# POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY

**Ministerio de Industria y Comercio**

**Viceministerio de Comercio**

**República del Paraguay**

**DOC-PKI-02**

**VERSIÓN 4.0**

## CONTROL DOCUMENTAL

| Documento | |
|---|---|
| **Título:** Política de Certificación de la Autoridad Certificadora Raíz del Paraguay. | **Nombre Archivo:** |
| **Código:** DOC-PKI-02 | **Soporte Lógico:** |
| **Fecha:** 28/10/2016 | **Ubicación Física:** DGFDyCE |
| **Versión:** 4.0 | |

| Registro de Cambios | | |
|---|---|---|
| **Versión** | **Fecha** | **Motivo de Cambio** |
| | | |
| | | |
| | | |

| Distribución del documento | |
|---|---|
| **Nombre** | **Área** |
| Ministerio de Industria y Comercio (MIC) | Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE) |
| Autoridad Certificadora (CA) | Prestadores de Servicio de Certificación (PSC) |
| Documento Público | www.acraiz.gov.py |

| Control del Documento | | |
|---|---|---|
| **Preparado por:** | **Revisado por:** | **Aceptado por:** |
| | | |
| ***Ing. Lucas Sotomayor***<br>***Lic. Claudia Dacak***<br>***M. Sc. Mario Monges*** | ***Lic. Noelia Smith*** | ***M. Sc. Rodys Rolón*** |

## CONTENIDO

# 1. INTRODUCCIÓN

## 1.1. DESCRIPCIÓN GENERAL

El Ministerio de Industria y Comercio (MIC), a través del Viceministerio de Comercio, se constituye en la Autoridad de Aplicación (AA) conforme lo dispone la Ley que rige la materia. La Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE) es la dependencia designada para ejecutar las funciones atribuidas al MIC en su calidad de AA.

Entre sus funciones principales se encuentran:

- Administrar la Autoridad Certificadora Raíz del Paraguay (CA Raíz).
- Dictar las normas que regulen los servicios de certificación digital en el país.
- Recepcionar, procesar y expedirse sobre solicitudes de habilitación de interesados en constituirse en Prestador de Servicios de Certificación (PSC).
- Inspeccionar y auditar al Prestador de Servicios de Certificación habilitado.
- Revocar la habilitación del PSC
- Imponer sanciones al PSC.

En la cúspide de la jerarquía de la Infraestructura de Clave Pública del Paraguay (PKI Paraguay), por sus siglas en inglés Public Key Infrastructure, se ubica la CA Raíz, la misma cuenta con un certificado autofirmado y aceptado por los terceros que confían en la PKI Paraguay.

Los certificados digitales emitidos por la CA Raíz, se rigen y ajustan a la presente Política de Certificación (CP), cuyo cumplimiento es de carácter obligatorio.

Esta CP fue elaborada conforme a las recomendaciones establecidas en el RFC 3647 ‘’INTERNET X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework’’; y contiene los principios y reglas relativos a la gestión de certificados digitales, las normas mínimas y básicas que debe cumplir la CA Raíz, el uso de los certificados digitales, entre otras cuestiones relacionadas con la PKI Paraguay.

En resumen, esta CP es específicamente aplicable a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz).
- Prestador de Servicios de Certificación (PSC).
    - Autoridad de Certificación Intermedia.
    - Autoridad de Registro (RA).
    - Autoridad de Validación (VA).
- Suscriptor.
- Parte que confía.

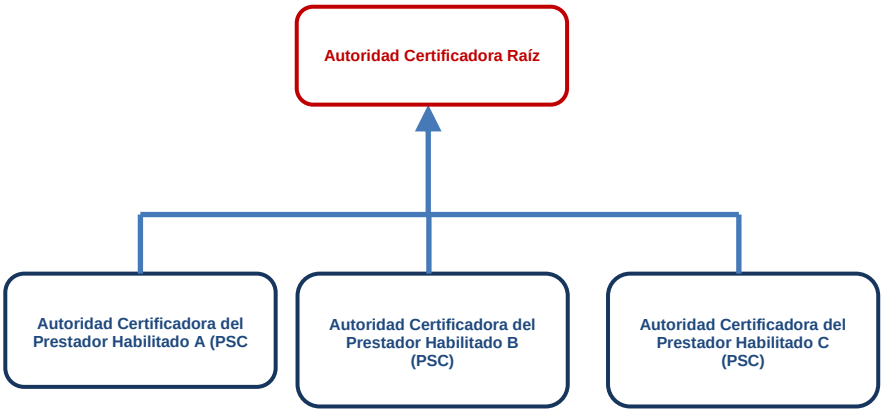
Esta política contempla los siguientes tipos de certificados:

- Certificado de CA Raíz.
- Certificado de PSC.

El PSC, una vez habilitado, pasa a ser parte de la cadena de confianza de la PKI Paraguay, y debe contar con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera una estructura jerárquica como se muestra en la figura 1.

En el Paraguay, la cadena de certificación tiene como máximo dos niveles, en el primer nivel se encuentra la CA Raíz, en el segundo nivel, uno o varios PSC; éstos solo podrán emitir certificados digitales a usuarios finales.

**Figura 1**



### 1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

**Nombre**: Política de Certificación de la Autoridad Certificadora Raíz del Paraguay.

**Versión**: 4.0

**Fecha de aprobación**: _____

**Sitio de Internet oficial**: www.acraiz.gov.py/cps/politicas.pdf

### 1.3. PARTICIPANTES DE LA PKI

Las entidades y personas intervinientes en la PKI son:

- Autoridad de Certificación (CA).
- Autoridad de Registro (RA).
- Suscriptores.
- Terceros que confían.
- Otros participantes.

#### 1.3.1 AUTORIDAD DE CERTIFICACIÓN (CA).

Son las entidades autorizadas a emitir certificados de claves públicas dentro de la PKI Paraguay. Esto incluye a:

- **Ministerio de Industria y Comercio (MIC)**, en su carácter de Autoridad Certificadora Raíz del Paraguay (CA Raíz) o Autoridad de Certificación Raíz del Paraguay (CA Raíz), indistintamente; emite certificados a los PSC bajo la jerarquía del Certificado Raíz, el cual es auto-firmado y a partir de él, se inicia la cadena de confianza. Subordinados al Certificado Raíz, se encuentran los certificados emitidos al PSC;
- **Prestador de Servicios de Certificación (PSC),** en su carácter de Autoridad Certificadora Intermedia, es la persona jurídica que emite certificados digitales para personas físicas y/o jurídicas que permiten identificar a dichos titulares. El PSC, una vez habilitado, pasa a ser parte de la cadena de confianza de la PKI Paraguay, y debe contar con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera, una estructura jerárquica.

### 1.3.2. AUTORIDAD DE REGISTRO (RA)

La RA ejecuta labores de identificación y autenticación del solicitante de un Certificado, valida los requisitos de identificación y atributos del solicitante, dependiendo del tipo de certificado y de la especificación de la Política pertinente. Además, tramita las solicitudes de emisión y revocación de certificados. La DGFDyCE y el PSC cumplen funciones de RA.

La actividad de identificación y registro del PSC será realizada durante el proceso de habilitación, no habiendo otra autoridad de registro en el ámbito de la CA Raíz, más que la DGFDyCE.

El PSC podrá delegar las funciones de registro a otras organizaciones, que siempre estarán bajo su responsabilidad y control, cumpliendo las normas y procedimientos establecidos en la normativa vigente, previa comunicación y autorización de la AA.

La RA podrá llevar a cabo sus actividades en una sede fija o en modalidad móvil, siempre que medie autorización de la AA.

### 1.3.3. SUSCRIPTORES

Respecto a la CA Raíz, es suscriptor el PSC; en relación a este último, es suscriptor toda persona física o jurídica a quien se emite un certificado digital, dentro de la jerarquía PKI Paraguay.

### 1.3.4. PARTE QUE CONFÍA

Es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales relacionadas con el mismo, emitidos dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

### 1.3.5. OTROS PARTICIPANTES

Sin estipulaciones.

## 1.4. USO DEL CERTIFICADO

### 1.4.1 USOS APROPIADOS DEL CERTIFICADO

| TIPO | DESCRIPCIÓN DE USO APROPIADO |
|---|---|
| Certificado de CA Raíz | Es un certificado autofirmado utilizado para firmar certificados de PSC y CRL de la CA Raíz.<br>● Firma de Certificado (Certificate Signing)<br>● Firma de CRL sin conexión (Off line CRL Signing) |
| Certificado de PSC. | Certificado emitido por la CA Raíz, utilizado por el PSC con el único propósito de validar la cadena de confianza de la PKI, firmar los certificados emitidos a sus suscriptores finales y firmar la lista de certificados revocados.<br>● Firma de Certificado (Certificate Signing)<br>● Firma de CRL (CRL Signing) |

### 1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos deben ser utilizados en el marco de la normativa vigente que rige la materia.

Cualquier otro uso de los certificados no especificado en esta CP y en la normativa vigente, está fuera del alcance y responsabilidad de esta CP. El uso indebido del certificado, será sancionado por la AA, inclusive con la revocación del mismo.

