

Firma

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

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

ANEXO

1 INTRODUCCIÓN

1.1 Descripción General

En el marco de la Ley N° 4017/2010, reglamentada por el Decreto N° 7.369/2011 y la Ley N° 4610/2012, se reconoce la validez jurídica de la firma Electrónica, la Firma Digital, los Mensajes de Datos y el Expediente Electrónico.

Dichas normativas establecen el marco de uso de la Firma Digital; establece y regula a los Prestadores de Servicios de Certificación.

Se establece como Autoridad de Aplicación de las normativas mencionadas al Ministerio Industria y Comercio, el cual como ente regulador debe:

- Administrar la Autoridad Certificadora Raíz del Paraguay.
- Dictar las normas que regulen la Certificación Digital del País.
- Habilitar a los Prestadores de Servicios de Certificación.
- Auditar a los Prestadores de Servicios de Certificación.
- Revocar la habilitación de los Prestadores de Servicios de Certificación.
- Imponer sanciones a los Prestadores de Servicio de Certificación.

En el esquema establecido por la normativa vigente se definen como Prestadores de Servicios de Certificación a las Personas Jurídicas que fueran habilitadas por el Ministerio de Industria y Comercio en base a las disposiciones de las Leyes Nros. 4017/2010 y 4610/2012 y del Decreto N° 7369 que la reglamenta.

Todo Prestador de Servicios de Certificación habilitado deberá contar con un certificado emitido por la Autoridad Certificadora Raíz de Paraguay, generando de esta manera una estructura jerárquica como se muestra en la figura.

Abog. Silvia Santander Florentín
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

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

- 2 -

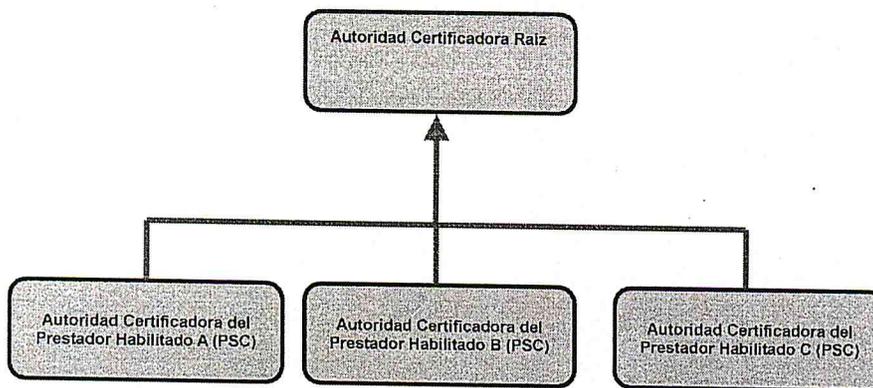


Figura 1 Infraestructura de PKI Paraguay

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.

Dicha Autoridad Certificadora es la raíz de toda la Jerarquía de PKI, cuenta con un certificado autofirmado y aceptado por los Terceros que establezcan confianza en la infraestructura de Clave Pública del Paraguay.

El Ministerio de Industria y Comercio como Autoridad de Aplicación de la normativa vigente habilita tecnológicamente la operación de los Prestadores de Servicios de Certificación (PSC) en la República del Paraguay, emitiendo certificados digitales. De esta manera los Prestadores de Servicio de Certificación pasan a ser parte de la cadena de confianza de la Infraestructura de Clave Pública o Public Key Infrastructure (PKI)

Los certificados emitidos por la Autoridad Certificadora Raíz se rigen por la presente Política de Certificación y por la Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

Los interesados en ser Prestadores de Servicios de Certificación, y los habilitados deberán cumplir con los requisitos y disposiciones establecidos en las Leyes N° 4017/2010 y N° 4610/2012, en el Decreto Reglamentario N° 7369/2011, las resoluciones y demás disposiciones reglamentarias dictadas por la Autoridad de Aplicación.



Abog. Silvia Santacruz Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 3 -

El presente documento contiene la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay administrada por el Ministerio de Industria y Comercio a través del Viceministerio de Comercio. Contiene los principios y reglas relativas a la emisión y gestión de Certificados Digitales, establece las reglas mínimas que deben cumplir los Prestadores de Servicios de Certificación y los usuarios finales, el uso de los certificados entre otras reglamentaciones más.

Los Prestadores de Servicios de Certificación deben contar con una Política de Certificación y Declaración de Practicas de Certificación con relación a los procedimientos que aplican en la prestación de sus servicios, emisión y gestión de los certificados que deberá estar en concordancia con la presente política y con la normativa vigente.

1.2 Identificación de la Política de Certificación

Nombre: Política de Certificación de la Autoridad de Certificación Raíz del Paraguay

Versión: 1.0

Fecha de elaboración:

Fecha de última actualización:

Sitio web de publicación: www.acraiz.gov.py/documentacion/politicas.pdf

1.3 Participantes de la Infraestructura de Clave Pública - PKI Paraguay

1.3.1 Autoridad de Aplicación – Función de Regulación.

Conforme a la Ley N° 4610/2012 se establece como Autoridad de Aplicación al Ministerio de Industria y Comercio a través del Viceministerio de Comercio.

El Ministerio de Industria y Comercio en su carácter de ente Regulador tendrá las siguientes funciones:

- Dictar las normas y reglamentos.
- Establecer los estándares tecnológicos y operativos de la implementación de las leyes N° 4017/2010 y 4610/2012.
- Autorizar, conforme al Artículo 26 y siguientes de la Ley 4017/2010, Art. 7 y siguientes del Decreto Reglamentario N° 7.369/2011 y de más reglamentaciones, la habilitación de los Prestadores de Servicios de Certificación en el territorio nacional.



Abog. Silvia Santómer Florentín



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 1165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 4 -

- d) Velar por el adecuado funcionamiento y la eficiente prestación de servicio por parte de los Prestadores de Servicios de Certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad.
- e) Efectuar auditorías e inspecciones a los Prestadores de Servicios de Certificación.
- 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.
- 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 (P.S.C.) 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 (P.S.C) por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación de servicio.
- k) Otorgar o revocar las licencias a los Prestadores de Servicios de Certificación y supervisar su actividad, según las exigencias establecidas por la reglamentación.
- l) Homologar los dispositivos tecnológicos de creación y verificación de firmas digitales con ajuste a las normas y procedimientos establecidos por la reglamentación.
- m) Imponer y aplicar las sanciones establecidas en la normativa vigente.
- n) Mantener un registro público de Prestadores de Servicios de Certificación habilitados de conformidad a lo establecido en el Artículo 10 del Decreto N° 7369/2011

1.3.2 Autoridad de Aplicación – Función de Registro.

Las funciones de Registro, son parte de los servicios de una Autoridad de Certificación que consiste en iniciar el proceso de emisión, renovación y revocación de certificados bajo las Políticas de Certificación y Declaraciones de Prácticas de Certificación definidas así como de la normativa vigente.

La Autoridad de Aplicación, como Autoridad de Registro debe desempeñar las siguientes funciones:

- a) Iniciar el proceso de emisión del certificado digital para cada Prestador de Servicios de Certificación, de acuerdo a lo establecido en el punto 4.1 de la presente Política;
- b) Iniciar el proceso de revocación de los certificados digitales emitidos por la Autoridad Certificadora Raíz del Paraguay para los prestadores los Prestadores de Servicios de Certificación, de acuerdo a lo establecido en el punto 4.10 de la presente Política;

Abog. Silvia Santander Florentín
Secretaria General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 1165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 5 -

- c) Iniciar el proceso de renovación de certificados digitales emitidos por la Autoridad Certificadora Raíz del Paraguay para los prestadores los Prestadores de Servicios de Certificación, de acuerdo a lo establecido en el punto 4.5 de la presente Política;

1.3.3 Autoridad Certificadora Raíz del Paraguay

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; cuenta con funciones relativas a la gestión de los certificados digitales que habiliten o deshabiliten tecnológicamente a los Prestadores de Servicios de Certificación según lo expuesto en la presente política y la normativa vigente.

