MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

ASUNCIÓN, 08 de AGOSTO de 2013

VISTO: El Memorándum DGFD&CE N° 0174 de fecha 05 de agosto de 2013, de la Dirección General de Firma Digital y Comercio Electrónico, remitida a la Subsecretaría de Estado de Comercio de este Ministerio, en el cual solicita la modificación y ampliación parcial de la Resolución N° 165/2013, con el objeto de lograr la operatividad técnica de la Dirección General, habilitar a los interesados en prestar servicios de certificación, y principalmente para una eficiente prestación del servicio de certificación por parte de las entidades de certificación que fueren habilitadas para prestar Servicios de Certificación Digital; y

CONSIDERANDO: La Ley Nº 4017 de fecha 23 de diciembre de 2010 "DE VALIDEZ JURIDICA DE LA FIRMA ELECTRONICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRONICO".

La Ley Nº 4610 de fecha 7 de mayo de 2012 "QUE MODIFICA Y AMPLIA LA LEY N° 4017/10 "DE VALIDEZ JURIDICA DE LA FIRMA ELECTRONICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRONICO".

El Decreto N° 7369 de fecha 23 de setiembre de 2011 "POR EL CUAL SE APRUEBA EL REGLAMENTO GENERAL DE LA LEY N° 4017/2010 "DE VALIDEZ JURIDICA DE LA FIRMA ELECTRONICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRONICO".

La Resolución N° 165 de fecha 06 de marzo de 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY".

Que el Artículo 38 de la Ley 4610/2012, instituye al Ministerio de Industria y Comercio, a través de la Subsecretaria de Estado de Comercio como Autoridad de Aplicación de la normativa vigente.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

Que, la Dirección de Firma Digital por Memorándums DGFD&CE-DFD Nros. 58, 61 y 69 de fechas 28 de junio, 1 y 29 de julio de 2013, recomiendan la modificación de la Política de Certificación de la Autoridad Certificadora Raíz y la Declaración de Prácticas de la Autoridad Certificadora Raíz.

Que la Dirección de Asuntos Legales de la Dirección General de Firma Digital y Comercio Electrónico, a través del Memorándum DAL N° 17 de fecha 01 de agosto de 2013, recomienda la modificación de la Política de Certificación y la Declaración de Prácticas de Certificación respecto al Módulo Criptográfico que utilizarán los Prestadores de Servicios de Certificación. No obstante, es conveniente que se tenga en cuenta que cualquiera sea el dispositivo criptográfico (hardware/software) de generación y protección de clave que se establezca o autorice su uso, deberá ser lo suficientemente seguro y reunir los requisitos establecidos en la normativa vigente.

Que el Ministerio de Industria y Comercio como Autoridad de Aplicación, conforme a las disposiciones del Artículo 39 de la Ley N° 4017/2010 y modificado por el Artículo 1° de la Ley N° 4610/2012, tiene la facultad de aprobar y elaborar las Políticas de Certificación de la Autoridad Certificadora Raíz que contiene los principios y reglas relativas a la emisión y gestión de Certificados Digitales, asimismo establece las reglas mínimas que deben cumplir los Prestadores de servicios de Certificación y los usuarios finales.

Que la Dirección General de Asuntos Legales, por Dictamen Jurídico N° 377 de fecha 07 de agosto de 2013, recomienda proseguir con los trámites administrativos pertinentes para la promulgación de la Resolución.