## 1.5 ADMINISTRACIÓN DE LA POLÍTICA

### 1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

**Nombre**: Ministerio de Industria y Comercio.

**Dirección:** Avenida Mcal. López 3333. Asunción, Paraguay.

**Teléfono:** (+595) (21) 616-3000.

**Dirección de correo electrónico**: consultas@mic.gov.py

**Página Web:** www.mic.gov.py

### 1.5.2. PERSONA DE CONTACTO

**Nombre:** Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE).

**Dirección:** Capitán Pedro Villamayor esq. Capitán Nicolás Blinoff. Asunción, Paraguay.

**Teléfono:** (+595) (21) 616-3000.

**Dirección de correo electrónico**: info-dgfdce@mic.gov.py.

### 1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA POLÍTICA

En el caso de la CPS de la CA Raíz, la Máxima Autoridad Institucional, será la encargada de determinar la adecuación de la Declaración de Prácticas de Certificación (CPS) a la CP de la CA Raíz.

El PSC deberá designar ante la AA, el responsable competente para determinar la adecuación de su CPS a las CP que implementen según la normativa vigente.

### 1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA POLÍTICA DE CERTIFICACIÓN (CP)

El MIC aprobará el contenido de la presente Política de Certificación y sus posteriores enmiendas o modificaciones, por resolución ministerial. Se podrá someter a consideración de entidades públicas y privadas relacionadas al área, para que emitan sus comentarios y sugerencias, previo al trámite de aprobación

El PSC deberá establecer sus procedimientos para aprobación y puesta en vigencia de las CP que implementan y ser aprobadas por la AA.

## 1.6 DEFINICIONES Y ACRÓNIMOS

### 1.6.1 DEFINICIONES

**Acuerdo de Suscriptores:** es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita de las partes intervinientes.

**Armario ignífugo:** armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.

**Autenticación:** proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.

**Autoridad de Aplicación (AA):** se designa al Ministerio de Industria y Comercio como órgano regulador competente 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”. Ejerce funciones a través de su unidad administrativa, la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio.

**Autoridad de Certificación (CA):** entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI Paraguay, son Autoridades de Certificación, la CA Raíz del Paraguay y el PSC.

**Autoridad Certificadora Raíz o Autoridad de Certificación Raíz (CA Raíz):** es el órgano técnico dentro de la PKI, cuya función principal es habilitar al PSC y emitir a éste, el certificado digital correspondiente. Posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza.

**Autoridad de Certificación Intermedia (CA)**: entidad cuyo certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz; es responsable de la emisión de certificados a usuarios finales.

**Autoridad de Registro (RA):** entidad responsable de la identificación y autenticación de titulares de certificados digitales; la misma no emite ni firma certificados. Una RA interviene en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA, no necesita ser un organismo separado, sino que puede ser parte de la CA.

**Autoridad de Validación (VA):** entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una autoridad de registro y certificados por la autoridad de certificación. La VA, no necesita ser un organismo separado sino que puede ser parte de la CA.

**Cadena de certificación:** lista ordenada de certificados que contiene un certificado de usuario final y certificados de CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado de CA y a su vez, el emisor del certificado de CA es el titular del certificado de CA Raíz. El usuario final o la parte que confía, debe verificar la validez de los certificados en la cadena.

**Ceremonia de claves:** procedimiento mediante el cual es generado un par de claves de CA, su clave privada es generada y almacenada en un módulo criptográfico, y debe ser respaldada con el mismo nivel de seguridad que la clave original. Este procedimiento debe ser documentado.

**Certificado Digital (CD):** es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.

**Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que solo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.

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

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

**Clave pública y privada:** la criptografía en la se basa la PKI Paraguay, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado digital, mientras que a la otra se le denomina privada y está bajo la custodia del titular del certificado.

**Cofre de seguridad:** compartimiento para almacenar materiales o documentos sensibles de la CA, debe ser resistente al fuego y ofrecer protección a aperturas forzadas.

**Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.

**Data Center (Centro de Datos):** infraestructura compuesta por el espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una CA, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados digitales emitidos por la CA.

**Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

**Declaración de Prácticas de Certificación (CPS):** declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP

vigente.

**Delta CRL:** partición del CRL, dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.

**Emisión:** comprende la generación del certificado, cuyo proceso es una función de la CA.

**Emisor del certificado:** organización cuyo nombre aparece en el campo emisor de un certificado.

**Estándares Técnicos Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

**Firma Digital:** es una firma electrónica certificada por un prestador habilitado, 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.

**Grupo Electrógeno:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la CA, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.

**Habilitación:** autorización que otorga el MIC al PSC para emitir certificados digitales a usuarios finales, una vez cumplidos los requisitos y condiciones establecidos en la norma.

**Huella digital (Código de verificación o resumen):** secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) el mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo (2) sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo (3) sea improbable, por medios técnicos, que se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

**Identificación:** procedimiento de reconocimiento de la identidad de un solicitante o titular de certificado dentro de la jerarquía PKI Paraguay.

**Identificador de Objeto (OID):** los identificadores de objeto son un sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.

**Infraestructura de Clave Pública (PKI):** es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos

**Integridad:** característica que indica que un mensaje de datos o un documentos electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

**Jerarquía PKI:** jerarquía de confianza que se conforma por un conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior (CA Raíz) garantiza la confiabilidad de una o varias de nivel inferior (PSC) y a su vez, de los certificados emitidos por éstos a los suscriptores.

**Lista de certificados revocados (CRL**): lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

**Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.

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

**No Repudio:** refiere que la posesión de un documento electrónico y la firma digital asociada al mismo, será prueba efectiva del contenido y del autor del documento.

**Par de claves:** son las claves privada y pública 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.

**PKCS#1**: estándar de criptografía de clave pública #1, desarrollado por RSA Security Inc., que proporciona las definiciones básicas y recomendaciones para la implementación de algoritmo RSA para criptografía de clave pública.

**PKCS#10** (Certification Request Syntax Standard): Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

**Parte que confía:** es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido bajo la jerarquía de la PKI Paraguay.

**Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

**Periodo de operación:** periodo de vigencia de un certificado, que comienza en la fecha y la hora en que es emitido por una CA, y termina en la fecha y la hora en que

expira o se revoca el mismo.

**Periodo de uso:** rrefiere al tiempo establecido para los certificados emitidos dentro la jerarquía de la PKI para determinados usos.

**Política:** orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

**Política de Certificación: (CP)** documento en el cual la CA, define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.

**Práctica:** modo o método que particularmente observa alguien en sus operaciones.

**Prestador de Servicios de Certificación (PSC):** entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz del Paraguay y solo podrá emitir certificados a usuarios finales.

**Registro de Auditoría:** registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.

**Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.

**Rol de confianza:** función crítica que desempeña personal de la CA, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.

**Ruta del certificado:** secuencia ordenada de certificados de entidades que, junto a la clave pública de la entidad inicial en la ruta, puede ser procesada para obtener la clave pública de la entidad final en la ruta.

**Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.

**Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una CA.

**Solicitud de Firma de Certificado (CSR):** es una petición de certificado digital que se envía a la CA. Mediante la información contendida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

**Suscriptor:** persona física o jurídica titular de un certificado digital emitido por una CA.

**Usuario final:** persona física o jurídica que adquiere un certificado digital de un PSC.

**Validez de la firma:** aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado.

**Verificación de la firma:** determinación y validación de: a) que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

**X. 500**: estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511. X.518, X.519, X.520, X.521, X.525.

**X. 509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

### 1.6.2 ACRÓNIMOS

| Acrónimo | Descripción |
|---|---|
| C | País (C por sus siglas en inglés, Country) |
| CA | Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority) |
| CAI | Autoridad de Certificación Intermedia (Certificate Authority Intermediate) |
| CA Raíz | Autoridad Certificadora Raíz del Paraguay |
| CI | Cédula de identidad |
| CN | Nombre común (CN por sus siglas en inglés, Common Name) |
| CP | Políticas de Certificación (CP por sus siglas en inglés, certificate policy) |
| CPS | Declaración de Prácticas de Certificación (CPS por sus siglas en inglés, certification practice statement) |
| CRL | Lista de certificados revocados (CRL por sus siglas en inglés, certificate revocation list) |
| CSR | Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request) |
| CWA | Documento de referencia del Comité Europeo de Normalización (CEN) desarrollado y aprobado en un taller de trabajo, algunos de los CWA son específicos para firma electrónica (CEN Workshopp Agreement) |
| DGFDyCE | Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio. |
| DNS | Servicio de nombre de dominio (DNS por sus siglas en inglés Domain Name server) |
| FIPS | Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés, Federal Information Processing |

| | |
|---|---|
| | Standards). |
| HSM | Módulo de seguridad criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware security module) |
| ISO | Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization). |
| ITU-T | Unión Internacional de Telecomunicaciones – Sector de normalización de las telecomunicaciones (ITU-T por sus siglas en inglés International Telecomunication Union – Telecomunication Standardization Sector) |
| MIC | Ministerio de Industria y Comercio |
| O | Organización (por su sigla en inglés, Organization) |
| OCSP | Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol). |
| OID | Identificador de Objeto (OID por sus siglas en inglés, Object Identifier). |
| OU | Unidad Organizacional (OU por sus siglas en inglés, Organization Unit) |
| PIN | Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number) |
| PKCS | Norma de criptografía de clave pública (PKCS por sus siglas en inglés, Public Key Cryptography Standard) |
| PKI | Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure). |
| PSC | Prestador de Servicios de Certificación |
| PY | Paraguay |
| RA | Autoridad de Registro (RA por sus siglas en inglés, Registration Authority). |

| | |
|---|---|
| RFC | Petición de Comentarios (RFC por sus siglas en inglés, Request for Comments) |
| RSA | Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman |
| RUC | Registro único del contribuyente |
| SN | Número de Serie (por sus siglas en inglés, Serial Number) |
| TLS | Capa de conexión segura (TLS por sus siglas en inglés, Transport Layer Security) |
| UPS | Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply) |
| URL | Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator). |
| VA | Autoridad de validación (VA por sus siglas en inglés, Validation Autorithy) |

# 2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

## 2.1. REPOSITORIOS

Conforme a lo estipulado en la CPS.