Como Autoridad de Certificación, la Autoridad Certificadora Raíz del Paraguay tiene las siguientes funciones:

- a) Emitir, renovar y revocar el Certificado Público de la Autoridad Certificadora Raíz del Paraguay.
- b) Emitir, renovar y revocar los certificados de los Prestadores de Servicios de Certificación de conformidad a la normativa y reglamentación vigente.
- c) Publicar y mantener actualizada la Lista de Certificados Revocados (CRL)
- d) Publicar y mantener actualizado el listado de Prestadores de Servicios de Certificación Habilitados en el País.
- e) Publicar y mantener actualizada la presente Política, la Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Paraguay y las informaciones establecidas en el Punto 2.3 de la presente Política.
- f) Publicar los certificados emitidos a los Prestadores de Servicios de Certificación.

1.3.4. Prestadores de Servicios de Certificación

Los Prestadores de Servicios de Certificación para operar en el País deben ser habilitados por el Ministerio de Industria y Comercio quien es la Autoridad de Aplicación. Su Política de Certificación y Declaración de Prácticas de Certificación deberán también estar aprobadas por la Autoridad de Aplicación, y las mismas deben concordar con la presente Política y con la Declaración de Prácticas de la Autoridad Certificadora Raíz del Paraguay

En el Paraguay, la cadena de Certificación tiene como máximo dos niveles, en el nivel uno se encuentra la Autoridad Certificadora Raíz del Paraguay y en el nivel dos las Prestadoras de Servicios de Certificación que estén habilitadas

Los Prestadores, solo podrán emitir certificados digitales (firma digital) a suscriptores o usuarios finales.



Abog. Silvia Santander Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 6 -

Cada Prestador de Servicios de Certificación Habilitado deberá:

- a) Emitir, renovar y revocar los Certificados Digitales a los usuarios finales que lo soliciten, sin distinción y privilegios, de acuerdo con su Política de Certificación, su Declaración de Prácticas de Certificación y la normativa vigente.
- b) Deberá mantener la infraestructura física y tecnológica necesaria para la operación de su Autoridad Certificadora
- c) Mantener actualizada y publicada su Política de Certificación.
- d) Mantener actualizada y publicada su Declaración de Prácticas de Certificación.
- e) Deberá mantener un repositorio público de documentación el cual contenga como mínimo, la Política de Certificación a la cual se atiene, la Declaración de Prácticas de Certificación, la lista de firmas digitales vigentes y revocadas, información relevante de la última auditoría realizada, resoluciones y cualquier otra información que considere pertinente.
- f) Deberá publicar en forma permanente e ininterrumpida la lista de certificados vigentes y revocados.
- g) Cumplir con las disposiciones establecidas en el Artículo 32 de la Ley N° 4017/2010

1.3.5 Suscriptores

Se considera suscriptores bajo esta Política a todo Prestador de Servicios de Certificación habilitado por el Ministerio de Industria y Comercio a través del Viceministerio de Industria y Comercio.

Es obligación de todo suscriptor el conocimiento y cumplimiento de la presente Política y de la Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Paraguay, 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 bajo la presente Política de Certificación.

Estas Personas o Entidades utilizarán los certificados emitidos por los Prestadores de Servicios de Certificación para validar la cadena de confianza.



Abog. Silvia Santamaría Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

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

- 7 -

1.4 Uso de los certificados

1.4.1 Usos permitidos de los Certificados

Los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay solo podrán ser utilizados por los Prestadores de Servicios de Certificación para el fin para lo cual fueron habilitados.

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

1.4.2 Restricciones en el Uso de los Certificados

Los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay solo podrán utilizarse dentro del marco de la Ley N° 4617/2010, su modificatoria la Ley N° 4610/12, el Decreto Reglamentario N° 7369/2011, de las reglamentaciones de la Autoridad de Aplicación y los usos especificados en el punto 1.4.1 de la presente Política y normativa vigente.

Cualquier otro uso de los certificados no especificado en esta Política de Certificación y en la normativa vigente, está fuera del alcance y responsabilidad de la Autoridad de Aplicación. Asimismo el uso indebido de los certificados deberá ser sancionado por la Autoridad de Aplicación, pudiendo llegar a la revocación del mismo.

1.5 Administración de la Política de Certificación

La administración de la presente Política de Certificación es responsabilidad del Ministerio de Industria y Comercio a través del Viceministerio de Comercio de conformidad a la normativa vigente.

Para consultas o sugerencias, se establece el siguiente contacto:

Nombre: Ministerio de Industria y Comercio
Dirección: España N° 323 casi EE.UU. Asunción - Paraguay
Dirección de correo: info@acraiz.gov.py
Página Web: www.acraiz.gov.py
Teléfono: (+595) (21) 214279

Abog. Silvia Sanabria Florant
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 8 -

1.6 Relación entre la Política de Certificación y otras disposiciones

La presente Política se relaciona con otras disposiciones como leyes, decretos, reglamentaciones, que regulan el servicio de Certificación en el país y la Infraestructura de Clave Publica – PKI Paraguay.

A su vez se relaciona con documentación técnica y de seguridad, basada en Estándares Tecnológicos y Mejores Prácticas Internacionales que guardan relación con la operación de las Autoridades de Certificación.

1.7 Procedimiento de Aprobación y Mantenimiento de la Política de Certificación

La Autoridad de Aplicación, aprobará mediante resolución la presente Política de Certificación y sus posteriores enmiendas o modificaciones. Asimismo, garantiza mediante procedimientos, el correcto mantenimiento de la presente Política de Certificación, la reglamentación que la acompaña entre otras disposiciones.

Cada Prestador de Servicios de Certificación habilitado deberá implementar los procedimientos necesarios para mantener sus Políticas y documentaciones actualizadas y publicadas.

1.8 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 la Infraestructura de Clave Publica - 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 de Servicios de Certificación debe reunir para trabajar con este tipo de certificado. Las Políticas son promovidas, aprobadas y mantenidas por la Autoridad de Aplicación.

Abog. Silvia Santamaría Florentín
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 9 -

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.

Módulo de Hardware de Seguridad (HSM – Hardware Security Module): dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.



Abog. Silvia Sanzanger Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

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

- 10 -

2 ASPECTOS GENERALES

2.1 Obligaciones y Derechos

Las obligaciones que surgen de la presente Política de Certificación son de cumplimiento obligatorio.

2.1.1 Obligaciones de la Autoridad de Aplicación – Función de Regulación

En el marco de la Infraestructura de Certificación Digital de la República del Paraguay son obligaciones del Ministerio de Industria y Comercio como Autoridad de Aplicación conforme al artículo 40 de la Ley 4017/2010:

- a) La elaboración y actualización de la presente Política.
- b) La elaboración y actualización de procedimientos y normas que permitan el correcto funcionamiento de la Infraestructura de PKI del Paraguay.
- c) El estudio y la posterior aprobación o denegación de cambios solicitados a la presente Política.
- d) El estudio y la posterior aprobación o denegación de las solicitudes de los aspirantes a Prestadores de Servicios de Certificación.
- e) La habilitación formal y tecnológica de los Prestadores de Servicios de Certificación.
- f) La revocación formal y tecnológica de los Prestadores de Servicios de Certificación.
- g) La publicación de la lista de Prestadores de Servicios de Certificación Habilitados. Así como también la publicación de los certificados renovados y revocados.
- h) Auditar a los Prestadores de Servicios de Certificación para asegurar que los mismos cumplen con la presente Política y Declaración de Prácticas, con la normativa vigente, y con sus Políticas de Certificación definidas por ellos.
- i) La publicación en el sitio oficial de:
 - o La presente Política y la Declaración de Prácticas de la Autoridad Certificadora Raíz del Paraguay, así como también sus modificaciones.
 - o Certificados emitidos y revocados a los Prestadores de Servicios de Certificación.
 - o La resolución que ordena la habilitación y revocación de los Prestadores de Servicios de Certificación
 - o El Certificado de la Autoridad Certificadora Raíz del Paraguay.

