

Firma

"Año del Bicentenario de la Proclamación de la República 1813-2013"



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

**ANEXO**

**1 INTRODUCCIÓN**

**1.1 Descripción General**

ES COPIA FIEL DEL ORIGINAL

La Infraestructura Nacional de Certificación Digital de Paraguay, es administrada por la Autoridad de Aplicación, ejercida por el Ministerio de Industria y Comercio a través del Viceministerio de Comercio designada como Autoridad de Aplicación por Ley N° 4610/12 "De validez Jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico".

El Ministerio de Industria y Comercio a través del Viceministerio de Comercio tiene entre sus cometidos la administración de la Autoridad Certificadora Raíz del Paraguay.

En el marco de la Ley 4017/10, la Ley N° 4610/12, y el Decreto Reglamentario N° 7369/11, la Autoridad de Aplicación cuenta con las siguientes atribuciones:

- a) dictar las normas reglamentarias y de aplicación de la presente Ley;
- b) establecer los estándares tecnológicos y operativos de la implementación de la presente Ley;
- c) autorizar, conforme a la reglamentación expedida por el Poder Ejecutivo, la operación de entidades de certificación en el territorio nacional;
- d) velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad;
- e) efectuar las auditorías de que trata la presente Ley;
- f) determinar los efectos de la revocación de los certificados de los prestadores de servicios de certificación;
- g) instrumentar acuerdos nacionales e internacionales, a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.**

- 2 -

- h) determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;
- i) requerir en cualquier momento a las entidades de certificación para que suministren información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren;
- j) imponer sanciones a las entidades de certificación por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio;
- k) otorgar o revocar las licencias a los prestadores del servicio de certificación habilitados y supervisar su actividad, según las exigencias establecidas por la reglamentación;
- l) homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación; y,
- m) Aplicar las sanciones previstas en la reglamentación."

Además, el Art. 40 de la Ley N° 4017/10 establece que en su calidad de titular de Certificado Digital, la Autoridad de Aplicación tiene las mismas obligaciones que los titulares de certificados y que lo certificadores licenciados. En especial y en particular, debe:

- a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;
- b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación.
- c) Publicar en internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital; y



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL  
PARAGUAY.**

- 3 -

- d) Supervisar la ejecución del plan de cese de actividades de los Prestadores de Servicio de Certificación Habilitados que discontinúan sus funciones.

Y las Obligaciones establecidas en las Políticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

Los Certificados emitidos por la Autoridad Certificadora Raíz del Paraguay, están regidos por la normativa vigente, la Política de Certificación y la presente Declaración de Prácticas de Certificación; por tanto, los Prestadores de Servicios de Certificación y los usuarios finales de los Certificados, cuentan con el respaldo de la PKI Paraguay (Infraestructura de Clave Publica), para las operaciones de Firma Digital que correspondan.

La Declaración de Prácticas de Certificación, es el instrumento que establece los términos bajo los cuales será prestado el Servicio de Certificación Digital; estos términos establecen el marco legal sobre el cual opera la Autoridad Certificadora Raíz del Paraguay junto con lo establecido en la Legislación vigente. La presente Declaración de Prácticas de Certificación contiene las prácticas empleadas por la Autoridad Certificadora Raíz del Paraguay para la gestión de Certificados y revocación de los mismos.

Abog. Silvia Santander Florentín  
Secretaría General





MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 4 -

**1.2 - Identificación de la Declaración de Prácticas de Certificación**

Nombre: Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

Versión: 1.0

Fecha de elaboración:

Fecha de última actualización:

Sitio web de publicación: [www.acraiz.gov.py/cps/dpc\\_acrp.pdf](http://www.acraiz.gov.py/cps/dpc_acrp.pdf)

**1.3 - Participantes de la Infraestructura de Clave Pública - PKI Paraguay**

**1.3.1 – Autoridad Aplicación – Función de Regulación**

El rol de Regulación en la Infraestructura de Certificación Digital del Paraguay es desempeñado por la Autoridad de Aplicación, ejercida por el Ministerio de Industria y Comercio, y sus funciones están estipuladas en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay y la legislación vigente.

**1.3.2 - Autoridad de Aplicación – Función de Registro**

Las funciones de Registro, son parte de los servicios de una Autoridad de Certificación. De conformidad al artículo 10 del Decreto Reglamentario N° 7369/11, se establece que la Autoridad de Aplicación mantendrá un Registro de los Prestadores de Servicios de Certificación habilitados, el que deberá contener los datos definidos en la normativa. Las funciones de registro que debe desempeñar la Autoridad de Aplicación están establecidas en las Políticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**1.3.3 - Autoridad Certificadora Raíz del Paraguay**

La Autoridad Certificadora Raíz del Paraguay (ACRP) es administrada por la Autoridad de Aplicación, y sus funciones están estipuladas en la Política de Certificación y la Normativa vigente.

Abog. Silvia Sandoval Florentín  
Secretaría General



ES COPIA DEL ORIGINAL



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 5 -

**1.3.4 –Prestadores de Servicios de Certificación**

Entidad Jurídica habilitada por la Autoridad de Aplicación, para la prestación de Servicios de Certificación de firmas digitales, dicha entidad que deberá contar con un Certificado emitido por la Autoridad Certificadora Raíz del Paraguay y solo podrá emitir Certificados para usuarios finales.

**1.3.5 - Suscriptores**

Los suscriptores de los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay son los Prestadores de Servicios de Certificación habilitados, y sus funciones se encuentran detalladas en la Política de Certificación y normativa vigente.

Es obligación de todo suscriptor el conocimiento de la presente Declaración de Prácticas de Certificación, así como de la normativa vigente.