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO
Abog. Laura
Encargada de Despacho
Secretaría General

POR TANTO,

EL MINISTRO DE INDUSTRIA Y COMERCIO

R E S U E L V E:

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

Art. 1°.- Modificar y ampliar parcialmente el Anexo de la Resolución N° 165 de fecha 06 de marzo de 2013, en los siguientes puntos: 1.1, 1.2, 1.3.1, 1.3.4, 1.3.5, 1.4.1, 1.5, 1.6, 1.8, 2.2, 2.5, 3.2 inc a), 3.3, 4.1.3, 5.2, 5.10, 5.12, 6, 7.1.1, 7.1.2, 7.2, 7.3, 8, 9.1

Quedando redactado de la siguiente manera:

"1.1 **Descripción general**

En el marco de la Ley N° 4017/2010 su Decreto Reglamentario Nº 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 aplicación 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 Ministerio de Industria y Comercio como ente regulador debe:

- Administrar la Autoridad de 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 definido 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 Nro. 4017/2010 y 4610/2012 y del decreto reglamentario N° 7369/2011.

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

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.

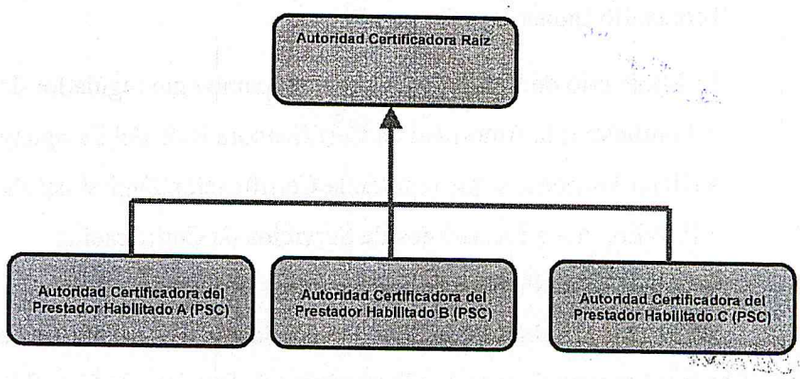

Figura 1 Infraestructura de PKI Paraguay

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 Publica 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 Infraestructure (PKI)

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Abog. Laura Minarro
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

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 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.

Los interesados en ser Prestadores de Servicios de Certificación, y los habilitados deberán cumplir con los requisitos y disposiciones establecidos en las Leyes Nº 4017/2010 y Nº 4610/2012, en el Decreto Reglamentario Nº 7369/2011, las resoluciones y demás disposiciones reglamentarias dictadas por la Autoridad de Aplicación.

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.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Miranda
Encargada de Despacho
Secretaría General

1.2 Identificación de la Política de Certificación

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

Versión: **2.0**

Fecha de aprobación: 06 de Marzo de 2013

Fecha de última actualización: 08 de agosto 2013

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

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL 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:

a) Establecer los estándares tecnológicos y operativos de conformidad a las Leyes Nros. 4017/2010 y 4610/2012.

b) **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.**

c) 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.

d) Efectuar auditorías e inspecciones a los Prestadores de Servicios de Certificación.

e) Determinar los efectos de la revocación de los certificados de los Prestadores de Servicios de Certificación.

f) 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.

g) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones.

h) Requerir en cualquier momento a las entidades de certificación (P.S.C.) para que suministren información relacionada con los certificados digitales emitidos y los documentos en soporte informático que custodien o administren.

i) **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.**

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO
Abog. Sandra Miranda
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

j) Otorgar o revocar la habilitación a los Prestadores de Servicios de Certificación y supervisar su actividad, según las exigencias establecidas por la reglamentación.

k) Homologar los dispositivos tecnológicos de creación y verificación de firmas digitales con ajuste a las normas y procedimientos establecidos por la reglamentación.

l) Imponer y aplicar las sanciones establecidas en la normativa vigente.

m) Mantener un registro público de Prestadores de Servicios de Certificación habilitados de conformidad a lo establecido en el Artículo 10 del Decreto Nº 7369/2011.

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 Practicas 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 usuarios finales.

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.

ES COPIA FIEL DEL ORIGINAL
Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

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 certificados digitales vigentes y revocados, 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 Articulo 32 de la Ley Nº 4017/2010

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 Practicas de Certificación de la Autoridad Certificadora Raíz del Paraguay, así como de la normativa vigente.