Abog. Silvia Santana Florentín
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 11 -

- j) Mantener y Garantizar la seguridad de la información tratada.
- k) Disponer de un servicio de atención que permita responder a las consultas de los Prestadores de Servicios de Certificación, así como también de la parte que confía.
- l) Atender los requerimientos de revocación de certificados solicitados por los Prestadores de Servicios de Certificación o por una autoridad competente de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación.
- m) Notificar a los Prestadores de Servicios de Certificación de cualquier incidente que pudiera comprometer la clave privada de la Autoridad Certificadora Raíz del Paraguay.
- n) Y demás obligaciones establecidas en el Art. 40 de la Ley 4017/2010.

2.1.2 Obligaciones de la Autoridad Certificadora Raíz del Paraguay

- a) Elaborar y mantener actualizada la Declaración de Practicas de Certificación.
- b) Generar su clave privada según lo pautado en el Guión de Ceremonias de Claves.
- c) Proteger su clave privada.
- d) Emitir y renovar su propio certificado según lo pautado en el Guión de Ceremonias de Claves.
- e) Revocar su propio certificado ante cualquier sospecha real de que se encuentre comprometida la clave privada.
- f) Emitir, revocar y renovar los certificados de los Prestadores de Servicios de Certificación.
- g) La emisión de la Lista de Certificados Revocados (CRL)
- h) Garantizar el acceso permanente y gratuito al sitio de publicación que contiene su propio certificado, certificados emitidos a los Prestadores de Servicios de Certificación y la lista de los certificados revocados.
- i) Mantener y Garantizar la seguridad de la información tratada. (disponibilidad, integridad, o confidencialidad según corresponda).

2.1.3 Obligaciones de la Autoridad Aplicación- Funciones de Registro

- a) Validar la Habilitación formal de un Prestador de Servicios de Certificación que desee ser Habilitado.
- b) Comprobar la validez de la Habilitación para los Prestadores de Servicios de Certificación que solicitan la emisión, revocación o renovación de un certificado;
- c) Procesar las solicitudes de emisión, renovación y revocación de los certificados para los Prestadores de Servicios de Certificación de conformidad a la normativa vigente.
- d) Mantener un Registro Público de Prestadores de Servicios de Certificación, el que deberá contener lo referido en el Artículo 10 del Decreto N° 7369/2011.



Abog. Silvia Santander Florantín
Secr



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 12 -

2.1.4 Obligaciones de los Prestadores de Servicios de Certificación

Son obligaciones de los Prestadores de Servicios de Certificación:

- a) Adjudicar una firma digital a quien lo solicite sin distinciones ni privilegios de ninguna clase, siempre y cuando el solicitante presente los recaudos establecidos a tal efecto.
- b) Desarrollar, mantener y publicar su propia Política de Certificación de conformidad con la presente Política y la normativa vigente.
- c) Desarrollar, mantener y publicar su Declaración de Prácticas de Certificación de conformidad con la presente Política y la normativa vigente.
- d) Publicar su Certificado en su sitio web oficial
- e) Publicar la Lista de Certificado Digitales vigentes y revocadas en su sitio Web Oficial.
- f) Proveer toda la información que le sea requerida de modo completo y preciso referente a la obtención de un certificado digital condiciones precisas de utilización, responsabilidad, efectos etc.
- g) Proteger su clave Privada
- h) Solicitar la inmediata revocación del certificado emitido por la Autoridad Certificadora Raíz del Paraguay en el caso de compromiso o sospecha de su clave privada.
- i) Utilizar su certificado de acuerdo a sus Políticas de Certificación, siguiendo su Declaración de Prácticas de Certificación y de acuerdo a la presente Política y normativa vigente.
- j) Cumplir con las obligaciones establecidas en la presente Política de Certificación y en la normativa vigente.
- k) Cumplir con las obligaciones establecidas en el Artículo 32 de la Ley N° 4017/2010

2.1.5 Obligaciones de Registro de los Prestadores de Servicio de Certificación

Las obligaciones son asumidas por el Prestador de Servicios:

- a) Comprobar la validez de la documentación del usuario final que solicita un certificado digital,;
- b) Procesar las solicitudes de emisión o revocación de certificados emitidos;
- c) Dar aviso a los usuarios finales ante la ocurrencia de un evento que así lo requiera según lo estipulado por la presente Política de Certificación;

Abog. Silvia Santander Florentín
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 13 -

2.2 Responsabilidades

La Autoridad de Aplicación no asume responsabilidad en caso de utilización no autorizada o permitida del certificado, tampoco responde por eventuales inexactitudes en el certificado que resulten de la información facilitada por el Prestador.

De conformidad al Artículo 33 de la Ley N° 4017/2010 "De Validez Jurídica de la Firma Digital, la Firma Electrónica, los Mensajes de Datos y el Expediente Electrónico" los Prestadores de Servicios de Certificación Habilitados por la Autoridad de Aplicación serán responsables por los daños y perjuicios causados a toda persona física o jurídica que confíe razonablemente en el certificado digital por él emitido, en lo que respecta a:

- a) la inclusión de todos los campos y datos requeridos por la ley y a la exactitud de los mismos, al momento de su emisión;
- b) que al momento de la emisión de un certificado reconocido por el prestador de servicios de certificación autorizado, la firma en él identificada obedezca a los datos de creación de las firmas correspondientes a los datos de verificación incluidos en el certificado reconocido por el prestador, con el objeto de asegurar la cadena de confianza;
- c) los errores u omisiones que presenten los certificados digitales que emitan; y,
- d) el registro en tiempo y forma de la revocación de los certificados reconocidos que haya emitido, cuando así correspondiere.

Corresponde al Prestador de Servicios de Certificación demostrar que no actuó ni con culpa ni con dolo.

No obstante, este articulado establece que los Prestadores no serán responsables de los daños y perjuicios causados por el uso que exceda de los límites de las Políticas de Certificación indicados en el certificado, ni de aquéllos que tengan su origen en el uso indebido o fraudulento de un certificado de firma digital.

Tampoco responderá por eventuales inexactitudes en el certificado reconocido que resulten de la información verificada facilitada por el titular, siempre que el Prestador de Servicios de Certificación acreditado pueda demostrar que ha cumplido todas las medidas previstas en sus políticas y procedimientos de certificación.



Abog. Silvia Sanjaider Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 14 -

A los efectos de salvaguardar los intereses de las partes que utilizan los servicios de certificación, el Prestador de Servicios de Certificación deberá contar con un medio de garantía suficiente para cubrir las responsabilidades inherentes a su gestión, entre los que se podría citar: pólizas de seguros, cauciones bancarias o financieras o en fin cualquier sistema que el Reglamento de la presente Ley establezca para el efecto.