**1.3.6 – Parte que confía**

Por parte que confía se entienden todas las personas o entidades que confían en los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay para los Prestadores y que luego estas personas o entidades utilizarán los certificados emitidos por Prestadores de Servicios de Certificación habilitados para validar la cadena de confianza.

**1.4 - Uso de los certificados**

Los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay y de acuerdo a la presente Declaración de Prácticas de Certificación deben ser utilizados por los Prestadores de Servicios de Certificación con el único propósito de validar la cadena de confianza de la PKI Paraguay, firmar los certificados emitidos a sus suscriptores finales y firmar las Listas de Certificados Revocados correspondientes.

Los certificados no pueden ser utilizados con otro fin. La utilización de la clave privada asociada al certificado para otro fin es considerada causal de revocación del mismo y/o la Suspensión de la Habilitación del Prestador de Servicios de Certificación. (ver Política de Certificación).



Abog. Silvia Santamaría Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL  
PARAGUAY.**

- 6 -

**1.5 - Administración de la Declaración de Prácticas**

La Administración de la presente Declaración de Prácticas de Certificación es responsabilidad de la Autoridad de Aplicación. Para consultas o sugerencias, se establece los siguientes contactos:

Nombre: Ministerio de Industria y Comercio

Dirección: España N° 323 casi EE.UU. Asunción - Paraguay

Dirección de correo: [info@acraiz.gov.py](mailto:info@acraiz.gov.py)

Página Web: [www.acraiz.gov.py](http://www.acraiz.gov.py)

Teléfono: (+595) (21) 214279

ES COPIA FIEL DEL ORIGINAL

**1.5.1 - Procedimiento de aprobación**

La Autoridad de Aplicación, aprobará mediante resolución la presente Declaración de Prácticas de Certificación y sus posteriores enmiendas o modificaciones.

**1.6 - Definiciones y abreviaturas**

**Autoridad de Aplicación (AA):** MIC – Ministerio de Industria y Comercio a través del Viceministerio de Comercio. Órgano Regulador competente designado por Ley, creado por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 “De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico”.

**Autoridad Certificadora Raíz del Paraguay (ACRP):** Conjunto de Sistemas informáticos, Personal, Políticas y procedimientos que en la estructura de PKI Paraguay por herencia, constituyen la raíz de confianza. Permite certificar a otras entidades encargadas de emitir certificados dentro de PKI Paraguay.

**Política de Certificación: (PC)** Conjunto de Políticas que indican la aplicabilidad de un certificado con requerimientos comunes de seguridad y además definen los requisitos que cualquier prestador debe respetar para trabajar con este tipo de certificado. Las Políticas son promovidas, aprobadas y mantenidas por la Autoridad de Aplicación.



Abog. Silvia Sánchez Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.**

- 7 -

**Infraestructura de Clave Pública o Public Key Infrastructure (PKI):** La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad. Es un conjunto de equipos y programas informáticos, políticas, normas y procedimientos utilizados para crear, almacenar y publicar los certificados digitales, así como para la publicación de la información y consultas de vigencia y validez de los mismos permitiendo la ejecución con garantías de operaciones criptográficas.

**Prestador de Servicios de Certificación (PSC):** Entidad Jurídica habilitada ante la Autoridad de Aplicación, encargada de operar una Autoridad de Certificación en el marco del PKI Paraguay. Dicha PSC debe contar con un certificado emitido por la Autoridad Certificadora Raíz y solo podrá emitir certificados a usuarios finales.

**Declaración de Prácticas de Certificación (DPC):** Es la declaración de las Prácticas que emplea una entidad Certificadora en la gestión de los certificados emitidos por ella.

**Certificado Digital (CD):** Es todo mensaje de dato u otro registro emitido por una Entidad legalmente habilitada para el efecto y que confirme la vinculación entre el titular de una firma digital y los datos de creación de la misma.

**Firma Digital (FD):** Es una firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

**Solicitud de Firma de Certificado (SFC):** Es la petición de certificado que se envía a la autoridad de certificación. Mediante la información contenida en el SFC (CSR) la autoridad de certificación puede emitir el certificado una vez realizadas las comprobaciones que correspondan. La Autoridad de Certificación Raíz recibirá peticiones generadas por los Prestadores de Servicios de Certificación y ellos recibirán las solicitudes de los usuarios finales. CSR, es la sigla en inglés de la Solicitud de Firma de Certificado.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 8 -

**2 – Aspectos Generales de la Política de Certificación**

**2.1. - Obligaciones**

Estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**2.2. – Responsabilidades**

Estipulado en la Política de Certificación de la Autoridad de Certificadora Raíz del Paraguay.

**2.3. - Interpretación y aplicación de las normas**

Estipulado en la Política de Certificación de la Autoridad de Certificadora Raíz del Paraguay.

**2.4. - Publicación y Repositorios**

**2.4.1. - Publicación de información**

La Autoridad de Aplicación dispone del siguiente sitio web como repositorio público de información: [www.acraiz.gov.py](http://www.acraiz.gov.py) Este servicio de publicación de información estará disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema o de sufrir inconvenientes deberán ser solucionados en un plazo no mayor a 48hs. La Autoridad de Aplicación dedicará sus mejores esfuerzos para que el servicio se restablezca y esté disponible rápidamente.

La información mínima que la Autoridad de Aplicación publica en el sitio web está estipulada en la sección 2.3.1 de la Política de Certificación.

**2.4.2. - Frecuencia de publicación**

Las publicaciones antes mencionadas serán actualizadas con un máximo de un (1) día hábil desde que se dispongan o surjan cambios.

