ANEXO 10:

FICHA DE SOLICITUD DE ACREDITACIÓN COMO ENTIDAD DE CERTIFICACIÓN (EC)

indecopi **COMISIÓN DE REGLAMENTOS TÉCNICOS Y COMERCIALES**

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

Ficha de Solicitud de Acreditación como Entidad de Certificación (EC)

- Antes de llenar esta solicitud consulte los documentos que establecen los criterios de acreditación generales, específicos y complementarios[1] (legislación y guías de acreditación) que correspondan a la modalidad de EC y nivel de seguridad que desea acreditar. Mayores precisiones se pueden encontrar en la Cartilla de Instrucciones que figura en la parte final del presente documento

SEÑOR SECRETARIO TÉCNICO DE LA COMISIÓN DE REGLAMENTOS TÉCNICOS Y COMERCIALES (CRT) 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 _____

Solicito a la Comisión de Reglamentos Técnicos y Comerciales del INDECOPI el siguiente procedimiento:

I. TIPO DE PROCEDIMIENTO (Marcar donde corresponda)

Acreditación como EC raíz o ECERNEP y EC de nivel subsiguiente o ECEP	☐	Renovación de la acreditación	☐
Acreditación como EC de nivel subsiguiente o ECEP	☐	Acreditación por homologación	☐
Autorización para realizar certificación cruzada	☐		

Siendo el nivel de seguridad al que postulo el siguiente[2]:

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

Medio (M)	☐
Medio Alto (M+)	☐

[1] La acreditación es un procedimiento administrativo, por lo tanto, las reglas que lo rigen son parte de la legislación nacional y se encuentran disponibles mediante su publicación en el Diario Oficial. En tal sentido, la suscripción de la solicitud implica conforme a lo expuesto la aceptación de dichas condiciones y la intención de ser calificado en el marco de ellas.

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

Para lo cual se adjuntan los documentos siguientes[3] (marcar donde corresponda):

III. DOCUMENTOS QUE SE ACOMPAÑAN (Marcar donde corresponda)

1.Copia del documento de identidad del solicitante	☐	*10. Documento(s) que acredite(n) vinculación con una (o más) Entidades de Registro o Verificación*	☐
2. Documentos que acrediten la existencia y vigencia de la persona jurídica	☐	*11. Informe favorable de la entidad sectorial correspondiente*	☐
3. Poderes del representante legal	☐	*12. Documento que acredite contratación de seguros o garantías bancarias*	☐
4. Memoria descriptiva y organigrama estructural y funcional	☐	*13. Documentación que acredite contar con respaldo económico*	☐
5. Documentos que acrediten domicilio en el país	☐	*14. Constancia que acredite pago de derechos administrativos*	☐
6. Políticas de Certificación (CP)	☐	*15. Documento donde conste el mapeo CP, CPS - APEC*	☐
7. Declaración de Prácticas de Certificación (CPS)	☐	*16. Acreditación otorgada en el país de origen de la solicitante*	☐
8. Política General de Certificación (CP, caso ECERNEP)	☐	*17. Documentos que acrediten condición de economía miembro del APEC*	☐
9. Documentos que acrediten vinculación con un tercero que administre sistema de gestión, software, hardware u otros componentes	☐	*18. Resolución de acreditación de la Entidad de Certificación Raíz (caso EC de nivel subsiguiente, cuya EC Raíz se encuentra acreditada)*	☐

Especificando los siguientes datos técnicos:

IV. DATOS TÉCNICOS (Completar)

Módulo Criptográfico (HSM)[4]: N° serie _____

Proveedor _____

N° Factura _____

Certificación[5] FIPS 140-2 ☐ Common Criteria EAL4+ ☐

_____

Tarjetas inteligentes: Proveedor _____

N° Factura _____

Certificación HW[6] FIPS 140-2 _____

Certificación FW[7] FIPS 140-2 ☐ Common Criteria EAL4+ ☐

Adjunto las constancias que acreditan las certificaciones declaradas.

[3] 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 Entidades de Certificación EC.
[4] La información a consignar debe corresponder a cada raíz intermedia que se implemente.
HSM (*Hardware Security Module*): dispositivo que almacena la clave privada.
[5] Tanto el hardware como el firmware
[6] HW: hardware
[7] FW: firmware ("sistema operativo")

POR TANTO:

Declaro bajo juramento:

1. Conocer los criterios, requisitos y condiciones de acreditación establecidos por la Comisión de Reglamentos Técnicos y Comerciales; 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 certificación digital cuya acreditación se solicita.
4. 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 la Comisión de Reglamentos Técnicos y Comerciales.
5. Aceptar la visita comprobatoria que efectuará la Comisión de Reglamentos Técnicos y Comerciales 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.
6. Contratar los seguros o garantías bancarias que determine la Comisión de Reglamentos Técnicos y Comerciales una vez obtenida la correspondiente acreditación, como requisito para poder ingresar formalmente a la IOFE.
7. Contar con los documentos correspondientes a la Política y al Plan de Privacidad, y a la Política de Seguridad, y cumplir con los requerimientos de Usabilidad, de acuerdo a lo establecido por INDECOPI. Esta exigencia será verificada y evaluada durante la Fase II, Evaluación Técnica del proceso de acreditación.

