ANEXO 8:
REGLAMENTO ESPECÍFICO DE ACREDITACIÓN ENTIDAD DE CERTIFICACIÓN - EC

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1°.- Objeto
El presente Reglamento establece los criterios de acreditación de las Entidades de Certificación, tanto públicas como privadas, de primer nivel -raíz- o de nivel subsiguiente, así como los derechos y obligaciones que deben de cumplir para poder ser acreditadas por la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica (CFE) del INDECOPI, en su condición de Autoridad Administrativa Competente (AAC) conforme a ley.

En todos los casos en que en el presente reglamento se haga mención a las EC, se entenderán incluidas en este concepto tanto a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) como a las Entidades de Certificación del Estado Peruano (ECEP).

Asimismo, en todos los casos en que se haga mención al Reglamento, se entenderá referido al presente instrumento legal. En caso en que se haga mención al Reglamento General, se entenderá referido al Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.

CAPÍTULO II
DEFINICIONES

Artículo 2°.- Definiciones
Para efectos del presente Reglamento se aplican las definiciones establecidas contenidas en el Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.

CAPÍTULO III
ASPECTOS GENERALES DEL PROCEDIMIENTO DE ACREDITACIÓN COMO EC

Artículo 3°.- Norma aplicable
El procedimiento de acreditación se rige en particular por lo establecido en el presente Reglamento en concordancia con la normativa contenida en el Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.

En caso de conflicto entre estas dos normas, primará lo establecido en el presente Reglamento.

Artículo 4°.- Tipo de acreditación que se solicita
En el formato de solicitud que se presentará para efectos de la correspondiente acreditación, deberá especificarse el tipo de acreditación que se solicita, la misma que puede ser:

a. Acreditación como EC raíz y EC de nivel subsiguiente
b. Acreditación como EC de nivel subsiguiente
c. Autorización para la realización de certificación cruzada con otras EC
d. Renovación de acreditación
e. Acreditación por homologación

Artículo 5°.- Acreditación como EC raíz y EC de nivel subsiguiente
La acreditación como EC raíz y EC de nivel subsiguiente se solicita para Entidades que soliciten funcionar:
a. como EC raíz: emiten certificados digitales para EC de nivel subsiguiente; y
b. como EC de nivel subsiguiente.

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

Artículo 6°.- Acreditación como EC de nivel subsiguiente
La 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 ECEP para efectos de su incorporación a la IOFE.

Artículo 7°.- Autorización para la realización de certificación cruzada con otras EC
La certificación cruzada es un procedimiento a partir del cual una EC acreditada nacional reconoce la validez de un certificado emitido por otra, previa autorización de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica del INDECOPI, y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

La autorización deberá solicitarse para el caso de certificación cruzada entre una EC acreditada con otra EC, sea esta nacional o extranjera.

Artículo 8°.- Niveles de seguridad
En la solicitud de acreditación como EC se deberá establecer el nivel de seguridad al que se postula, debiéndose para tales efectos cumplir con los lineamientos y requisitos exigidos en el documento del APEC[1] y las condiciones técnicas particulares para el nivel de seguridad establecido.

Artículo 9°.- Nivel de seguridad medio
Los certificados de nivel de seguridad medio (M) están concebidos para:

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

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.

Artículo 10°.- Condiciones técnicas nivel de seguridad medio
Para efectos de las especificaciones técnicas se tendrá en consideración las siguientes precisiones:

a. 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.

[1] Ver: http://publications.apec.org/publication-detail.php?pub_id=411

b. La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada tres (3) años.
c. 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.

Artículo 11°.- Nivel de seguridad medio alto
Los certificados de Nivel de Seguridad Medio Alto (M+) están concebidos para:

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

Adicionalmente, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital – PSC con las siguientes certificaciones:

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

Artículo 12°.- Condiciones técnicas del nivel de seguridad medio alto
Para efectos de las especificaciones técnicas se tendrá en consideración las siguientes precisiones:

a. 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+.
b. La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años.
c. Los certificados a nivel de entidad final –usuarios– deben ser generados de manera individual y separados para las siguientes funciones: cifrado, firma (no repudio) y autenticación.

Artículo 13°.- Renovación de acreditación
La renovación de acreditación se rige por el procedimiento establecido en el Capítulo VII del presente Reglamento.

Artículo 14°.- Acreditación por homologación
La acreditación por homologación se rige por el procedimiento establecido en el Capítulo VII del presente Reglamento.

Artículo 15°.- Servicios Adicionales a los de certificación digital
En caso que la EC solicitante decida realizar servicios adicionales inherentes a la certificación digital, para efectos 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 PSC 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 ER.

La acreditación como EC no implica de manera automática la acreditación como SVA ni ER, las mismas que se rigen por sus propios procedimientos de acreditación.

CAPÍTULO IV
SOLICITUD DE ACREDITACIÓN Y DOCUMENTOS SUSTENTATORIOS

Artículo 16°.- Solicitud de acreditación como EC
La solicitud de acreditación será dirigida al Secretario Técnico de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica del INDECOPI, especificando el tipo de acreditación que se solicita y el nivel de seguridad al que se postula.