1.3.5 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. Laura M...
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

1.4.1 Usos permitidos de los Certificados

Los certificados emitidos por la Autoridad Certificadora Raíz dei 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 usuarios finales y firmar las Listas de Certificados Revocados correspondientes.

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: Capitán Pedro Villamayor esquina Teniente Teófilo del Puerto. Bloque B Asunción - Paraguay
Dirección de correo: info-dgfdce@mic.gov.py
Página Web: www.acraiz.gov.py
Teléfono: (+595) (21) 513-532 (21) 527-235

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 Practicas Internacionales que guardan relación con la operación de las Autoridades de Certificación.

Abog. Laura Dinardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

La Autoridad de Aplicación adopta los estándares internacionales vigentes que se mencionan a continuación, sin perjuicio a nuevas y a mejoras de las citadas convenciones:

Referencia	Descripción
ISO/IEC 27001 (International Organization for Standardization/ International Electrotechnical Commission)	Tecnología de la Información- Técnicas de la seguridad- Sistema de Gestión de la seguridad.
ISO/IEC 27002 (International Organization for Standardization/ International Electrotechnical Commission)	Tecnología de la Información - Técnicas de Seguridad- Código de las buenas prácticas para la gestión de la seguridad de la información.
ISO/IEC 27005 (International Organization for Standardization/ International Electrotechnical Commission)	Tecnología de la Información- Técnicas de seguridad.- Información gestión de riesgos de seguridad.
ANSI(American National Standards Institute)-**CWA**	Gestión de Sistemas para la Autoridad de Certificación de Confianza.
ANSI (American National Standards Institute) -**RSA**	Soporte para capacidades de longitud de Clave.
ANSI (American National Standards Institute) - **PKCS**	Estándar de Sintaxis de Solicitud de Certificación. Estándar de Sintaxis de Certificados. Estándar de Sintaxis de Lista de Certificados Revocados.
ANSI (American National Standards Institute) -**TIA**	Estándar de la Infraestructura de Telecomunicaciones para Centros de Datos.

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

ETSI (European Telecommunications Standards Institute)-**TS**	Requisitos de Política para Entidades de Certificación que emiten Certificados de Clave Pública.
IETF(Internet Engineering Task Force) – **RFC**	Certificados en general, gestión de claves y Lista de Revocación de Certificados [CRL].
ITU-T (International Telecommunications Union - Telecommunication)	Formatos Estándar para Certificados de Claves Públicas.
NIST(National Institute of Standards and Technology) - **EAL+4**	Requisitos de seguridad para módulos criptográficos.
NIST(National Institute of Standards and Technology) –**FIPS**	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware.
NIST(National Institute of Standards and Technology) – **AES**	Estándar de Cifrado Avanzado
NIST(National Institute of Standards and Technology) – **DES, 3DES**	Estándar de cifrado de datos.

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, establecido 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

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

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.

Infraestructura de Clave Pública o Public Key Infraestructure (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.

Usuario final: Persona física o jurídica que adquiera un certificado digital de una PSC habilitada. Sinónimo de titular, firmante suscriptor o signatario.

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.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

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.

Lista de certificados revocados (CRL: Certificate Revocation List): Lista firmada digitalmente por una autoridad de certificación, publicada periódicamente que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento. La lista generalmente indica el nombre de la persona que emite la fecha de emisión y fecha de la próxima edición prevista, además de los números de serie de los certificados revocados y la fecha de la revocación.

Renovación de certificados: Proceso para obtener un nuevo certificado antes de la expiración del certificado existente. En la Autoridad de Certificación, es obligatorio para generar nuevas claves de cifrado para cada certificado expedido.