La información relativa a datos de contacto será actualizada con un máximo de un (1) día hábil desde que surjan cambios.

La Lista de Certificados Revocados (CRL) deberá ser actualizada cuando ocurra al menos uno de los siguientes hechos:

- a) Se produzca la revocación de un certificado;
- b) Tres meses después de la última emisión



Abog. Silvia Sánchez Florentín  
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL  
PARAGUAY.**

- 9 -

**2.4.3. - Acceso a la información publicada.**

La Autoridad de Aplicación brinda acceso irrestricto y gratuito a toda la información contenida en el repositorio y establece controles adecuados para restringir la posibilidad de escritura y modificación de la información publicada, garantizando su integridad.

**2.5. - Auditorías**

Se encuentra estipulado en la Política de Certificación, legislación y reglamentación vigente.

**2.6. - Confidencialidad**

A los efectos de la determinación del carácter de confidencial de la información recibida por la Autoridad de Aplicación se estará a los recaudos previstos de acuerdo con lo establecido en la Ley N° 1682/2011 "Que Reglamenta la Información de Carácter Privado" y su modificatoria la Ley N° 1969/2002 y la normativa vigente inherente.

**2.6.1. - Publicación de información sobre los Prestadores de Servicios de Certificación**

Las siguientes informaciones referidas a los Prestadores serán publicadas por la Autoridad de Aplicación:

- a) Identificación, domicilio y formas de contacto
- b) Información sobre las Auditorías realizadas al Prestador de Servicios de Certificación en los casos que hubiere.
- c) Resoluciones que habiliten, revoquen o denieguen a los Prestadores de Servicios de Certificación.
- d) La publicación referida a su certificado.

**2.6.2. - Publicación de información sobre la revocación o suspensión de un Prestador de Servicios de Certificación**

La información referida a la revocación de un certificado no se considera confidencial y será publicada por la Autoridad de Aplicación a través de su Lista de Certificados Revocados, disponible en el sitio [www.acraiz.gov.py/arl/ac\\_raiz\\_py.crl](http://www.acraiz.gov.py/arl/ac_raiz_py.crl) La información sobre el estado de suspensión de un Prestador de Servicios de Certificación es competencia de la Autoridad de Aplicación, y su tratamiento se estipula en la Política de Certificación.



Abog. Silvia Santarini Florentín  
Secretaria General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL  
PARAGUAY.**

- 10 -

**2.6.3. - Divulgación de información a autoridades judiciales**

La información que la Autoridad de Aplicación tenga en carácter de secreta o confidencial dejará de serlo ante un requerimiento de la Justicia en el marco de un Proceso Judicial con orden judicial de por medio.

**2.6.4. - Divulgación de información por solicitud del Prestador de Servicios de Certificación**

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del Prestadores de Servicios de Certificación o de cualquier otra información generada o recibida durante el ciclo de vida del certificado, solo se hará efectiva previa autorización de dicho Prestador. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público.

**2.6.5. - Otras circunstancias de divulgación de información**

Excepto en los casos previstos en los apartados anteriores, toda información en poder de la Autoridad de Aplicación con relación a los Prestadores de Servicios de Certificación solo podrá ser divulgada previa autorización de los mismos.

Esta restricción no se aplica para la información que haya sido obtenida de fuentes públicas.

**2.7. - Derechos de Propiedad Intelectual**

La Autoridad de Aplicación mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la presente documentación y aplicaciones pertenecientes a ella.

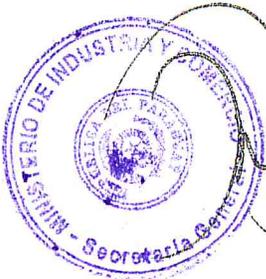
**3 - Identificación y Autenticación**

**3.1 – Registro Inicial**

En el contexto de la presente Declaración de Prácticas de Certificación, la Identificación y Autenticación de los datos del solicitante comprende el proceso que va desde que el Prestador de Servicios de Certificación, se presenta ante la Autoridad de Aplicación para solicitar su habilitación hasta la solicitud del Certificado. La Autoridad de Aplicación validará la identidad del Prestador de Servicios de Certificación y lo habilitará.

Los certificados para los Prestadores de Servicios de Certificación son emitidos bajo la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay y de acuerdo a la presente Declaración de Prácticas de Certificación.

Abog. Silvia Santander Florentín  
Secretaría General





MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.**

- 11 -

El Prestador de Servicios de Certificación será habilitado mediante Resolución dictada por la Autoridad de Aplicación.

Los certificados emitidos por la Autoridad de Certificadora Raíz del Paraguay de acuerdo a la Política de Certificación y la presente Declaración de Prácticas de Certificación habilitan tecnológicamente para que puedan operar los Prestadores de Servicios de Certificación como Autoridades de Certificación subordinadas de la Autoridad Certificadora Raíz del Paraguay dentro de la cadena de confianza de la PKI Paraguay.

No se permite en el contexto de la PKI Paraguay la existencia de una Autoridad Certificadora del Prestador de Servicios de Certificación subordinada a ella.

**3.1.1 – Formato de la Denominación**

El Prestador de Servicios de Certificación debe elegir el nombre con el que va operar; el cual deberá ser aprobado por la Autoridad de Aplicación.

El nombre de la Prestadora de Servicios de Certificación utilizará el campo Subject del Certificado emitido por la Autoridad Certificadora Raíz del Paraguay y deberá cumplir el estándar de la Unión Internacional de Telecomunicaciones UIT X.509.V3 (Subscriber DN Distinguished Name).

Se aplicará el formato de la siguiente manera:

- CommonName: Nombre Distintivo elegido por el Prestador
- Country: PY
- Organization: Nombre del Prestador de Servicios.

