose asimismo acreditar las facultades de este funcionario.
d. En el caso de los Notarios, se estará a lo establecido en el Decreto Ley No. 26662 – Ley del Notariado.

(4) Documentos que acrediten contar con un domicilio en el país[28].

Para acreditar la condición de domiciliada de una ER solicitante, debe presentarse el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), donde debe constar la condición de "habida". Cualquier otra documentación será evaluada por la Comisión.

(5) 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 AAC[29].

La Guía no especifica los documentos que pueden utilizar el solicitante para acreditar que cuenta con la infraestructura e instalaciones necesarias para la prestación del servicio[30], requisito solicitado por el TUPA vigente.

[28] Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

[29] Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

[30] El Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7) se limita a requerir que se suscriba la Ficha de Solicitud de Acreditación que contiene la Declaración Jurada de contar con tales elementos.

Sin perjuicio de ello, solicitante deberá cumplir con todos los controles físicos: control de acceso, evaluación de riesgos, seguridad física, planificación de contingencias, riesgos, relativos al local físico, previstos en los Anexos 3 y 4 de la Guía de Acreditación.

Para acreditar la aceptación de la visita comprobatoria de la AAC es suficiente presentar la Declaración Jurada, que forma parte integrante de la Ficha de Solicitud de Acreditación como ER, por lo que bastará la suscripción de este documento para que se entienda efectuada. Sin perjuicio de ello, la ER solicitante podrá elaborar las mencionadas Declaraciones Juradas en documentos independientes, los mismos que se deberán acompañar a la solicitud de acreditación.

(6) Memoria Descriptiva que contenga los procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.

La Memoria descriptiva y el Organigrama Estructural y Funcional deberán ser realizados conforme al Formato denominado: Memoria Descriptiva y Organigrama Estructural y Funcional – Entidad de Registro o Verificación (ER), descritos en el Anexo 8 de la Guía de Acreditación [31].

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

La "Guía de Acreditación para Entidades de Verificación/ Registro de Datos" [32] define la Declaración de Prácticas de Registro o Verificación (RPS) como el documento en el que constan de manera detallada las políticas y procedimientos que aplica la ER para la prestación de sus servicios. Esta Declaración deberá estar elaborada en estricta observancia de los Lineamientos para Infraestructura de clave pública (PKI) del APEC, según el documento "Marco de la Política de Registro para la emisión de certificados digitales", así como de la Norma Marco sobre Privacidad y deberán establecer procedimientos detallados que garanticen el cumplimiento de las funciones legalmente establecidas para las ER. Asimismo, se tendrá que asegurar la verificación presencial de la identidad del solicitante de un nuevo certificado digital.

Las Políticas de Registro y la Política de Seguridad deberán observar los lineamientos y procedimientos detallados en la "Guía de Acreditación para Entidades de Verificación/ Registro de Datos" [33].

La Política y el Plan de Privacidad deben cumplir con los parámetros establecidos en la Norma Marco sobre Privacidad APEC (Anexo 6 de la Guía de Acreditación)[34].

---

31 Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

32 Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

33 Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7)

34 La Política y el Plan de Privacidad deberán dar cumplimiento a la Ley de N° 29733 – Ley de Protección de Datos Personales, en sus términos vigentes.

(8) Declaración Jurada del cumplimiento de los requisitos señalados en los artículos 30 y 31 del Reglamento.

Esta declaración jurada no forma parte integrante de la Ficha de Solicitud de Acreditación como ER, por lo que la ER solicitante deberá elaborar la mencionada Declaración Jurada en documento independiente, el mismo que se deberá acompañar a la solicitud de acreditación.

En dicho documento se deberá dejar constancia que la ER cumple con sus obligaciones y responsabilidades, que son las siguientes:

a) Cumplir con los requerimientos de la AAC 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 AAC 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 AAC 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 AAC a que se refiere el artículo 31 del Reglamento.
g) Brindar todas las facilidades al personal autorizado por la AAC para efectos de supervisión y auditoría.

En cuanto a la responsabilidad por riesgo, para operar en el marco de IOFE y afrontar los riesgos que puedan surgir como resultado de sus actividades de registro o verificación, las ER 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 AAC establecerá la cuantía mínima de las pólizas de seguros o garantías bancarias. Asimismo, la AAC determinará los criterios para evaluar el cumplimiento de este requisito.

Nota:

Los Prestadores de Servicios de Certificación Digital están exonerados hasta el 31 de Diciembre de 2013[35] de la contratación de seguros o garantías bancarias; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

(9) Otros documentos o requisitos establecidos por la AAC.

Los siguientes son documentos solicitados por la AAC en la "Guía de Acreditación para Entidades de Verificación/ Registro de Datos"[36] para su presentación, según el caso, en el proceso de acreditación:

- Documentos que acrediten vinculación con un tercero que administre los servicios de almacenamiento de datos u otros

Documentos que deben servir para acreditar de manera suficiente la viabilidad de la prestación de los servicios de certificación digital bajo estas condiciones y la disponibilidad de estos elementos para la evaluación y supervisión que la Comisión considere necesaria.

En caso de existir tercerización de servicios de almacenamiento de datos u otros, con la especificación del nivel del servicio acordado, deberán acompañarse los contratos de tercerización respectivos.

- Documentos que acrediten vinculación con entidades de identificación:

A efectos de realizar una óptima prestación de sus servicios, la ER solicitante deberá contar con convenios o acuerdos de colaboración con las entidades encargadas de las bases de datos nacionales de identificación y Registro Civil y de Registros Públicos, para efectos de la verificación de la información proporcionada por los solicitantes.
El acceso a dichas bases de datos será restringido a los fines propios de la prestación de sus servicios y no podrá ser comercializado bajo ninguna modalidad. Debiendo respetar para estos efectos los principios a que se refiere la Norma Marco sobre Privacidad.
Para efectos del procedimiento de acreditación, bastará brindar una declaración jurada del cumplimiento de este requerimiento, la cual forma parte integrante de la Ficha de Solicitud de Acreditación como ER, por lo que bastará la suscripción de este documento para que se entiendan efectuadas las mencionadas Declaraciones Juradas. Sin perjuicio de ello, la ER solicitante podrá elaborar la mencionada Declaración Jurada en un documento independiente, el mismo que deberá acompañar a la solicitud de acreditación.

- Documentación que acredite la contratación de seguros o garantías bancarias para salvaguardar las actividades de certificación.

Para efectos de la presentación de la solicitud de acreditación bastará adjuntar Declaración Jurada en la cual se señale que en caso se obtenga la acreditación por parte del INDECOPI, se procederá a la contratación del seguro o garantía bancaria correspondiente[37].

---

35 Disposición Décimo Primera del Reglamento, modificada por D.S. N° 105-2012-PCM.

36 Reglamento Específico de Acreditación Entidad de Registro o Verificación – ER (Anexo 7 de la Guía de Acreditación para Entidades de Verificación/Registro de Datos)

37 Los Prestadores de Servicios de Certificación Digital están exonerados hasta el 31 de Diciembre de 2013[37] de la contratación de seguros o garantías bancarias; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

- Documentación que acredite contar con respaldo económico.

El anterior Reglamento, en su artículo 17° establecía que las ER deben acreditar contar con respaldo económico suficiente para operar bajo la IOFE. No obstante, bastará para acreditar este hecho la presentación de la declaración jurada correspondiente. Esta declaración jurada se encuentra incluida en la solicitud.

