# DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DE LA PKI-Paraguay

LIZ ROSANNA CRAMER CAMPOS

Firmado digitalmente por LIZ ROSANNA CRAMER CAMPOS
Fecha: 2020.09.30 16:50:29 -04'00'

**DOC-PKI-03**

**Versión 2.0**

**CONTROL DOCUMENTAL**

| **Documento** | |
|---|---|
| **Título:** DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC) | **Nombre Archivo:** DOC-PKI-03 V2.0 |
| **Código:** DOC-PKI-03 | **Soporte Lógico:** https://www.acraiz.gov.py/ |
| **Fecha:** 30/09/2020 | **Ubicación Física:** DGFDyCE |
| **Versión:** 2.0 | |

| **Registro de cambios** | | |
|---|---|---|
| **Versión** | **Fecha** | **Motivo de cambio** |
| 1.0 | 03/11/2016 | Versión inicial |
| 1.1 | 28/11/2019 | 1.3.5.2 - Autoridad de Validación (AV).<br>3.2.2 - Autenticación de Identidad de Persona Jurídica.<br>3.2.3 - Autenticación de Identidad de Persona Física.<br>4.1.1 - Quién puede presentar una solicitud de certificado.<br>4.9.7 - Frecuencia de emisión del CRL. |
| 2.0 | 30/092020 | 1. Introducción<br>2. Responsabilidades de publicación y del Repositorio<br>3. Identificación y Autenticación<br>4. Requerimientos operacionales del ciclo de vida del certificado<br>5. Controles de seguridad física, de gestión y de operaciones<br>6. Controles técnicos de seguridad<br>7. Perfil de certificados, CRL y OCSP<br>8. Auditoría de cumplimiento y otras evaluaciones<br>9. Otros asuntos legales y comerciales<br>10. Documentos de referencia |

| **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 Servicios de Certificación (PSC) |
| Documento Público | https://www.acraiz.gov.py/ |

| Control del documento | | |
|---|---|---|
| **Elaborado por:** | **Verificado por:** | **Aprobado por:** |
| JENNY ELIZABETH RUIZ DIAZ LEZCANO<br>Digitally signed by JENNY ELIZABETH RUIZ DIAZ LEZCANO<br>Date: 2020.09.30 14:12:09 -04'00' | MARIA LUJAN OJEDA CHAMORRO<br>Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO<br>Fecha: 2020.09.30 15:13:55 -04'00' | LUCAS ATILIO SOTOMAYOR LLANO<br>Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO<br>Fecha: 2020.09.30 15:31:44 -04'00' |
| ***JENNY RUÌZ DÍAZ*** | ***LUJAN OJEDA*** | ***LUCAS SOTOMAYOR*** |

**Contenido**

# 1. INTRODUCCIÓN

## 1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que deben ser obligatoriamente cumplidos por los Prestadores de Servicios de Certificación (PSC) en su carácter de autoridad certificación intermedia (CAI) y como integrantes de la Infraestructura de Clave Pública del Paraguay (PKI-Paraguay) en la formulación y elaboración de su Declaración de Prácticas de Certificación (CPS). La CPS es un documento que describe los procedimientos empleados por una autoridad de certificación (CA) para la correcta ejecución de sus servicios.

Toda CPS elaborada en el ámbito de la PKI-Paraguay debe obligatoriamente adoptar la misma estructura de este documento, la cual se basa en el RFC 3647.

El PSC responsable mantendrá actualizada toda la información de su CPS.

## 1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificada la CPS, indicando como mínimo el nombre, versión, fecha de aprobación, localización y el OID (Object Identifier) del documento.

## 1.3. PARTICIPANTES DE LA PKI

### 1.3.1. AUTORIDADES CERTIFICADORAS (CA)

En este ítem deben ser identificadas las CAs integrantes de la PKI-Paraguay a la que se refiere la CPS. Estas pueden ser:

I. CA Raíz-Py; y
II. CAI.

Un PSC es una entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI-Paraguay, debe contar con un certificado digital emitido por la CA Raíz-Py y solo podrá emitir certificados a usuarios finales. En el ámbito de la PKI-Paraguay un PSC es considerada una CAI.

### 1.3.2. AUTORIDADES DE REGISTRO (RA)

En este ítem debe identificarse la dirección de la página web (URL), donde se publican los datos referentes a las autoridades de registro (RA) habilitadas por el PSC para el proceso de recepcionar y encaminar solicitudes de emisión o de revocación de certificados digitales y de identificar presencialmente a los solicitantes. Las informaciones a ser publicadas en el sitio son:

a) la lista de todas las RA habilitadas;
b) para cada RA, las direcciones de todas las instalaciones técnicas, autorizadas por la CA Raíz-Py para funcionar;
c) acuerdos operacionales celebrados entre un PSC y una RA delegada; y
d) la lista de todas las RA cuya habilitación fue revocada, con la indicación de la fecha de revocación.

El PSC deberá mantener las informaciones siempre actualizadas.

La RA puede ser propia del PSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la CA Raíz-Py con la habilitación correspondiente.

Las RA delegadas son autoridades de registro vinculadas a un PSC mediante un acuerdo operacional.

### 1.3.3. SUSCRIPTORES

En este ítem se especifican las personas físicas o jurídicas que podrán ser titulares de los certificados emitidos según esta CPS.

### 1.3.4. PARTE QUE CONFÍA

Se entenderá por parte que confía, toda persona física o jurídica, diferente al titular del certificado que decide aceptar y confiar en un certificado digital emitido dentro de la PKI-Paraguay.

Una parte que confía puede o no, ser un suscriptor.

