ANEXO 9

FICHA DE SOLICITUD DE ACREDITACIÓN COMO ENTIDAD DE REGISTRO O VERIFICACIÓN (ER)

PARA SER LLENADO POR CFE
Ficha de Solicitud Nº
Expediente Nº
Fecha de Ingreso al INDECOPI

Ficha de Solicitud de Acreditación como Entidad de Registro o Verificación (ER)

Antes de llenar esta solicitud consulte los documentos que establecen los criterios de acreditación generales, específicos y complementarios (legislación y guías de acreditación) que correspondan a la modalidad de ER que desea acreditar.

Mayores precisiones se pueden encontrar en la Cartilla de Instrucciones que se encuentra en la parte final del presente documento.

SEÑOR SECRETARIO TÉCNICO DE LA COMISIÓN TRANSITORIA PARA LA GESTIÓN DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA (CFE) DEL INDECOPI:

Yo, _____
(Nombres y Apellidos)

Identificado con _____en representación legal de la
(DNI, Pasaporte, C. de extranjería u otro)

Empresa/Entidad Pública _____
(Nombre de la empresa/entidad pública)

Con Domicilio sito en _____

Y Domicilio Procesal en _____

Correo Electrónico _____

Teléfono (s) (Fijo/Móvil) _____

Solicito a la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica del INDECOPI el siguiente procedimiento:

I. TIPO DE PROCEDIMIENTO (Marcar donde corresponda)

1. Acreditación como ER – Persona jurídica (incluye a las EREP)	☐	3. Renovación de la acreditación	☐
2. Acreditación como ER – Persona natural (notarios)	☐		

Siendo el nivel de seguridad al que postulo el siguiente[1]:

II. TIPO DE NIVEL DE SEGURIDAD (Marcar donde corresponda)

Medio (M)	☐
Medio Alto (M+)	☐

III. SEDE E INSTALACIONES

Indique la dirección completa de cada uno de los sitios o instalaciones en las cuales efectúa actividades para desarrollar el alcance de la acreditación solicitada, señalando las actividades que se realizan en cada uno:

Sitio	Dirección completa y país de ubicación	Actividades en cada sitio
1	Oficina Principal:	
2	Sucursales:	
3	Centro de Datos Principal:	
4	Centro de Datos Alterno:	
5	Centro de custodia de información y documentación:	
6	Otro (Cuál):	

IV. CONSULTORIA PARA LA IMPLEMENTACIÓN DE LOS REQUISITOS DE ACREDITACIÓN

SI utilizó consultores externos para la implementación de los requisitos de acreditación, por favor indique el nombre del (los) consultor (es) y de la organización a la que pertenecen, si aplica.

Nombre (s) del (los) consultor (es):	
Nombre de la organización de consultoría, si aplica:	

[1] Mayor información sobre el particular se encuentra en la Cartilla de Instrucciones.

Para lo cual se adjuntan los documentos siguientes[2] (marcar donde corresponda):

V. DOCUMENTOS QUE SE ACOMPAÑAN (Marcar donde corresponda)

1. Copia del documento de identidad del solicitante	☐	*6. Declaración de Prácticas de Registro o Verificación*	☐
2. Documentos que acrediten la existencia y vigencia de la persona jurídica	☐	*7. Constancia que acredite pago de derechos administrativos*	☐
3. Poderes del representante legal	☐	*8.Documentos que acrediten vinculación con un tercero que administre los servicios de almacenamiento de datos u otros*	☐
4. Memoria descriptiva y organigrama estructural y funcional	☐	*9. Contrato con la Entidad de Certificación emisora de los certificados digitales.*	☐
5. Documentos que acrediten domicilio en el país	☐		

POR TANTO:

Declaro bajo juramento:

1. Conocer los criterios, requisitos y condiciones de acreditación establecidos por la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica; así como las obligaciones y derechos que involucra obtener la correspondiente acreditación.
2. Que la información indicada en la presente solicitud es verdadera.
3. Contar con la infraestructura e instalaciones necesarias para prestar los servicios de registro o verificación cuya acreditación se solicita.
4. Aceptar las visitas comprobatorias que efectuará la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica o las personas o institución que ésta designe para tales efectos, así como brindar las facilidades necesarias en todas las instalaciones en donde se lleven a cabo las evaluaciones para verificar el cumplimento de los requisitos necesarios para la acreditación.
5. 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.
6. Contar con los documentos correspondientes a la Política y al Plan de Privacidad, y a la Política de Seguridad, de acuerdo a lo establecido por INDECOPI. Esta exigencia será verificada y evaluada durante la Fase II, Evaluación Técnica del proceso de acreditación.
7. Cumplir con los requisitos señalados en los artículos 16° y 17° del Reglamento de la Ley de firmas y certificados digitales, los mismos que se transcriben a continuación:
   "Artículo 16º .- Obligaciones
   Las entidades de Registro o Verificación registradas tienen las siguientes obligaciones:
   a) Cumplir con su Declaración de Prácticas de Registro o Verificación.
   b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante de certificado digital bajo responsabilidad.

