



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772.-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS 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° 166/2013, 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 N° 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 N° 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° 733369/2011 "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° 166 de fecha 06 de marzo de 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRACTICAS 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 Subsecretaría de Estado de Comercio como Autoridad de Aplicación de la normativa vigente.

Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 2 -

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.

POR TANTO,

EL MINISTRO DE INDUSTRIA Y COMERCIO

RESUELVE:

Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 3 -

Art. 1º.- Modificar y ampliar parcialmente el Anexo de la Resolución N° 166 de fecha 06 de marzo de 2013, en los siguientes puntos: 1.2, 1.3.1, 1.3.2, 1.3.4, 1.3.5, 1.4, 1.5, 1.5.1, 1.6, 2.6, 2.6.2, 3.1.2.1, 3.1.2.2, 3.1.2.3, 4.1, 4.2, 4.3, 4.4, 4.6, 5, 5.5, 6.1.2, 6.2.1, 6.2.2, 6.3, 8.1.

Quedando redactado de la siguiente manera:

"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

1.3.1 – Autoridad Aplicación – Función de Regulación

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

Abog. *Laura Mijangos*
Encargada de Despacho
Secretaría General



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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 4 -

1.3.2 - Autoridad de Aplicación – Función de Registro

Las funciones de Registro, son parte de los servicios de una Autoridad de Certificación.

Las funciones de registro que debe desempeñar la Autoridad de Aplicación están establecidas en las Políticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

1.3.4 –Prestadores de Servicios de Certificación

Entidad Jurídica habilitada por la Autoridad de Aplicación, para la prestación de Servicios de Certificación Digital, dicha entidad que deberá contar con un Certificado emitido por la Autoridad Certificadora Raíz del Paraguay y solo podrá emitir Certificados para usuarios finales. En el Paraguay, la cadena PKI tiene como máximo dos niveles, en el nivel uno se encuentra la Autoridad Certificadora Raíz del Paraguay y en el nivel dos los Prestadores de Servicio de Certificación.

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

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



Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 5 -

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 para los Prestadores de Servicios de Certificación habilitados y los Certificados a su vez emitidos por estos, para validar la cadena de confianza.

1.4 - Uso de los certificados

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

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

Abog. *Clara Miranda*
Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 6 -

1.5 - Administración de la Declaración de Prácticas

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

Nombre: Ministerio de Industria y Comercio

Dirección: Cap. Villamayor esq. Tte. 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/ 527 235

1.5.1 - Procedimiento de aprobación

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

Los Prestadores de Servicios de Certificación habilitados deberán implementar los procedimientos necesarios para mantener su Declaración de Prácticas de Certificación y sus posteriores enmiendas o modificaciones.



Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 7 -

1.6 - Definiciones y abreviaturas

Autoridad de Aplicación (AA): MIC – Ministerio de Industria y Comercio a través del Viceministerio de Comercio. Órgano Regulador competente designado por Ley, 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 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 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.

Abog. *Laura Miranda*
Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 8 -

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.

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.





MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 9 -

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 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.



Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 10 -

Clave Pública: La clave pública hace parte del sistema de "Infraestructura de Clave Pública" (PKI por sus siglas en inglés) 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 propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

Abog. Laura M. García
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 11 -

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.


Abog. Laura Minardi
Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 12 -

2.6. - Confidencialidad

A los efectos de la determinación del carácter de confidencial de la información recibida por la Autoridad de Aplicación se estará a los recaudos previstos de acuerdo con lo establecido en la Ley N° 1682/2001 "Que Reglamenta la Información de Carácter Privado" y su modificatoria la Ley N° 1969/2002 y la normativa vigente inherente.

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

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

ES COPIA FIEL DEL ORIGINAL

Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 13 -

3.1.2.1 – Identidad

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

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

3.1.2.2 – Habilitación

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

Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 14 -

3.1.2.3 - Clave privada

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

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 - Solicitud de Certificado

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

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



Abog. *Laura Aliardi*
Encargada de Despacho
Secretaría General

ES COPIA FIEL DEL ORIGINAL



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 15 -

Para solicitar el certificado, el Prestador de Servicios de Certificación genera las claves de su Autoridad Certificadora en presencia del/los funcionario/s de la Autoridad de Aplicación, y genera una solicitud en formato de archivo CSR (PKCS#10). Dicha solicitud debe contener únicamente la clave pública generada y los datos del DistinguishedName de la Autoridad Certificadora del Prestador de Servicios de Certificación, de acuerdo a lo estipulado en la Política de Certificación de la Autoridad de Certificadora Raíz del Paraguay. El CSR es entregado al funcionario de la Autoridad de Aplicación en un medio removible autorizado por él, de forma de continuar con el proceso de emisión.