## 2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Conforme a lo estipulado en la CPS.

## 2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Conforme a lo estipulado en la CPS.

## 2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Conforme a lo estipulado en la CPS.

# 3. IDENTIFICACIÓN Y AUTENTICACIÓN

## 3.1 NOMBRES

### 3.1.1 TIPOS DE NOMBRES

Todos los titulares de certificados requieren un nombre distintivo (Distinguished Name) conforme con el estándar X.500.

A continuación se presentan los formatos de los nombres para el suscriptor del certificado dependiendo de su tipo.

**En el caso de la CA Raíz**

| Campo | Contenido | Descripción |
|---|---|---|
| Country (C) | PY | Código de país es asignado de acuerdo al estándar ISO 3166 |
| Organization (O) | Ministerio de Industria y Comercio | Ministerio de Industria y Comercio es el responsable la administración de la CA Raíz de Paraguay |
| Common Name (CN) | Autoridad Certificadora Raíz del Paraguay | Nombre de la CA Raíz de la PKI Paraguay |

**En el caso del PSC**

| Campo | Ejemplo | Descripción |
|---|---|---|
| Country (C) | PY | Código de país es asignado de acuerdo al estándar ISO 3166 |

| | | |
|---|---|---|
| Organization (O) | Firma Fiel S.A. | Denominación o Razón Social de la Persona Jurídica habilitada como PSC |
| Common Name (CN) | CA-Firma Fiel S.A. | Nombre de la CA |
| Serial Number {OID: 2.5.4.5} | RUC 99999999-9 | RUC Registro Único de Contribuyente correspondiente al PSC emitido por la Subsecretaría de Estado de Comercio del Ministerio de Hacienda. Debe ser validado durante el proceso de registro. |

### 3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Conforme a lo estipulado en la CPS.

### 3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Conforme a lo estipulado en la CPS.

### 3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

La regla utilizada por la CA Raíz para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

Para el certificado de PSC se requiere:

La Cédula Tributaria – RUC es expedida por la Subsecretaría de Estado de Tributación del Ministerio de Hacienda y debe cumplir el siguiente formato :

| Tipo de Documento | Prefijo | Formato |
|---|---|---|
| Cédula Tributaria – RUC | RUC | RUC 99999999-9 |

### 3.1.5 UNICIDAD DE LOS NOMBRES

El conjunto de nombre distintivo (Distinguished Name), más el contenido de la extensión Policy Identifier, debe ser único y no ambiguo. El uso del número RUC del PSC en la sección Número de Serie (Serial Number) del campo Sujeto (Subject)

garantiza la unicidad del mismo.

### 3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Conforme a lo estipulado en la CPS.

### 3.2 VALIDACIÓN INICIAL DE IDENTIDAD

La CA Raíz garantiza que el PSC sea la persona identificada en la solicitud del certificado, y que la información que se incluya en el certificado sea exacta. En principio, la exactitud y veracidad de la información proporcionada por el suscriptor es atribuida al mismo, sin perjuicio de la respectiva comprobación por parte de la CA Raíz.

### 3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

El solicitante del certificado debe demostrar que posee la clave privada correspondiente a la clave pública que deberá ser listada en el certificado. La posesión de la clave privada, correspondiente a la clave pública para la que se solicita que se genere el certificado, quedará probada mediante la generación y entrega de la solicitud de firma de certificado (CSR) en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por la DGFDyCE, en la cual se incluirá la clave pública firmada mediante la clave privada asociada. El CSR se genera en presencia del representante de la AA de acuerdo al procedimiento de habilitación del PSC.

### 3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

La CA Raíz en su función de autoridad de registro valida la identidad de la organización solicitante.

La CA Raíz garantiza que el titular del certificado sea la misma persona jurídica identificada en la solicitud de un certificado, y que la información que se incluye en el certificado sea verdadera y exacta. Como mínimo, valida:

- Nombre o razón social;
- Documento que acredite la creación de la persona jurídica;

- RUC;
- Documento que acredite al representante legal;
- Nombre y documento de identidad del representante legal; y
- Domicilio de la persona jurídica.

**3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA**

No aplica.

**3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA**

No aplica.

**3.2.5. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)**

La CA Raíz determina si el solicitante se encuentra apto para solicitar un tipo de certificado específico. Además, valida que el solicitante no posee impedimentos legales.

Verifica:

- Nombre o razón social y cédula tributaria;
- Nombre y documento de identidad del representante legal; y
- Mayoría de edad del representante legal.

La información suministrada por el solicitante debe ser corroborada contra los datos oficiales correspondientes.

**3.2.6. CRITERIOS PARA INTEROPERABILIDAD**

Conforme lo estipulado en la CPS.

**3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES**

**3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES RUTINARIA**

No se permite la re emisión de claves.

**3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RE EMISIÓN DE CLAVES DESPUÉS DE UNA REVOCACIÓN**

No se permite bajo estas circunstancias, la re emisión de claves. Luego del

procedimiento de revocación, se debe solicitar la emisión de un nuevo certificado.

### 3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

El procedimiento de revocación asegura, que la solicitud de revocación ha sido generada por el suscriptor del certificado o por una entidad autorizada para tales propósitos. El PSC deberá informar a la AA sobre las personas autorizadas para solicitar la revocación.

Los procedimientos aceptados para la autenticación del solicitante de la revocación incluyen algunos de los siguientes mecanismos:

- El envío de un mensaje de datos firmado digitalmente al sistema de información designada por la AA.
- Presencialmente a través de los procesos de autenticación de identidad (secciones 3.2.2. y 3.2.3.)
- Cualquier otro medio aprobado por la DGFDyCE que permita una identificación veraz y segura.

Los sujetos habilitados para solicitar la revocación se encuentran establecidos en la sección 4.9.2 y los procedimientos de revocación en la sección 4.9.3.

# 4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

## 4.1 SOLICITUD DEL CERTIFICADO

### 4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

La solicitud de certificado para un PSC solo es posible después de la aprobación de su solicitud de habilitación como tal.

Una vez emitida la resolución de habilitación, se realizará el proceso de emisión de certificado conforme a los procedimientos establecidos en la "**GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA HABILITACIÓN Y AUDITORÍA A PRESTADORES DE SERVICIOS DE CERTIFICACIÓN**".

La solicitud debe ser presentada por el representante legal o apoderado del PSC con poder suficiente, utilizando el estándar definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

### 4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

La DGFDyCE tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad del PSC;
- Validar la información suministrada en la solicitud de firma de certificado (CSR);
- Velar que el PSC cumpla con los requisitos establecidos en la normativa vigente que rige la materia;
- Informar al PSC de sus deberes y responsabilidades por el uso del certificado; y
- Emitir y entregar el certificado de acuerdo con la información suministrada por el solicitante.

El solicitante tiene las siguientes responsabilidades

- Presentar la solicitud de Habilitación ante el MIC conforme a las

disposiciones de la normativa vigente;

- Acreditar los requisitos básicos previstos en la normativa vigente;
- Generar el CSR conforme a lo estipulado en el apartado 3.2.1 de la presente política; y
- Firmar el Acuerdo de Suscriptores.

El MIC a través de la DGFDyCE, ejecuta funciones de identificación y autenticación de acuerdo con las disposiciones establecidas en el punto 3.2 de esta política.

**4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO**

El MIC lleva adelante la aceptación o rechazo de la solicitud de certificado, conforme a la normativa vigente y a lo establecido en esta política.

**4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO**

El tiempo de procesamiento del CSR, será como máximo de cinco días hábiles contados a partir de la notificación al PSC de la Resolución Ministerial de Habilitación.

**4.3 EMISIÓN DEL CERTIFICADO**

**4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS**

Finalizado todo el proceso de evaluación del solicitante a PSC, y una vez emitida la resolución de habilitación, el MIC procede al proceso de emisión de certificado.

La emisión del certificado se realiza en las instalaciones de la CA Raíz del Paraguay y estará a cargo del personal técnico calificado y autorizado para tales efectos.

La CA Raíz ejecuta sus procedimientos internos de emisión de certificado y asegura ante los mismos, el cumplimiento de las condiciones de seguridad requeridas en la sección 5.

La emisión de un certificado implica, la realización de las siguientes acciones por parte de la CA Raíz:

- Asegura que la generación de un par de claves y un certificado se haya realizado de manera segura de acuerdo a la sección 3.2.1;
- Certifica la asociación del par de claves y que corresponde a un suscriptor, y que el par de claves se encuentra en su posesión; y
- Emite el certificado digital para su uso operativo, de acuerdo con el nombre distintivo asociado con el suscriptor. La CA Raíz, asegura que el certificado emitido pueda ser instalado por el PSC en presencia del personal asignado por la CA Raíz.
- Entrega del certificado emitido, en el formato definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**, al representante legal del PSC presente en la ceremonia.