## 1.3.5. OTROS PARTICIPANTES

### *1.3.5.1. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)*

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los Prestadores de Servicio de Soporte (PSS) vinculados al PSC, sea directamente o sea por intermedio de sus RA.

PSS son entidades externas a las que recurre la CA o la RA para desempeñar actividades descritas en esta CPS o en una CP y se clasifican en tres categorías, conforme al tipo de actividades prestadas;

a) disponibilización de infraestructura física y lógica;
b) disponibilización de recursos humanos especializados; y
c) disponibilización de infraestructura física y lógica y de recursos humanos especializados.

El PSC deberá mantener las informaciones arriba citadas siempre actualizadas.

El funcionamiento de un PSS vinculado a un PSC mediante un acuerdo operacional deberá ser autorizado por la CA Raíz-Py con la habilitación correspondiente.

### *1.3.5.2. AUTORIDADES DE VALIDACIÓN (VA)*

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a las Autoridades de Validación (VA) vinculadas al PSC.

La VA puede ser una entidad propia o externa a un PSC responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una RA y certificados por la autoridad de certificación.

El funcionamiento de una VA vinculada a un PSC mediante un acuerdo operacional deberá ser autorizado por la CA Raíz-Py con la habilitación correspondiente.

### *1.3.5.3. PRESTADORES DE SERVICIO DE ALMACENAMIENTO (PSA)*

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los Prestadores de Servicios de Almacenamiento vinculados al PSC.

El PSA es una entidad vinculada indefectiblemente a un PSC mediante un acuerdo operacional que deberá ser autorizada por la CA Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.

Un PSC habilitado, conforme a las disposiciones de la normativa vigente, tiene prohibido almacenar y copiar claves privadas de sus suscriptores, por lo cual no puede constituirse en un PSA.

## 1.4. USO DEL CERTIFICADO

### 1.4.1. USOS APROPIADOS DEL CERTIFICADO

En este ítem, la CPS debe relacionar e identificar las CP implementadas por el PSC, que definen como deberán ser utilizados los certificados emitidos. En estas CP estarán especificadas las aplicaciones para las cuales sean adecuados, el uso de los certificados emitidos por un PSC.

### 1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Este ítem de la CPS debe relacionar e identificar las CP implementadas por el PSC, que definen las aplicaciones para las que esté prohibido el uso de los Certificados emitidos por el PSC.

## 1.5 ADMINISTRACIÓN DE LA POLÍTICA

### 1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PSC:

### 1.5.2. PERSONA DE CONTACTO

Nombre:

Teléfono:

Fax:

Página web:

E-mail:

Otros:

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

Nombre:

Teléfono:

E-mail:

Otros:

### 1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CPS

Los procedimientos para la aprobación de CPS del PSC son establecidos a criterio de CA Raíz-Py de la PKI-Paraguay.

## 1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS

### 1.6.1 DEFINICIONES

1) **Acuerdo de Suscriptores:** es un acuerdo entre la CA Raíz-Py 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. Este acuerdo, requiere la aceptación explícita de las partes intervinientes.
2) **Agente de registro:** persona responsable de la realización de las actividades inherentes a la RA. Es la persona que realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificado.
3) **Armario ignífugo:** armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.
4) **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.
5) **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
6) **Autoridad de Certificación:** 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-Py y el PSC.
7) **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la PKI-Paraguay. La CA Raíz-Py tiene los certificados

de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la CA Raíz-Py son ejercidas por la AA.

8) **Autoridad de Certificación Intermedia**: entidad cuyo certificado de clave pública ha sido firmado digitalmente por la CA Raíz-Py; es responsable de la emisión de certificados a usuarios finales. Un Prestador de Servicios de Certificación es considerado una Autoridad de Certificación Intermedia.
9) **Autoridad de Registro:** entidad responsable de la interfaz entre el usuario y el Prestador de Servicios de Certificación (PSC). Siempre está vinculado a un PSC y su función es recibir solicitudes de emisión o revocación de certificados digitales del solicitante, identificar de forma presencial al mismo y remitir la solicitud al PSC. La RA puede ser propia del PSC o delegada a un tercero.
10) **Autoridad de Validación:** 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 puede ser propia del PSC o delegada a un tercero.
11) **Cadena de certificación:** lista ordenada de certificados que contiene un certificado de usuario final y certificados de las CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado del PSC y a su vez, el emisor del certificado del PSC es el titular del certificado de CA Raíz-Py. El usuario final o la parte que confía debe verificar la validez de los certificados en la cadena de certificación.
12) **Certificado Digital:** 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.
13) **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.
14) **Cifrado asimétrico:** tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
15) **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos
16) **Clave pública y privada:** la criptografía en la que 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 exclusivo control del titular del certificado.

17) **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
18) **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.
19) **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.
20) **Declaración de Prácticas de Certificación:** 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.
21) **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión/revocación del certificado digital será considerada la cédula de identidad o el pasaporte del solicitante.
22) **Dossier de titular del certificado:** Conjunto formado por la verificación de los documentos de identificación utilizados para la emisión del certificado, solicitud de certificado y acuerdo de suscriptores, y por la solicitud de revocación, cuando sea el caso. Este dossier deberá estar en formato de archivo digital, en el cual se escanean los documentos en formato papel, si los hubiere y se firma la solicitud de certificado y acuerdo de suscriptores con la clave privada del titular, después de la autorización del AGR por medio de la firma de dichos documentos, siempre y cuando sea informado y aceptado su contenido por parte de su solicitante y firmada digitalmente después de la generación de las claves y anterior a la instalación del certificado correspondiente.
23) **Emisor del certificado:** persona jurídica cuyo nombre aparece en el campo emisor de un certificado.
24) **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
25) **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.