Clave Privada: La clave privada también hace parte del sistema de "Infraestructura de Clave Pública" (PKI por sus siglas en ingles) y representa uno de los puntos de partida más importantes para la seguridad de la información. La Clave Privada (o llave privada) es una cadena de longitud variable de dígitos (512K, 1024K, 2048K) que conforman una serie numérica y se obtiene a partir de la aplicación de algoritmos matemáticos complejos donde la probabilidad de tener dos claves privadas iguales es casi nula. La Clave privada se obtiene a partir de una función matemática que es el

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

complemento aritmético perfecto de la Clave pública asociada pero siendo no derivable, es decir, es imposible llegar a la otra conociendo una de estas.
La Clave privada es parte esencial del sistema PKI y está solamente en posesión del usuario final del certificado. Solo existe una copia de esta clave en el caso de certificados de firma digital.

Clave Pública: La clave pública hace parte del sistema de "Infraestructura de Clave Pública" (PKI por sus siglas en ingles) y representa uno de los puntos de partida más importantes para la seguridad de la información. La Clave pública (o llave pública) es una cadena de longitud variable de dígitos (512K, 1024K, 2048K) que conforman una serie numérica y se obtienen a partir de la aplicación de algoritmos matemáticos complejos y de esta forma garantizar que la probabilidad de encontrarse dos claves públicas iguales sea casi nula. La Clave pública se obtiene a partir de una función matemática que es el complemento perfecto de la Clave privada asociada siendo estas no derivables. Es decir, conociendo una de estas es imposible llegar a la otra.
Como su nombre lo indica, la Clave Pública es la parte del sistema PKI que se expone al conocimiento general y las Autoridades de Certificación (CAs) tienen la obligación de suministrarla y publicarla en sus sitios Web para efectos de verificación de la identidad de quien posea un certificado digital o para verificar la integridad de un documento firmado digitalmente.

Clave Maestra: clave que se instancia en un Módulo Hardware de Seguridad (HSM) y la cual es dividida en custodios considerando la contraposición de intereses, cuyo fin es encriptar la clave privada.

Claves criptográficas: Valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

Cifrado asimétrico: Tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionado.

Par de claves: son las claves privadas y públicas de un criptosistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Miranda
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

Huella digital: la huella digital o resumen de un mensaje se obtiene aplicando una función denominada hash a ese mensaje, esto da como resultado un conjunto de datos singular de longitud fija.

Módulo criptográfico: Software o Hardware criptográfico que genera y almacena claves criptográficas.

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

Módulo de Software de Seguridad: sistema criptográfico basado en software que genera, almacena y protege claves criptográficas.

Repositorio: Sistema en línea confiable y asequible, mantenido por la Autoridad de Certificación con el fin de difundir su información pública.

Seguridad Física: El objetivo principal de la implementación de controles de seguridad física es restringir el acceso a las áreas críticas de la organización, evitando el acceso no autorizado que puede causar daños en el equipo, el acceso no autorizado a la información, el robo de equipos, entre otros.
Los controles de acceso físico podrán ser implementados en conjunto con controles de acceso lógico.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

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.

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

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 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.

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

Abog. Laura Martínez
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

mantenimiento del certificado. Los datos no podrán ser obtenidos o utilizados para otro fin, sin el consentimiento expreso del titular de los datos.

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° 1682/2001 "Que Reglamenta la Información de Carácter Privado" y su modificatoria la Ley N° 1969/2002 y la normativa vigente.

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 sociedades 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 requeridas por la Autoridad de Aplicación deberán ser visadas por el consulado del país de origen y posteriormente legalizadas en el Ministerio de Relaciones Exteriores.

Abog. Liliana Mina
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

En el contexto de la Infraestructura PKI Paraguay, la Infraestructura Tecnológica del Prestador de Servicios de Certificación habilitado por la Autoridad de Aplicación necesariamente deberá situarse dentro del territorio paraguayo, por tanto no podrá utilizar una infraestructura tecnológica establecida en el extranjero.. No obstante, el Prestador de Servicios de Certificación habilitado podrá utilizar servicios tecnológicos prestados desde el extranjero.