La solicitud será realizada en base a la Ficha de Solicitud de Acreditación como Entidad de Certificación (EC).

Artículo 17°.- Los documentos que se deben acompañar a la mencionada Ficha de Solicitud de Acreditación, son los que se detallan a continuación:
a. Copia simple del documento de identidad del solicitante.
b. Documentos que acrediten la existencia y vigencia de la persona jurídica solicitante.
c. Documentos que acrediten los poderes en virtud a los cuales los representantes legales se encuentran facultados para solicitar la acreditación.
d. Memoria descriptiva y organigrama estructural y funcional.
e. Documentos que acrediten domicilio en el país.
f. Declaración jurada de contar con infraestructura e instalaciones necesarias, según el nivel de seguridad solicitado.
g. Políticas de certificación (CP) y Declaración de Prácticas de Certificación (CPS).
h. Política General de Certificación (caso ECERNEP).
i. Documentación relativa al sistema de gestión que permita el mantenimiento de las condiciones señaladas en el artículo 9º del Reglamento de la Ley de Firmas y Certificados Digitales.
j. Declaración jurada declarando cumplir con 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 AAC.
k. Declaración jurada de aceptación de las visitas comprobatorias.
l. Documentos que acrediten vinculación con una o más ERs.
m. Informe favorable de la entidad sectorial correspondiente.
n. Documentación que acredite la contratación de seguros o garantías bancarias.
o. Documentación que acredite contar con respaldo económico.
p. Constancia de pago de los derechos administrativos.
q. Documento donde conste el mapeo correspondiente: CP, CPS – APEC, en caso que no se hayan elaborado siguiendo el esquema establecido en el anexo 1 de Guía de Acreditación de Entidad de Certificación (EC).

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 CFE 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.

Los documentos deberán estar conforme a lo establecido en la Guía de Acreditación de Entidad de Certificación – EC versión 4.0 y sus anexos, según corresponda.

Artículo 18°.- Acreditación de la existencia y vigencia de la persona jurídica
La existencia y vigencia de la persona jurídica deberá acreditarse con el documento de vigencia respectivo 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.

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.

Artículo 19°.- Acreditación de los poderes de los representantes legales
Para la verificación de las facultades de los representantes legales, se tendrán en cuenta las reglas siguientes:

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 acreditarse las facultades de este funcionario.

Artículo 20°.- Memoria descriptiva – Organigrama Estructural y Funcional
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).

Artículo 21°.- Documentos que acrediten domicilio en el país
La condición de domiciliada de una EC solicitante, 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 para la Gestión de la Infraestructura Oficial de Firma Electrónica.

Artículo 22°.- Políticas de Certificación (CP)
Las Políticas de Certificación es el documento que describe de manera general las políticas y procedimientos que aplica la Entidad de Certificación para la prestación de sus servicios.

Artículo 23°.- Declaración de Prácticas de Certificación (CPS)
La Declaración de Prácticas de Certificación es el documento en el que constan de manera detallada las políticas y procedimientos que aplica la Entidad de Certificación para la prestación de sus servicios.

Las CP y CPS deberán estar elaborados en estricta observancia de los Lineamientos para Infraestructura de clave pública (PKI), según el documento Marco de la Política de emisión de certificados digitales, así como de la Norma Marco sobre Privacidad.

En el caso de las CP y CPS de las ECEPs deberá dejarse expresa constancia en estos documentos, 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 de la Ley de Firmas y Certificados Digitales.

Artículo 24°.- Documentación relativa al sistema de gestión
La documentación relativa a la implementación del sistema de gestión dentro de los alcances de lo establecido en el artículo 9º del Reglamento de la Ley de Firmas y Certificados Digitales, será contrastado a través de la información contenida en la CP y CPS de la entidad solicitante.

Artículo 25°.- Software, hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales
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.

En este caso, la AAC tiene derecho a precisar los términos bajo los cuales se rigen este tipo de servicios de certificación digital.

Artículo 26°.- Documentos que acrediten relación con alguna ER acreditada
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.

Artículo 27°.- Informe favorable de la entidad sectorial correspondiente
Este requisito será necesario en el caso que la EC solicitante sea una persona jurídica supervisada.

El informe deberá versar sobre la legalidad y seguridad de la prestación de servicios de certificación y será emitido por la Entidad Sectorial correspondiente.

Artículo 28°.- Documentación que acredite la contratación de seguros o garantías bancarias
En su oportunidad, la CFE procederá a definir los criterios y condiciones requeridas para acreditar la contratación de seguros o garantías bancarias.

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.

Artículo 29°.- Documentación que acredite contar con respaldo económico
La EC 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. 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.

Artículo 30°.- Constancia de pago de los derechos administrativos
Los derechos administrativos que deben cancelarse para efectos del procedimiento de acreditación como EC asciende al 100% del valor de la UIT.

Artículo 31°.- Documentación para la realización de evaluación técnica
Para efectos de la documentación que se debe acompañar para efectos de la realización de la evaluación técnica, deberá tomarse en cuenta lo siguiente:

a. 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.
b. 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".
c. 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.
d. 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.