26) **Generador:** 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.
27) **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
28) **Identificador de Objeto:** 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.
29) **Identificación del Titular de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a través de la presencia física del interesado, con base en los documentos de identificación, y la etapa de emisión del certificado, conforme a la presente CPS.
30) **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados digitales y claves criptográficas emitidas por esta infraestructura.
31) **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
32) **Lista de Certificados Revocados:** lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
33) **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
34) **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
35) **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente CPS.

36) **Parte que confía (relying parties):** es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido en el marco de la PKI-Paraguay.
37) **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
38) **Política de Certificación:** 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.
39) **Prestador de Servicios de Almacenamiento**: es una entidad vinculada indefectiblemente a un PSC mediante un acuerdo operacional que deberá ser autorizada por la CA Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.
40) **Prestador de Servicios de Certificación:** 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-Py y solo podrá emitir certificados a usuarios finales.
41) **Prestador de Servicios de Soporte:** entidad externa vinculada a un PSC mediante un acuerdo operacional a la que recurre la CA o la RA y autorizada la CA Raíz-Py para desempeñar actividades descritas en la CPS o en una CP.
42) **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.
43) **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.
44) **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.
45) **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.
46) **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una CA.
47) **Solicitud de Firma de Certificado:** petición de certificado digital que se envía a la CA. Mediante la información contenida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

48) **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado suscripto por el solicitante en nombre propio en el caso de certificados para persona física, o bien en nombre del titular en el caso de certificados de persona jurídica ya sea en un documento específico de la solicitud o como parte del Acuerdo de Suscriptores.
49) **Suscriptor:** persona física o jurídica titular de un certificado digital emitido por una CA. Un suscriptor puede ser un PSC o un usuario final.
50) **Usuario final:** persona física o jurídica titular de un certificado digital emitido por un PSC.
51) **Verificación de firma:** determinación y validación de 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 y que el mensaje no ha sido alterado desde que su firma digital fue creada.
52) **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.
53) **X.509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

### 1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

| Sigla/Acrónimo | Descripción |
|---|---|
| AA | Autoridad de Aplicación |
| AGR | Agente de Registro |
| C | País (C por su sigla en inglés, Country) |
| CA | Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority) |
| CAI | Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate) |
| CA Raíz-Py | 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) |
| DGFDyCE | Dirección General de Firma Digital y Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios. |
| 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). |
| 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) |
| PAS | Pasaporte |
| PCN | Plan de Continuidad del Negocio |
| PIN | Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number) |

| | |
|---|---|
| PKI | Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure). |
| PKI-Paraguay | Infraestructura de Claves Públicas del Paraguay |
| PSA | Prestador de Servicios de Almacenamiento |
| PSC | Prestador de Servicios de Certificación |
| PSS | Prestador de Servicios de Soporte |
| 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 Rivest, Shamir y Adleman |
| RUC | Registro único del Contribuyente |
| SN | Número de Serie (por sus siglas en inglés, Serial Number) |
| 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 Authority) |

# 2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

## 2.1. REPOSITORIOS

En este ítem se deben incluir las obligaciones que debe cumplir el repositorio:

a) poner a disposición, inmediatamente después de su emisión, los certificados emitidos por el PSC y su CRL/OCSP;
b) estar disponible para consultas las 24 (veinticuatro) horas del día, los 7 (siete) días de la semana;
c) implementar los recursos necesarios para la seguridad de los datos allí almacenados; y
d) proporcionar 02 (dos) repositorios, en infraestructuras de red segregada, para la distribución del CRL/OCSP.

En este ítem deben ser descriptos, los requisitos aplicables a los repositorios utilizados por el PSC responsable de la CPS, tales como:

a) localización física y lógica;
b) disponibilidad;
c) protocolos de acceso; y
d) requisitos de seguridad.

## 2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

En este ítem se debe definir la información que será publicada por el PSC responsable de la CPS. El servicio de publicación de información de un PSC debe estar disponible durante las veinticuatro horas, los siete días de la semana. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0.5% anual.

Las siguientes informaciones, como mínimo, deberán ser publicadas por el PSC en su servicio de repositorio:

a) CP y CPS que implementan;
b) el certificado de la CA Raíz-Py;
c) su propio certificado;
d) la lista de certificados revocados;

e) certificados emitidos;
f) proforma de acuerdo del suscriptor;
g) las resoluciones que habilitan o revocan al PSC:
h) la información relevante del resultado de la última auditoría que hubiere sido objeto;
i) leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI-Paraguay;
j) Identificación, domicilio y medios de contacto;
k) una lista, actualizada periódicamente, que contiene las RA propias y delegadas con sus respectivas direcciones de las instalaciones técnicas de operación;
l) una lista, actualizada periódicamente de los PSS vinculados a un PSC;
m) una lista, actualizada periódicamente de los PSA vinculados a un PSC.

## 2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

En este ítem se debe definir, la frecuencia de publicación de las informaciones del ítem anterior, de modo a asegurar la disponibilidad, siempre actualizada de sus contenidos.

## 2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

En este ítem deben ser descriptos, los controles y las eventuales restricciones para el acceso, lectura y escritura de las informaciones publicadas por el PSC, de acuerdo a lo establecido en las normas, criterios, prácticas y procedimientos de la PKI-Paraguay.

# 3. IDENTIFICACIÓN Y AUTENTICACIÓN

El PSC comprobará la identidad y/o atributos de las personas físicas y jurídicas antes de incluir estos atributos en un certificado digital en el marco de la PKI-Paraguay. Se prohíbe a las personas físicas y jurídicas utilizar en sus certificados nombres que violen los derechos de propiedad intelectual de terceros. El PSC se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

El PSC mantendrá políticas y procedimientos internos que deben ser revisados periódicamente para cumplir con los requisitos establecidos por la CA Raíz-Py,

Todo el proceso de identificación del titular del certificado debe ser registrado y firmado digitalmente por los ejecutantes. Dichos registros deben realizarse de tal manera que permitan la completa reconstrucción de los procesos realizados, para fines de auditoría.