Con respecto a la protección de datos personales, los Prestadores de Servicios de Certificación sólo podrán recolectar los datos personales directamente de la persona a quien esos datos se refieran, después de haber obtenido su consentimiento expreso y sólo en la medida en que los mismos sean necesarios para la emisión y mantenimiento del certificado. Los datos no podrán ser obtenidos o utilizados para otro fin, sin el consentimiento expreso del titular de los datos.

2.2.1 Sanción por Infracciones cometidas

En la Ley N° 4610/2012 "Que modifica y amplía la Ley N° 4017/2010", en su Artículo 43 y siguientes se establecen las infracciones de los Prestadores de Servicios de Certificación con sus respectivas sanciones. Las Infracciones son clasificadas en leves, moderadas y graves.

Las sanciones, de acuerdo a la gravedad de las infracciones podrán ir desde 500 a 10.000 jornales mínimos para actividades diversas no especificadas.



Abog. Silvia Santacruz Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 15 -

2.3 Publicación y Repositorios

2.3.1 Publicación de información

La Autoridad de Aplicación dispone del siguiente sitio web como repositorio público de información: www.acraiz.gov.py y cuyo acceso será irrestricto.

La información contenida en dicho sitio web deberá estar disponible las 24hs 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 Ministerio de Industria y Comercio como ente regulador debe publicar la siguiente información:

- a) El certificado de la Autoridad Certificadora Raíz del Paraguay.
- b) Publicación de los certificados habilitados, renovados y revocados.
- c) La Lista de Certificados Revocados de la Autoridad Certificadora Raíz del Paraguay
- d) La presente Política de Certificación y sus posteriores modificaciones.
- e) La Declaración de Prácticas de Certificación y sus posteriores modificaciones.
- f) Los requerimientos de habilitación de un Prestador de Servicios de Certificación.
- g) Las Resoluciones que habilitan, suspenden o revocan a los Prestadores de Servicios de Certificación con las respectivas aclaraciones con respecto a los motivos.
- h) La información relativa de las auditorías realizadas
- i) Identificación, domicilio y medios de contacto de la Autoridad de Aplicación así como también la identificación, domicilio y medios de contacto de los Prestadores de Servicios de Certificación habilitados
- j) Leyes, Decretos, Reglamentos y Normativas que rigen la actividad de la Infraestructura de Certificación de Clave Publica de la República de Paraguay.



Abog. Silvia Santander Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 16 -

2.3.2 Frecuencia de publicación

Las publicaciones antes mencionadas serán actualizadas lo más pronto posible y 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

2.4 Auditoría

La Autoridad Certificadora Raíz del Paraguay deberá ser auditada periódicamente para asegurar el correcto funcionamiento respecto a la presente Política, las prácticas definidas y la normativa vigente.

De la misma forma la Autoridad de Aplicación deberá auditar a los Prestadores de Servicios de Certificación para garantizar el correcto funcionamiento de la Infraestructura de Certificación y el cumplimiento de la normativa vigente. La disposición o resolución que ordena una Auditoría o Inspección no es recurrible.

Cuando se ordene la suspensión de las actividades del Prestador de Servicios de certificación, como resultado de una Auditoría, el Prestador de Servicios de Certificación sólo podrá realizar servicios de soporte técnico y atención a los usuarios finales ya existentes. En ningún caso podrá seguir brindando servicio de certificación. El incumplimiento de esta disposición será considerado una falta muy grave por parte del Prestador de Servicios de Certificación.

La Autoridad de Aplicación diseñará y aprobará el sistema de auditoría así como también establecerá el arancel correspondiente.

La información relevante de los informes de las auditorías será publicada en el sitio web.



Abog. Silvia Sarmiento Florentín
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 17 -

2.5 Confidencialidad

A los efectos de la determinación del carácter 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° 1969/2012 y la normativa vigente.

2.5.1 Publicación de Información sobre los Prestadores de Servicios de Certificación

La Autoridad de Aplicación hará pública la siguiente información de los Prestadores de Servicios de Certificación:

- a) Identificación, domicilio y formas de contacto
- b) Información sobre la Auditoría realizada 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.

2.5.2 Publicación de Información sobre Revocación de Certificados

La información sobre revocación de certificados de Prestadores de Servicios de Certificación no se considera confidencial y será publicada por la Autoridad de Aplicación mediante su Lista de Certificados Revocados (CRL).

2.5.3 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.

2.5.4 Divulgación de información por solicitud del Prestador de Servicios de Certificación

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.

2.5.5. Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales la Autoridad de Aplicación divulgue información.



Abog. Silvia Santander Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

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

- 18 -

2.6 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.



Abog. Silvia *[Signature]* Carretero
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

1165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 19 -

3 PROCEDIMIENTO PARA LA HABILITACIÓN

3.1 Solicitud

Los interesados en ser Prestadores de Servicios de Certificación deberán efectuar el procedimiento establecido en la legislación vigente y presentar la solicitud de habilitación ante la Autoridad de Aplicación.

El Ministerio de Industria y Comercio habilitara al Prestador de Servicios de Certificación si cumplen con todos los requisitos establecidos en la normativa vigente.

La única prueba fehaciente de dicha habilitación es la Resolución dictada por la Autoridad de Aplicación (Ministerio de Industria y Comercio)

3.2 Solicitud de Habilitación de Entidades Extranjeras y/o Consorciadas con Entidades Nacionales

a) Entidad Extranjera:

La Entidad Extranjera interesada en obtener su habilitación deberá cumplir con los requisitos exigidos por la Ley y el reglamento vigente. Deberá acompañar a dicha solicitud copia autenticada de los documentos que acrediten la identidad, certificado de antecedentes penales para extranjero, certificado de INTERPOL de los representantes legales, y demás documentaciones establecidas en la normativa vigente.

Las entidades extranjeras que deseen ejercer la actividad de certificación digital en el territorio nacional, deberán constituir domicilio en el país; acreditando además que la entidad ha sido constituida como certificadora de acuerdo a las leyes de su país. Asimismo deberán cumplir íntegramente los requisitos contemplados en el Código Civil Paraguayo para las sociedad extranjeras que se constituyan en el País.

El capital mínimo exigido será de 400 salarios mínimos para actividades diversas no especificadas.

Todas las documentaciones que provengan del extranjero y que se acompañen a la solicitud de habilitación y las documentaciones que le sean requerida por la Autoridad de Aplicación deberán ser visado por el consulado del país de origen y posteriormente legalizado en el Ministerio de Relaciones Exteriores.

b) Entidades Extranjeras consorciadas con Entidades Nacionales

Las entidades consorciadas deberán cumplir con todos los requisitos legales y efectuar los trámites mencionados más arriba

El capital mínimo exigido será de 400 salarios mínimos para actividades diversas no especificadas.

Abog. Silvia Santander Florentín
Secretaría General



ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

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

- 20 -

3.3. Infraestructura Tecnológica en el extranjero

En el caso de que algún Prestador de Servicios de Certificación que requieran o utilicen infraestructura o servicios tecnológicos prestados desde el Extranjero, la inspección y auditoría podrá ser realizada por una entidad auditora o persona autorizada del lugar donde se encuentre la infraestructura, a fin de constatar el cumplimiento de lo señalado en la ley y reglamentaciones vigentes.



Abog. Silvia Santander Florentín
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 21 -

4 IDENTIFICACIÓN Y AUTENTICACIÓN

4.1 Identificación y Autenticación

Los interesados en ser Prestadores de Servicios de Certificación deberán ser habilitados por el Ministerio de Industria y Comercio. Serán habilitados si cumplen con todos los requisitos establecidos en la normativa vigente.