### 4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

Aprobada y suscripta la resolución de habilitación, el MIC informa al PSC de la fecha para la generación del CSR y emisión de certificado. Todos los procedimientos se realizan conforme lo establecido en la "**GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA HABILITACIÓN Y AUDITORÍA A PRESTADORES DE SERVICIOS DE CERTIFICACIÓN**".

## 4.4. ACEPTACIÓN DEL CERTIFICADO

### 4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Una vez recibido el certificado, el PSC verifica que la información contenida en el certificado sea correcta.

Aceptado el certificado, el PSC deberá entregar al MIC el acuerdo de suscriptores firmado por el representante legal y proceder a la instalación del certificado en su infraestructura en presencia de los funcionarios del MIC.

En caso de rechazo del certificado, la CA Raíz lo revocará.

### 4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA CA

La CA Raíz publica en su repositorio público su certificado y todos los

certificados por ella emitidos, además del número de la resolución que concede la habilitación al PSC, el nombre o razón social de éste, la dirección social, el número de teléfono, sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros que exige la Ley.

### 4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA CA A OTRAS ENTIDADES

No se definen entidades externas que necesiten o requieran ser notificados respecto a los certificados emitidos por la CA.

## 4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

### 4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

El uso de la clave privada correspondiente a la clave pública, contenida en el certificado, solamente se permite una vez que el PSC haya aceptado el certificado emitido, dicho uso, debe realizarse conforme a la normativa vigente, lo estipulado en esta política y en el acuerdo de suscriptores.

El PSC debe proteger su clave privada del uso no autorizado y una vez expirado o revocado el certificado, su uso queda expresamente prohibido.

La utilización de la clave privada para un fin distinto a lo establecido en la normativa puede ser causal de revocación de certificado y/o suspensión de la habilitación del PSC.

**Certificado de CA Raíz**

La Clave privada y el certificado de la Autoridad Certificadora Raíz del Paraguay, será utilizado con el único propósito de:

- Firmar certificado de PSC; y,
- Firmar la Lista de Certificados Revocados (CRL) correspondientes.

**Certificado de PSC**

La clave privada y el certificado del PSC podrá ser utilizado con el único propósito de:

- Firmar los certificados que emite el PSC.

- Firmar la Lista de Certificados Revocados (CRL) correspondientes.
- Firmar los Certificados de OCSP.

### 4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA

La parte que confía debe aceptar las estipulaciones establecidas en la presente política, en todo lo que les resulte aplicable, como condición indispensable para confiar en el certificado.

Antes de cualquier acto de confianza la parte que confía debe realizar las siguientes comprobaciones:

- Que el certificado sea utilizado para un propósito apropiado, y que no esté prohibido o restringido por la presente Política y las Resoluciones que dicte la AA. Una CA no es responsable de esta tarea.
- El estado del certificado y el estado de todos los certificados de las CA en la cadena que emitieron los certificados.

## 4.6 RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVE

Cuando un certificado requiera ser renovado debe solicitarse uno nuevo, de acuerdo con la sección 4.1 de esta CP.

El PSC debe solicitar la emisión del nuevo certificado a la CA Raíz, con una antelación mínima de seis meses a la expiración del tiempo de uso del certificado que posee, conforme al punto 5.6 de la presente CP.

### 4.6.1 CAUSA PARA RENOVACIÓN DE CERTIFICADO

La causa para la emisión de un nuevo certificado al PSC es por la caducidad o revocación. La emisión del nuevo certificado realizada en el ámbito de esta CP será con cambio de claves.

### 4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

El representante legal o apoderado del PSC con poder suficiente puede solicitar la emisión del nuevo certificado.

### 4.6.3 PROCEDIMIENTO DE SOLICITUD DE RENOVACIÓN DE CERTIFICADO

El PSC debe solicitar la emisión del nuevo certificado a la CA Raíz, con una antelación mínima de seis meses a la expiración del tiempo de uso del certificado que posee, conforme al punto 5.6 de la presente CP.

### 4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

Una vez admitida la solicitud de emisión de un nuevo certificado, el MIC informa al PSC de la fecha para la generación del CSR y emisión de certificado. Los procedimientos serán iguales a los realizados en el proceso de habilitación.

### 4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Se realiza conforme a lo que está estipulado en el punto 4.4.1.

### 4.6.6 PUBLICACIÓN POR LA CA DEL CERTIFICADO RENOVADO

Se realiza conforme a lo que está estipulado en el punto 4.4.2.

### 4.6.7 NOTIFICACIÓN POR LA CA DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

Se realiza conforme a lo que está estipulado en el punto 4.4.3.

## 4.7 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE

La renovación del certificado sin cambio de clave no está permitida por esta CP.

### 4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

No aplica.

### 4.7.2 QUIEN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

No aplica.

### 4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO

No aplica.

### 4.7.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

### 4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

No aplica.

### 4.7.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS RE-EMITIDOS

No aplica.

### 4.7.7 NOTIFICACIÓN POR LA CA DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

No aplica.

## 4.8 MODIFICACIÓN DE CERTIFICADOS

### 4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

No aplica.

### 4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

No aplica.

### 4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

No aplica.

### 4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

### 4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No aplica.

### 4.8.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS MODIFICADOS

No aplica.

### 4.8.7 NOTIFICACIÓN POR LA CA DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

No aplica.

## 4.9 REVOCACIÓN Y SUSPENSIÓN

### 4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Las causales para revocación de certificados son:

- Cuando existan evidencias de que la clave privada se encuentra **comprometida**, o con riesgo cierto de estarlo;
- Cuando la información incluida en el certificado es incorrecta o ha cambiado;
- Incumplimiento del acuerdo de suscriptor;
- Insolvencia, quiebra o liquidación del PSC;
- Cese de actividades;
- Si se comprueba la expedición de certificados con información falsa;
- Incumplimiento grave de la CP y/o CPS aplicable;
- Uso indebido del certificado digital;
- Si se constata que los procedimientos de emisión de los certificados han dejado de ser seguros; y
- Otras causales especificadas en la normativa y reglamentación vigente.

### 4.9.2 QUIEN PUEDE SOLICITAR REVOCACIÓN

Los habilitados para realizar la solicitud de revocación son:

- El MIC en su función de CA Raíz, respecto a su propio certificado, o de oficio, del certificado del PSC, emitido por él.;
- El PSC por medio de su representante legal o apoderado con poder suficiente; y
- Autoridad Judicial competente.

### 4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

El procedimiento de revocación de un certificado se inicia con la solicitud de revocación y termina con la emisión de una nueva Lista de Certificados Revocados

(CRL).

Un certificado revocado será válido únicamente para la verificación de firmas generadas durante el periodo en que el referido certificado era válido.

La AC raíz, determinará mediante una Resolución Ministerial, la revocación de su propio certificado, así como del emitido al PSC, previo dictamen técnico y jurídico, debida y suficientemente fundada.

El PSC podrá solicitar la revocación de su certificado indicando las causales y el motivo del pedido de revocación de las siguientes maneras:

- Presencial: a través de los procesos de autenticación de identidad, indicados en esta CP.
- Correo electrónico: enviando al correo oficial de la DGFDyCE, la solicitud de revocación firmada digitalmente por el representante legal, siempre que lo haga con un certificado vigente, salvo que la clave privada se encuentre en entredicho, en cuyo caso la solicitud de revocación solamente podrá hacerse en forma presencial.

En los casos que la solicitud de revocación provenga de una Autoridad Judicial Competente, la CA Raíz iniciara el procedimiento de revocación. Antes de comenzar con el proceso de revocación se deberá notificar al PSC.

El MIC podrá revocar de oficio el certificado de un PSC en caso de comprobar una infracción grave por parte de la misma.

En caso que el PSC a quien se le ha revocado su certificado, desee no obstante seguir operando como tal, y si no existe impedimento o prohibición, deberá solicitar nuevamente ante el MIC su habilitación, presentando las documentaciones indicadas en la normativa y reglamentación vigente.

### 4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

No se estipulan periodo de gracia para revocación de certificados.

### 4.9.5 TIEMPO DENTRO DEL CUAL LA CA DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

El plazo máximo entre la recepción de la solicitud de revocación y la actualización de la Lista de Certificados Revocados (CRL), indicando los motivos de la revocación, es de veinticuatro (24) horas.

### 4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

Las partes que confían deben evaluar el estado del certificado y el estado de todos los certificados de las CA en la cadena a la que pertenece el certificado, antes de confiar en él.

Para ello, las partes que confían pueden verificar el estado del certificado mediante el servicio de: OCSP o CRL más reciente, proveída por las CA.

### 4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

La Lista de Certificados Revocados de la CA Raíz deberá ser actualizada y publicada cuando ocurra al menos uno de los siguientes hechos:

- Cuando se produzca la revocación de su propio certificado o de un certificado digital emitido al PSC
- Tres meses después de la última emisión del CRL

### 4.9.8 LATENCIA MÁXIMA PARA CRLS

La CA Raíz debe publicar la CRL en el repositorio en un plazo no mayor a una hora posterior a su generación.

### 4.9.9 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN/ ESTADO EN LÍNEA

La CA Raíz debe mantener disponible un repositorio con información del estado de los certificados emitidos, el cual puede ser accedido vía web.

Se debe garantizar la disponibilidad de las CRL con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

La AC Raíz deberá publicar en su repositorio de información los certificados

emitidos así como también la CRL correspondiente para su consulta online.

### 4.9.10 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

La parte que confía debe verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección anterior.