(10) Constancia de pago de los derechos administrativos.

Los derechos administrativos que deben cancelarse para efectos del procedimiento de acreditación como SVA ascienden al 100% del valor de la UIT.

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

La relación de documentos antes señalada no es taxativa. En tal sentido, la Comisión podrá considerar y solicitar cualquier documentación adicional que sea necesaria a efectos de poder tomar una decisión informada sobre la acreditación o no del solicitante.

3. ACREDITACION DE PRESTADORES DE SERVICIOS DE VALOR AÑADIDO (SVA)

Servicios de Valor Añadido son los servicios complementarios de la firma digital brindados dentro o fuera de la IOFE 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 IOFE es brindado por persona natural o jurídica acreditada ante la AAC.

3.1 Tipos de Procedimientos de Acreditación de SVA:

Pueden solicitarse los siguientes tipos de acreditación de una SVA:

A. Acreditación como SVA que realiza procedimientos sin firma digital de usuarios finales

Se solicita para los casos de servicios de valor añadido como Time Stamping, que no requieren en ninguna etapa de la prestación del servicio la firma digital del usuario final en documento o formulario alguno.

B. Acreditación como SVA que realiza procedimientos con firma digital de usuarios finales (Sistemas de Intermediación Electrónicos – SIE)

Se solicita para los casos de servicios de valor añadido como el Sistema de Intermediación Electrónico, en donde se requiere en determinada etapa del procedimiento la firma digital por parte del usuario final en algún tipo de documento o formulario.

Para la acreditación como SVA que realiza procedimientos con firma digital de usuarios finales, se requiere el empleo de un aplicativo (software) que se encuentre acreditado conforme a lo establecido en el Reglamento para la acreditación de una aplicación (SW) de clave pública (PKI).

C. Renovación de la acreditación

La renovación de la acreditación deberá cuando menos realizarse dentro de los 120 días anteriores al vencimiento de la acreditación conferida.

D. Acreditación por homologación

La homologación deberá solicitarse dentro de los 30 días posteriores a la realización de alguna de las auditorías anuales a las que será sometida la SVA acreditada.

Dependiendo del tipo de acreditación al que se postule, deberá también tomarse en cuenta los lineamientos y criterios particulares establecidos en la "Guía para la Acreditación de aplicaciones de software – Requerimientos para acreditar una aplicación (SW) de clave pública (PKI)" que explicamos más adelante.

Nota.-
La SVA que opere en modalidad que incluya, como parte del servicio de valor añadido, la conservación de algún tipo de mensaje de datos o documento electrónico, requerirá la ACREDITACIÓN ADICIONAL de la línea de producción de las microformas conforme al Decreto Legislativo No. 681, mediante el cual se establecen las normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto a la producida por procedimientos informáticos en computadoras, así como sus normas complementarias y reglamentarias. Al efecto téngase en consideración el Artículo 5° del Reglamento[38] que elimina mecanismos adicionales para la conservación de documentos firmados digitalmente

3.2 Solicitud de Acreditación como SVA. Documentos Sustentatorios

Para solicitar la acreditación de un Prestador de Servicios de Valor Añadido (SVA) deben cumplirse los requerimientos dispuestos por el Reglamento, la "Guía de Acreditación para Prestadoras de Servicios de Valor Añadido"[39] publicada por la AAC, y el TUPA vigente[40].

Se deberán presentar los siguientes documentos:

(1) Ficha de Solicitud de Acreditación

El formato de la solicitud debe presentarse en el formato de la AAC, que puede descargarse del link http://www.indecopi.gob.pe/RepositorioAPS/0/6/par/GUIAS3/anexo%209-sol.acreditacion%20como%20sva%20(nov2007).pdf

38 Artículo 5° del Reglamento, modificado por D.S. N° 105-2012-PCM (21 de Octubre 2012).

39 La Guía de acreditación vigente es la Versión 3.3 y cuenta con 12 Anexos. Se puede acceder a los documentos a través del portal web de INDECOPI http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=6&JER=454

40 TUPA aprobado por D.S. N° 085-2012-PCM publicado el 19 de Agosto de 2012, modificado por D.S. N° 110-2010-PCM de 16 de Diciembre de 2010 y R.M. N° 346-2011-PCM de 22 de Diciembre de 2011.

Deben cumplirse las siguientes especificaciones[41]:

- Estar dirigida al Secretario Técnico de la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias del INDECOPI.

- Indicar el tipo de procedimiento solicitado.

- Indicar el Tipo de Nivel de seguridad al que se postula y que será empleado en la prestación de servicios de certificación digital.

  Los niveles de seguridad pueden ser MEDIO y MEDIO ALTO. El primero para trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio; información crítica y de seguridad nacional en redes cifradas, acceso a información clasificada o de acceso especial en redes protegidas; y, aplicaciones de valor financiero medio o de comercio electrónico, tales como las planillas, contratos, compra de vehículos, etc. El segundo nivel para todas las aplicaciones para nivel medio; trámites con el Estado en las transacciones económicas de alto monto y alto riesgo, y el intercambio de documentos y transacciones monetarias de alto riesgo; información crítica no clasificada o de seguridad nacional en redes no cifradas; acceso a información clasificada o de acceso especial en redes no protegidas; y aplicaciones de valor financiero de riesgo y monto medio alto o de comercio electrónico.

  Según el nivel de seguridad y el tipo de transacciones objeto de los procesos de la ER, se debe tener en consideración lo siguiente:

  - Los dispositivos criptográficos físicos, hardware y firmware (sistema operativo), que almacenan las claves privadas de la entidad final (usuarios) deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.
  - La longitud de clave privada mínima debe ser de 1024 bits y el certificado debe ser renovado como máximo anualmente para el Nivel Medio y de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años para el Nivel Medio Alto.
  - Los certificados a nivel de entidad final (usuarios) deben ser generados de manera individual y separados para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.
  - Adicionalmente, para el caso de transacciones de nivel de seguridad medio alto, la SVA deberá contar con una certificación de acuerdo al Decreto Legislativo Nº 681[42] o de calidad ISO 9001:2000 para los procesos inherentes a su función o certificación de seguridad ISO 27001 para dichos procesos y la infraestructura tecnológica respectiva.

- La acreditación de una SVA implica la acreditación de sus agencias (sucursales), las cuales deben de cumplir con lo establecido en la VAPS y demás documentos relevantes de la SVA. Debe entregarse un documento donde se especifique la localización de las agencias, así como los nombres de los responsables de los procesos de registro en cada una de las mismas.

---

41 Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 7)

42 Decreto Legislativo N° 681 – Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto de la elaborada en forma convencional como la producida por procedimientos informáticos en computadoras, publicado el 14 de octubre de 1991.

- La solicitud deberá estar suscrita por el representante legal de la SVA solicitante y deberán incluirse sus datos de contacto.

(2) Copia simple del documento de identidad del solicitante[43].

En el caso que el solicitante sea un nacional deberá acompañar su Documento Nacional de Identidad con la correspondiente constancia de sufragio en las últimas elecciones. En el caso de solicitantes extranjeros, deberán acompañar su Carné de Extranjería o Pasaporte con el visado correspondiente.

(3) 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[44].

Respecto de la existencia y vigencia de la persona jurídica, deberá acreditarse con:

a. Documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente.
b. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por autoridad competente en su país de origen.
c. En el caso de las instituciones del Estado, deberán acreditar la existencia de una Oficina, Gerencia o dependencia interna a la cual se le otorgan funciones como prestador de servicios de una SVA.