[2] Relación de documentos establecida en base a la Ley de firmas y certificados digitales, su Reglamento, el TUPA del INDECOPI y la Guía de Acreditación de Entidad de Registro o Verificación (ER)

c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.
d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
e) Acreditar domicilio en el Perú.
f) Mantener vigente la contratación de seguros o garantías bancarias que permitan indemnizar por los daños que puedan ocasionar como resultado de las actividades de certificación.
Estas obligaciones podrán ser precisadas por la AAC, a excepción de las que señale expresamente la Ley.
Artículo 17º .- Respaldo financiero
Las entidades de registro o verificación acreditada deberán contar con el respaldo económico suficiente para operar bajo la IOFE; así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y en el Reglamento. La AAC definirá los criterios para evaluar el cumplimiento de este requisito."

Asimismo, me compromete formalmente a:

- Cumplir con los requisitos de acreditación establecidos por la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica.
- Respetar el procedimiento de acreditación establecido por la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica.
- Abonar todos los gastos administrativos y de evaluación que se originen.
- Facilitar el acceso a la información, los documentos y los registros que sean necesarios para la evaluación sobre la procedencia o no de la acreditación solicitada.
- En caso de obtener la acreditación, declarar frente a terceros estar acreditado sólo respecto al alcance de la acreditación que me sea otorgada, distinguiéndola permanentemente de otras actividades que presten fuera de dicho alcance.
- No usar la acreditación de manera que afecte la reputación de la Infraestructura Oficial de Firma Electrónica y/o la competencia de la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica en su condición de Autoridad Administrativa Competente.
- En caso que la acreditación sea cancelada, suspendida o reducida, interrumpiré inmediatamente el uso del logotipo o declaración de acreditación en todos los documentos y material publicitario relacionados con la acreditación afectada.
- Cumplir con mantener confidencialidad de la información relativa a los solicitantes o titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital. Quedando expresamente impedido de comercializar de cualquier forma las bases de datos o archivos digitales con información personal de los solicitantes o titulares de certificados digitales. Asimismo, me comprometo expresamente a respetar los principios de privacidad contenidos en la Norma Marco sobre Privacidad.

_____
Firma

_____
Nombre del Representante legal

Fecha de solicitud:

CARTILLA DE INSTRUCCIONES

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

Marco legislativo: El procedimiento de acreditación de un prestador de Servicios de Valor Añadido, se rige por la Ley de Firmas y Certificados digitales –Ley 27269–, su Reglamento aprobado por Decreto Supremo No. 004-2007-PCM, el TUPA del Indecopi, aprobado por Decreto Supremo No. 088-2005-PCM, así como la Guía de Acreditación de Entidad de Registro o Verificación – ER, aprobada por la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica del Indecopi.

Presentación de la solicitud: la solicitud deberá ser presentada ante la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica del Indecopi que es la primera instancia administrativa ante la cual debe tramitarse el procedimiento de acreditación. El plazo total del procedimiento es de 120 días hábiles. La solicitud deberá ser suscrita por representante legal con facultades de representación suficientes. Los datos de identidad de esta persona deberán ser consignados en la parte introductoria de la ficha de solicitud.

I. Tipo de procedimiento: deberá marcarse sólo un recuadro dependiendo del tipo de acreditación que se solicita. Para tales efectos debe tenerse presente lo siguiente:

- La acreditación como ER – Persona Jurídica, será solicitada por todas las personas jurídicas privadas y las EREP.
- La acreditación como ER – Persona Natural, sólo podrá ser solicitada por Notarios en ejercicio de sus funciones.
- La renovación de la acreditación deberá cuando menos realizarse dentro de los 120 días anteriores al vencimiento de la acreditación conferida.

II. Tipo de nivel de seguridad: según el punto IV de la Guía de Acreditación de Entidad de Registro o Verificación – ER, existen dos niveles de seguridad aplicables, cuyas características se describen a continuación:

- Nivel de Seguridad Medio (M)

  Los certificados digitales de nivel de seguridad medio son concebidos para:

  1. Trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio.
  2. Información crítica y de seguridad nacional en redes cifradas.
  3. Acceso a información clasificada o información de acceso especial en redes protegidas.
  4. Aplicaciones de valor financiero medio o de comercio electrónico, tales como las planillas, contratos, compra de vehículos, etc.