4.1.1 Nombre del Prestador de Servicios de Certificación

El Prestador de Servicios de Certificación debe elegir el nombre con el que va a operar. Dicho nombre debe ser propio, único en el ámbito de la Infraestructura de Certificación del Paraguay (PKI PARAGUAY) y asociado semánticamente al nombre legal.

Los nombres de los Prestadores de Servicios de Certificación deberán ser aprobados por la Autoridad de Aplicación y se emitirá el certificado con el nombre especificado en la resolución que habilita al Prestador de Servicios de Certificación.

La Autoridad de Aplicación resolverá los conflictos que se generen respecto a la elección y utilización de los nombres

4.1.2 Formato

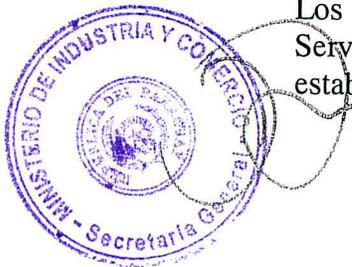
El nombre de la Prestadora de Servicios de Certificación utilizará el campo Subject del Certificado emitido por la Autoridad Certificadora Raíz y deberá ser del estándar de la Unión Internacional de Telecomunicaciones UIT. El formato para indicar el nombre deberá ser X.509. V3 (DistinguishName).

Se aplicará el formato de la siguiente manera:

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

4.1.3 Validación inicial de identidad

Los requisitos necesarios y procedimientos para la Habilitación de un Prestador de Servicios de Certificación se encuentran en la legislación vigente, reglamentaciones establecidas por la Autoridad de Aplicación y en la presente Política de Certificación.



Abog. Silvia Santander Florentin
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 1165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 22 -

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:

- 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)

4.1.4 Clave Privada

Para la emisión del Certificado, que será utilizado por el Prestador, la Autoridad Certificadora Raíz debe validar que la clave privada correspondiente a la clave pública del CSR (Certificate Signing Request) emitido para el Prestador, esté en posesión del mismo y sea utilizado para firmarlo.

Para garantizar esto, funcionarios designados de la Autoridad de Aplicación y el representante del Prestador de Servicios de Certificación deberán estar presentes en el acto de generación de las claves. Una vez emitido el certificado el Prestador de Servicios de Certificación deberá prestar su conformidad por escrito con el proceso.

En ningún caso el Prestador de Servicios de Certificación se encuentra autorizado a compartir la clave privada con la Autoridad Certificadora Raíz del Paraguay.

4.1.5 Solicitud de cambio de clave

No está permitido el cambio de claves. En caso de querer cambiar las claves de un certificado emitido se deberá realizar el procedimiento de revocación del certificado y posterior solicitud de un nuevo certificado.

4.1.6 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 el mecanismo que se realizara para salvaguardar a los usuarios finales titulares de un certificado, y la Autoridad de Aplicación se expedirá al respecto aprobando o denegando la solicitud de revocación teniendo en consideración la normativa vigente.



Abog. Silvia Sánchez Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución Nº

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 23 -

5 CICLO DE VIDA DE LOS CERTIFICADOS

5.1 Emisión de certificado

La Emisión del Certificado se realizará en las instalaciones de la Autoridad de Aplicación y deberá ser realizado por el personal técnico especializado y autorizado.

Los Prestadores de Servicios de Certificación deberán designar a la Persona Física que participara en el proceso de creación y emisión del certificado emitido por la Autoridad Certificadora Raíz del Paraguay. Para la emisión del certificado, deberá presentarse la persona designada por el Prestador con las documentaciones pertinentes para su identificación en la fecha y hora en la que se generarán las claves.

5.2 Proceso de emisión del Certificado

La emisión del certificado deberá realizarse en un ambiente seguro y de acuerdo con los requerimientos establecidos en la presente Política.

La Autoridad Certificadora Raíz deberá verificar que:

- La información contenida en el CSR es consistente con la Resolución de habilitación dictada por la Autoridad de Aplicación.
- El CSR se encuentra firmado con la clave privada correspondiente a la clave pública en él contenida.
- Existen pruebas de que la clave privada está bajo absoluto control del Prestador de Servicios de Certificación y que además fue generada de acuerdo a los requerimientos estipulados en la presente Política. 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 CSR contiene los campos necesarios especificados para la generación del certificado, requeridos por la presente Política de Certificación conforme a lo estipulado en el punto 7 Perfiles de Certificados y lista de Certificados Revocados

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



Abog. Silvia Santander Florentín
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 24 -

5.3 Aceptación de certificado

Una vez emitido el certificado, el Prestador de Servicios de Certificación deberá aceptar el mismo.

Una vez aceptado el certificado, el Prestador deberá presentar ante la Autoridad de Aplicación el Acuerdo de Suscripción firmado por su o sus representantes legales en un plazo no mayor a 24 hs. Una vez aceptado el certificado deberá ser instalado en la infraestructura del Prestador de Servicios de Certificación en presencia del/los funcionario/s designado/s por la Autoridad de Aplicación.

En caso de que el Prestador de Servicios de Certificación no acepte el certificado por tener discrepancias, se deberá proceder a la revocación del mismo.

5.4 Uso del Certificado y de Par de Claves

Los Prestadores de Servicios de Certificación deben utilizar la clave privada para firmar únicamente los certificados emitidos a los usuarios finales y para firmar la Lista de Certificados Revocados (CRL).

En ningún caso se podrá utilizar la clave privada para firmar otro tipo de documentación, cifrar información o realizar funciones de autenticación.

La utilización del certificado para otros fines no permitido o autorizado, es causal de revocación del certificado emitido y/o la suspensión de la habilitación del Prestador.

Una vez extinguido la vigencia del certificado o en caso de que haya sido revocado el Prestador no podrá bajo ningún sentido utilizar la clave privada asociada a su certificado.

Los Prestadores de Servicios de Certificación deberán tomar todas las medidas técnicas y de seguridad necesarias para proteger la clave privada.

5.5 Renovación del certificado

La renovación del certificado es el proceso en el que la Autoridad Certificadora Raíz emite un nuevo certificado al Prestador de Servicios de Certificación para que continúe sus operaciones. No está permitido mantener el mismo par de claves para diferentes certificados, por lo que se debe generar un par de claves nueva con los requerimientos de seguridad definidos en esta Política de Certificación.

El Prestador de Servicios de Certificación debe solicitar la emisión de un nuevo certificado ante la Autoridad de Aplicación con una antelación máxima de 3 a 6 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.



Abog. Silvia Alexander Florentín
Secretaría de Certificación



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 25 -

Luego de la emisión del nuevo certificado y hasta la expiración del anterior certificado, podrá operar con los dos certificados. El certificado anterior podrá ser utilizado únicamente para firmar la lista de Revocación de Certificados y validar la cadena de confianza del PKI Paraguay y el nuevo certificado emitido podrá ser utilizado para las operaciones de emisión de nuevos certificados y firma de la nueva lista de Revocación de Certificados.

5.6 Re-emisión del certificado

No se realizarán re-emisiones de certificados, debe en su lugar realizarse los procedimientos de revocación y emisión de un nuevo certificado en el mencionado orden.

5.7 Cambio de Clave del Certificado

No se realizará en ningún caso el cambio de claves de un certificado, debe en su lugar realizarse los procedimientos de revocación y emisión de un nuevo certificado, en el mencionado orden.

5.8 Modificación del certificado

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

5.9 Suspensión del Certificado

No se realizarán en ningún caso suspensiones de los Certificados.

Sin embargo si se podrá ordenar la suspensión administrativa de un Prestador de Servicios de Certificación, 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.