Respecto a la acreditación de poderes de los representantes legales:

a. En el caso de personas jurídicas constituidas en el país: en el documento que acredite la representación, deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia del poder respectivo.
b. En el caso de personas jurídicas constituidas en el extranjero: los correspondientes poderes deberán ser legalizados por un funcionario consular peruano y de encontrarse redactados en idioma extranjero, será necesario que sean traducidos, debiendo el responsable de la traducción suscribir el correspondiente documento.
c. En el caso de instituciones del Estado, deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la certificación digital. Debiéndose asimismo acreditar las facultades de este funcionario.

(4) Documentos que acrediten contar con un domicilio en el país[45].

Para acreditar la condición de domiciliada de una SVA solicitante, debe presentarse el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), donde debe constar la condición de “habida”. Cualquier otra documentación será evaluada por la Comisión.

43 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

44 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

45 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

(5) 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 AAC[46].

La Guía no especifica los documentos que pueden utilizar el solicitante para acreditar que cuenta con la infraestructura e instalaciones necesarias para la prestación del servicio[47], requisito solicitado por el TUPA vigente

Para acreditar la aceptación de la visita comprobatoria de la AAC es suficiente presentar la Declaración Jurada, que forma parte integrante de la Ficha de Solicitud de Acreditación como SVA, por lo que bastará la suscripción de este documento para que se entienda efectuada. Sin perjuicio de ello, la SVA solicitante podrá elaborar las mencionadas Declaraciones Juradas en documentos independientes, los mismos que se deberán acompañar a la solicitud de acreditación.

(6) Memoria Descriptiva que contenga los procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.

La Memoria descriptiva y el Organigrama Estructural y Funcional deberán ser realizados conforme al Formato denominado: Memoria Descriptiva y Organigrama Estructural y Funcional de Prestador de Servicios de Valor Añadido (SVA), descritos en el Anexo 8 de la Guía de Acreditación [48].

(7) Las Políticas de Registro, la Declaración de Prácticas de Valor Añadido (VAPS), la Política de Seguridad, la Política y el Plan de Privacidad.

La "Guía de Acreditación para Prestadoras de Servicios de Valor Añadido" [49] define la Declaración de Prácticas de Valor Añadido, como el documento en donde constan de manera detallada las políticas y procedimientos que aplica el SVA para la prestación de sus servicios. Deberá estar elaborada en estricta observancia de los lineamientos establecidos en el documento Marco de la Política de Prestación de Servicios de Valor Añadido (Anexo 1) para el caso de los Sistemas de Intermediación Electrónicos; y por los lineamientos establecidos por el RFC 3628: *Policy Requirements for Time-Stamping Authorities* (TSAs), en concordancia con el estándar ISO/IEC 18014-1:2002 "*Information technology -- Security techniques -- Time-Stamping Services -- Parte 1: Framework*", para el caso de las Autoridades de Sellado de Tiempo.

En ambos casos, deben cumplir con la Norma Marco sobre Privacidad (Anexo 5) de la presente Guía de Acreditación[50].

---

46 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

47 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

48 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

49 Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

50 La Política y el Plan de Privacidad deberán dar cumplimiento a la Ley de N° 29733 – Ley de Protección de Datos Personales, en sus términos vigentes.

(8) 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 AAC.

Para acreditar la operatividad de los elementos para la prestación de servicios y las condiciones de seguridad es suficiente presentar la Declaración Jurada, que forma parte integrante de la Ficha de Solicitud de Acreditación como SVA, por lo que bastará la suscripción de este documento para que se entienda efectuada. Sin perjuicio de ello, la SVA solicitante podrá elaborar las mencionadas Declaraciones Juradas en documentos independientes, los mismos que se deberán acompañar a la solicitud de acreditación.

En el caso que cualquiera de los elementos señalados sean administrados por un tercero, el solicitante deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones y la disponibilidad de estos elementos para la evaluación y supervisión que la AAC considere necesarias.

Los documentos presentados (contrato, acuerdo, convenio de outsourcing u otro tipo de documentación permitida bajo el ordenamiento peruano) deben servir para acreditar de manera suficiente la viabilidad de la prestación de los servicios de valor añadido bajo estas condiciones y la disponibilidad de estos elementos para la evaluación y supervisión que la Comisión considere necesaria. En este caso, la Comisión tiene derecho a precisar los términos bajo los cuales se rigen este tipo de servicios de certificación digital.

(9) Declaración Jurada del cumplimiento de las obligaciones y los requisitos señalados en los artículos 37 y 38 del Reglamento.

Esta declaración jurada no forma parte integrante de la Ficha de Solicitud de Acreditación como SVA, por lo que la SVA solicitante deberá elaborar la mencionada Declaración Jurada en documento independiente, el mismo que deberá acompañar a la solicitud de acreditación.

En dicho documento se deberá dejar constancia que la SVA cumple con sus obligaciones que son las siguientes:

a) Cumplir con los requerimientos de la AAC 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 AAC 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 AAC.
e) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la AAC conforme a lo establecido en el Reglamento.
f) Cumplir con las disposiciones de la AAC a que se refiere el artículo 38 del Reglamento.

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

En cuanto a la responsabilidad por riesgo, para operar en el marco de IOFE y afrontar los riesgos que puedan surgir como resultado de sus actividades de valor añadido, las SVA 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
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 AAC.
- Sistema de Sellado de Tiempo: certificación internacional de calidad para la provisión de sus servicios, de acuerdo a lo establecido por la AAC.

La AAC 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 AAC determinará los criterios para evaluar el cumplimiento de este requisito.

Nota:
Los Prestadores de Servicios de Certificación Digital están exonerados hasta el 31 de Diciembre de 2013[51] de la contratación de seguros o garantías bancarias; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

(10) Otros documentos o requisitos establecidos por la AAC.

Los siguientes son documentos solicitados por la AAC en la "Guía de Acreditación para Prestadoras de Servicios de Valor Añadido" [52] para su presentación, según el caso, en el proceso de acreditación:

- Documento en el que conste el mapeo entre la VAPS y Marco de la Política de Prestación de Servicios de Valor Añadido (caso SIE):

Este documento será requerido para el caso de los SVA en la modalidad de Sistemas de Intermediación Electrónico (SIE) que no hubieran elaborado su VAPS de acuerdo al esquema establecido en el documento Marco de la Política de Prestación de Servicios de Valor Añadido. En este supuesto, el documento versará en un mapeo que deberá realizarse entre la VAPS del solicitante y el mencionado documento.
Este documento deberá tenerse presente para efecto de la realización de la evaluación técnica.

- Documento en el que conste la acreditación del software y autorización para su uso:

Este documento sólo deberá ser acompañado en el caso de SVA que realiza procedimientos con firma digital de usuarios finales. En cuyo supuesto se deberá acompañar el documento en el que

[51] Disposición Décimo Primera del Reglamento, modificada por D.S. N° 105-2012-PCM.

[52] Reglamento Específico de Acreditación Prestador de Servicios de Valor Añadido (Anexo 7)

conste la acreditación por parte de la Comisión del software empleado para el servicio de valor añadido que presta. En el caso que el software que empleara no fuera de desarrollo propio, deberán acompañar adicionalmente el documento en el que conste la autorización para su uso por parte del propietario del mismo (contrato de uso, convenio, etc).
Este documento deberá tenerse presente para efecto de la realización de la evaluación técnica.