### 4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

Sin estipulaciones

### 4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

El compromiso de la clave privada de una CA será notificado, en la medida posible, a todos los participantes de la PKI Paraguay, en especial a:

- Todos los suscriptores de certificados emitidos por esa CA; y
- Terceros que confían, los que se tenga conocimiento.

Además la CA deberá publicar el compromiso de su clave en su sitio principal de Internet y procederá a la inmediata gestión de la revocación de su certificado y el de sus suscriptores. La CA, publicará el certificado revocado en el repositorio.

En caso de haberse revocado el certificado de la CA Raíz y subsanada la circunstancia que la motivó, ésta debe:

- Generar su nuevo certificado;
- Emitir un nuevo certificado para el PSC habilitado; y
- Asegurar que todos los nuevos certificados emitidos por el PSC estén firmados con la nueva clave.

En el caso de que la clave privada comprometida sea de la CA Raíz, se eliminará el certificado de todas las aplicaciones y se distribuirá uno nuevo.

En caso de haberse revocado el certificado del PSC y subsanada las circunstancias que la motivó, ésta debe:

- Solicitar nuevamente su habilitación; y
- Emitir un nuevo certificado a sus suscriptores.

El plan de continuidad del negocio del PSC, deberá establecer que en el caso de compromiso de su clave, el certificado asociado será inmediatamente revocado, igualmente serán revocados todos los certificados que hayan sido emitidos con ese certificado, pudiendo el PSC como política comercial, disponer la emisión de un nuevo certificado a sus suscriptores en forma gratuita por un periodo igual al restante para que el certificado revocado llegare a su término de extinción

**4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN**

Según la normativa no se aplica la suspensión del Certificado.

**4.9.14 QUIEN PUEDE SOLICITAR LA SUSPENSIÓN**

No aplica.

**4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN**

No aplica.

**4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN**

No aplica.

**4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO**

**4.10.1 CARACTERÍSTICAS OPERACIONALES**

La CA Raíz pública en su repositorio de información, los certificados emitidos así como también la CRL correspondiente para su consulta online. El repositorio se encuentra en https://www.acraiz.gov.py.

Los PSC deberán implementar servicios de validación de estado OSCP. Estos servicios son adicionales a la CRL, y deberán documentar su mecanismo de uso en su CPS y proveer la URL de consulta en la misma.

**4.10.2 DISPONIBILIDAD DEL SERVICIO**

Los sistemas de distribución de CRL y de consulta en línea del estado de los certificados deberán estar disponibles con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

**4.10.3 CARACTERÍSTICAS OPCIONALES**

Sin estipulaciones

### 4.11 FIN DE LA SUSCRIPCIÓN

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado, por cualquiera de las causas establecidas en la presente política, antes del vencimiento (fecha de expiración); y
- Expiración del certificado.

### 4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

#### 4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

La CA Raíz mantiene respaldo de sus propias claves privadas de acuerdo con el Plan de Continuidad de Negocio.

Para los efectos del Plan de Continuidad de Negocio, las claves privadas de las CA deben estar en custodia y respaldadas bajo estrictas normas de seguridad, y almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3 overall, que garantizan la no divulgación de las claves.

#### 4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN

No aplica

# 5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

## 5.1 CONTROLES FÍSICOS

### 5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

Conforme lo estipulado en la CPS.

### 5.1.2 ACCESO FÍSICO

Conforme lo estipulado en la CPS.

### 5.1.3 ENERGÍA Y AIRE ACONDICIONADO

### 5.1.4 EXPOSICIONES AL AGUA

Conforme lo estipulado en la CPS.

### 5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Conforme lo estipulado en la CPS.

### 5.1.6 ALMACENAMIENTO DE MEDIOS

Conforme lo estipulado en la CPS.

### 5.1.7 ELIMINACIÓN DE RESIDUOS

Conforme lo estipulado en la CPS.

### 5.1.8 RESPALDO FUERA DE SITIO

Conforme lo estipulado en la CPS.

## 5.2 CONTROLES PROCEDIMENTALES

### 5.2.1 ROLES DE CONFIANZA

Conforme lo estipulado en la CPS.

### 5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Conforme lo estipulado en la CPS.

### 5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Conforme lo estipulado en la CPS.

### 5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

Conforme lo estipulado en la CPS.

### 5.3 CONTROLES DE PERSONAL

#### 5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Conforme lo estipulado en la CPS.

#### 5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Conforme lo estipulado en la CPS.

#### 5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Conforme lo estipulado en la CPS.

#### 5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Conforme lo estipulado en la CPS.

#### 5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Conforme lo estipulado en la CPS.

#### 5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Conforme lo estipulado en la CPS.

#### 5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Conforme lo estipulado en la CPS.

#### 5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Conforme lo estipulado en la CPS.

### 5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

#### 5.4.1 TIPOS DE EVENTOS REGISTRADOS

Conforme lo estipulado en la CPS.

#### 5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO

Conforme lo estipulado en la CPS.

#### 5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍA

Conforme lo estipulado en la CPS.

#### 5.4.4 PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Conforme lo estipulado en la CPS.

#### 5.4.5 PROCEDIMIENTOS DE RESPALDO DE REGISTRO DE AUDITORÍA

Conforme lo estipulado en la CPS.

### 5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)

Conforme lo estipulado en la CPS.

### 5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Conforme lo estipulado en la CPS.

### 5.4.8 EVALUACIÓN DE VULNERABILIDADES

Conforme lo estipulado en la CPS.

## 5.5 ARCHIVOS DE REGISTROS

### 5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Conforme lo estipulado en la CPS.

### 5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

Conforme lo estipulado en la CPS.

### 5.5.3 PROTECCIÓN DE ARCHIVOS

Conforme lo estipulado en la CPS.

### 5.5.4 PROCEDIMIENTOS DE RESPALDO DE ARCHIVO

Conforme lo estipulado en la CPS.

### 5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Conforme lo estipulado en la CPS.

### 5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Conforme lo estipulado en la CPS.

### 5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Conforme lo estipulado en la CPS.

## 5.6 CAMBIO DE CLAVE

Conforme lo estipulado en la CPS.

## 5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

### 5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Conforme lo estipulado en la CPS.

### 5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

Conforme lo estipulado en la CPS.

### 5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

Conforme lo estipulado en la CPS.

### 5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Conforme lo estipulado en la CPS.

## 5.8 TERMINACIÓN DE UNA CA

Conforme lo estipulado en la CPS.

# 6 CONTROLES TÉCNICOS DE SEGURIDAD

Todos los controles serán aprobados por la DGFDyCE, antes de que se pongan en práctica. En esta sección, se definen las medidas de seguridad tomadas por la CA para proteger sus claves criptográficas y los datos de activación. La gestión de las claves es un factor crítico que permite asegurar que todas las claves privadas estén protegidas y solamente puedan ser activadas por personal autorizado.

## 6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

La CA mantendrá controles para brindar seguridad razonable de que el par de claves de la CA, se genera e instala de acuerdo con el protocolo definido para la generación de claves.

### 6.1.1 GENERACIÓN DEL PAR DE CLAVES

El proceso de generación de claves, ejecutado por la CA previene la pérdida, divulgación, modificación o acceso no autorizado a las claves privadas que son generadas. Este requerimiento aplica para toda la jerarquía de PKI Paraguay.

**Certificados de CA Raíz**

El par de claves de la CA Raíz, debe generarse mediante un proceso seguro por medio del módulo criptográfico de hardware (HSM – Hardware Security Module), que cumple como mínimo el estándar FIPS 140-2 nivel 3. Dicha generación se realiza en las instalaciones de la CA, siguiendo los procedimientos establecidos en el guion de la ceremonia de constitución de la CA Raíz del Paraguay.

**Certificados de PSC**

Las claves deben generarse mediante un proceso seguro por medio del módulo criptográfico de hardware (HSM – Hardware Security Module), que cumple como mínimo el estándar FIPS 140-2 nivel 3 y a un procedimiento establecido por el PSC, en su CP, CPS u otros documentos, acorde con la “**CEREMONIA DE GENERACIÓN DE CLAVES**” implementada por la CA Raíz. El PSC garantizará que

la clave privada de firma, nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de claves.

El proceso de generación de claves de PSC debe producir claves que:

- sean apropiadas para la aplicación o propósito destinado y que sean proporcionales a los riesgos identificados;
- usen un algoritmo establecidos en la sección 7.1.3;
- tengan una longitud de clave que sea apropiada para el algoritmo y para el período de validez del certificado del PSC, de acuerdo con la sección 6.1.5 de tamaños de clave;
- tomen en cuenta los requisitos del tamaño de clave de la CA Raíz.

Toda CA debe elaborar un documento en el que especifique el procedimiento que indica los pasos de la **CEREMONIA DE CREACIÓN DE CLAVES**, y el mismo debe estar en conocimiento de las personas involucradas.

**El módulo criptográfico de Hardware (HSM) debe cumplir con los siguientes requisitos:**

- Permitir el gerenciamiento seguro del ciclo de claves asimétricas (generación asociación del certificado, backup, activación de uso y destrucción) para una CA;
- Soportar los roles definidos en el punto 5.2.1 roles de confianza;
- Generar registros de auditoría como mínimo de: iniciación, cierre, creación de usuarios, remoción de usuarios;
- Realizar auto test documentados con el objetivo de identificar un eventual compromiso del sistema. Como mínimo el auto test debe ocurrir con cada iniciación del HSM;
- Permitir la configuración de activación de claves criptográficas a través de esquemas de secretos compartidos entre usuarios;
- Soportar la configuración de autenticación de usuario basado en dos factores (conocimiento y posesión;

- Permitir el backup de seguridad de claves criptográficas y parámetros críticos de seguridad mediante autorización utilizando un esquema de secreto compartido entre usuarios;
- La rutina de restauración de backup de claves criptográficas del HSM debe poseer un mecanismo de verificación de integridad del backup; y
- Debe ser un equipamiento independiente. No está permitido el uso de placas criptográficas.