4.2 - Procesamiento de Solicitud de Certificado

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

La Autoridad Certificadora Raíz deberá verificar que:

Abog. *Laura Miranda*
Encargada de Despacho
Secretaría General
La información contenida en el archivo CSR es consistente con la Resolución de habilitación dictada por la Autoridad de Aplicación.

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 16 -

- La información contenida en el archivo CSR deberá ser generada en un dispositivo removible autorizado por la Autoridad Certificadora Raíz del Paraguay, provista por el Prestador de Servicios de Certificación.
- El archivo CSR se encuentra firmado con la clave privada correspondiente a la clave pública en él contenida.
- Existen pruebas de que la clave privada generada está bajo absoluto control del Prestador de Servicios de Certificación y que además fue generada de acuerdo a los requerimientos estipulados en la presente Declaración de Prácticas y en la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay. Para este punto es suficiente una declaración de conformidad por parte del funcionario designado para presenciar la generación o por los auditores designados para tal tarea.
- El archivo CSR contiene los campos necesarios especificados para la generación del certificado, conforme a lo estipulado en el punto 8 de la Política de Certificación de Autoridad Certificadora Raíz del Paraguay.

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

Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 17 -

4.3 - Emisión de Certificado

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

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

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

El certificado emitido es retirado del sistema donde fue generado en un dispositivo removible provisto por el Prestador de Servicios de Certificación y aprobado por la Autoridad de Certificación Raíz del Paraguay. Este dispositivo es entregado al representante del Prestador de Servicios de Certificación, dejando una constancia formal del acto mediante la firma del Acuerdo para Suscriptores.

Una copia del certificado es almacenada en el directorio de certificados de la Autoridad Certificadora Raíz del Paraguay. Esta copia no es publicada en el repositorio de información durante esta instancia.


Abog. Laura Minardi
Encargada de Despacho
Secretaría General

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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 18 -

4.4 - Aceptación del Certificado

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

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

Abog. *Laura M. Mendi*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY"

- 19 -

4.6 - Renovación del Certificado

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

Para la renovación del certificado se deberá generar un nuevo par de claves en todos los casos. Otros requisitos para la renovación están estipulados en el punto 5.5 de la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

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

El objetivo de los controles de seguridad física, los controles de los procedimientos y del personal tienen como objetivo mantener un ambiente seguro y controlado para la protección de la Clave Privada de la Autoridad Certificadora Raíz del Paraguay, la información de los Prestadores de Servicios de Certificación, el ciclo de vida de los certificados emitidos etc.

Abog. Laura Minardi
Encargada de Despacho
Secretaría General



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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 20 -

Para esto, se contará con un Sistema de Gestión de la Seguridad de la Información, con Políticas y Procedimientos para garantizar la seguridad en sus operaciones. Dicho Sistema de Gestión de Información está alineado y se ajusta al ISO 27002, el cual está enfocado a proteger el material criptográfico involucrado en el ciclo de vida de los certificados de la Autoridad Certificadora Raíz del Paraguay y de los Prestadores de Servicios de Certificación.

5.5 – Retención de Registros e Información

Cada tipo de registro tiene definido el tiempo de retención. Los registros relativos a la gestión de claves y de certificados deberán mantenerse por un periodo de 10 (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.

No obstante los certificados emitidos por la Autoridad Certificadora Raíz del Paraguay son mantenidos en su directorio público por tiempo indefinido, incluso luego de su expiración y/o revocación, para permitir a terceros validar las firmas que fueron realizadas con ellos.

Los datos proporcionados por el titular del certificado deberán ser conservados indefinidamente por los Prestadores cualquiera sea el estado en que se encuentre el Certificado.

Abog. *Laura Minarelli*
Encargada de Despacho
Secretaría General



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 21 -

6.1.2 –Prestador de Servicios de Certificación

Se encuentra estipulado en el punto 7.1.2 de la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

6.2.1 – Autoridad Certificadora Raíz del Paraguay

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

6.2.2 –Prestador de Servicios de Certificación

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

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

Abog. *Laura Miranda*
Encargada de Despacho
Secretaría General



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



MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 772-

POR LA CUAL SE MODIFICA Y AMPLIA PARCIALMENTE EL ANEXO DE LA RESOLUCIÓN N° 166 DE FECHA 06 DE MARZO DE 2013 "POR LA CUAL SE APRUEBA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY"

- 22 -

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

6.3 – Protección de clave privada y controles de Módulos Criptográficos

Se encuentra estipulado en el punto 7.2.4.1 y 7.2.4.2 de la Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

8.1 – Procedimiento para modificaciones

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

Art. 2°.-

Comunicar a quienes corresponda y cumplida, archivar.

ES COPIA FIEL DEL ORIGINAL



Abog. *Laura Minardi*
Encargada de Despacho
Secretaría General

DIEGO ZAVALA
Ministro

DZ/lm/gb