Se debe mantener un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física o jurídica y anexar al dossier del Titular del Certificado. Dichas copias podrán conservarse en papel o en formato digital, sujeto a las condiciones definidas en el documento DOC-PKI-05 [2].

## 3.1. NOMBRES

### 3.1.1. TIPOS DE NOMBRES

En esta sección, deben ser definidos los tipos de nombres admitidos para los titulares de los certificados emitidos por el PSC responsable de la CPS. Entre los tipos de nombres considerados podrán estar el *distinguished name* según lo establecido en la ITU X.500, direcciones de correo y la direcciones de página web (URL).

### 3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

En este apartado, la CPS debe definir la necesidad de usar nombres significativos, es decir, nombres que permitan determinar la identidad de la persona física o jurídica, a los efectos de identificar a los titulares de los certificados emitidos por el PSC.

### 3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

No se admite el anonimato en los certificados emitidos por un PSC. Asimismo, el seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

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

En esta sección deben ser descriptas, cuando sea aplicable, las reglas para la interpretación de varias formas de nombres admitidas por la CPS.

#### *3.1.4.1 CERTIFICADO DE PERSONA JURÍDICA Y CERTIFICADO DE PSC*

La Cédula Tributaria es expedida por la Subsecretaría de Estado de Tributación y debe cumplir el siguiente formato:

Tabla Nº 2 - Certificado de Persona Jurídica

| Tipo de Documento | Prefijo | Formato | Descripción |
|---|---|---|---|
| Cédula Tributaria – RUC | RUC | RUC99999999-9 | Siglas RUC seguido del número de RUC. |

#### *3.1.4.2 CERTIFICADO DE PERSONA FÍSICA*

La Cédula de Identidad civil es expedida por el Departamento de Identificaciones de la Policía Nacional, y debe cumplir el siguiente formato:

Tabla Nº 3 - CI Certificado de Persona Física

| Tipo de Documento | Prefijo | Formato | Descripción |
|---|---|---|---|
| Cédula de identidad | CI | CI999999 | Siglas CI seguido del número de cédula de identidad, el cual puede ser alfanumérico. |

El Pasaporte es expedido por un órgano nacional competente y en el caso de extranjeros por un órgano de su país de origen, y debe cumplir el siguiente formato:

Tabla Nº 4 - PAS Certificado de Persona Física

| Tipo de Documento | Prefijo | Formato | Descripción |
|---|---|---|---|
| Pasaporte | PAS | PASQ999999 | Siglas PAS seguido del número de Pasaporte, el cual puede ser alfanumérico. |

#### *3.1.4.3 CERTIFICADO DE MÁQUINA O APLICACIÓN*

Tabla Nº 5 - Certificado de máquina o aplicación

| Tipo de Documento | Prefijo | Formato | Descripción |
|---|---|---|---|
| Cédula de identidad | CI | CI999999 | Siglas CI seguido del número de cédula de identidad, el cual puede ser alfanumérico. |
| Cédula Tributaria | RUC | RUC99999999-9 | Siglas RUC seguido del número de RUC. |
| Pasaporte | PAS | PASQ999999 | Siglas PAS seguido del número de Pasaporte, el cual puede ser alfanumérico |

### 3.1.5. UNICIDAD DE NOMBRES

En este ítem, la CPS debe establecer, qué identificadores del tipo “Distinguished Name” (DN), deberán ser únicos para cada titular del certificado, en el ámbito del PSC emitente. Números y letras adicionales podrán ser incluidos al nombre de cada entidad para asegurar la unicidad del campo.

### 3.1.6 PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

La CPS debe reservar al PSC, el derecho de tomar todas las decisiones en el caso de que haya conflicto derivado de los nombres iguales entre varios solicitantes de certificados. También debe contemplar que, durante el proceso de confirmación de identidad, corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico.

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

En este apartado, la CPS debe establecer que los procesos de tratamiento, reconocimiento, autenticación y rol de marcas registradas serán ejecutados de acuerdo con la legislación vigente sobre la materia.

## 3.2 VALIDACIÓN INICIAL DE IDENTIDAD

En esta sección y en la siguiente, la CPS debe describir en detalle, los requisitos y procedimientos utilizados por las RA vinculadas al PSC responsable para llevar a cabo los siguientes procesos:

a) identificación del titular del certificado: identificación de la persona física o jurídica, titular del certificado, con base en los documentos de identificación mencionados en los ítems 3.2.2, 3.2.3 y 3.2.4, observando lo siguiente:
   I. para certificados de persona física: prueba de que la persona que se presenta como titular del certificado, es realmente aquel cuyos datos aparecen en la documentación presentada. Queda prohibido cualquier tipo de poder para tal fin.
   II. para certificados de personas jurídicas: prueba de que los documentos presentados refieren efectivamente a la persona jurídica que es el titular del certificado, y que la persona física que se presenta como un representante de la persona jurídica realmente posea tal atribución conforme a los estatutos o normas correspondientes a su funcionamiento que se encuentren vigentes al momento de la solicitud.
   III. para certificados de máquina o aplicación: conforme al literal I. si el responsable corresponde a una persona física y el literal II. si corresponde a una persona jurídica.

b) emisión del certificado: verificación de los datos de solicitud de certificado con los contenidos en los documentos presentados y autorización de la emisión del certificado en el sistema del PSC. Se considera que la extensión del Subject *Alternative Name* está fuertemente relacionada con la clave pública contenida en el certificado, por lo que todas las partes de esa extensión deben ser verificadas, y el solicitante del certificado debe demostrar que tiene los derechos sobre esta información ante los organismos competentes, o que está autorizado por el titular de la información para utilizarlos.