**3.1.2 - Validación Inicial de Identidad**

La existencia de la entidad que solicita ser Prestador de Servicios de Certificación se demostrara con las documentaciones pertinentes.

La Autoridad de Aplicación en su función de Registro validara la identidad del solicitante antes de la habilitación y emisión del certificado.

**3.1.2.1 – Identidad**

La persona física designada por el Prestador de Servicios de Certificación para tramitar la habilitación y la emisión de un certificado, deberá demostrar ante la Autoridad Aplicación su identidad, de la siguiente forma:



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.**

- 12 -

- a) nombres y apellidos,
- b) documento de identidad.
- c) documentación respaldatoria de la representación que ostenta, extendida por el Prestador de Servicios de Certificación.
- d) requisitos documentales establecidos en la normativa vigente y los reglamentados por la Autoridad de Aplicación (Habilitación)

**3.1.2.2 – Habilitación**

Cumplidos los requisitos necesarios y los procedimientos para la habilitación de un Prestador de Servicios de Certificación; la Autoridad de Aplicación deberá emitir resolución aprobando o denegando la solicitud de habilitación. En caso de aprobación se lo habilitará a la persona jurídica a ser Prestador de Servicios de Certificación y podrá operar en el País en el marco de la Infraestructura de Clave Pública – PKI Paraguay.

**3.1.2.3 - Clave privada**

Se cumplirá con lo estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay para este punto, designándose el/los funcionario/s de la Autoridad de Aplicación para presenciar el acto de generación de Claves

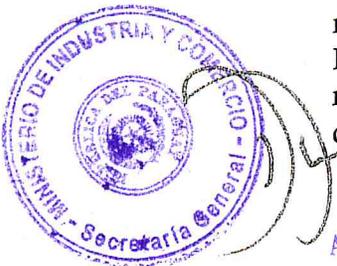
**3.1.3 - Solicitud de Cambio de Clave**

No está permitido el cambio de clave pública y privada del certificado conforme el Punto 4.1.5 de las Políticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**3.1.4 - Solicitud de Revocación**

Para la revocación de un Certificado emitido por la Autoridad Certificadora Raíz del Paraguay, el Prestador de Servicios de Certificación deberá presentar la solicitud de revocación ante la Autoridad de Aplicación

La solicitud de revocación contendrá las causales y motivos del pedido de revocación, y la Autoridad de Aplicación se expedirá al respecto aprobando o denegando la solicitud de revocación teniendo en consideración la normativa vigente.



Abog. Silvia Santaró Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

160.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 13 -

**4 - Ciclo de Vida de los Certificados**

En esta sección se declaran los controles que realiza la Autoridad de Aplicación para asegurar una gestión segura del Ciclo de Vida de los Certificados emitidos, y también se especifican controles que los Prestadores de Servicios de Certificación, como suscriptores de esos certificados, deben considerar.

**4.1 - Solicitud de Certificado**

El Prestador de Servicios de Certificación solicita la emisión de un certificado ante la Autoridad de Aplicación presentando la información requerida.

La Autoridad de Aplicación verificará que la generación de las claves satisfaga los requerimientos de seguridad y controles estipulados en la presente Declaración de Prácticas de Certificación.

Para solicitar el certificado, el Prestador de Servicios de Certificación genera las claves de su Autoridad Certificadora en presencia del/los funcionario/s de la Autoridad de Aplicación, y genera una solicitud en formato de archivo CSR (PKCS). Dicha solicitud debe contener únicamente la clave pública generada y los datos del DistinguishedName de la Autoridad Certificadora del Prestador de Servicios de Certificación, de acuerdo a lo estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay. El CSR es entregado al funcionario de la Autoridad de Aplicación en un medio removible autorizado y por él provisto, de forma de continuar con el proceso de emisión.

**4.2 - Procesamiento de Solicitud de Certificado**

La emisión del certificado deberá generarse en un ambiente seguro y de acuerdo con los requerimientos establecidos en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

La Autoridad Certificadora Raíz deberá verificar que:

- La información contenida en el archivo CSR es consistente con la Resolución de habilitación dictada por la Autoridad de Aplicación.

• El archivo CSR se encuentra firmado con la clave privada correspondiente a la clave pública en él contenida.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1106.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 14 -

- Existen pruebas de que la clave privada generada está bajo absoluto control del Prestador de Servicios de Certificación y que además fue generada de acuerdo a los requerimientos estipulados en la presente Declaración de Prácticas y en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay. Para este punto es suficiente una declaración de conformidad por parte del funcionario designado para presenciar la generación o por los auditores designados para tal tarea.
- El archivo CSR contiene los campos necesarios especificados para la generación del certificado, conforme a lo estipulado en el punto 7 de la Política de Certificación de Autoridad Certificadora Raíz del Paraguay.

En caso de cumplirse con todas las formalidades y verificaciones se inicia el proceso de emisión del certificado.

#### 4.3 - Emisión de Certificado

La emisión del certificado se realiza en las instalaciones de la Autoridad de Aplicación, y deberá ser realizado por el personal técnico especializado y autorizado para dichos fines.

El período de validez del certificado emitido debe ser de diez (10) años, excepto que sea revocado con anterioridad a la fecha de expiración.

Sin perjuicio de lo señalado, la evolución tecnológica puede determinar una regulación específica de la Autoridad de Aplicación, por lo que esta emisión no implica la constitución de derechos adquiridos por todo el período.