- Contrato con la Entidad de Certificación emisora de los certificados digitales de autenticación empleados dentro del sistema del servicio brindado:

Este documento será requerido para el caso de los SVA en la modalidad de Sistemas de Intermediación Electrónico (SIE) que ofrezcan certificados digitales de autenticación, de uso exclusivo dentro del servicio de domicilios electrónicos brindado.
Este documento deberá tenerse presente para efecto de la realización de la evaluación técnica.

- Documentos que acrediten cumplimiento de requisitos de Decreto Legislativo No. 681, así como sus normas complementarias y reglamentarias

Documentos que acrediten que se cuenta con la acreditación de la línea de producción de las microformas, siempre que la entidad brinde adicionalmente el servicio de conservación o almacenamiento digital.

- Documentación que acredite la contratación de seguros o garantías bancarias para salvaguardar las actividades de certificación.

Para efectos de la presentación de la solicitud de acreditación bastará adjuntar Declaración Jurada en la cual se señale que en caso se obtenga la acreditación por parte del INDECOPI, se procederá a la contratación del seguro o garantía bancaria correspondiente[53].
Este requisito no será exigible para los SVAs públicos (SERVEPs), como parte de la Arquitectura Jerárquica de Certificación del Estado Peruano

- Documentación que acredite contar con respaldo económico.

Para tales efectos la SVA solicitante deberá presentar estados financieros (balance general, estado de ganancias y pérdidas y notas contables), con una antigüedad no mayor a dos meses del cierre contable del mes anterior a la presentación de la solicitud, acreditando solvencia económica.

Los estados financieros antes señalados deberán ser individuales (no consolidados) y encontrarse auditados. Si una empresa presentara estados financieros con pérdidas acumuladas de ejercicios anteriores, para acreditar solvencia económica deberá capitalizar dicha pérdida o realizar nuevos aportes en cuantía que compense el desmedro y mostrar el nuevo capital suscrito y pagado e inscrito en Registros Públicos.
Este requisito no será exigible para los SVAs públicos (SERVEPs).

(11) Constancia de pago de los derechos administrativos.

Los derechos administrativos que deben cancelarse para efectos del procedimiento de acreditación como SVA ascienden al 100% del valor de la UIT.

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

[53] Los Prestadores de Servicios de Certificación Digital están exonerados hasta el 31 de Diciembre de 2013[53] de la contratación de seguros o garantías bancarias; sin perjuicio de aquellos que opten voluntariamente por el cumplimiento de dichos requerimientos.

La relación de documentos antes señalada no es taxativa. En tal sentido, la Comisión podrá considerar y solicitar cualquier documentación adicional que sea necesaria a efectos de poder tomar una decisión informada sobre la acreditación o no del solicitante.

4. ACREDITACION DE APLICACIONES DE SOFTWARE

El objeto de esta acreditación es que la aplicaciones de software utilizadas para la prestación de servicios de certificación digital puedan interactuar con la infraestructura llamada "Infraestructura de Clave Pública" establecida por la IOFE, cuya AAC es el INDECOPI.

La tecnología de clave pública es aquélla que permite proveer la seguridad tecnológica, además, bajo el amparo de la IOFE, la seguridad jurídica, para desarrollar entornos digitales (*paperless*) que descansan sobre un marco legal que otorga seguridad a las transacciones electrónicas.

4.1 Solicitud de Acreditación Aplicaciones de Software. Documentos Sustentatorios

Para solicitar la acreditación de Aplicaciones de Software deben cumplirse los requerimientos dispuestos por el Reglamento, la "Guía de Acreditación de Aplicaciones de Software – Requerimientos para acreditar una aplicación (SW) de Clave Pública (PK)" [54] publicada por la AAC, y el TUPA vigente[55].

Se deberán presentar los siguientes documentos[56]:

(1) Ficha de Solicitud de Acreditación

El formato de la solicitud debe presentarse en el formato de la AAC, que puede descargarse del link http://www.indecopi.gob.pe/repositorioaps/0/6/jer/legis_firmasdigitales/software.pdf

Deben cumplirse las siguientes especificaciones:

- Estar dirigida al Secretario Técnico de la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias del INDECOPI.
- Indicar el objeto de la solicitud.
- La solicitud deberá estar suscrita por el representante legal de la solicitante y deberán incluirse sus datos de contacto.

[54] La Guía de acreditación vigente es la Versión 3.4. que cuenta con 4 Anexos. Se puede acceder a los documentos a través del portal web de INDECOPI http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=6&JER=423

[55] TUPA aprobado por D.S. N° 085-2012-PCM publicado el 19 de Agosto de 2012, modificado por D.S. N° 110-2010-PCM de 16 de Diciembre de 2010 y R.M. N° 346-2011-PCM de 22 de Diciembre de 2011.

[56] Los requisitos para solicitar acreditación de aplicación de software se encuentran precisados en el portal de INDECOPI. Se puede acceder a través del link http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=6&JER=1311

(2) Copia simple del documento de identidad del solicitante.

En el caso que el solicitante sea un nacional deberá acompañar su Documento Nacional de Identidad con la correspondiente constancia de sufragio en las últimas elecciones. En el caso de solicitantes extranjeros, deberán acompañar su Carné de Extranjería o Pasaporte con el visado correspondiente.

(3) 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.

Respecto de la existencia y vigencia de la persona jurídica, deberá acreditarse con:

a. Documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente.
b. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por autoridad competente en su país de origen.
c. En el caso de las instituciones del Estado, deberán acreditar la existencia de una Oficina, Gerencia o dependencia interna a la cual se le otorgan funciones como prestador de servicios de certificación digital.

Respecto a la acreditación de poderes de los representantes legales se deberá acreditar contar con facultades suficientes para solicitar la acreditación o autorización solicitada. Adicionalmente, se deberá tener en cuenta lo siguiente:

a. En el caso de personas jurídicas constituidas en el país: en el documento que acredite la representación, deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia del poder respectivo.
d. En el caso de personas jurídicas constituidas en el extranjero: los correspondientes poderes deberán ser legalizados por un funcionario consular peruano y de encontrarse redactados en idioma extranjero, será necesario que sean traducidos, debiendo el responsable de la traducción suscribir el correspondiente documento.
e. En el caso de instituciones del Estado, deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la certificación digital. Debiéndose asimismo acreditar las facultades de este funcionario.

(4) Documentos que acrediten contar con un domicilio en el país.

Para acreditar la condición de domiciliada de una EC solicitante, debe presentarse el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), donde debe constar la condición de “habida”. Cualquier otra documentación será evaluada por la Comisión.

(5) Documento en el que consten los derechos de propiedad sobre el programa y/o la autorización para su uso.

Se deberá acompañar el documento en el que conste la titularidad del solicitante sobre el software. En el caso que el software que empleara no fuera de desarrollo propio, deberá acompañarse el

documento en el que conste la autorización para su uso por parte del propietario del mismo (contrato de uso, convenio, etc).

(6) Medio óptico/magnético que contenga el programa.

La aplicación de software debe cumplir todos los requerimientos que se mencionan en la Guía.