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

La CPS debe indicar los procedimientos ejecutados por el PSC responsable y sus RA, a ella vinculadas para confirmar que la persona física o jurídica solicitante, posea la clave privada correspondiente a la clave pública para el cual está siendo solicitado el certificado digital, pudiendo utilizar las referencias contenidas en el RFC 4210 y RFC 6712. En el caso que sean requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esa CP, en el ítem correspondiente.

### 3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

En este ítem deben ser definidos los procedimientos empleados por las RA vinculadas para la confirmación de la identidad de una persona jurídica.

Será designado como responsable del certificado el representante de la persona jurídica conforme al ítem 3.2, numeral 'a', punto (ii), quien será el poseedor de la clave privada.

La confirmación de la identidad de la persona jurídica y de la persona física deberá realizarse en los siguientes términos:

a) presentación de la lista de documentos enumerados en el punto 3.2.2.1;
b) presentación de la lista de documentos del responsable del certificado, enumerados en el ítem 3.2.3.1;
c) presencia física del responsable del certificado; y
d) firma digital de la Solicitud de Certificado y Acuerdo de Suscriptores mencionado en el ítem 4.1 por el responsable del certificado.

Podrá ser implementado adicionalmente un proceso de identificación biométrica del responsable del certificado.

Además, la RA podrá solicitar una firma manuscrita del responsable del certificado en un caso específico para su comparación con el documento de identidad o estatuto de sociedad. En este caso, se adjuntará al expediente electrónico del certificado, el documento manuscrito digitalizado y firmado digitalmente por el Agente de Registro, pudiendo descartarse el original en papel.

### *3.2.2.1 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA.*

La confirmación de la identidad de una persona jurídica se hará mediante la presentación, de por lo menos los siguientes documentos:

a) si la entidad es pública:
   i. copia simple de la Ley o Carta Orgánica que crea o autoriza su creación;
   ii. documento (original o copia autenticada) que acredite la representación; y
   iii. cédula tributaria.
b) si la entidad es privada:
   i. copia autenticada del estatuto o documento de creación;
   ii. copia autenticada del acta de la última asamblea ordinaria y extraordinaria o del documento equivalente que acredite la representación;
   iii. prueba de la inscripción en el registro oficial correspondiente; y
   iv. cédula tributaria.

La comprobación de los documentos citados precedentemente podrán realizarse por vía electrónica, siempre que se trate de fuentes oficiales de organismos competentes. Estas validaciones deberán incluirse obligatoriamente en el dossier del titular del certificado.

Los documentos, que no puedan comprobarse conforme a las condiciones del párrafo anterior deberán verificarse:

a) por un AGR que no sea el que realizó el paso de identificación; y
b) antes del inicio de la validez del certificado, debiendo ser revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

### *3.2.2.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA JURÍDICA*

La información obligatoria contenida en los campos del certificado expedido a una persona jurídica debe coincidir exactamente con la información contenida en los siguientes documentos:

a) nombre de la razón social según documento constitutivo y sin abreviaturas;
b) número de registro único del contribuyente (RUC) según la cédula tributaria;
c) nombre completo de la persona física responsable del certificado según documento de identidad; y
d) número de cédula de identidad policial o número de pasaporte de la persona física responsable del certificado según documento de identidad.

Cada CP puede definir como obligatorio llenar otros campos. Además, el responsable del certificado, a su criterio y mediante una declaración expresa en el documento de solicitud de certificado y acuerdo de suscriptores, puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del responsable del certificado;
b) nombre de la unidad de la organización en el que presta servicio el responsable del certificado;
c) posición o función asignada al responsable del certificado en la organización en el que presta servicio; y
d) el título académico del responsable del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas al dossier del titular del certificado.

Respecto a la responsabilidad derivada del uso del certificado de una persona jurídica, los actos realizados con el certificado digital de una persona jurídica están sujetos a las obligaciones establecidas en la normativa y a las facultades de representación conferidas al responsable de uso indicado en el certificado.

### 3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

En esta sección se deben definir los procedimientos empleados por la RA para confirmar la identidad de la persona física.

La confirmación de la identidad de la persona física deberá realizarse en los siguientes términos:

a) presentación del documento de identidad vigente según lo establecido en el punto 3.2.3.1;
b) presencia física del titular del certificado; y
c) firma digital de la Solicitud y Acuerdo de Suscriptores mencionado en el ítem 4.1 por el titular del certificado.

Podrá ser implementado adicionalmente un proceso de identificación biométrica del titular del certificado.

Además, la RA podrá solicitar una firma manuscrita del titular del certificado en un caso específico para su comparación con el documento de identidad. En este caso, se adjuntará al expediente electrónico del certificado, el documento manuscrito digitalizado y firmado digitalmente por el Agente de Registro, pudiendo descartarse el original en papel.

***3.2.3.1 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA FÍSICA.***

Para la confirmación de la identidad de la persona física se debe presentar en su versión original, vigente y en buen estado las siguientes documentaciones:

i. cédula de identidad paraguaya o;
ii. pasaporte expedido por el órgano competente.

En el caso que el solicitante sea de nacionalidad extranjera deberá presentar su versión original, vigente y en buen estado:

i. pasaporte expedido por el órgano competente en su país de origen.