El certificado emitido es retirado del sistema donde fue generado en un dispositivo removible provisto por la Autoridad de Certificación Raíz del Paraguay. Este dispositivo es entregado al representante del Prestador de Servicios de Certificación, dejando una constancia formal del acto mediante la firma del Acuerdo para Suscriptores. Una copia del certificado es almacenada en el directorio de certificados de la Autoridad Certificadora Raíz del Paraguay. Esta copia no es publicada en el repositorio de información durante esta instancia.



Abog. Silvia Sanzander Florentín  
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 15 -

**4.4 - Aceptación del Certificado**

El/los funcionario/s a cargo de la emisión del certificado se dirigirán a las instalaciones del Prestador de Servicios de Certificación y entregaran personalmente el medio removible que contiene el certificado. Al momento de entrega del certificado, el Prestador de Servicios de Certificación procede a la aceptación del mismo. Verificara que la información contenida en el certificado y la firma de la Autoridad Certificadora Raíz del Paraguay sean correctas. En caso de que el Prestador acepte el certificado, deberá entregar a la el Acuerdo de Suscriptores firmado por su representante legal en un plazo no mayor a veinticuatro horas y luego se procederá a la instalación del certificado en su infraestructura en presencia del/los funcionario/s de la Autoridad de Aplicación que lo entregó. En caso contrario, se procede a la revocación del mismo dependiendo de la magnitud de la discordancia.

La Autoridad de Aplicación publicara el certificado emitido, junto a la información de contacto del Prestador de Servicios de Certificación Habilitado, en su repositorio público de información. A partir de dicha instancia se considera válida la operación del Prestador de Servicios de Certificación.

**4.5 - Uso del Certificado y del Par de Claves**

Se encuentra estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**4.6 - Renovación del Certificado**

El Prestador de Servicios de Certificación debe solicitar la emisión de un nuevo certificado ante la Autoridad de Aplicación con una antelación máxima de 6 a 12 meses antes de que expire el certificado que posee, adjuntará a dicha solicitud la constancia del certificado emitido con anterioridad y constancia de habilitación como Prestador de Servicios de Certificación.

Para la renovación del certificado se deberá generar un nuevo par de claves en todos los casos. Otros requisitos para la renovación están estipulados en el punto 4.5 de la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**4.7 - Cambio de Clave del Certificado**

No se realizaran en ningún caso cambios de clave de Certificados. Debe en su lugar aplicarse los procedimientos de revocación y emisión de un nuevo certificado, en el mencionado orden.



Abog. Silvia Santander Florentín  
Se

*[Handwritten signature]*



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

1166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 16 -

**4.8 - Modificación del Certificado**

No se realizan modificaciones de certificados. Para estos casos el titular deberá solicitar primero una revocación del certificado en vigor y posteriormente la solicitud de un nuevo certificado.

**4.9 - Suspensión y Revocación del Certificado**

**4.9.1 - Revocación del Certificado**

Se deberá agregar a la Lista de Certificados Revocados el identificador del certificado revocado y la fecha de revocación.

Las causales para la revocación del certificado están estipuladas en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

Se procederá a la revocación del certificado del Prestador de Servicios de Certificación en el caso q se constate que la misma ha incurrido en alguna de las causales de revocación.

El proceso de revocación del certificado y la publicación de la nueva Lista de Certificados Revocados se realiza en un plazo no mayor a veinticuatro horas (24) a partir de la aprobación de la solicitud de revocación,

Se dispondrá de un funcionario de la Autoridad de Aplicación para presenciar el proceso de revocación efectiva de todos los certificados emitidos por el Prestador de Servicios de Certificación, así como del proceso de destrucción efectiva de la clave privada asociada a la misma.

**4.9.2 - Suspensión del certificado**

No se realizará en ningún caso suspensiones de los Certificados.

Por otro lado la suspensión administrativa de un Prestador de Servicios de Certificación se deberá realizar conforme al procedimiento establecido, impidiendo que el Prestador siga operando durante el periodo de suspensión, en tal caso se procederá a la revocación de su certificado.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución Nº

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.**

- 17 -

**4.10 - Servicio de Estado de los Certificados**

La Autoridad de Aplicación publicara los certificados emitidos, así como también la Lista de Certificados Revocados para su consulta online en el sitio oficial. La Autoridad de Aplicación no se responsabiliza por ningún tipo de incidente que derive de una falta de verificación de la Lista de Certificados Revocados en el momento de validación de un certificado por parte de los terceros aceptantes. Este servicio de publicación de información estará disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema o de sufrir inconvenientes deberán ser solucionados en un plazo no mayor a 48hs. La Autoridad de Aplicación dedicará sus mejores esfuerzos para que el servicio se encuentre disponible rápidamente.

El Repositorio del certificado de la Autoridad Certificadora Raíz del Paraguay se encuentra en [www.acraiz.gov.py/crt/ac\\_raiz\\_py.crt](http://www.acraiz.gov.py/crt/ac_raiz_py.crt) y la Lista de Certificados Revocados se encuentra en [www.acraiz.gov.py/arl/ac\\_raiz\\_py.crl](http://www.acraiz.gov.py/arl/ac_raiz_py.crl)

**4.11 - Finalización de los Servicios de Certificación**

En la eventualidad de que la Autoridad Certificadora Raíz del Paraguay finalice sus servicios:

- a) se publicará la fecha de finalización por lo menos con noventa (90) días de antelación en el Sitio Oficial de la Autoridad Certificadora Raíz del Paraguay y deberá también publicar, la fecha de suspensión de servicios, por el plazo de 3 días consecutivos en un diario de gran circulación 10 días hábiles antes de la suspensión efectiva;
- b) se notificará a los Prestadores de Servicios de Certificación habilitados con al menos sesenta (60) días de antelación a la fecha del cese;
- c) se procederá a la revocación de todos los certificados emitidos que se encuentren vigentes a la fecha de terminación;
- d) se procederá a la destrucción de la clave privada de la Autoridad Certificadora Raíz del Paraguay mediante un mecanismo que impida su reconstrucción.