El algoritmo a ser utilizado para las claves criptográficas de la CA Raíz está definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

### 6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

La CA es responsable de la generación de su par de claves y por lo tanto del resguardo y custodia del mismo.

La CA Raíz no tendrá acceso ni mantendrá copia de la clave privada de su suscriptor.

### 6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Las claves públicas transferidas deben ser entregadas a través de mecanismos que aseguren su autenticidad e integridad, impidiendo que sean alteradas en el tránsito.

La clave pública generada bajo el control del PSC es entregada a la CA Raíz mediante la entrega de una solicitud de firma de certificado (CSR) en el formato definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**.

Todo el proceso de generación de CSR se realiza conforme a los procedimientos para ello establecidos.

### 6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA CA A LAS PARTES QUE CONFÍAN

La distribución de la clave pública se realiza a través del certificado digital que lo contiene. En el repositorio público están publicados, el certificado de la CA Raíz y los certificados de los PSC habilitados en el formato definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**.

### 6.1.5 TAMAÑO DE LA CLAVE

El tamaño de las claves debe ser suficientemente largo para prevenir que otros puedan determinar la clave privada utilizando cripto-análisis durante el periodo de uso del par de claves.

El tamaño de las claves para los certificados de la CA Raíz y del PSC debe ser conforme a los establecido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

### 6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVE PÚBLICA Y VERIFICACIÓN DE CALIDAD

No se establecen condiciones especiales para la generación de parámetros de claves asimétricas, más allá de los que corresponden con el algoritmo de generación RSA según su especificación técnica.

La generación del par de claves y verificación de calidad debe realizarse en un módulo criptográfico seguro conforme al establecido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

### 6.1.7 PROPÓSITOS DE USOS DE CLAVE

**Certificado de CA Raíz**

La clave privada de la CA Raíz podrá ser utilizado con el único propósito de:

- Firmar los certificados digitales de PSC; y
- Firmar la CRL correspondiente.
- Autofirmarse su certificado en la Ceremonia de Generación de Claves de la

CA Raíz.

El valor del campo key usage para este certificado es: KeyCertsign=1; OfflineCRLSign=1.

**Certificado de PSC**

La clave privada del PSC podrá ser utilizado con el único propósito de:

- Firmar los certificados de sus Suscriptores;
- Firmar la CRL correspondiente; y
- Firmar peticiones de OCSP.

El valor del campo key usage para este certificado es: KeyCertsign=1; CRLSign=1.

### 6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

La CA debe mantener controles para asegurar que su clave privada permanezca confidencial, mantenga su integridad, y que el acceso al hardware criptográfico esté limitado a personas autorizadas.

La copia de respaldo de la clave privada de la CA debe realizarse conforme se especifica en el punto 6.2.4 de la presente CP.

El módulo criptográfico que la CA adopta está definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

### 6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

El control multi persona garantiza que nadie tenga el control de forma individual y completa de las actuaciones críticas.

Para la activación de la clave privada de la CA se debe utilizar controles de acceso de múltiples partes (es decir, “m” de “n”) con un valor mínimo de 3 para “m”.

Si las claves privadas de la CA son respaldadas, éstas deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro. La cantidad de personal autorizado para llevar a cabo esta función debe mantenerse al mínimo.

### 6.2.3 CUSTODIA DE LA CLAVE PRIVADA

La CA no podrá almacenar ni copiar las claves privadas de sus suscriptores, ni los datos de activación de los módulos criptográfico hardware que los contienen, por estricta prescripción legal.

### 6.2.4 RESPALDO DE LA CLAVE PRIVADA

Los respaldos de clave privada de la CA son únicamente para propósitos de recuperación en caso de una contingencia o desastre. Los planes de continuidad del negocio de la CA deben incluir procesos de recuperación de desastres para todos los componentes críticos del sistema de la CA, incluyendo el hardware, software y claves, en el caso de falla de uno o más de estos componentes.

La clave privada de la CA debe ser respaldada, guardada y recuperada por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro.

La copia de respaldo de la clave privada de la CA debe estar sujeta al mismo o mayor nivel de controles de seguridad que la clave que actualmente está en uso. La recuperación de la clave de la CA debe llevarse a cabo de una forma tan segura como el proceso de respaldo.

La clave privada de respaldo debe estar almacenada y archivada en el módulo criptográfico de hardware (HSM) conforme la sección 6.1.1 de la presente CPS, compatible con el FIPS 140-2 nivel 3 y al cual solo tienen acceso personal autorizado de la CA.

### 6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

La CA debe archivar su par de claves (pública y privada) en concordancia con las disposiciones de protección de claves definidas en esta CP.

### 6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

La clave privada de la CA es generada por un módulo criptográfico seguro, en caso de transporte de clave debe almacenarse de manera cifrada en un

dispositivo seguro. Cuando la copia de seguridad o restauración, requiera la transferencia de la clave privada de o hacia el módulo criptográfico, éste debe estar sujeto a los mismos controles empleados para la generación de la clave original. La clave privada de la CA puede ser exportada del módulo criptográfico únicamente para propósitos de respaldo.

### 6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Los dispositivos criptográficos utilizados para el almacenamiento del respaldo de la clave privada de la CA debe ser guardado de forma segura, en un sitio alterno, con los mismos niveles de seguridad que el sitio principal, para que sea recuperado en el caso de un desastre.

Las partes de la clave secreta o los componentes necesarios para usar y gestionar los dispositivos criptográficos de recuperación de desastres, deberían estar también guardados con seguridad en una ubicación fuera del sitio principal.

La clave privada de la CA debe ser almacenada y utilizada dentro de un dispositivo criptográfico de hardware seguro (HSM) que cumpla como mínimo con el perfil de protección apropiado de los requisitos del estándar FIPS 140-2 nivel 3 “Overall”.

### 6.2.8 MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

Los métodos de activación de clave de la CA están protegidos, y para accederlos se deben contar con al menos dos factores de autenticación. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.

### 6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Para la CA Raíz es obligatorio que los módulos criptográficos, los cuales han sido activados, no estén desatendidos o abiertos al acceso no autorizado. Después de usarlos, estos deben ser desactivados manualmente o por un tiempo de expiración por estado pasivo.

Cuando la clave privada de la CA fuera desactivada, por expiración o revocación, debe ser eliminada del módulo criptográfico. Se debe asegurar que no se permita la recuperación de copias.

### 6.2.10 DESTRUCCIÓN DE CLAVE PRIVADA

El procedimiento de destrucción de clave privada debe estar documentado y realizado por personal con rol de confianza con control multipersona. La destrucción de la clave privada debe constar en los registros de auditoría.

La CA, eliminará sus claves privadas y el respaldo de las mismas cuando hayan expirado o hayan sido revocadas.

La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del módulo criptográfico de hardware la parte en la que estaban grabadas las claves, para ello, éste debe ser limpiado por medio de inicialización de ceros (zeroize command).

### 6.2.11 CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

Los módulos criptográficos (HSM) de la CA Raíz y de los PSC deben tener la certificación FIPS 140-2 nivel 3 “Overall”.

## 6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

### 6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

La CA debe mantener controles para sus propias claves, de acuerdo a lo estipulado en la sección 5.5. Las claves archivadas de la CA deberían estar sujetas al mismo o mayor nivel de control de seguridad que las claves que están en uso actualmente. La clave pública debe ser archivada por diez años desde el fin de su fecha de operatividad.

### 6.3.2 PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES

Los periodos de uso de la clave son descriptos en la sección 5.6 de la presente CP.

### 6.4 DATOS DE ACTIVACIÓN

La CA mantiene estrictos controles en los datos de activación para operar los módulos criptográficos y que necesitan ser protegidos. (Ejemplo: un PIN, un código de acceso o “password”, autenticación biométrica).

#### 6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Se debe contar con datos de activación de múltiples factores para protección de los accesos al uso de claves privadas y su activación requiere de un control de múltiples partes (es decir, “m” de “n”) con un valor mínimo de 3 (tres) para “m”. Se deben elegir contraseñas seguras para proteger sus claves privadas de acuerdo a una política de contraseñas seguras.

#### 6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación deberían estar almacenados en un nivel de seguridad semejante al de los módulos criptográficos para protegerlos, y en una localización diferente a la de los mismos.

#### 6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de los módulos criptográficos de la CA Raíz deben ser cambiados al menos una vez cada año. Y en el caso del PSC la frecuencia debe ser al menos una vez cada seis meses.

### 6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

Se implementa políticas, estándares y procedimientos que permiten una operación segura. Se instrumentan los siguientes aspectos:

- Definición de roles y responsabilidades;
- Clasificación de la información;
- Seguridad vinculada a los recursos humanos;
- Seguridad lógica de los sistemas y redes;
- Control del acceso lógico;
- Seguridad física del ambiente y de los sistemas;
- Gestión de respaldos;

- Continuidad de la operativa y disponibilidad;
- Registros de auditoría;
- Archivo de datos históricos y auditoria de la CA y usuarios;
- Respuesta a incidentes; y
- Utilización de criptografía para las sesiones de comunicación y base datos.