5.10 Revocación del Certificado

La Revocación de un Certificado es un procedimiento que anula definitivamente la validez de un certificado emitido, independientemente de su fecha de expiración. Un certificado revocado será válido únicamente para la verificación de firmas digitales generadas durante el periodo en el que el referido certificado era válido.

El certificado revocado deberá ser publicado en la Lista de Certificados Revocados para que los terceros aceptantes sean informados.

Abog. Silvia Santander Florentín
Secretaría General



ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 26 -

En caso de que el Prestador de Servicios de Certificación a quien se le ha revocado su certificado, desee no obstante seguir operando como Prestador de Servicios de Certificación, y si no existe ningún impedimento o prohibición, podrá solicitar nuevamente su habilitación ante la Autoridad de Aplicación presentando las documentaciones indicadas en la normativa y reglamentación vigente para el efecto.

5.10.1 Causales de revocación

La Autoridad Certificadora Raíz revocará los certificados en los siguientes casos:

- a) Cuando existan evidencias de que la clave privada se encuentre comprometida, o con riesgo cierto de estarlo.
- b) Si se constata un incumplimiento grave de la Política de Certificación y/o Declaración de Prácticas de Certificación que el Prestador debe Implementar.
- c) Si se constata un incumplimiento grave de la presente Política de Certificación y/o Declaración de Prácticas de Certificación.
- d) Si se constata que se está haciendo uso indebido del Certificado.
- e) Si se constata que los procedimientos de emisión de certificados han dejado de ser seguros.
- f) Si se constata que la información contenida en el certificado ha dejado de ser válida.
- g) Si por resolución de la Autoridad de Aplicación se revoca o suspende la habilitación del Prestador de Servicios de Certificación
- h) Si el Prestador de Servicios de Certificación desea finalizar su operación en el marco de la PKI Paraguay.
- i) Por pedido de revocación de una autoridad judicial competente.
- j) Otras causales especificadas en la reglamentación vigente.

Constatado cualquiera de dichas causales la Autoridad de Aplicación por resolución dispondrá la revocación de los Certificados si correspondiere.

5.10.2 Legitimación para solicitar la revocación

Los habilitados para realizar la solicitud de revocación son:

- a) El Prestador de Servicios de Certificación
- b) La Autoridad Judicial Competente
- c) El Ministerio de Industria y Comercio como Autoridad de Aplicación



Abog. Silvia Santamaría
Secretaría

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 27 -

5.10.3 Procedimientos de solicitud de revocación

En todos los casos la solicitud de revocación deberá ser presentada ante la Autoridad de Aplicación.

En caso que el solicitante sea el Prestador de Servicios de Certificación, el mismo deberá presentar la solicitud escrita firmada por su representante legal y dirigida a la Autoridad de Aplicación.

En caso de que el solicitante sea la Autoridad Judicial competente la misma deberá emitir una comunicación oficial a la Autoridad de Aplicación solicitando la revocación.

La Autoridad de Aplicación deberá evaluar las solicitudes y tomar una decisión sobre la misma. Antes de comenzar con el proceso de revocación se deberá notificar al Prestador lo cual no implicará aun la revocación efectiva del certificado.

Por resolución resolverá la solicitud de revocación. Una vez dictada la resolución, se revocará el certificado y se publicará en la Lista de Certificados Revocados. El Prestador de Servicios de Certificación queda notificado de la resolución que dispone la revocación con la publicación de la misma en sitio web oficial.

5.10.4 Plazo

La Autoridad de Aplicación contará con un plazo máximo de 24 horas para la publicación del certificado revocado en la Lista de Certificados Revocados a partir de la fecha en que se dictó la Resolución que ordena la Revocación.

El Prestador de Servicios de Certificación cuenta con un plazo máximo de 24 horas, a partir de la fecha en que se publicó el certificado revocado, para la revocación de todos los certificados emitidos a los usuarios finales. Una vez revocados todos los certificados, el Prestador de Servicios de Certificación deberá destruir su clave privada mediante un procedimiento que no permita la reconstrucción, este procedimiento deberá ser auditado por personal de la Autoridad de Aplicación.

Los Prestadores de Servicios de Certificación que continúan operando en el país deberán mantener publicada la Lista de Certificados Revocados y además solicitar nuevamente su habilitación ante la Autoridad de Aplicación.

ES COPIA FIEL DEL ORIGINAL



Abog. Silvia Sanja de Florentis
Secretaria



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

1165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 28 -

5.10.5 Plazo máximo de procesamiento de revocación

La Autoridad de Aplicación procesará la solicitud de revocación en el menor tiempo posible, que no será mayor al plazo de 24 horas a partir de la aprobación de la revocación

5.11 Verificación del estado del certificado

La Autoridad de Aplicación publicará 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.

5.12 Finalización del servicio de Certificación

Refiere en los casos que se extinga el plazo de vigencia del certificado y no se haya solicitado una renovación o en el caso que el Prestador de Servicios de Certificación finalice sus servicios y por lo tanto deje de operar o que la Autoridad Certificadora Raíz del Paraguay finalice sus servicios.

En caso que el certificado llegue a su fecha de expiración los terceros aceptantes no podrán confiar en dicho certificado y el Prestador de Servicios de Certificación no deberá seguir utilizándolo para su operación. Las operaciones realizadas con anterioridad a la fecha de vencimiento serán válidas.

La Autoridad de Certificación Raíz especificará en su Declaración de Prácticas de Certificación el procedimiento para la finalización de sus servicios.

En el caso de que un Prestador de Servicios de Certificación deje de operar deberá cumplir con las siguientes tareas:

1. Debe publicar en su sitio Web oficial la fecha de suspensión de los servicios con al menos 60 días de anticipación.

Abog. Silvia Santanor Florentín





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 29 -

2. 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 o cese de las operaciones
3. Notificar a sus suscriptores (usuarios finales) por lo menos 30 días antes de la suspensión efectiva o cese de las operaciones.
4. Proceder a la eliminación y destrucción de la clave privada según el procedimiento establecido en su Declaración de Practicas de Certificación y en la presente Política.

En caso de que el Prestador de Servicios de Certificación deje de operar, no podrá bajo ningún sentido emitir ningún certificado pero deberá continuar dando soporte a las operación de revocación de certificados y publicación de CRL. Recién una vez vencidos o revocados todos los certificados emitidos y cuya revocación esté publicada, cesa automáticamente la responsabilidad de los Prestadores.

Los suscriptores de los Prestadores de Servicios de Certificación podrán seguir utilizando los certificados emitidos hasta que se extinga el plazo de vigencia o hasta que fuera revocado. En caso que el certificado llegue a su fecha de expiración no se podrá confiar en dicho certificado.

La Autoridad de Aplicación custodiará toda la información referida al cese de la operación del Prestador de Servicios de Certificación y publicará en su sitio web oficial el cese de actividades o finalización del servicio del Prestador de Servicios de Certificación.

Abog. Silvia Santa Cruz Florentín
Secretaria General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución Nº 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 30 -

6 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.

Las actividades o eventos como: los controles de seguridad física, procedimientos y los controles de personal deberán estar documentados para su uso interno y en las Declaraciones de Practicas de Certificación se deberá especificar un resumen de los mismos.

Todos los controles deberán ser aprobados por la Autoridad de Aplicación antes de que se pongan en práctica.