Los Prestadores de Servicios de Certificación, como suscriptores, no podrán continuar utilizando certificados emitidos por la Autoridad Certificadora Raíz del Paraguay y los terceros aceptantes no deberán confiar en ellos.



Abog. Silvia Santander Florentín  
Secretaría de Asesoría Legal



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1160.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 18 -

El procedimiento para el cese de actividades de un Prestador de Servicios de Certificación está estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**5 – Controles de Seguridad Física, De Procedimiento y de Personal**

El objetivo de los controles de seguridad física, los controles de los procedimientos y del personal tienen como objetivo mantener un ambiente seguro y controlado para la protección de la Clave Privada de la Autoridad Certificadora Raíz del Paraguay, la información de los Prestadores de Servicios Certificación, el ciclo de vida de los certificados emitidos etc. Para esto, se contará con un Sistema de Gestión de la Seguridad de la Información, con Políticas y Procedimientos para garantizar la seguridad en sus operaciones. Dicho Sistema de Gestión de Sistemas de Información está alineado y se ajusta a las buenas prácticas ISO 27002, el cual está enfocado a proteger el material criptográfico involucrado en el ciclo de vida de los certificados de la Autoridad Certificadora Raíz del Paraguay y de los Prestadores de Servicios de Certificación.

**5.1 - Controles de seguridad física**

La Autoridad de Aplicación implementa las siguientes medidas de seguridad para la protección física de las instalaciones donde se encuentran los sistemas informáticos y equipos asociados al ciclo de vida de los certificados emitidos:

- a) Delimitación de las áreas seguras e inseguras en las instalaciones donde se procesan o almacenan claves criptográficas y certificados;
- b) medidas para impedir el acceso no autorizado a las instalaciones a través de puertas, ventanas y muros; c) medidas de control de acceso físico que permiten identificar y autorizar a los individuos que ingresan y egresan a la institución (lectores biométricos, tarjetas de aproximación, guardias de seguridad);
- d) medidas restrictivas para el acceso a las áreas seguras dentro de la institución (ingreso del mínimo personal requerido);
- e) medidas de detección del acceso en áreas vacantes (sensores de movimientos, alarmas, cámaras de video);
- f) medidas para el control de la temperatura del equipamiento en funcionamiento;
- g) medidas de protección contra incendios (detectores de humo, extintores de polvo);
- h) medidas de protección contra inundaciones;
- i) utilización de cerraduras y racks cerrados para la protección de sistemas e información crítica.

Abog. Silvia Soriano Florentín  
Secretaría





MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1166

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 19 -

Para la protección del equipamiento de las áreas de trabajo, se implementan las siguientes medidas:

- a) Inventario actualizado de los sistemas y medios de almacenamiento de la organización;
- b) procedimientos para el ingreso y egreso a los sistemas y a la institución que requieren la aprobación explícita de los niveles gerenciales;
- c) procedimientos para la destrucción física de medios de almacenamiento;
- d) política de escritorios limpios, retirando de las áreas de trabajo aquella información que no esté siendo utilizada;
- e) separación entre los ambientes de producción, respaldo y pruebas;
- f) copias de seguridad periódicas almacenadas en instalaciones geográficamente distantes y bajo las mismas medidas de protección.

**5.2 - Controles Procedimentales**

Para evitar que una sola persona pueda llevar a cabo operaciones sensitivas, se requiere para misma la participación concurrente de varias personas con diferentes roles. Se pueden identificar los siguientes roles en la operativa de la Autoridad Certificadora Raíz del Paraguay:

**Gerente de Sistemas** – Es el responsable de las decisiones de diseño y planificación de la infraestructura tecnológica para el soporte de las actividades de la autoridad certificadora. Se encarga de aprobar la incorporación de equipamiento, dispositivos de red y medios de almacenamiento, así como de software a ser utilizado durante el ciclo de vida de los certificados. El Gerente de Sistemas tiene también la responsabilidad de aprobar los procedimientos administrativos y técnicos destinados a mitigar los riesgos de seguridad asociados a la operativa. Además, define y aprueba el control de acceso lógico a los sistemas de información.

**Administrador de Sistemas y Redes** – Es el encargado de administrar los sistemas y dispositivos de comunicación. Ejecuta los procedimientos de instalación de software, instalación de dispositivos, configuración de sistemas.

**Oficial de seguridad** – Se encarga de dar soporte a la aplicación de los procedimientos administrativos definidos y asegurar su cumplimiento. Brinda apoyo a las decisiones gerenciales que impliquen cambios en el control del acceso, incorporación de equipamiento o cambios en el software. Realiza un seguimiento y participa durante el desarrollo de los planes de capacitación sobre seguridad de la información al personal de la organización.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL  
PARAGUAY.**

- 20 -

**Auditor** – Tiene la función de controlar a través de registros de auditoría el cumplimiento con los procedimientos desarrollados. El rol de auditor está asignado a un individuo neutral e independiente de la organización.

**Operador** - Se encarga de la operación de los sistemas, ejecutando los procedimientos de emisión y revocación de certificados, emisión de CRL, etc. Para aquellas tareas críticas como la gestión de la clave privada de la autoridad certificadora, se implementan medidas de división del conocimiento y contraposición de intereses.