Los requerimientos generales incluyen:

a. Automatización preferente de los Procedimientos
b. Uso de Módulos Criptográficos Evaluados
c. Ámbito Computacional seguro

Los requerimientos específicos se agrupan en cuatro grandes familias:

a. Manejo de claves que incluye las funciones de generar y almacenar el par de claves; así como almacenar y guardar los puntos de confianza. La seguridad de las claves privadas y los puntos de confianza es crítica.
b. Interfaz PKI que incluye funciones para el uso de los servicios de la PKI.
c. Servicios de cifrado que incluyen las funciones para cifrar y descifrar información usando tanto los algoritmos de cifrado simétricos como asimétricos y para calcular el mensaje resumen (hash o digest). Estos servicios también incluyen la generación de claves simétricas y números aleatorios (random).
d. Procesamiento de verificación necesarios antes y después de realizar el proceso de firma, cifrado y autenticación, que comprenda funciones para verificar la TSL[57], así como para obtener cadenas de certificación que incluyan la verificación de la validez de los certificados de la cadena.

Las aplicaciones deben estar firmadas empleando un certificado de firma de código a fin de garantizar lo siguiente:

- La autenticidad de la aplicación. Es decir, se puede comprobar la identidad de la organización que distribuye el código inspeccionando el nombre del titular del certificado con el que se firma.
- La integridad del código, para estar seguros de que es lícito y no ha sido modificado de forma no autorizada después de haber sido aprobado por el autor.

Las aplicaciones deben identificar todas las condiciones y dependencias necesarias para que la aplicación realice sus funciones de manera segura.

Las aplicaciones deben ser configurables para operar con la IOFE y deben operar automáticamente con ella, requiriendo la mínima configuración posible.

Las aplicaciones deben incluir sus correspondientes documentos, manuales e instrucciones. Los documentos deben contener procedimientos y responsabilidades como usuarios.

[57] **TSL** (Lista de Estado de Servicio de Confianza, por sus siglas en inglés)**:** lista de confianza que incluye a los PSCs acreditados, autorizados a operar en el marco de la IOFE. El propósito de la TSL es proveer de modo ordenado información del estado de los proveedores de servicios, teniendo un rol preponderante en los servicios considerados confiables (acreditados) y los proveedores supervisados por la AAC.

La aplicación de software (SW) deberá contar con certificación de calidad ISO 9001:2000 para los procesos de diseño y desarrollo de software o certificación de calidad CMMI (nivel 2 mínimo para nivel Medio Alto, nivel 3 mínimo para nivel Alto), relativo a transacciones seguras de comercio y gobierno electrónico (considerando para su desarrollo, la Guía para la Acreditación de aplicaciones de software).

(7) Formatos correspondientes al Anexo A de la Guía de Aplicación de Software, en lo que sea aplicable.

Remitirse a la Guía de Aplicación, Formatos de Anexo A, en caso de ser pertinente.

(8) Constancia de pago de los derechos administrativos.

Los derechos administrativos que deben cancelarse para efectos del procedimiento de acreditación como Aplicación de SW ascienden al 100% del valor de la UIT.

(9) Otros documentos o requisitos establecidos por la AAC

Los siguientes son documentos solicitados por la AAC[58] para su presentación, según el caso, en el proceso de acreditación:

- Declaración Jurada de la aceptación de auditorías.

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

La relación de documentos antes señalada no es taxativa. En tal sentido, la Comisión podrá considerar y solicitar cualquier documentación adicional que sea necesaria a efectos de poder tomar una decisión informada sobre la acreditación o no del solicitante.

III. PROCEDIMIENTOS DE ACREDITACION

Dependiendo del objeto de la acreditación se deben cumplir las siguientes fases o etapas.

1. PROCEDIMIENTO DE ACREDITACION DE PRESTADORES DE SERVICIOS DE CERTIFICACION DIGITAL (PSC). FASES. ETAPAS

El procedimiento de Acreditación de Prestadores de Servicios de Certificación Digital consta de tres fases, cada una integrada por diferentes etapas, las que comentamos a continuación.

[58] Artículo 18-A del Reglamento General de Acreditación para Prestadores de Servicios de Certificación Digital.

FASE I: Inicio

I. Recepción, revisión y admisión de la solicitud

Presentación de la documentación requerida por la PSC a efectos de obtener la correspondiente acreditación.

Recibida la solicitud, la Comisión revisará la documentación con el objeto de comprobar que la información acompañada esté completa y corresponda con la requerida para efectos de la acreditación solicitada. La Comisión evaluará en función a su capacidad la oportunidad de atender la solicitud presentada dentro de los plazos establecidos. Si la documentación no estuviera completa o la información no estuviera claramente definida, se pondrá este hecho en conocimiento del solicitante, el mismo que contará con un plazo de cinco (5) días hábiles para la subsanación de estas omisiones.

Si no se levantan las observaciones formuladas dentro del plazo establecido, se declarará la inadmisibilidad de la solicitud y la conclusión del procedimiento.

Si no existieran observaciones o se cumple con subsanar las observaciones formuladas dentro del plazo establecido, la Comisión declarará la admisibilidad de la solicitud y se procederá a la etapa siguiente del procedimiento de acreditación. De ser el caso, y siempre que la Comisión lo estime necesario para efectos del procedimiento de acreditación, en esta misma resolución se procederá a la designación del Comité Evaluador encargado de prestar apoyo en la etapa de evaluación técnica.

II. Designación del Comité Evaluador

Designado el Comité Evaluador, el PSC solicitante podrá presentar en un plazo de dos (2) días hábiles de recibida la notificación de admisibilidad, las observaciones sobre la participación de los miembros del Comité Evaluador. La Comisión tiene un plazo de cinco (5) días hábiles para pronunciarse sobre la observación formulada y de ser el caso proceder a la designación de un miembro reemplazante. Vencido el plazo sin formulación de observaciones, se entenderá aceptado el Comité Evaluador designado.

III. Evaluación documentaria

Aceptado el Comité Evaluador, la Comisión tendrá un plazo de diez (10) días hábiles para analizar detalladamente la documentación presentada y pronunciarse respecto a su procedencia legal. En esta etapa del procedimiento no se realizará ningún tipo de evaluación respecto a la documentación de índole tecnológico. En caso se identifique alguna omisión o se efectúe algún tipo de observación a la documentación presentada, la Comisión notificará este hecho al PSC solicitante, otorgando un plazo máximo de diez (10) días hábiles para su subsanación.

Si no se levantan las observaciones formuladas dentro del plazo establecido, se declarará la improcedencia de la solicitud y la conclusión del procedimiento.

Si no existieran observaciones o se cumple con subsanar las observaciones formuladas dentro del plazo establecido, la Comisión declarará la conformidad de la documentación presentada y se procederá a la etapa siguiente del procedimiento de acreditación.

En el caso de la acreditación como EC o SVA, en esta misma resolución se citará al representante técnico designado del PSC solicitante a efectos de realizar las coordinaciones necesarias para la etapa de evaluación técnica

En todos los supuestos antes señalados, la Comisión deberá fundamentar claramente su decisión.

La resolución en esta etapa no importa pronunciamiento sobre la idoneidad de la documentación técnica ni pruebas tecnológicas que deberán efectuarse en la evaluación técnica como parte del procedimiento administrativo de acreditación.

En cualquiera de las modalidades de PSC, de no encontrarse conforme con la decisión emitida, el solicitante tiene un plazo de quince (15) días útiles, para efectos de interponer los recursos impugnatorios que considere pertinentes. Con la resolución que se emita en esta segunda instancia, quedará agotada la vía administrativa.[59]

FASE II: Evaluación Técnica

IV. Evaluación Técnica

La etapa de evaluación técnica tiene por objetivo verificar el cumplimiento de los criterios de acreditación y evaluar la idoneidad del PSC para prestar los servicios cuya acreditación solicita. Esta evaluación será llevada a cabo con la asesoría correspondiente por parte del Comité Evaluador designado por la Comisión, en las instalaciones del PSC solicitante.