La comprobación de los documentos citados precedentemente podrán realizarse por vía electrónica, siempre que se trate de fuentes oficiales de organismos competentes. Estas validaciones deberán incluirse obligatoriamente en el dossier del titular del certificado.

Los documentos, que no puedan comprobarse conforme a las condiciones del párrafo anterior deberán verificarse:

a) por un AGR que no sea el que realizó el paso de identificación;
b) por la RA delegada o RA propia vinculadas al PSC; y

c) antes del inicio de la validez del certificado, debiendo ser revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

#### *3.2.3.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA FÍSICA*

La información obligatoria contenida en los campos del certificado expedido a una persona física debe coincidir exactamente con la información contenida en los siguientes documentos:

a) nombre completo de la persona física titular del certificado según el documento de identidad; y
b) número de cédula de identidad policial o número de pasaporte de la persona física, según documento de identidad.

Cada CP puede definir como obligatorio llenar otros campos. Además, el titular del certificado, a su criterio y mediante una declaración expresa en el documento de solicitud de certificado y acuerdo de suscriptores, puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del titular del certificado;
b) el nombre de la organización en el que presta servicio el titular del certificado;
c) el nombre de la unidad de la organización en el que presta servicio el titular del certificado;
d) el número de RUC de la organización en el que presta servicio el titular del certificado o el número de RUC del certificado si no se registran los datos de la organización en la que presta servicio;
e) posición o función designada al titular del certificado en la organización en el que presta servicio; y
f) el título académico del titular del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas al dossier del titular del certificado.

### 3.2.4. AUTENTICACIÓN DE IDENTIDAD DE UNA MÁQUINA O APLICACIÓN

En el caso de los certificados expedidos para máquina o aplicación, el titular será la persona física o jurídica que solicita el certificado, quien deberá indicar el responsable de la clave privada.

Si el titular del certificado es una persona física, se deberá confirmar su identidad según lo estipulado en el Ítem 3.2.3.1.

Si el titular del certificado es una persona jurídica, se deberá confirmar su identidad según lo estipulado en el Ítem 3.2.2.1.

#### *3.2.4.1 DOCUMENTOS REQUERIDOS PARA LA IDENTIFICACIÓN DE UNA MÁQUINA O APLICACIÓN*

Para la confirmación de la identidad de una máquina o aplicación se debe presentar en su versión original y vigente, las siguientes documentaciones:

**a)** para emisión de certificados de máquinas que se utilizan como servidores:
- **i.** declaración expresa en la solicitud del nombre del servidor y número de serie;
- **ii.** copia de factura o comprobante equivalente de compra del equipo; y
- **iii.** autorización firmada por el titular de la factura o comprobante para utilizar ese número de serie en caso que no coincida con el nombre del titular del certificado.

b) para los certificados de máquinas o aplicaciones que utilizan URL;
- i. registro del nombre de dominio por el órgano competente; y
- ii. autorización firmada por el titular del dominio para utilizar ese nombre en caso que no coincida con el nombre del titular del certificado.

La comprobación de los documentos citados precedentemente podrán realizarse por vía electrónica, siempre que se trate de fuentes oficiales de organismos competentes. Estas validaciones deberán incluirse obligatoriamente en el dossier del titular del certificado.

Los documentos, que no puedan comprobarse existan para verificación por medio aplicaciones oficiales de conforme a las condiciones del párrafo anterior entidades del gobierno, deberán verificarse:

a) por un AGR que no sea el que realizó el paso de identificación;
b) por la RA delegada o RA propia vinculados al PSC; y
c) antes del inicio de la validez del certificado, debiendo ser revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

#### *3.2.4.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA MÁQUINA O APLICACIÓN*

La información obligatoria contenida en los campos del certificado expedido a un dispositivo o aplicación, debe coincidir exactamente con la información contenida en los siguientes documentos:

a) URL o nombre de la aplicación; y
b) en el caso que el titular sea una persona jurídica:
   i. número de registro único del contribuyente (RUC) de la persona jurídica según la cédula tributaria;
   ii. nombre de la razón social de la persona jurídica, según documento constitutivo;
   iii. nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas; y
   iv. número de cédula de identidad policial o número de pasaporte de la persona física responsable del certificado según documento de identidad; o
c) en el caso que el titular sea una persona física:
   i. número de cédula de identidad policial o número de pasaporte de la persona física, según documento de identidad; y
   ii. nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas.

Además, el titular del certificado, a su criterio y mediante una declaración expresa en el documento de solicitud de certificado y acuerdo de suscriptores puede solicitar llenar los campos con las siguientes informaciones:

a) en el caso que el titular sea una persona jurídica:
   i. el correo del responsable del certificado;
   ii. nombre de la unidad de la organización en el que presta servicio el responsable del certificado;

iii. posición o función designada al responsable del certificado en la organización en el que presta servicio; y

iv. el título académico del responsable del certificado.

b) en caso de que el responsable es una persona física:

i. el correo del responsable del certificado;

ii. nombre de la de la organización en el que presta servicio el responsable del certificado

iii. nombre de la unidad de la organización en el que presta servicio el responsable del certificado;

iv. número de RUC correspondiente a la organización en el que presta servicio el titular del certificado o el número RUC del titular del certificado si no se registran los datos de la organización en la que presta servicio;

v. posición o función designada al responsable del certificado en la organización en el que presta servicio; y

vi. el título académico del responsable del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas al dossier del titular del certificado.

### 3.2.5. INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

No aplica.

### 3.2.6. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

La RA, debe validar la capacidad del solicitante de un certificado y que no posea impedimentos legales. En el caso de Certificados de Personas Físicas, debe validar que el solicitante sea mayor de edad y en el caso de certificados de Persona Jurídica debe además validar la autoridad invocada por el representante con facultades suficientes para solicitar el certificado.