3.3 Infraestructura Tecnológica en el extranjero (Eliminado)

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.

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, en nombre del Prestador de Servicios de Certificación.

d) requisitos documentales establecidos en la normativa vigente y los reglamentados por la Autoridad de Aplicación

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.

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 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 8 (ocho) 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.

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.

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, y subsanada o desaparecida la causal de revocación podrá solicitar la habilitación ante la Autoridad de Aplicación y posteriormente la emisión de un nuevo certificado.

Abog. Laura Mina
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

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.
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 usuarios finales, titulares de un certificado digital, 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 la 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.

COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO
Abog. Laura Alvarez
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

Los usuarios finales 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.

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 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

Abog. Laura Miranda
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

---

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 requerimientos 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.

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 diez años a partir de la fecha de vencimiento o revocación de los certificados. 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.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minadeo
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

7.1.1 Equipamiento de la Autoridad Certificadora Raíz del Paraguay

El equipamiento (hardware) fue dispuesto en rack cofre 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 dedicado a la gestión de certificados del Prestador de Servicios de Certificación Habilitado, deber ser instalado en presencia del personal especializado y autorizado por la Autoridad de Aplicación, de forma a certificar su correcta instalación.
Los Prestadores podrán introducir cambios tecnológicos siempre que estos cumplan con la normativa y sean notificados a la autoridad de aplicación y aprobados por la misma.
Los Prestadores de Servicio de Certificación solicitantes, podrán utilizar su infraestructura tecnológica siempre y cuando los equipos destinados a la prestación del servicio en donde se generarán los certificados digitales, estén separados por medio de rack independiente, con la mayor seguridad física, las cuales están establecidas por la Autoridad de Aplicación mencionadas en el punto 6 de la presente Política y en el Punto 5 de la Declaración de Prácticas de Certificación.

Abog. Laura Miranda
Encargada de Despacho
Secretaría General

7.2 Generación e instalación del par de claves

7.2.1 Generación del par de claves

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

7.2.1.1 Autoridad Certificadora Raíz del Paraguay

El par de claves de la Autoridad Certificadora Raíz del Paraguay se genera durante la ceremonia de claves. Dicha generación de Claves se realiza en las instalaciones de la Autoridad de Aplicación siguiendo los procedimientos establecidos en el Guión de la Ceremonia de constitución de la Autoridad Certificadora Raíz de Paraguay y la normativa vigente.
El algoritmo de firma es el SHA-256RSA y SHA-1RSA, con longitud de clave RSA 4096 bits.

7.2.1.2 Prestadores de Servicios de Certificación

La generación de las Claves se debe realizar en la infraestructura tecnológica 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, la Declaración de Prácticas de la Autoridad Certificadora Raíz del Paraguay y la normativa vigente.
Este procedimiento debe realizarse en presencia del personal de la Autoridad de Aplicación.

Se debe crear una Solicitud de Firma de Certificado (CSR, Certificate Signing Request) en formato PKCS#10 de los estándares ITU-T X.509 v.3.

7.2.2 Entrega de la clave privada

7.2.2.1 Autoridad Certificadora Raíz del Paraguay
Una vez generadas las claves, las mismas se almacenarán en el módulo de hardware de seguridad (HSM), el cual cumple con los requisitos adoptados y definidos para tales fines e indicados en el Punto 7.2.5.1 de la presente Política.
Las claves deberán ser custodiadas por la Autoridad Certificadora Raíz del Paraguay para asegurar su integridad.

7.2.2.2 Prestadores de Servicios de Certificación
La Autoridad de Aplicación se abstiene de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de la clave privada de las

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

Prestadoras de Servicio de Certificación, de acuerdo a lo establecido en la normativa vigente.

7.2.3 Entrega de la clave publica

7.2.3.1 Autoridad Certificadora Raíz del Paraguay
Es responsabilidad de la Autoridad de Certificación Raíz del Paraguay el almacenamiento, el resguardo y la publicación de sus certificados.