Entre los controles necesarios se debe incluir:

1. Controles de Seguridad Física: La Autoridad Certificadora Raíz del Paraguay y los Prestadores de Servicios de Certificación contarán con medidas sólidas de seguridad que protejan su equipamiento, datos e instalaciones, acceso restringido así como también medidas de seguridad contra siniestros (incendios e inundaciones).
2. Para ingresar al recinto donde se encuentran los equipos el personal autorizado debe atravesar varios niveles de seguridad. Los equipos se encuentran alojados en instalaciones que brindan condiciones adecuadas de suministro de energía eléctrica y de aire acondicionado para permitir una operación segura.
3. Controles Procedimentales: Todos los procesos que hacen a la operación de la Autoridad Certificadora Raíz del Paraguay y los Prestadores de Servicios de Certificación deberán estar debidamente documentados y ser utilizados por el personal especializado. La aprobación, ejecución y control de las tareas desarrolladas deberán basarse en la contraposición de intereses interviniendo siempre varias personas. Para la gestión de la clave privada se deberá proceder de conformidad a lo establecido en la presente Política de Certificación y normativa vigente.
4. Seguridad del Personal: Los requerimiento de seguridad ligada al personal, procedimiento para la contratación, desvinculación y manejo del mismo, así como los requisitos de seguridad para la contratación que empleen tanto la Autoridad Certificadora Raíz del Paraguay y los Prestadores de Servicios de Certificación deberán estar documentados y además deberán estar especificados en sus respectivas declaraciones de Practicas de Certificación.



Abog. Silvia Salsander Florentín
Secretaría



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

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

- 31 -

5. Registro de Eventos: Tanto la Autoridad Certificadora Raíz como los Prestadores de Servicios de Certificación deberán definir que operaciones se deben registrar. Mínimamente se deben registrar todas las actividades relativas a la gestión de claves (generación, destrucción, activación etc), a la gestión de certificados (emisión, revocación, renovación etc) y la emisión de la Lista de Certificados Revocados, así como también las actividades diarias de la Autoridad de Aplicación (reglamentación, acuerdos, resoluciones, auditorías etc.) Los registros relativos a las mencionadas actividades u operaciones deberán mantenerse por un periodo de 12 años como mínimo. Los Registros relativos a otras actividades deben mantenerse por al menos dos años.
6. Continuidad de las Operaciones: La Autoridad Certificadora Raíz del Paraguay y los Prestadores de Servicios de Certificación deberán tener definidos planes de continuidad y recuperación que le permitan continuar con su operativa en la eventualidad de falla de equipamiento y/o siniestros.
7. Se deberá documentar de la misma forma las acciones pertinentes a la finalización de las actividades o terminación de las operaciones.



Abog. Silvia Schneider Florentín
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 32 -

7 CONTROLES DE SEGURIDAD TÉCNICA

Los controles técnicos de seguridad tienen como objetivo la protección del par de claves de la Autoridad Certificadora Raíz así como el par de claves de los Prestadores de Servicios de Certificación. Se especifica además medidas generales para la protección de los sistemas de información que dan soporte a las actividades de la Autoridad Certificadora Raíz del Paraguay y los Prestadores de Servicios de Certificación.

7.1 Instalación del Equipamiento Informático

7.1.1 Equipamiento de la Autoridad Certificadora Raíz del Paraguay

El equipamiento (hardware) fue dispuesto en rack en los respectivos Data Center tanto de producción como de contingencia ante la presencia de personal de la Autoridad de Aplicación.

Los Servidores y HSM que corresponden a la Autoridad Certificadora Raíz del Paraguay fueron dispuestos en los rack cofre, cuyas llaves están en poder del personal autorizado de la Autoridad de Aplicación.

El Sistema Operativo de los Servidores de la CA Offline fue instalado previo a la Ceremonia con la presencia de Personal de la Autoridad de Aplicación.

No se instaló ningún otro software sobre dichos servidores hasta la Ceremonia de Claves.

Los HSM solo fueron dispuestos en los Rack Cofre manteniendo el software de transporte y las tarjetas en blanco hasta el momento de la Ceremonia.

7.1.2 Equipamiento de los Prestadores de Servicios de Certificación

El equipamiento que implementan los Prestadores de Servicios de Certificación, deberá instalarse y configurarse en presencia de personal especializado de la Autoridad de la Aplicación a fin de asegurar su correcta instalación e implementación.

Los Prestadores podrán introducir cambios tecnológicos siempre que estos cumplan con la normativa y sean notificados a la autoridad de aplicación y sean aprobados por la misma.

Abog. Silvia Bastander Florentín
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

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

- 33 -

7.2 Generación e instalación del par de claves

7.2.1 Autoridad Certificadora Raíz del Paraguay

El par de claves de la Autoridad Certificadora Raíz del Paraguay deberá generarse durante la ceremonia de claves. Dicha generación de Claves se realizará en las instalaciones de la Autoridad de Aplicación siguiendo los procedimientos establecidos en el Guión de la Ceremonia y la normativa vigente.

7.2.2 Prestadores de Servicios de Certificación

La generación de las Claves se debe realizar en las instalaciones del Prestador de Servicios de Certificación bajo los procedimientos establecidos en su Política y Declaración de Prácticas, así como también bajo el procedimiento de la presente Política y la Declaración de Prácticas de la Autoridad Certificadora Raíz del Paraguay.

El procedimiento de generación de claves debe ser en presencia del personal de la Autoridad de Aplicación.

7.2.3 Entrega de la clave privada

La clave privada será generada en dispositivos criptográficos definidos para tales fines y deberán ser custodiadas por la Autoridad Certificadora Raíz del Paraguay o por el Prestador de Servicios de Certificación en su caso, para asegurar su integridad.

7.2.4 Entrega de la clave pública

La generación de la clave pública tanto para la Autoridad Certificadora Raíz del Paraguay y para el Prestador de Servicios de Certificación se realiza en las instalaciones de cada una de ellas. Una vez generada la petición de certificación y que la misma haya sido procesada se dará entrega del certificado digital.

Es responsabilidad del Prestador de Servicios de Certificación la publicación de sus certificados.

7.2.5 Hardware / software de generación de claves

Para la generación y protección de las claves se deberán utilizar Módulos criptográficos HSM FIPS 140 versión 2 nivel 3.

Abog. Silvia Santander Florentín
Secretaría de





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 34 -

7.2.6 Fines de uso de las claves

Los usos de las claves de la Autoridad Certificadora Raíz del Paraguay solo permiten emitir certificados de Prestadores de Servicios de Certificación y Listas de Revocación de Certificados.

Las claves de los Prestadores de Servicio de Certificación solo podrán utilizarse para la emisión de certificados de usuarios finales y listas de revocación de certificados.

7.3 Protección de la clave privada

Toda clave privada debe ser protegida por módulos criptográficos HSM con claves maestras que hayan sido generadas con algoritmos criptográficos sólidos. El cifrado a utilizar debe ser AES 256 o 3DES con clave de largo triple (asimétrico).

Las claves maestras de la Autoridad Certificadora Raíz del Paraguay y de la Autoridad Certificadora de los Prestadores de Servicios de Certificación no podrán ser retiradas de los HSM más que para procedimientos de backup y procedimientos de cambio de módulos criptográficos. Toda clave maestra que sea retirada del HSM deberá ser dividida al menos en 3 custodios y la elección de los mismos se debe realizar considerando la contraposición de intereses.

Una vez vencido el certificado debe procederse a la destrucción de la clave privada así como la clave maestra del módulo criptográfico de forma que no pueda recuperarse.

Los HSM que custodien las claves deberán proveer dichas funcionalidades.

La destrucción de la clave privada de la Autoridad Certificadora Raíz del Paraguay, se debe realizar conforme los procedimientos estipulados en la Declaración de Prácticas de Certificación y en la presente Política. Los Prestadores de Servicios de Certificación deberán contar con procedimientos para la destrucción de la clave privada; dicho procedimiento deberá estar contemplado en su Declaración de Prácticas de Certificación y que sea previamente aprobado por la Autoridad de Aplicación.