Asimismo, me compromete formalmente a:

- Cumplir con los requisitos de acreditación establecidos por la Comisión de Reglamentos Técnicos y Comerciales.
- Respetar el procedimiento de acreditación establecido por la Comisión de Reglamentos Técnicos y Comerciales.
- 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 de Reglamentos Técnicos y Comerciales 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 certificación, 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 una Entidad de Certificación, así como la solicitud para la realización de certificación cruzada, 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 Certificación EC aprobada por la Comisión de Reglamentos Técnicos y Comerciales del Indecopi.

Presentación de la solicitud: la solicitud deberá ser presentada ante la Comisión de Reglamentos Técnicos y Comerciales 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:

- Las entidades de certificación raíz –lo cual incluye a la Entidad de Certificación Nacional para el Estado Peruano, ECERNEP– emiten certificados digitales para Entidades de Certificación de Nivel subsiguiente.
- Las entidades de certificación de nivel subsiguiente –lo cual incluye a las Entidades de Certificación del Estado Peruano, ECEPs– emiten certificados digitales para usuarios finales personas naturales o jurídicas.
- La certificación cruzada es un procedimiento a partir del cual una entidad de certificación acreditada nacional reconoce la validez de un certificado emitida por otra, previa autorización de la Comisión de Reglamentos Técnicos y Comerciales del Indecopi y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.
- La renovación de la acreditación deberá cuando menos realizarse dentro de los 120 días anteriores al vencimiento de la acreditación conferida.
- 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.

II. Tipo de nivel de seguridad: según el punto IV de la Guía de Acreditación de Entidad de Certificación – EC, 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 emisión de certificados digitales"[8] 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.

[8] El documento (ver anexo 1 de la Guía de Acreditación de Entidad de Certificación – EC) establece los lineamientos para la elaboración de la CPS; 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.

Condiciones técnicas:
Aplicable todo el documento "Marco de la Política de 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+.
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.
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.
4. Memoria descriptiva: la misma que deberá ser realizada conforme al Formato denominado: Memoria Descriptiva y Organigrama estructural y funcional de Entidad de Certificación – EC.
5. Organigrama estructural y funcional: el mismo que deberá ser elaborado conforme al Formato indicado en el punto anterior.
6. 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 de Reglamentos Técnicos y Comerciales.
7. Políticas de Certificación (CP): Documento que describe de manera general las políticas y procedimientos que aplica la Entidad de Certificación para la prestación de sus servicios.
8. Declaración de Prácticas de Certificación (CPS): Documento constan de manera detallada las políticas y procedimientos que aplica la Entidad de Certificación para la prestación de sus servicios.
   En el caso de las CP y CPS de las ECEPs que soliciten acreditación, deberá dejarse expresa constancia del procedimiento de información al usuario respecto a los alcances y restricciones en el empleo de los certificados digitales que emiten; en el sentido que carecerán del respaldo de la IOFE si se utilizan para fines distintos al ejercicio de funciones administrativas, procedimientos administrativos o administración interna del Estado o procedimientos y coordinaciones entre entidades públicas, de conformidad con lo establecido en inciso b) del artículo 33° del Reglamento.
9. Documentos que acrediten vinculación con un tercero que administre sistema de gestión, software, hardware u otros componentes: 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 certificación digital bajo estas condiciones y la disponibilidad de estos elementos para la evaluación y supervisión que la Comisión de Reglamentos Técnicos y Comerciales 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.
10. Documento que acredite vinculación con una Entidad de Registro o Verificación (ER): 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 su acreditación de conformidad con la Guía de Acreditación de Entidad de Registro o Verificación – ER. En este caso, su acreditación como EC quedará condicionada a la obtención de la correspondiente acreditación como ER.
11. Informe favorable de la entidad sectorial correspondiente: este informe versará sobre la legalidad y seguridad de la prestación de servicios de certificación y será necesario siempre que la solicitante sea una persona jurídica supervisada. Ejemplo: Instituciones Bancarias.

12. Documento que acredite contratación de seguros o garantías bancarias: Este requisito no será exigible para la ECERNEP ni ECEPs. Para el caso de EC particulares, este requisito será exigible a partir de julio de 2008. Para efectos del procedimiento de acreditación, bastará suscribir la presente 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. En su oportunidad, la CRT procederá a definir los criterios y condiciones requeridas para acreditar la contratación de seguros o garantías bancarias.
13. Documentación que acredite contar con respaldo económico: Este requisito no será exigible para la ECERNEP ni ECEPs. 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.
14. Constancia que acredite pago de derechos administrativos: los mismos que ascienden a 100% de la UIT (S/. 3,450.00 para el año 2007).
15. Documento donde conste el mapeo CP, CPS - APEC: este documento será requerido 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.
16. 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 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.
17. Documentos que acrediten condición de economía miembro del APEC: este documento se presentará en el caso que la 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.
18. 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.