### 6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Los equipos donde operan los sistemas de la CA, que requieran acceso remoto, deben poseer autenticación mutua y los sistemas operativos deberían estar configurados de acuerdo con los estándares del sistema operativo de la CA y ser revisados periódicamente.

Las actualizaciones y parches de los sistemas operativos deberían ser aplicados de manera oportuna y la utilización de programas utilitarios del sistema debería ser restringida al personal autorizado, y debe estar estrictamente controlado.

La CA debe utilizar cortafuegos para proteger la red de producción contra intromisiones internas y externas y limitar la naturaleza y fuente de actividades de red que pueden acceder a sistemas de producción.

El acceso directo a las bases de datos de la CA que soportan las operaciones de la misma está limitado a personas autorizadas.

### 6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Los sistemas sensibles de la CA requieren un ambiente informático dedicado y aislado, que implemente el concepto de sede computacional confiable con procesos de auditoría.

## 6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

La CA debe mantener controles en los equipos de seguridad (hardware y software) requeridos para operar en una infraestructura PKI desde el momento de la

compra hasta su instalación, de forma que reduzcan la probabilidad que cualquiera de sus componentes sea violentado.

Todo el hardware y software que ha sido identificado para operar las CA debe ser enviado y entregado con métodos que provean una adecuada cadena de custodia. Y además, las configuraciones deben ser verificadas en un ambiente de prueba antes de iniciar operaciones.

### 6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

La CA debe mantener controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la CA.

Los nuevos sistemas, o para la expansión de los sistemas existentes, deben especificar los requisitos de control, seguir procedimientos de prueba de software y control de cambios para la implementación de software. Toda la documentación del ciclo de vida del sistema, debe estar disponible para su verificación.

La CA debe mantener controles sobre el acceso a las bibliotecas fuente de programas.

### 6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Se documenta y controla la configuración del sistema, así como toda modificación o actualización, habiéndose implementado un método de detección de modificaciones no autorizadas. Los Administradores de la CA son los responsables de garantizar que se cumplan los procedimientos de seguridad correctamente. Además de ejecutar revisiones periódicas para asegurar el cumplimiento de los estándares de implementación de seguridad.

### 6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Debe existir un inventario actualizado con los sistemas de información y medios de almacenamiento asociados a la operativa de la CA. Todos los medios a ser incorporados, retirados o trasladados fuera de las fronteras de la organización deben estar sujetos a previa autorización de la alta dirección, en procedimientos definidos para ello. Dicho inventario debe ser mantenido por la CA, y revelado sólo a

los encargados de la auditoría, es decir, no forma parte de la información a publicar.

**6.7 CONTROLES DE SEGURIDAD DE RED**

El equipo de la CA debe estar dentro de los límites de la red interna, operando bajo un nivel de seguridad de red crítico. La red de la CA debe estar protegida contra ataques. Los puertos y servicios que no se requieran deben estar apagados.

La CA Raíz debe estar off-line y aislada de la red organizacional.

Los niveles críticos de seguridad de red, deben incluir:

- La encriptación de las conexiones involucradas con las operaciones de la CA;
- Los sitios web están provistos de certificados SSL;
- La red está protegida por firewalls y sistemas de detección de intrusos;
- Los accesos externos a información de bases de datos de la CA están prohibidos;
- La CA debe controlar la ruta de acceso del usuario desde la terminal hasta los servicios;
- Los componentes de la red local deben mantenerse en un ambiente físicamente seguro y sus configuraciones deben ser auditadas periódicamente; y
- Los datos sensibles deben encriptarse cuando se intercambian sobre redes públicas o no confiables o ser intercambiados mediante un canal seguro.

La CA debe definir los procedimientos de control del cambio para el hardware, los componentes de la red y los cambios de configuración del sistema.

**6.8. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO**

El módulo criptográfico de la CA adopta el estándar definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

# 7. PERFILES DE CERTIFICADOS, CRL Y OCSP

## 7.1 PERFIL DEL CERTIFICADO

El certificado digital debe cumplir con:

- ITU-T X.509 V.3 Information technology Open systems interconnection The Directory: Public-key and attribute certificate frameworks
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”.
- RFC – 3279 ‘’ Internet X.509 Public Key Infrastructure Algorithm Identifier’’

Cómo mínimo el certificado contiene:

### 7.1.1 NÚMERO (S) DE VERSIÓN

Todos los certificados emitidos dentro de la PKI Paraguay deben corresponder al estándar X.509 versión 3.

### 7.1.2 EXTENSIONES DEL CERTIFICADO

Las extensiones de los certificados se estipulan en los perfiles

### 7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS

El certificado de la CA Raíz es firmado usando el algoritmo definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

### 7.1.4 FORMAS DEL NOMBRE

Los nombres dentro de la PKI Paraguay deben cumplir las regulaciones de la sección 3.1.1.

El Nombre del emisor deberá ser completado en cada certificado emitido conteniendo el mismo nombre distinguido que utiliza en su certificado.

### 7.1.5 RESTRICCIONES DEL NOMBRE

Los nombres se escriben en mayúsculas y sin tildes, únicamente se debe aceptar el carácter ‘’Ñ ‘’como un caso especial para los nombres de personas físicas y jurídicas.

El código de país es de dos caracteres y se asigna de acuerdo al estándar ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”.

### 7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

La CA gestionará la obtención del OID correspondiente a cada clase de certificado.

### 7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)

Sin estipulaciones.

### 7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)

Se utilizarán los calificadores definidos en el RFC5280. Particularmente se utilizará el calificador “CPS Pointer qualifier” donde se colocara la URL en la que se accede a la Política.

### 7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES)

Sin estipulaciones.

### 7.1.10 PERFILES

#### 7.1.10.1. PERFIL DE CERTIFICADO DE LA CA RAÍZ

Se utilizarán los siguientes campos del formato X.509 versión 3:

| Campo | Valor o restricciones |
|---|---|
| Versión (Version) | V3 |

| | |
|---|---|
| Número de serie (Serial number) | Valor único emitido dentro del ámbito de la CA Raíz.<br>0c 21 b4 38 46 c5 1b f5 50 20 d3 ab ed 33 5c a5 |
| Algoritmo de firma (Signature algorithm) | SHA 256 RSA. |
| Algoritmo hash de firma (Signature hash algorithm) | SHA256 |
| Emisor (Issuer DN) | CN = Autoridad Certificadora Raíz del Paraguay<br>O = Ministerio de Industria y Comercio<br>C = PY |
| Válido desde (Valid from) | Este Campo especifica la fecha y hora a partir de la cual el certificado es válido. Las fechas establecidas para el periodo de validez deben ser sincronizadas con respecto a la hora oficial de la República del Paraguay.<br>Martes, 07 de agosto de 2012 4:36:59 |
| Válido hasta (Valid to) | Este Campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Las fechas para la validez del certificado deben ser sincronizadas con el horario oficial de la República del Paraguay.<br>Sábado, 07 de agosto de 2032 4:36:59 |
| Sujeto (Suscriber DN) | CN = Autoridad Certificadora Raíz del Paraguay<br>O = Ministerio de Industria y Comercio<br>C = PY |
| Clave pública del sujeto (Subject Public Key) | Clave pública RSA de 4096 bits. |

Extensiones:

| Campo | Valor o restricciones | Criticidad |
|---|---|---|
| Directivas del certificado (Certificate Policies) | Describe las políticas aplicables al certificado y la dirección URL donde se encuentra disponible la CP respectiva.<br>[1]Directiva de certificados:<br>Identificador de directiva=Todas las directivas de emisión<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador: http://www.acraiz.gov.py/cps/politicas.pdf | No Crítica |
| Identificador de la clave del titular (Subject Key Identifier) | Hash de 20 bytes del atributo Subject Public Key. | No Crítica |
| Restricciones básicas (Basic Contraitns) | Tipo de asunto=Entidad de certificación (CA).<br>Restricción de longitud de ruta=Ninguno. | Crítica |
| Uso de la clave (Key usage) | DigitalSignature = 0<br>NonRepudiation = 0<br>KeyEncipherment = 0 | Crítica |

| | | |
|---|---|---|
| | DataEncipherment = 0<br>KeyAgreement = 0<br>KeyCertSign = 1<br>CRLSign = 1<br>EncipherOnly = 0<br>DecipherOnly = 0 | |

Propiedades:

| Campo | Valor o restricciones |
|---|---|
| Algoritmo de identificación | Sha1 |
| Huella Digital (Thumbprint) | a1 af 42 e8 ec 9d ec 9f 3c 56 81 9c d3 44 0b e2 cb d2 81 79 |