7.4 Compromiso de la Clave Privada de la Autoridad Certificadora Raíz.

Ante sospecha de compromiso de la clave privada, se deberá inmediatamente proceder a la revocación del certificado.

Abog. Silvia Santander Florentín
Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 35 -

En tal situación se deberá realizar la ceremonia de generación de un nuevo par de claves, publicar el nuevo certificado y emitir nuevos certificados a los Prestadores de Servicios de Certificación Habilitados.

Antes de la revocación efectiva, la Autoridad de Aplicación deber comunicar a los Prestadores que su certificado será revocado y que por ende las claves privadas asociadas a su certificado no deben ser utilizadas

7.5 Otros aspectos de la gestión del par de claves

Todas las claves generadas para la Autoridad Certificadora Raíz del Paraguay y la Autoridad Certificadora del Prestador de Servicio de Certificación deben tener un Largo de 4096 bits.

El certificado de la Autoridad Certificadora Raíz de Paraguay tiene una vigencia de veinte 20 años a partir de la fecha de generación de las claves.

El certificado de un Prestador de Servicios de Certificación tiene validez por 10 años a partir de la fecha de generación del certificado.

El periodo de validez máximo del par de Claves de la Autoridad Certificadora Raíz del Paraguay y el de los Prestadores de Servicio de Certificación es el de su Certificado. Transcurrido dicho periodo o en caso de revocación del certificado, la Clave Privada correspondiente a la Clave Pública contenida en el Certificado debe ser eliminada.

7.6 Métodos de activación

Por activación se entiende, al procedimiento previo, a la utilización de la clave privada, que permita hacerla disponible para ser usada. En todos los casos es obligatorio contar con un mecanismo de activación que implique la presencia de más de una persona y que la distribución de las personas designadas se realice considerando la contraposición de intereses.

7.7 Controles de seguridad informática

La Autoridad Certificadora Raíz de Paraguay y la Autoridad de Certificación de los Prestadores de Servicio de Certificación deben implementar políticas, estándares y procedimientos que permitan una operación segura.

Abog. Silvia Szlander Florentín
Secretaría General



ES COPIA DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 36 -

Se deben instrumentar como mínimo 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 lógico;
- 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.

Con relación a los Prestadores de Servicio de Certificación, dichos controles serán auditados y validados por la Autoridad de Aplicación.

7.8 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.

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.

7.9 Seguridad de la red

Deben implementarse las medidas adecuadas de protección para la operación de la Autoridad Certificadora Raíz del Paraguay y la Autoridad Certificadora del Prestador de Servicios de Certificación si las mismas están conectadas en red.

Los controles serán objeto de regulación de la Autoridad de Aplicación.

7.10 Fecha y Hora de la emisión del certificado

La Autoridad de Certificación 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 Estampado Tiempo)



Abog. Silvia Santander Florentín
Secretaría

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N°

1165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 37 -

8 PERFILES DE CERTIFICADO Y DE LISTA DE CERTIFICADOS REVOCADOS

El formato de los certificados cumple con lo especificado en el estándar ITU-T X.509 versión 3
La Lista de Certificados Revocados cumple con el estándar ITU-T X.509 versión 2.

8.1 Perfil de certificado de la Autoridad Certificadora Raíz

A continuación se especifican los campos del Certificado de la Autoridad Certificadora Raíz del Paraguay.

Atributo	Valor
Versión	3
Serial Number	N° de serie asignado por la Autoridad Certificadora Raíz del Paraguay
Issuer DN	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
SignatureAlgorithm	SHA256RSA
ValidFrom	<fecha de ceremonia>
ValidTo	<fecha de ceremonia>+20 años
Suscriber DN	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
SubjectPublic Key	Clave Pública de la Autoridad RSA de 4096 bits
Extensiones	
Subject Key Identifier	Hash de 20 bytes del atributo SubjectPublic Key
Key Usage	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0
CertificatePolicies	URI = www.acraiz.gov.py/documentacion/politicas.pdf
Basic Constraints	CA = TRUE



Abog. Silvia Santander Florentín
Secretaría de Estado



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 38 -

8.2 Perfil de Certificados del Prestador de Servicios de Certificación

A continuación se especifican los campos de los certificados de los Prestadores de Servicios de Certificación Habilitados en la República del Paraguay.

Atributo	Valor
Versión	3
Serial Number	N° de serie asignado por la Autoridad Certificadora Raíz del Paraguay
Issuer DN	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
SignatureAlgorithm	SHA256RSA
ValidFrom	<fecha de emisión>
ValidTo	<fecha de emisión>+10 años
Suscriber DN	Nombre distintivo definido en el punto 0
SubjectPublic Key	Clave Pública Generada según los requerimientos establecidos en el punto ¡Error! No se encuentra el origen de la referencia.
Extensiones	
Authority Key Identifier	Identificador de la clave publica de la Autoridad Certificadora Raíz del Paraguay.
Subject Key Identifier	Hash de 20 bytes de la clave publica
Key Usage	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0
CertificatePolicies	URI = Nombre del dominio elegido por el PSC y el Directorio Creado para el repositorio de dicho documento.
Basic Constraints	CA = TRUE Largo = 0
CRL DistributionPoints	URI = Nombre del dominio elegido por el PSC y el Directorio Creado para el repositorio de dicho documento.
AuthorityInformation Access	URI = www.acraiz.gov.py/

ES COPIA FIEL DEL ORIGINAL

Abog. Silvia Santander Florentín

Secretaría General





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY.

- 39 -

8.3 Perfil de Listas de Certificados Revocados de la Autoridad Certificadora Raíz del Paraguay

A continuación se listan los atributos de las Listas de Certificados Revocados según el estándar X.500.

Atributo	Valor
Versión	2
Issuer DN	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
SignatureAlgorithm	SHA256RSA
Efective Date	Día y Hora de Emisión de la CRL
NextUpdate	<fecha de emisión>+3 meses
RevokedCertificates	Lista de Certificados revocados incluyendo el N° de serie (Serial Number) y la fecha de revocación.
Extensiones	
Authority Key Identifier	Identificador de la clave pública de la Autoridad Certificadora Raíz del Paraguay.
CRL Number	Número Secuencial asignado por la Autoridad Certificadora Raíz.
Key Usage	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0
CertificatePolicies	URI = www.acraiz.gov.py/documentacion/politicas.pdf
Basic Constraints	CA = TRUE Largo = 0
CRL DistributionPoints	URI = www.acraiz.gov.py/crl/acraiz_raiz_py.crl
AuthorityInformation Access	URI = < www.acraiz.gov.py >

ES COPIA FIEL DEL ORIGINAL

Abog. Silvia Sánchez Florentín
Secretaría de Estado





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 165.-

POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY.

- 40 -

9 ADMINISTRACIÓN DOCUMENTAL

9.1 Procedimiento para modificaciones

La Autoridad de Aplicación cuenta con procedimientos internos para la modificación y actualización de la presente política. Las modificaciones serán establecidas y aprobadas por la Autoridad de Aplicación.

En caso de que un Prestador de Servicios de Certificación desee una modificación en la presente política, deberá solicitar formalmente a la Autoridad de Aplicación la modificación esgrimiendo las razones. La Autoridad de Aplicación evaluará las solicitudes realizadas y se expedirá al respecto por medio de un dictamen.

En caso que la solicitud sea aprobada, se deben realizar los cambios necesarios en la presente política y generar una nueva versión de la misma.

9.2 Procedimientos de Publicación y Notificación

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

Abog. Silvia Schneider Florentín
Sra.