### 5.3 - Seguridad asociada al Personal

La Autoridad Certificadora Raíz del Paraguay cumple con los siguientes requerimientos de seguridad asociados al Personal:

- procedimientos para la incorporación de personal que permiten comprobar sus credenciales, referencias, antecedentes laborales y antecedentes judiciales (exclusivamente mediante el certificado de antecedentes judiciales que expide la Corte Suprema de Justicia);
- comunicación al individuo contratado o reasignado cual será su rol y responsabilidades dentro de la dirección;
- exigencia al individuo contratado o reasignado la aprobación y cumplimiento de las políticas de seguridad y de los acuerdos de confidencialidad;
- planes de capacitación periódicos en seguridad de la información (específicos para cada rol) para todo el personal de la organización;
- procedimientos para el retiro de personal de la organización.

### 5.4 – Registros de Eventos

La Autoridad de Aplicación tiene definida una política de registros de eventos que define qué operaciones se registran y cómo se garantiza la integridad de esos registros.

Se registran todas las actividades relativas a la gestión de claves (generación, destrucción, activación, etc.), a la gestión de certificados (emisión, revocación, renovación) y a la emisión de la Lista de Certificados así como también las actividades diarias de la Autoridad de Aplicación (reglamentación, acuerdos, resoluciones, auditorías etc.). Todos los registros se almacenan con la fecha en que fueron generados o realizados, los objetos afectados, el resultado de dicha operación y la identificación del/los autores. Los registros se almacenan de tal forma que se asegura su disponibilidad e integridad, impidiendo la modificación indebida, eliminación y su lectura.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 21 -

**5.5 – Retención de Registros e Información**

Cada tipo de registro tiene definido el tiempo de retención. Los registros relativos a la gestión de claves y de certificados deberán mantenerse por un periodo de 12 años. Los Registros relativos a otras actividades deben mantenerse por al menos dos años

No obstante los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay son mantenidos en su directorio público por tiempo indefinido, incluso luego de su expiración y/o revocación, para permitir a terceros validar las firmas que fueron realizadas con ellos. Los datos proporcionados por el titular del certificado deberán ser conservados indefinidamente por los Prestadores cualquiera sea el estado en que se encuentre el Certificado.

**5.6 – Cambio de Claves**

No se realizara en ningún caso el cambio de claves de un certificado

**5.7 – Continuidad de Operaciones**

La Autoridad Certificadora Raíz del Paraguay tiene definidos planes de contingencia para la continuidad del servicio y recuperación ante desastres o siniestros, que le permitirán continuar con su operativa en la eventualidad de fallas de equipamiento y/o siniestros. Estos planes contienen un análisis de riesgos de interrupción del servicio y las estrategias de recuperación propuestas, así como también las ventanas máximas de interrupción aceptables. Los servicios de publicación de la Lista de Certificados Revocados y certificados emitidos por la Autoridad Certificadora Raíz del Paraguay estarán disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema o de sufrir inconvenientes deberán ser solucionados en un plazo no mayor a 48hs. La Autoridad de Aplicación dedicará sus mejores esfuerzos para que el servicio se restablezca y esté disponible rápidamente.

**6 – Controles de Seguridad Técnica**

Los controles técnicos descriptos en esta sección tienen el objetivo de proteger el par de claves de la Autoridad Certificadora Raíz del Paraguay durante su ciclo de vida. Se especifican además medidas generales para la protección de los sistemas de información que dan soporte tanto a las actividades de la Autoridad Certificadora Raíz del Paraguay y la Autoridad de Certificación del Prestador de Servicios de Certificación.



Abog. Silvia Santander Florentín  
Secretaría General

ES COPIA DEL ORIGINAL



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N°

166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 22 -

**6.1 – Instalación de equipamiento**

**6.1.1 – Autoridad Certificadora Raíz del Paraguay**

La emisión del Certificado Digital de la Autoridad Certificadora Raíz del Paraguay se realizó durante la "Ceremonia de Generación de Claves" de la misma. Durante dicho evento se procedió a la puesta en marcha de los sistemas tecnológicos de producción y los requerimientos de atestigüamientos, que se detallan en el punto 6.2.1 de la presente Declaración de Prácticas de Certificación.

**6.1.2 – Prestador de Servicios de Certificación**

El sistema tecnológico que implementan los Prestadores de Servicios de Certificación, deberán instalarse y configurarse en presencia de personal especializado y autorizado por la Autoridad de Aplicación asegurando el cumplimiento de las buenas prácticas de los estándares internacionales en lo que se refiere a las Políticas de Seguridad técnica, física etc, del manejo de la información y su correcta implementación

**6.2 – Generación e Instalación del par de claves**

**6.2.1 – Autoridad Certificadora Raíz del Paraguay**

El par de claves del Certificado Digital de la Autoridad Certificadora Raíz del Paraguay fue generado durante la "Ceremonia de Generación de Claves". Dicha ceremonia se llevó a cabo en las instalaciones designadas por la Autoridad de Aplicación, conforme a la presente Declaración de Prácticas de Certificación y de acuerdo a lo estipulado en el Guión de la Ceremonia de Claves.

**6.2.2 – Prestador de Servicios de Certificación**

El Prestador de Servicios de Certificación deberá elaborar un guión detallado de las actividades a realizar para poner en marcha su Autoridad Certificadora, incluyendo la generación de claves y deberá realizar la instalación en forma auditada y de acuerdo a dicho guión.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1166

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 23 -

Se deberá cubrir todo el proceso de instalación: sistema operativo, aplicaciones de la Autoridad Certificadora, configuración de las aplicaciones, generación y respaldo de claves, generación del CSR, instalación del certificado luego de emitido por la Autoridad Certificadora Raíz y puesta en funcionamiento final de las funcionalidades de gestión de certificados y servicios de estado

El acto de generación del par de claves para la Autoridad Certificadora del Prestador de Servicios de Certificación se realiza en las instalaciones de dicho Prestador, en presencia de funcionario/s designado/s por la Autoridad de Aplicación, y de acuerdo a los requerimientos estipulados por la presente Declaración de Prácticas de Certificación.