### 7.1.10.2. PERFIL DE CERTIFICADOS DE LOS PSC

| Campo | Valor o restricciones |
|---|---|
| Versión (Version) | V3 |
| Número de serie (Serial number) | Valor único emitido dentro del ámbito de la CA Raíz. |
| Algoritmo de firma (Signature algorithm) | SHA 256 RSA. |
| Algoritmo hash de firma (Signature hash algorithm) | SHA256 |
| Emisor (Issuer DN) | CN = Autoridad Certificadora Raíz del Paraguay<br>O = Ministerio de Industria y Comercio<br>C = PY |
| Válido desde (Valid from) | Este Campo especifica la fecha y hora a partir de la cual el certificado |

| | |
|---|---|
| | es válido. Las fechas establecidas para el periodo de validez deben ser sincronizadas con respecto a la hora oficial de la República del Paraguay. |
| Válido hasta (Valid to) | Este Campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Las fechas para la validez del certificado deben ser sincronizadas con el horario oficial de la República del Paraguay. |
| Sujeto (Suscriber DN) | Ver sección 7.1.4 |
| Clave pública del sujeto (Subject Public Key) | Clave pública RSA de 4096 bits. |

Extensiones:

| **Campo** | **Valor o restricciones** | **Criticidad** |
|---|---|---|
| Identificador de la clave del titular (Subject Key Identifier) | Hash de 20 bytes del atributo Subject Public Key. | No Crítica |
| Identificador de clave de entidad emisora | Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada. | No Crítica |
| Acceso a la información de entidad emisora | [1]Acceso a información de autoridad | |

| | | |
|---|---|---|
| | Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo:<br>Dirección URL=http://www.acraiz.gov.py/crt/ac_raiz_py_sha256.crt<br>[2]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)<br>Nombre alternativo:<br>Dirección URL del PSC | |
| Directivas del certificado | [1]Directiva de certificados:<br>Identificador de directiva= Directivas del certificado<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br><br>http://www.acraiz.gov.py/cps/politicas.pdf<br>[1,2]Información de certificador de directiva:<br>Id. de certificador de | |

| | | |
|---|---|---|
| | directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Certificados emitidos dentro del marco de la PKI Paraguay bajo la jerarquía de su AC Raíz<br>[1,3]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Issued Certificates in the scope of the PKI Paraguay under the hierachy of ROOT CA. | |
| Puntos de distribución CRL | [1]Punto de distribución CRL<br>Nombre del punto de distribución:<br>Nombre completo:<br>Dirección URL=http://www.acraiz.gov.py/arl/ac_raiz_py.crl | |
| Restricciones básicas (Basic Contraitns) | Tipo de asunto=Entidad de certificación (CA).<br>Restricción de longitud de ruta=Ninguno. | Crítica |
| Uso de la clave (Key usage) | DigitalSignature = 0 | Crítica |

| | | |
|---|---|---|
| | NonRepudiation = 0<br>KeyEncipherment = 0<br>DataEncipherment = 0<br>KeyAgreement = 0<br>KeyCertSign = 1<br>CRLSign = 1<br>EncipherOnly = 0<br>DecipherOnly = 0 | |

Propiedades:

| Campo | Valor o restricciones |
|---|---|
| Algoritmo de identificación | Sha1 |
| Huella Digital (Thumbprint) | Huella digital del certificado del PSC |

### 7.2 PERFIL DE LA CRL

La lista de revocación de certificados cumple con el RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” y contienen los elementos básicos especificados en el siguiente cuadro:

#### 7.2.1 NÚMERO (S) DE VERSIÓN

La PKI Paraguay soporta las CRL X.509 versión 2.

#### 7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

Atributos:

| Campo | Valor o restricciones |
|---|---|
| Versión (Version) | V2 |
| Emisor (Issuer) | Entidad que emite y firma la CRL. |
| Fecha efectiva (Effective Date) | Fecha de emisión de la CRL. |
| Próxima actualización (NextUpdate) | Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL está |

| | |
|---|---|
| | acorde con lo requerido en la sección 4.9.7 |
| Algoritmo de firma (Signature Algorithm) | Algoritmo usado para la firma del CRL, puede ser como mínimo SHA256WithRSAEncryption |
| Algoritmo hash de firma (Signature hash algorithm) | Sha256 |
| Certificados revocados (Revocation List) | Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación. |

Extensiones:

| | |
|---|---|
| Número CRL(CRL Number) | Orden secuencial de emisión de CRL |
| Identificador de clave de Entidad Emisora (Authority Key Identifier) | Identificador de la clave pública de CA |
| Emitir puntos de distribución (Distribuition Points) | Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado |

## 7.3 PERFIL DE OCSP

### 7.3.1 NÚMERO (S) DE VERSIÓN

No aplica

### 7.3.2 EXTENSIONES DE OCSP

Sin estipulaciones.

# 8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

## 8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Conforme lo estipulado en la CPS.

## 8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL EVALUADOR

Conforme lo estipulado en la CPS.

## 8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Conforme lo estipulado en la CPS.

## 8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Conforme lo estipulado en la CPS.

## 8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

Conforme lo estipulado en la CPS.

## 8.6 COMUNICACIÓN DE RESULTADOS

Conforme lo estipulado en la CPS.

# 9. OTROS ASUNTOS LEGALES Y COMERCIALES

## 9.1 TARIFAS

Las tarifas establecidas para habilitación e inspección u otros conceptos están establecidas por resolución ministerial y está disponible en la página https://www.acraiz.gov.py.

### 9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

La CA Raíz no percibirá contraprestación económica por la emisión de certificados.

### 9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

La CA Raíz no se encuentra habilitada para el cobro de tarifas de acceso a certificados.

### 9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

La CA Raíz, no se encuentra habilitada para el cobro de tarifas de acceso a estado o revocación de los certificados.

### 9.1.4 TARIFAS POR OTROS SERVICIOS

La CA Raíz, no se encuentra habilitada para el cobro de tarifas para acceder a información de la Política y la Declaración de Prácticas de Certificación.

### 9.1.5 POLÍTICAS DE REEMBOLSO

No estipulado.

## 9.2 RESPONSABILIDAD FINANCIERA

### 9.2.1 COBERTURA DE SEGURO

Conforme lo estipulado en la CPS.

### 9.2.2 OTROS ACTIVOS

Conforme lo estipulado en la CPS.

### 9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

Conforme lo estipulado en la CPS.

### 9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

#### 9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Conforme lo estipulado en la CPS.

#### 9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Conforme lo estipulado en la CPS.

### 9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

#### 9.4.1 PLAN DE PRIVACIDAD

Conforme lo estipulado en la CPS.

#### 9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Conforme lo estipulado en la CPS.

#### 9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

Conforme lo estipulado en la CPS.

#### 9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

Conforme lo estipulado en la CPS.

#### 9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Conforme lo estipulado en la CPS.

#### 9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Conforme lo estipulado en la CPS.

#### 9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Conforme lo estipulado en la CPS.

### 9.5 DERECHO DE PROPIEDAD INTELECTUAL

Conforme lo estipulado en la CPS.

### 9.6 REPRESENTACIONES Y GARANTÍAS

#### 9.6.1 REPRESENTACIONES Y GARANTÍAS DE LA CA

Conforme lo estipulado en la CPS.

### 9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Conforme lo estipulado en la CPS.

### 9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

Conforme lo estipulado en la CPS.

### 9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

Conforme lo estipulado en la CPS.

### 9.6.5 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Sin estipulaciones.

## 9.7 EXENCIÓN DE GARANTÍA

Conforme lo estipulado en la CPS.

## 9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

Conforme lo estipulado en la CPS.

## 9.9 INDEMNIZACIONES

Conforme lo estipulado en la CPS.

## 9.10 PLAZO Y FINALIZACIÓN

### 9.10.1 PLAZO

La CP de la CA Raíz empieza a ser efectiva en la fecha estipulada en la Resolución Ministerial de aprobación expedida por el MIC.

### 9.10.2 FINALIZACIÓN

La CP estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión.

### 9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

La finalización de la vigencia de la CP, puede ser por derogación expresa, enmiendas o modificaciones; todos los certificados emitidos bajo esa política seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Política contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

### 9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Conforme lo estipulado en la CPS.

### 9.12 ENMIENDAS

#### 9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

La DGFDyCE está facultada a introducir enmiendas o modificaciones, las que deberán ser documentadas y mantenerse a través de versiones y publicadas en el sitio de Internet de la CA Raíz. Por resolución Ministerial, se fijará el plazo al cual, el PSC deberá ajustarse a la nueva versión.

#### 9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Toda enmienda o modificación de la CP, se publicará en el sitio principal de Internet de la CA.

#### 9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Sin estipulaciones

### 9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Conforme lo estipulado en la CPS.

### 9.14 NORMATIVA APLICABLE

Conforme lo estipulado en la CPS.

### 9.15 ADECUACIÓN A LA LEY APLICABLE

La presente Política de Certificación se adecua a legislación vigente aplicable a la materia.

### 9.16 DISPOSICIONES VARIAS

#### 9.16.1 ACUERDO COMPLETO

No aplica

#### 9.16.2 ASIGNACIÓN

No aplica

#### 9.16.3 DIVISIBILIDAD

En el eventual caso que una cláusula de la CP sea declarada inconstitucional por la Corte Suprema de Justicia, el resto de las cláusulas de estas políticas se

mantendrán vigentes.

**9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)**

No aplica

**9.16.5 FUERZA MAYOR**

Conforme lo estipulado en la CPS.

**9.17 OTRAS DISPOSICIONES**

El PSC habilitado de conformidad a los términos de la CP derogada, deberá adecuarse a las disposiciones de la presente CP en el plazo establecido por la Resolución que la ponga en vigencia.

## 10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.
- ISO 3166 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- Ley Nro. 4017/2010 ‘’De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico’’
- Ley Nro. 4610/2012 que modifica y amplía la Ley Nro. 4017/2010
- Decreto Reglamentario Nro. 7369/2011