La evaluación técnica será llevada a cabo en estricta observancia de los procedimientos establecidos para tales efectos por la Comisión. Durante el procedimiento de evaluación, el Comité Evaluador designado para tales efectos dará cuenta de los hallazgos y eventuales no conformidades u observaciones encontradas en los procedimientos establecidos por el PSC en el desarrollo de sus actividades. El registro de no conformidades u observaciones detectadas, deberá contar con la firma y nombre del representante que fuera designado para tales efectos por el PSC solicitante.

Dentro del procedimiento de acreditación como EC, la evaluación técnica se divide en dos etapas: a. Evaluación de las CP, CPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad b. Evaluación de interoperabilidad

Dentro del procedimiento de acreditación como ER, la evaluación comprende el examen de la RPS, la Política y el Plan de Privacidad, y la Política de Seguridad de la ER, y establecer su equivalencia con los Lineamientos para Infraestructura de clave pública (PKI) del APEC. La ER deberá: a. Designar a un Responsable de Privacidad, quien será el primer contacto frente a incidentes de privacidad; b. Publicar en su página WEB la Política de Privacidad y el Plan de Privacidad y los datos de contacto del Responsable de Privacidad; c. Implementar el Plan de Privacidad de acuerdo a lo estipulado en el mismo documento,

[59] Este recurso impugnativo está especificado en la "Guía de Acreditación de Entidades de Certificación EC" dentro de la FASE II del Proceso de Acreditación; sin embargo no se encuentra contemplado en el TUPA vigente.

sujeto a las existentes obligaciones contractuales, licencias u otros arreglos de outsourcing;
d. Revisar y actualizar la Política de Privacidad y el Plan de Privacidad al menos una vez por año;
e. Elaborar y publicar en su página WEB una declaración de privacidad y seguridad.

Nota: si la ER cumple funciones de EC, el rol de Responsable de Privacidad podrá ser asumido por el Oficial de Privacidad designado.

El Comité Evaluador designado examinará la adecuación de la Declaración de Prácticas de Registro o Verificación de la solicitante con el documento Marco de la Política de Registro para la emisión de certificados digitales.

Dentro del procedimiento de acreditación como SVA, la evaluación técnica se divide en dos etapas:

a. Evaluación de la VAPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad.
El procedimiento se realizará sobre la base de los documentos acompañados para tales efectos por el SVA solicitante. De considerarlo necesario, el Comité podrá solicitar documentación complementaria o la realización de una evaluación o auditoría en las instalaciones del SVA.

b. Evaluación de interoperabilidad
Para el procedimiento, se tomará contacto con el personal designado para tales efectos por el SVA solicitante, a fin de realizar las pruebas correspondientes. La TSL de prueba que se genere durante esta etapa deberá ser alojada en la infraestructura tecnológica del SVA solicitante a efectos de realizar las pruebas correspondientes.

V. Informe de Evaluación

Culminada la etapa de evaluación técnica, el Comité Evaluador deberá elaborar un Informe de Evaluación con los resultados e información recopilada durante la evaluación. Como mínimo la información que debe contener el informe es la que se detalla a continuación:

a. Grado de cumplimiento de los requisitos técnicos requeridos para la acreditación.
b. Reporte de las no conformidades u observaciones detectadas durante la evaluación.
c. Otra información que el Comité Evaluador considere importante consignar.

En todos los supuestos antes señalados el Comité Evaluador deberá fundamentar claramente su informe.

De considerarlo pertinente, en el caso de acreditación de ER, el Comité podrá determinar dentro del plazo de evaluación técnica, la necesidad de realizar una visita comprobatoria a la ER. Este hecho debidamente fundamentado, se pondrá en conocimiento de la ER solicitante y correrá por cuenta de la misma los gastos que puedan generarse por esta evaluación.

Este informe no prejuzgará la decisión de la Comisión y deberá ser remitido al PSC solicitante una vez completado el procedimiento de acreditación.

VI. Procedimiento en caso de presentarse no conformidades u observaciones

En caso de presentarse no conformidades, el PSC solicitante tiene un plazo de cinco (5) días de culminada la evaluación técnica para presentar a la Comisión las propuestas de acciones correctivas que considere pertinentes y los plazos para su ejecución, los cuales no pueden ser superiores a un (1) mes.

La verificación del levantamiento de no conformidades se realizará mediante una evaluación complementaria.

VII. Facultad para solicitar la suspensión del procedimiento

En caso lo considere necesario, el PSC solicitante podrá solicitar la suspensión del procedimiento administrativo a efectos de poder implementar las medidas técnicas necesarias para superar las observaciones formuladas.

El plazo de subsanación de deficiencias técnicas observadas no puede ser mayor a seis (6) meses. Si, culminada la etapa de evaluación, subsisten observaciones, se denegará el Registro y se archivará el procedimiento.

VIII. Evaluación Complementaria

La evaluación complementaria se realizará únicamente respecto a las no conformidades detectadas y que fueron materia de pronunciamiento en su oportunidad por el Comité Evaluador.

Los resultados de esta evaluación deberán ser consignados por el Comité Evaluador en un Acta que formará parte del Informe final que emita.

FASE III: Decisión

IX. Decisión sobre la acreditación

La decisión respecto de la acreditación de un PSC compete en primera instancia, única y exclusivamente, a la Comisión. Esta decisión será tomada sobre la base de las evaluaciones legal y técnica efectuadas. Para lo cual se revisará el expediente del PSC solicitante y se tomará en cuenta el Informe Final del Comité Evaluador.

Sobre la base del análisis de la documentación antes detallada, la Comisión podrá pronunciarse en cualquiera de los sentidos siguientes:

a. Otorgar la acreditación al PSC solicitante, que ingresa de este modo a la IOFE. En este supuesto, se inscribirá al solicitante en el **Registro de Prestadores de Servicios de Certificación Digital,** que es de carácter público y se incorporará a la TSL[60] correspondiente.
b. Denegar la acreditación.
c. Otorgar la acreditación emitiendo determinadas recomendaciones y estableciendo el plazo dentro del cual las mismas deberán ser subsanadas por el PSC solicitante.

[60] **TSL** (Lista de Estado de Servicio de Confianza, por sus siglas en inglés)**:** lista de confianza que incluye a los PSCs acreditados, autorizados a operar en el marco de la IOFE. El propósito de la TSL es proveer de modo ordenado información del estado de los proveedores de servicios, teniendo un rol preponderante en los servicios considerados confiables (acreditados) y los proveedores supervisados por la AAC.

En todos los supuestos antes señalados la Comisión deberá fundamentar claramente su decisión.

El plazo máximo del procedimiento de acreditación es de ciento veinte (120) días hábiles, contados a partir de la recepción de la solicitud por la AAC.

Tanto la evaluación documentaria como la técnica se efectúan por una sola vez dentro del procedimiento de acreditación. En tal sentido, una vez concluida la etapa de evaluación documentaria no es admisible la incorporación de cambios en la documentación que se refieran al alcance de acreditación solicitada.

X. Impugnación de la Resolución

El PSC que no estuviere de acuerdo con la decisión de la Comisión podrá presentar dentro de los CINCO días (05) de emitida la misma y por escrito, el correspondiente Recurso de apelación[61], el mismo que será resuelto en segunda instancia por la Sala de Defensa de la Competencia del Tribunal del INDECOPI, en el plazo de 120 días hábiles.