**6.3 – Protección de clave privada y controles de Módulos Criptográficos**

Se deberá cumplir lo estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

La protección de la clave privada se realiza en un módulo HSM que cumple con la normativa estipulada en la Política de Certificación. La clave privada de la Autoridad Certificadora Raíz del Paraguay se encuentra siempre dentro del HSM.

El retiro de la clave privada de los HSM se realiza únicamente para procedimientos de backup y procedimientos de cambio de módulos criptográficos. Estos procedimientos son aprobados y controlados por la Autoridad de Aplicación.

Una vez que el certificado digital de la Autoridad de Certificadora Raíz del Paraguay expira, se procede a la destrucción de la clave privada. La destrucción se realiza con un mecanismo que impide su recuperación. El HSM utilizado provee funciones para la eliminación segura de la clave privada.

**6.4 – Otros aspectos de gestión de claves**

La Autoridad Certificadora Raíz del Paraguay mantiene un archivo de todos los certificados emitidos incluido su propio certificado, de esa manera es posible validar las cadenas de confianza de PKI Paraguay para cualquier instante de tiempo.

El período máximo de validez del certificado de la Autoridad de Certificadora Raíz del Paraguay es de veinte (20) años. El período máximo de validez del par de claves es el de su certificado; transcurrido dicho período o en caso de revocación del certificado, la clave privada correspondiente a la clave pública contenida en el certificado es eliminada.



Abog. Silvia Santander Florentín  
Secretaría General



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1166.-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 24 -

**6.5 – Datos de activación**

La Autoridad Certificadora Raíz del Paraguay entiende los procesos de activación y desactivación de la clave privada, de acuerdo a la definición dada para ellos en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

Para la activación de la clave privada del certificado de la Autoridad Certificadora Raíz del Paraguay se requiere la participación de varios individuos (custodios) cada uno con una función específica y establecida, impidiendo así que un individuo por sí solo tenga el conocimiento suficiente para activar la clave privada.

La clave privada se activa al iniciar el sistema para emitir una Lista de Certificados Revocados o un Certificado digital. Para el caso de la desactivación se realiza tras la emisión de la CRL o del certificado.

**6.6 – Seguridad tecnológica**

La Autoridad Certificadora Raíz del Paraguay implementa las políticas, los estándares y los procedimientos que permiten una operación segura.

Se establecen los siguientes aspectos:

- a) Definición de roles y responsabilidades;
- b) Clasificación de la información;
- c) Seguridad vinculada a los recursos humanos;
- d) Seguridad lógica de los sistemas y redes;
- e) Control del acceso;
- f) Seguridad física del ambiente y de los sistemas;
- g) Gestión de respaldos;
- h) Continuidad de la operativa y disponibilidad;
- i) Registros de auditoría;
- j) Respuesta a incidentes.

Estos controles son objeto de regulación por parte de la Autoridad de Aplicación.

**6.7 – Controles de seguridad sobre el ciclo de vida de los sistemas**

Existe un inventario actualizado con los sistemas de información y medios de almacenamiento asociados a la operativa de la Autoridad Certificadora Raíz del Paraguay. Todos los medios a ser incorporados, retirados o trasladados fuera de las fronteras están sujetos a previa autorización de la Autoridad de Aplicación, en procedimientos definidos para ello.

Abog. Silvia Sandoval Florentín  
Secretaría





MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 1166

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL  
PARAGUAY.**

- 25 -

Dicho inventario es mantenido en forma privada, y revelado sólo a los encargados de la auditoría, es decir, no forma parte de la información a publicar.  
Estos controles son objeto de regulación por parte de la Autoridad de Aplicación.

**6.8 – Fecha y Hora de la emisión del certificado**

La Autoridad Certificadora Raíz de Paraguay y la Autoridad Certificadora del Prestador de Servicio de Certificación deberán utilizar la fecha y hora oficial de la República del Paraguay al momento de emitir los certificados (las mismas serán ajustadas manualmente en los respectivos servidores mientras no se cuente con una Autoridad de Estampo Tiempo)

La sincronización horaria es objeto de control de las auditorías periódicas.

**7 – Perfil de certificados y de Listas de certificados revocados**

**7.1 Perfil de certificado de la Autoridad Certificadora Raíz**

Se encuentra estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**7.2 Perfil del Certificado del Prestador de Servicios de Certificación**

Se encuentra estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**7.3 Perfil de Listas de Certificados Revocados de la Autoridad Certificadora Raíz del Paraguay**

Se encuentra estipulado en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**8 – Administración Documental**

**8.1 – Procedimiento para modificaciones**

La Autoridad de Aplicación cuenta con procedimientos internos para la administración de los cambios a la presente Declaración de Prácticas de Certificación.



Abog. Silvia Santandrea Florentín



MINISTERIO DE INDUSTRIA  
Y COMERCIO

Resolución N° 166-

**POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS DE  
CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL  
PARAGUAY.**

- 26 -

**8.2 – Procedimientos de Publicación y Notificación**

Se publican en el sitio web de la Autoridad de Aplicación las modificaciones y actualizaciones de la presente Declaración de Prácticas de Certificación. Se publicara la nueva versión en un plazo no mayor a 24 horas.



Abog. Silvia Sarralde Florentín  
Secretaría General

ES COPIA FIEL DEL ORIGINAL