Artículo 32°.- Declaraciones juradas
Las declaraciones juradas a que se alude en los incisos f), j) y k) del artículo 16º forman parte integrante de la Ficha de Solicitud de Acreditación como Entidad de Certificación (EC), por lo que bastará la suscripción de este documento para que se entiendan efectuadas las mencionadas Declaraciones Juradas.

Sin perjuicio de lo regulado en el párrafo anterior, la EC solicitante podrá elaborar las mencionadas Declaraciones Juradas en documentos independientes, los mismos que deberán ser acompañados a la solicitud de acreditación.

CAPÍTULO V
EVALUACIÓN DOCUMENTARIA Y TÉCNICA

Artículo 33°.- Evaluación documentaria
Dentro del procedimiento de acreditación, la etapa de evaluación documentaría será llevada a cabo en estricta observancia de lo establecido en el Reglamento General.

Artículo 34°.- Comité Evaluador
En la resolución en la que se declara la procedencia de la solicitud de acreditación se designará al Comité Evaluador encargo de llevar a cabo la misma.

Entre los miembros del Comité Evaluador y la entidad solicitante –o su raíz- no deberá existir ningún tipo de vinculación directa o indirecta que pueda comprometer la imparcialidad.

En caso que la EC no se encuentre conforme con la designación de alguno de los miembros del comité evaluador, podrá efectuar las correspondientes observaciones, debiendo observar las condiciones y requisitos establecidos para estos efectos por el Reglamento General.

Artículo 35°.- Evaluación técnica
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

El procedimiento de evaluación técnica se rige por los lineamientos establecidos para tales efectos por el Reglamento General.

En ambas etapas, el Comité evaluador deberá emitir pronunciamiento claro y debidamente fundamentado.

Artículo 36°.- Evaluación de las CP, CPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad
El objetivo de esta evaluación es examinar la adecuación de las CP y CPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad de la EC solicitante, la Norma Marco sobre Privacidad y la norma ISO 27001, respectivamente.

El procedimiento de evaluación se realizará sobre la base de los documentos acompañados para tales efectos por la EC solicitante.

De considerarlo necesario, el Comité Evaluador podrá solicitar documentación complementaria o la realización de una evaluación o auditoría en las instalaciones de la EC.

Artículo 37°.- Evaluación de interoperabilidad
El objetivo de la evaluación de interoperabilidad es establecer el cumplimiento de las condiciones necesarias para el establecimiento de interoperabilidad entre la EC solicitante mediante el uso de la TSL –ETSI TS102.231–, como estándar para la creación de la lista segura de proveedores de servicios de certificación digital.

Para el procedimiento de evaluación de interoperabilidad, se tomará contacto con el personal designado para tales efectos por la EC solicitante, a fin de realizar las pruebas correspondientes.

Artículo 38°.- TSL de prueba
La TSL de prueba que se genere durante la etapa de evaluación de interoperabilidad deberá ser alojada en la infraestructura tecnológica de la EC solicitante a efectos de realizar las pruebas correspondientes,

Esta TSL únicamente tiene carácter de prueba y por ende no podrá ser utilizado por la EC solicitante para otros fines.

CAPÍTULO VI
DE LA ACREDITACIÓN COMO EC

Artículo 39°.- Alcances de la acreditación
La acreditación como EC implica el ingreso de esta entidad a la IOFE y su inscripción en el Registro de PSC acreditados, permitiéndole asimismo gozar de los beneficios, presunciones y efectos legalmente establecidos. Asimismo, una vez acreditada, la EC solicitante ingresará a la TSL que para tales efectos mantiene la CFE en su condición de AAC.

El procedimiento formal de acreditación como EC se rige por lo establecido en el Reglamento General.

Artículo 40°.- Requisito para el Ingreso a la IOFE

En caso se obtenga la correspondiente acreditación, la EC deberá cumplir con remitir al INDECOPI, dentro de un plazo perentorio de veinte (20) días, los documentos que acrediten la contratación de seguros o garantías bancarias correspondientes.

Este plazo podrá ser ampliado por igual tiempo y por una sola vez, en caso medie solicitud por escrito de la EC.

Artículo 41°.- Efectos de la acreditación
Una vez obtenida la correspondiente acreditación, la EC se encuentra obligada a prestar sus servicios en los mismos términos a los contenidos en la CP y CPS que fueran materia de evaluación por parte de la AAC.

Asimismo, deberá cumplir en todo momento las obligaciones a que se refiere el artículo 12° del Reglamento de la Ley de Firmas y Certificados Digitales. En el caso de la ECERNEP y las ECEP, adicionalmente deberán tomar en consideración las limitaciones a la prestación de sus servicios a que se refiere el artículo 33° del mencionado Reglamento de la Ley de Firmas y Certificados Digitales.

CAPÍTULO VII
DEL MANTENIMIENTO, RENOVACIÓN Y HOMOLOGACIÓN DE LA ACREDITACIÓN

Artículo 42°.- Aplicación supletoria del Reglamento General
El mantenimiento, renovación y homologación de la acreditación se rige por lo establecido en el Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.