XI. Registro de PSC acreditados

La Comisión registrará a los solicitantes que obtuvieran la correspondiente acreditación, en el Registro de Prestadores de Servicios de Certificación digital acreditados, indicando para tales efectos los alcances de su acreditación. Este Registro es de carácter público y estará disponible para quien lo solicite.
Adicionalmente, la acreditación de una EC implicará la inclusión de la misma en la Lista de Estado de Servicio de Confianza (TSL[62]) que mantendrá para tales efectos la Comisión en su condición de AAC.

2. VIGENCIA DE LA ACREDITACIÓN

La acreditación como PSC se otorga por un periodo de cinco (5) años[63], contados a partir de la fecha de la resolución correspondiente. Esta acreditación puede ser renovada por periodos similares, previo sometimiento al procedimiento de renovación establecido para tales efectos por la AAC. Durante la vigencia de la acreditación, el PSC solicitante se encuentra obligado al cumplimiento permanente de los criterios de acreditación y será sometido a auditorías anuales por parte de la Comisión.

---

61 Plazo establecido por el TUPA vigente. Por su parte, la "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" y la "Guía de Acreditación para Entidades de Verificación/ Registro de Datos" establecen 15 días para la interposición de recursos de reconsideración y apelación, que se rigen por lo establecido por la Ley del Procedimiento Administrativo General – Ley N° 27444.

62 **TSL** (Lista de Estado de Servicio de Confianza, por sus siglas en inglés)**:** lista de confianza que incluye a los PSCs acreditados, autorizados a operar en el marco de la IOFE. El propósito de la TSL es proveer de modo ordenado información del estado de los proveedores de servicios, teniendo un rol preponderante en los servicios considerados confiables (acreditados) y los proveedores supervisados por la AAC.

63 Artículo 69° del Reglamento vigente.

APORTE POR SUPERVISION Y CONTROL ANUAL

A partir de la fecha de la correspondiente resolución, el PSC acreditado se encuentra obligado al pago del aporte por supervisión y control anual a que se refiere el artículo 57° del Reglamento del año 2007. El Reglamento vigente no contiene disposición equivalente.

3. MANTENIMIENTO DE LA ACREDITACION

La "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" [64], "Guía de Acreditación para Entidades de Verificación/ Registro de Datos" [65] señalan que los PSC acreditados para mantener su acreditación, serán sometidos a evaluaciones posteriores a la acreditación, tales como visitas de supervisión, auditorías anuales y renovación de la acreditación.

3.1. Visitas de Supervisión:

Proceden cuando se presenten situaciones que lo ameriten o en alguno de los supuestos siguientes:

a. Cambios estructurales u organizacionales de PSC acreditados.
b. Cambios en los procedimientos de los PSC acreditados.
c. Cambios en las Políticas o Prácticas empleadas en la prestación de sus servicios por parte de los PSC acreditados.
d. Cuando haya un uso indebido o fuera del alcance de la acreditación obtenida.
e. Cuando el análisis de un reclamo o cualquier otra información ponga en duda el cumplimiento de las condiciones de acreditación.

Las visitas de supervisión se realizarán sin previo aviso al PSC acreditado, salvo que la Comisión disponga lo contrario en función a la finalidad de la visita de supervisión. Los resultados de la visita serán informados al PSC acreditado

3.2. Auditorias Anuales

Estas auditorías anuales buscan asegurar que el PSC, en el periodo transcurrido, contado desde la fecha de la resolución de acreditación, ha respetado las condiciones establecidas para el otorgamiento de la acreditación y que asimismo cumple con los criterios de acreditación y competencia técnicas correspondientes para la prestación de sus servicios en condiciones habituales.

Los resultados de estas auditorías anuales serán informados al PSC acreditado.

En el caso específico de las ER acreditadas serán sometidas a una auditoría pasados los tres (3) primeros meses de obtenida la acreditación, a efectos de verificar la implementación de sus Prácticas de Registro o Verificación y su Política de Seguridad.

3.3. Procedimiento en Caso de No Conformidades u Observaciones [66]:

Si como resultado de una vista de supervisión u auditoría anual de seguimiento se presentan no conformidades o se establece algún tipo de observación, el PSC acreditado deberá presentar sus

64 Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 7)

65 Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 5)

66 Este recurso impugnativo está especificado en las Guía de Acreditación citadas; sin embargo no se encuentra contemplado en el TUPA vigente.

propuestas de acción dentro de un plazo de diez (10) días de culminada la correspondiente evaluación por parte de la Comisión. Estas propuestas serán evaluadas y se notificará su aprobación en el plazo de cinco (5) días. En caso contrario, se comunicará su desaprobación y se otorgará por única vez un plazo de cinco (5) días adicionales para remitir nuevas propuestas de acción correctiva.

Las no conformidades u observaciones deberán ser levantadas en un plazo de treinta (30) días contados desde la notificación de aprobación de las propuestas de acción correctivas. Para verificar el levantamiento de las no conformidades u observaciones se realizará una evaluación complementaria similar al proceso de acreditación.

Para verificar el levantamiento de las no conformidades u observaciones se realizará una evaluación complementaria, con los alcances de las Evaluaciones Complementarias que se realizan dentro del proceso de acreditación de PSC.

3.4. Decisión para el Mantenimiento de la Acreditación

Tomando en consideración los resultados de la información recogida en el expediente de acreditación, los informes de las visitas de supervisión, los informes de la auditoría anual, las propuestas de acciones correctivas y la subsanación de no conformidades u observaciones, la Comisión decidirá sobre el mantenimiento de la acreditación mediante resolución debidamente motivada.
En caso que la Comisión determine la revocación de la acreditación otorgada, esta resolución deberá encontrarse debidamente motivada e implicará el retiro de la acreditación y del PSC de la TSL, siempre y cuando dicha resolución quede consentida.

4. RENOVACION DE ACREDITACION

La "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" [67], "Guía de Acreditación para Entidades de Verificación/ Registro de Datos" [68] establecen que transcurrido el periodo de vigencia de la acreditación[69], la Comisión evaluará la competencia técnica del PSC y demás aspectos que pudiesen haberse puesto de manifiesto durante la vigencia de la acreditación.

4.1. Procedimiento de Renovación

Esta evaluación se realizará mediante un procedimiento similar al aplicado para la evaluación inicial de acreditación.
La renovación de la acreditación deberá solicitarse ciento veinte (120) días anteriores al vencimiento de la vigencia de la acreditación, a fin de evitar intervalos en la continuidad de la misma.
La Comisión podrá admitir las solicitudes de renovación extemporáneas siempre y cuando la acreditación se encuentre vigente, debiendo informar claramente a los solicitantes que la continuidad de la acreditación podría verse afectada por el incumplimiento de la presentación de la solicitud dentro del plazo previsto.

---

67 Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 7)

68 Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 5 de la Guía de Acreditación para Entidades de Verificación/Registro de Datos)

69 Cinco (5) años de acuerdo al Artículo 69° del Reglamento vigente.

Si el PSC no presenta la solicitud de renovación dentro del plazo previsto o efectúa este pedido de manera extemporánea, se considera que el organismo acreditado ha renunciado a someterse al procedimiento de renovación de acreditación y por ende, cualquier pedido posterior será considerado como un nuevo procedimiento de acreditación y será sometido a las reglas establecidas para tal caso.