  Condiciones técnicas:

  Aplicable todo el documento "Marco de la Política de Registro para la emisión de certificados digitales"[3] con las siguientes especificaciones:

  5. 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 1 (mínimo) o Common Criteria EAL4.
  6. La longitud de clave privada mínima debe ser de 1024 bits y el certificado debe ser renovado como máximo anualmente.
  7. 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, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital – PSC sin certificación; que sólo cuentan con la aprobación de las auditorías correspondientes para la acreditación o implementación de las normas correspondientes.

- Nivel de Seguridad Medio Alto (M+)

  Los certificados digitales de nivel de seguridad medio son concebidos para:

  1. Todas las aplicaciones apropiadas para certificados de Nivel de Seguridad Medio (M).
  2. Intercambio de documentos y transacciones monetarias de alto riesgo, y trámites con el Estado en las transacciones económicas de alto monto y alto riesgo.
  3. Información crítica no clasificada o de seguridad nacional en una red no cifrada.
  4. Acceso a información clasificada o información de acceso especial en redes no protegidas.
  5. Aplicaciones de valor financiero de riesgo y monto medio alto o de comercio electrónico.

  Condiciones técnicas:

  Aplicable todo el documento "Marco de la Política de Registro para la emisión de certificados digitales" con las siguientes especificaciones:

  6. 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+.

[3] El documento (ver anexo 1 de la Guía de Acreditación de Entidad de Registro o Verificación – ER) establece los lineamientos para la elaboración de la RPS; está basado en los "Lineamientos para el marco de la política de emisión de certificados que pueden ser usados en comercio electrónico transnacional", emitido por el *APEC Telecommunications & Information Working Group - APEC eSecurity Task Group*: Draft Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction E-Commerce, Marzo 2004. Información disponible en: http://www.apectel29.gov.hk/download/estg_20.doc.

7. La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años.
8. 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, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital – PSC con las siguientes certificaciones:

- ER: ISO 9001:2000
- EC: ISO 27001
- SVA: ISO 9001:2000 o ISO 27001, y SW con ISO 9001:2000 o CMMI nivel 2 (mínimo)

III. Documentos que se acompañan: Toda la documentación que se acompañe a la solicitud, deberá estar en idioma español. Si las fuentes originales provinieran de otro idioma, éstas deberán ser traducidas de manera oficial. Las especificaciones de cada uno de los documentos se señalan a continuación:

1. Copia 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.
2. Documentos que acrediten la existencia y vigencia de la persona jurídica: deberá acreditarse este hecho con el documento de vigencia de persona jurídica expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. 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. Adicionalmente 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. En el caso de los Notarios, este hecho quedará demostrado con 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.
3. Poderes del representante legal: en donde se deberá acreditar contar con facultades suficientes para solicitar la acreditación o autorización solicitada. Adicionalmente, debe tenerse en cuenta que:
   - 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.
   - 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.
   - 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 acreditarse las facultades de este funcionario.
   - En el caso de los Notarios, se estará a lo establecido en el Decreto Ley No. 26662 – Ley del Notariado.
4. Memoria descriptiva y organigrama estructural y funcional: la misma que deberá ser realizada conforme al Formato denominado: Memoria descriptiva y organigrama estructural y funcional de Entidad de Registro o Verificación – ER.
5. Documentos que acrediten domicilio en el país: Este hecho se acredita con el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), donde debe constar con la condición de "habida". En su defecto, se podrá acompañar cualquier otra documentación que sirva para acreditar la condición de domiciliado en el país, la misma que será materia de evaluación por parte de la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica.
6. Declaración de Prácticas de Registro o Verificación: La Declaración de Prácticas de Registro o Verificación, es el documento en el que constan de manera detallada las políticas y procedimientos que aplica la ER para la prestación de sus servicios. La Declaración de Prácticas de Registro o Verificación deberán establecer procedimientos detallados que garanticen el cumplimiento de las funciones legalmente establecidas para las ER. Asimismo, tendrán que asegurar la verificación presencial de la identidad del solicitante de un nuevo certificado digital.
7. Constancia que acredite pago de derechos administrativos: los mismos que ascienden a 100% de la UIT (S/. 3,450.00 para el año 2007).
8. Documentos que acrediten vinculación con un tercero que administre los servicios de almacenamiento de datos u otros: los documentos presentados 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 Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica considere necesaria.