### 3.2.7. CRITERIOS PARA INTEROPERABILIDAD

Podrán ser reconocidos los certificados digitales extranjeros de conformidad a la normativa vigente. Para el efecto, el estado paraguayo deberá suscribir Acuerdos Internacionales con sus pares extranjeros, salvo que, por protocolo adicional a un tratado vigente, los países

suscriptores del mismo hayan acordado el reconocimiento recíproco de los certificados digitales emitidos en los respectivos países.

## 3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

### 3.3.1. IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES ANTES DE SU EXPIRACIÓN

En este ítem, el CPS deberá establecer los procesos de identificación del solicitante que utiliza el PSC responsable para la generación de un nuevo par de claves y su certificado correspondiente, antes de la expiración de un certificado vigente.

Este proceso se puede realizar de acuerdo con una de las siguientes posibilidades:

a) adopción de los mismos requisitos y procedimientos requeridos en los puntos 3.2.2, 3.2.3 o 3.2.4 según corresponda; y
b) solicitud por medios electrónicos firmada digitalmente utilizando un certificado vigente que sea del mismo nivel de seguridad solicitado o superior, limitada a una única vez. Tal hipótesis estará permitida sólo para certificados digitales para personas físicas y expedido el certificado por el mismo PSC, siempre y cuando el documento de identidad presentado se encuentre vigente.

### 3.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES DESPUÉS DE LA REVOCACIÓN O EXPIRACIÓN DEL CERTIFICADO

En este ítem, la CPS debe describir los procedimientos utilizados para confirmar la identidad de una persona física o jurídica que solicita un nuevo certificado, luego de la expiración o revocación del certificado emitido previamente. Si se requieren procedimientos específicos para las CP implementadas, se deben describir en dichas CP, en el ítem correspondiente.

Este proceso debe realizarse de acuerdo a los requisitos y procedimientos requeridos en los puntos 3.2.2, 3.2.3 o 3.2.4.

### 3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

El procedimiento para solicitar la revocación de un certificado por parte de CA Raíz-Py se describe en el ítem 4.9.3. En este apartado, la CPS debe describir los procedimientos utilizados para identificar al solicitante de la revocación de certificado. La CPS debe exigir que las solicitudes de revocación de certificados sean siempre registradas.

Solamente los agentes descriptos en el ítem 4.9.2 pueden solicitar la revocación del certificado de un PSC.

## 4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

### 4.1 SOLICITUD DEL CERTIFICADO

En este ítem de la CPS, deben ser descriptos todos los requisitos y procedimientos operacionales establecidos por el PSC responsable y las RAs, a ella vinculadas, para las solicitudes de emisión de certificados. Estos requisitos y procedimientos deberán comprender, en detalles, todas las acciones necesarias tanto del solicitante como del PSC y RA en el proceso de solicitud del certificado digital. La descripción también debe contemplar:

a) la comprobación de los atributos de identificación que constan en el certificado, conforme al ítem 3.2;
b) una solicitud y acuerdo de suscriptores firmado digitalmente por el titular del certificado o por el responsable del certificado, en el caso de un certificado de persona jurídica, de acuerdo con los **FORMATOS DE SOLICITUD Y ACUERDO DE SUSCRIPTORES** establecidos por la CA Raíz.

Ante la imposibilidad técnica de firmar digitalmente la solicitud de certificado y acuerdo de suscriptores se aceptará la firma manuscrita del solicitante siendo necesaria la verificación de su firma contra el documento identidad presentado.

### 4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

La presentación de la solicitud debe ser siempre a través de una RA.

En este ítem se detallan las personas que pueden presentar una solicitud de certificado, que en el marco de la PKI-Paraguay, son:

a) para el caso de certificado de persona física, toda persona, mayor de edad, sin distinción, con un documento de identidad válido, que será el sujeto a cuyo nombre se emita el certificado;
b) para el caso de certificado de persona jurídica, el representante de la persona jurídica; y
c) para el caso de certificado de máquina o aplicación, el representante si el solicitante es una persona jurídica, o toda persona, mayor de edad, sin distinción, con un documento de identidad válido si el solicitante es una persona física.

### 4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Los siguientes ítems deben describir las obligaciones generales de las entidades involucradas. Si existen obligaciones específicas para las CPs implementadas, se deben describir en dichas CPs, en el ítem correspondiente.

#### *4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PSC*

**Responsabilidades:**

a) el PSC es responsable de los daños que causa; y
b) el PSC responde solidariamente por los actos de las entidades de su cadena de certificación: RA, PSS y VA.

**Obligaciones**

Este ítem se deben incluir las obligaciones del PSC responsable de la CPS, conteniendo al menos lo siguiente:

a) operar de acuerdo a su CPS y CP que implementan;
b) generar y gestionar sus pares de claves criptográficas;
c) asegurar la protección de sus claves privadas;