7.2.3.2 Prestadores de Servicios de Certificación
Una vez firmada la Solicitud de Firma de Certificado (CSR - Certificate Signing Request)en las instalaciones de la Autoridad de Certificación Raíz del Paraguay, se dará entrega del certificado digital al Prestador de Servicios de Certificación habilitado para la instalación en su infraestructura tecnológica.
Es responsabilidad del Prestador de Servicios de Certificación el almacenamiento, el resguardo y la publicación de sus certificados.

7.2.4 Hardware / software de generación de claves

7.2.4.1 Autoridad Certificadora Raíz del Paraguay
La Autoridad de Certificación Raíz del Paraguay utiliza módulos de hardware de seguridad (HSM) que cumple con los requisitos definidos por la ITSEC, CommonCriteria o FIPS 140-2 Nivel 3 o superiores.

7.2.4.2 Prestadores de Servicios de Certificación
Los Prestadores de Servicios de Certificación deberán utilizar módulos criptográficos para generar su par de claves, estos módulos pueden constituirse ya sea como hardware o software.
Los requisitos que deben cumplir los Prestadores de Servicios de Certificación que utilicen módulo hardware de seguridad (HSM) están definidos en el punto 7.2.5.1 de la presente Política como base de requerimientos.

ES COPIA FIEL DEL ORIGINAL
Abog. Laura Alfonso
Encargada de Despacho
Secretaría General

Los Prestadores de Servicios de Certificación que utilicen software criptográfico de seguridad deberán utilizar Dispositivos Seguros de Creación de Firma (SSCD) con un nivel de seguridad como el CommonCriteria o FIPS 140-2 Nivel 3 o superior.

7.2.5 Fines de uso de las claves

7.2.5.1 Autoridad Certificadora Raíz del Paraguay

Los usos de las claves de la Autoridad Certificadora Raíz del Paraguay permiten generar su par de claves, su certificado autofirmado, emitir los certificados a los PSC, firmar las Solicitudes de Firma de Certificados de los Prestadores de Servicios de Certificación, y la emisión y publicación de la Lista de Certificados Revocados (CRL).

7.2.5.2 Prestadores de Servicios de Certificación

Las claves de los Prestadores de Servicio de Certificación solo podrán utilizarse para la emisión de certificados digitales a usuarios finales y su Lista de Certificados Revocados.

7.3 Protección de la clave privada

7.3.1 Normas para el módulo criptográfico

Establecidos en el ítem 7.2.4 de la presente Política de Certificación.

7.3.2 Control de la clave privada

Para la activación de la clave privada se deberá implementar procedimientos (clave maestra) que requieran la participación de un mínimo de tres (3) custodios y la asignación de los mismos debe considerar la contraposición de intereses.

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

7.3.3 Copia de seguridad de la clave privada

La Autoridad Certificadora Raíz del Paraguay y los Prestadores de Servicios de Certificación mantienen una copia de seguridad de su clave privada, en su infraestructura tecnológica principal y contingencia.

7.3.3.1 La Autoridad Certificadora Raíz del Paraguay no mantienen copia de las claves privadas de los Prestadores de Servicios de Certificación

7.3.3.2 Los Prestadores de Servicios de Certificación no mantienen copia de las claves privadas de los certificados digitales de sus usuarios finales.

7.3.4 Recuperación de la clave privada

Ante una situación que requiera de la recuperación de la clave privada, la Autoridad Certificadora Raíz del Paraguay cuenta con procedimientos y elementos para su restauración.

7.3.5 Método de destrucción de la clave privada

Ante las circunstancias de causales de revocación, deberá procederse a la destrucción de la clave privada así como la clave maestra del módulo criptográfico (Software/Hardware) de forma que imposibiliten su posterior recuperación o utilización, bajo las mismas medidas de seguridad que se emplearon para su creación, 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.