El procedimiento de renovación de la acreditación es el mismo que el establecido para la obtención inicial de acreditación, excepto en lo que respecta a la evaluación documentaria, la misma que no será necesaria, salvo que se haya producido un cambio en los criterios de acreditación bajo los cuales originalmente fue acreditado el PSC.

4.2. Procedimiento en caso de No Conformidades u Observaciones[70]

Las no conformidades u observaciones halladas durante la evaluación de la renovación pueden constituir supuestos de revocación de la acreditación que requieran una investigación. En tales casos y dependiendo de la naturaleza y gravedad de los hechos investigados, la Comisión podrá suspender el procedimiento de renovación hasta que culmine el eventual procedimiento administrativo sancionador que se hubiera iniciado, pues del resultado del mismo dependerá la continuidad de la condición del PSC como entidad acreditada.

4.3. Modificación de Acreditación

Dentro del procedimiento de renovación podrá solicitarse la modificación de los alcances de la acreditación, siempre y cuando ésta importe una reducción de la acreditación conferida. En tal sentido, como parte del procedimiento de renovación, no cabe solicitar la ampliación para la prestación de otro tipo de servicios de certificación digital, los mismos que requerirán ser sometidos a un procedimiento de acreditación independiente dependiendo del tipo de servicio del que se trate.

5. HOMOLOGACION DE ACREDITACION

La "Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas" [71,] "Guía de Acreditación para Entidades de Verificación/ Registro de Datos" [72] señalan que solo se aplica a las Entidades de Certificación (EC) y Prestadores de Servicios de Valor Añadido (SVA)

La solicitud procede cuando la PSC solicitante subcontrata la totalidad de la infraestructura tecnológica (incluyendo todos los procesos del sistema de gestión) utilizada también por un PSC acreditado, para lo cual deberá sustentar este hecho, pudiendo emplear la documentación de la Política de Seguridad presentada por el PSC acreditado En el caso de una EC, si se incorporaran modificaciones a la documentación referida, se deberán sustentar mediante las auditorías correspondientes.

5.1. Procedimiento de Homologación

[70] Este recurso impugnativo está especificado en la Guía de Acreditación citada; sin embargo no se encuentra contemplado en el TUPA vigente.

[71] Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 7)

[72] Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital (Anexo 5 de la Guía de Acreditación para Entidades de Verificación/Registro de Datos)

Deberá solicitarse dentro de los treinta (30) días posteriores a la realización de alguna de las auditorías anuales a las que será sometido el PSC acreditado, de conformidad con lo especificado en el Acápite anterior.

La Comisión no admitirá solicitudes de homologación extemporáneas

El procedimiento de acreditación por homologación es el mismo que el establecido para la obtención inicial de acreditación, excepto en lo que respecta a la evaluación técnica, realizada durante la última auditoría anual, correspondiente a la infraestructura tecnológica (y procesos de gestión) a utilizar.

El proceso de acreditación será completado mediante la realización de una evaluación documentaria complementaria, la cual incluye la Política de Seguridad actualizada.

Una evaluación completa será necesaria sólo si se hubiera producido un cambio en los criterios de acreditación bajo los cuales originalmente fue otorgada la acreditación a ser homologada.

5.2. Procedimiento en caso de No Conformidades u Observaciones[73]

Las no conformidades u observaciones halladas durante la evaluación de la homologación pueden constituir supuestos de revocación de la acreditación a ser homologada, y puede requerirse una investigación. En tales casos y dependiendo de la naturaleza y gravedad de los hechos investigados, la Comisión podrá suspender el procedimiento de acreditación hasta que culmine el eventual procedimiento administrativo sancionador que se hubiera iniciado, pues del resultado del mismo dependerá la continuidad de la condición del PSC afectado como entidad acreditada

5.3. Modificación de Acreditación

Dentro del procedimiento de homologación podrá solicitarse la modificación de los alcances de la acreditación, siempre y cuando ésta importe una reducción de la acreditación conferida. En tal sentido, como parte del procedimiento de homologación, no cabe solicitar la ampliación para la prestación de otro tipo de servicios de certificación digital, los mismos que requerirán ser sometidos a un procedimiento de acreditación independiente dependiendo del tipo de servicio del que se trate.

6. PROCEDIMIENTO DE ACREDITACION DE APLICACIÓN DE SOFTWARE

El procedimiento de Acreditación de Aplicación de Software consta de las siguientes etapas.

Etapa I: Inicio

I. Admisión o no admisión de la solicitud y designación del Comité Evaluador

II. Evaluación Legal, por parte de la Secretaria Tecnica de la Comisión, de los documentos presentados.

Etapa II: Evaluación Técnica

[73] Este recurso impugnativo está especificado en las Guías de Acreditación citadas; sin embargo no se encuentra contemplado en el TUPA vigente.

III. Verificación, por parte del Comité, del cumplimiento de las condiciones técnicas de inter-operabilidad.

IV. Verificación, por parte del Comité, del cumplimiento de las condiciones técnicas de seguridad.

En ambos casos, la subsanación idónea de las no conformidades se apreciará mediante una evaluación complementaria.

Etapa III: Decisión

V. Decisión de la Comisión sobre la acreditación de la aplicación de SW del solicitante.

Los plazos de duración de cada etapa y los recursos impugnativos son los mismos que en el procedimiento para la acreditación de PSC, con las siguientes modificaciones[74]:

Etapa del Proceso	Actividad	Plazo
Fase I, Inicio, Evaluación Preliminar	Subsanación, por parte del solicitante, de las observaciones formales a la documentación presentada	02 días hábiles
Fase I, Inicio, Evaluación Preliminar	Presentación de observaciones del solicitante a la conformación del Comité Evaluador	02 días hábiles
Fase I, Inicio, Evaluación Preliminar	Respuesta de la CNB a las observaciones del solicitante sobre la conformación del Comité Evaluador	03 días hábiles
Evaluación Legal	Análisis Legal por parte de la CNB de la documentación presentada por el solicitante	03 días hábiles
Evaluación Legal	Subsanación de las observaciones legales de la CNB, a cargo del recurrente	03 días hábiles
Evaluación de Interoperabilidad	Evaluación de los resultados por parte del Comité Evaluador	07 días hábiles
Evaluación Complementaria	Presentación de las propuestas de acciones correctivas por parte del solicitante	03 días hábiles
Evaluación Complementaria	Ejecución de las acciones correctivas por parte del solicitante	07 días hábiles
Evaluación Complementaria	Evaluación de los resultados por parte del Comité Evaluador	05 días hábiles
Fase III de Decisión	Resolución de acreditación o denegatoria de acreditación	07 días hábiles
Fase III de Decisión	Interposición de los recursos impugnatorios por parte del solicitante	15 días hábiles

Una vez obtenida la correspondiente acreditación, el solicitante se encuentra obligado a prestar sus servicios en los mismos términos que sometió a evaluación durante el procedimiento.

El mantenimiento, renovación y homologación de la acreditación se rigen por lo establecido en el Reglamento General.

[74] Plazos incorporados por Resolución N° 016-2011/CNB-INDECOPI de 01 de Junio de 2011.

IRIARTE & ASOCIADOS
Jr. Miró Quesada 191 - Of. 510. Lima 01 – Perú.
Telefax (+511) 427 0383
http://www.iriartelaw.com
contacto@iriartelaw.com

©2013 Iriarte & Asociados.