Los módulos criptográficos (Software/Hardware) que custodien las claves deberán proveer dichas funcionalidades.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Miranda
Encargada de Despacho
Secretaría General

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 del Paraguay

A continuación se especifican los campos del Certificado de la Autoridad Certificadora Raíz del Paraguay utilizando el Algoritmo Sha256RSA.

Campo	Valor
Versión (Versión)	V3
Número de Serie (Serial Number)	Nro. de serie asignado por la Autoridad Certificadora Raíz del Paraguay
Algoritmo de Firma(SignatureAlgorithm)	SHA256RSA
Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
Válido desde (ValidFrom)	<fecha de ceremonia>

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución Nº 771-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN Nº 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

Válido hasta (ValidTo)	<fecha de ceremonia>+20 años
Sujeto (Suscriber DN)	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
Clave Pública (SubjectPublic Key)	Clave Pública de la Autoridad RSA de 4096 bits
Directivas del Certificado (Certificate Policies)	URL: http://www.acraiz.gov.py/documentación/politicas.pdf
Extensiones	
Identificador de clave del titular (Subject Key Identifier)	Hash de 20 bytes del atributo SubjectPublic Key
Restricciones básicas (Basic Constraints)	Tipo de asunto. Restricción de longitud de ruta.
Uso de la clave (Key Usage)	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)
Algoritmo de Identificación (IdentifierAlgorithm)	Sha1
Huella digital (ThaumbPrint)	Resultado de aplicar algoritmos matemáticos a la información.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

8.2 Perfil de Certificados del Prestador de Servicios de Certificación

Los certificados de las Prestadoras de Servicios de Certificación Habilitados en la República del Paraguay deberán cumplir el estándar ITU-T X.509 versión 3, como se muestra en el Punto 8.1.

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

A continuación se listan los campos de las Listas de Certificados Revocados según el estándar ITU-T X.509 versión 2.

Campo	Valor
Versión (Versión)	V2
Emisor (Issuer)	CN = Autoridad Certificadora Raíz del Paraguay O = Ministerio de Industria y Comercio C = PY
Fecha Efectiva (Effective Date)	Día y Hora de Emisión de la CRL
Próxima Actualización (NextUpdate)	<fecha de emisión>+3 meses
Algoritmo de Firma (SignatureAlgorithm)	SHA1RSA
Número CRL (CRL Number)	Número Secuencial asignado por la Autoridad Certificadora Raíz del Paraguay.
Identificador de clave de Entidad Emisora (Authority Key Identifier)	Identificador de la clave pública de la Autoridad Certificadora Raíz del Paraguay.
Emitir puntos de distribución (IssuingDistribution Point)	Lista de Certificados revocados incluyendo el nro. de serie (Serial Number) y la fecha de revocación.

ES COPIA FIEL DEL ORIGINAL

Abog. Laura Elisa Sandi Pucheta
Encargada de Despacho
Secretaría General

MINISTERIO DE INDUSTRIA Y COMERCIO

Resolución N° 771.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 165 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

8.4 Perfil de Listas de Certificados Revocados del Prestador de Servicios de Certificación

La lista de certificados revocados de las Prestadoras de Servicios de Certificación Habilitados en la República del Paraguay deberán cumplir el estándar ITU-T X.509 versión 2, como se muestra en el Punto 8.3.

9 ADMINISTRACIÓN DOCUMENTAL

9. 1 Procedimiento para modificaciones

La autoridad de Aplicación, aprobará mediante resolución la presente Política de Certificación y sus posteriores enmiendas o modificaciones."

Art. 2°.- Comunicar a quienes corresponda y cumplida, archivar.

Abog. Laura Minardi
Encargada de Despacho
Secretaría General

DZ/lm/gb

ES COPIA FIEL DEL ORIGINAL

DIEGO ZAVALA
Ministro