d) notificar a la CA Raíz-Py, emisor de su certificado, cuando se presenta el compromiso de su clave privada y solicitar la revocación inmediata del correspondiente certificado;
e) notificar a sus usuarios cuando hay una sospecha de compromiso de su clave privada o una nueva emisión de su par de claves o la terminación de prestación de sus servicios;
f) distribuir su propio certificado;
g) emitir, expedir y distribuir los certificados de los AGR y de los usuarios finales;
h) informar la emisión del certificado al respectivo solicitante;
i) revocar los certificados por él emitidos;
j) emitir, gerenciar y publicar sus CRLs y disponibilizar la consulta online de la situación de los certificados emitidos (OCSP-On-line Certificate Status Protocol);
k) publicar, en su sitio principal Internet, su CPS, y las CP aprobadas que implementa;
l) publicar, en su sitio principal de Internet, las informaciones definidas en el ítem 2.2. de este documento;
m) publicar, en su sitio principal Internet, las informaciones sobre la desvinculación de una RA vinculada.
n) utilizar protocolo de comunicación segura para proporcionar servicios a los solicitantes y usuarios de certificados digitales a través de la web;
o) identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por el MIC.
p) adoptar las medidas de seguridad y de control previstas en la CPS, CP y políticas de seguridad (PS) que se implementa, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por el MIC.
q) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por el MIC y la normativa vigente;
r) mantener y garantizar la integridad, confidencialidad y seguridad de la información por ella tratada;
s) mantener y anualmente realizar prueba de su PCN;
t) mantener el contrato de seguro de responsabilidad civil resultante de las actividades de certificación digital y de registro, con una cobertura suficiente y compatible con el riesgo de dichas actividades.

u) informar a la parte que confía y los titulares de certificados sobre las garantías, cobertura, condiciones y limitaciones establecidas a la póliza de seguro de responsabilidad civil contraída en los términos indicado en el inciso t) de este ítem;

v) informar a la CA Raíz-Py, mensualmente, la cantidad de certificados digitales emitidos y revocados;

w) no emitir el certificado con una fecha de caducidad que se extienda más allá de la fecha de vencimiento de su propio certificado.

x) realizar las auditorías internas con sus profesionales y las auditorías externas con profesionales externos independientes, ambas habilitadas por CA Raíz-Py. El PSC debe presentar un informe de auditoría único para cada RA vinculada al PSC que utilizan sus servicios; y

y) asegurarse de que todas las aprobaciones de solicitudes de certificados sean realizadas por un AGR en una estación de trabajo autorizada.

#### *4.1.2.2 RESPONSABILIDADES Y OBLIGACIONES DE LA RA*

**Responsabilidades**

La RA será responsable de los daños que ocasione.

**Obligaciones**

En este apartado de la CPS, deben ser incluidas las obligaciones de las RAs vinculadas al PSC responsable de la CPS, conteniendo, como mínimo, las consideraciones mencionadas a continuación:

a) recibir las solicitudes de emisión y revocación de los certificados;

b) confirmar la identidad del solicitante y validar la solicitud;

c) remitir la solicitud de emisión o revocación del certificado al PSC responsable, por medio de acceso remoto al ambiente de la RA alojado en las instalaciones del PSC, utilizando un protocolo de comunicación seguro, conforme al patrón definido en el documento DOC-PKI-05 [2];

d) informar a los respectivos titulares la emisión o revocación de sus certificados;

e) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, criterios, prácticas y reglas establecidas por el PSC vinculado, el MIC y en especial con lo contenido en el documento DOC-PKI-05 [2];

f) mantener y anualmente realizar prueba de su PCN;

g) proceder a la comprobación de las firmas y de la validez de los documentos presentados en la forma de los ítems 3.2.2, 3.2.3 y 3.2.4.; y
h) divulgar sus prácticas, relacionadas con el PSC a la que está vinculada en conformidad a las normas establecidas en el marco de la PKI-Paraguay.

## 4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

### 4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

La RA vinculada al PSC debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el ítem 3.

### 4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

El PSC y la RA podrán, con la debida justificación formal, aceptar o rechazar solicitudes de certificados de los solicitantes de acuerdo con los procedimientos descriptos en esta CPS y la normativa vigente.

### 4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

El PSC debe cumplir con los procedimientos determinados por la CA Raíz-Py. No habrá tiempo máximo para procesar solicitudes en el marco de la PKI-Paraguay.

## 4.3 EMISIÓN DEL CERTIFICADO

### 4.3.1 ACCIONES DEL PSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

En esta sección de la CPS, deben ser descriptos, los requisitos operacionales establecidos por el PSC para la emisión de los certificados. En caso de que sean requeridos procedimientos específicos para cada CP implementada, los mismos deben ser descriptos, en el ítem correspondiente.

Las CPS deben indicar que un certificado será considerado válido a partir del momento de su emisión.

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

En este ítem de la CPS, deben ser descriptos los requisitos operacionales establecidos por el PSC responsable para la notificación al solicitante. En caso de que sean requeridos procedimientos específicos para cada CP implementada, los mismos deben ser descriptos, en el ítem correspondiente.

## 4.4 ACEPTACIÓN DEL CERTIFICADO

### 4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

En este ítem deben ser descriptos todos los requisitos y procedimientos operacionales referentes a la aceptación de un certificado por su titular. Deben ser apuntadas las implicancias de la aceptación, o de la no aceptación del certificado. En caso de que sean requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

La CPS debe garantizar que la aceptación de todo certificado emitido sea declarada expresamente por el respectivo titular en la Solicitud y Acuerdo de Suscriptores. En caso de los certificados emitidos para persona jurídica, máquina o aplicación, la declaración expresa deberá ser de la persona física responsable de ese certificado.

Posibles términos del contrato, o instrumentos similares, requeridos deben describirse en este ítem de la CPS.

### 4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC

El certificado del PSC y los certificados emitidos a usuarios finales, deberán ser publicados de acuerdo con el punto 2.2 de esta CPS.

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

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

## 4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

El titular de un certificado debe usar el par de claves y el certificado correspondiente de acuerdo a la Declaración de Prácticas de Certificación (CPS) y las Políticas de Certificación (CP) que implementa el PSC emitente de su certificado, establecidas de acuerdo con este documento y con el documento DOC-PKI-04 [1]**.**

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

El PSC debe utilizar su clave privada y garantizar la protección de esa clave según lo previsto en su propia CPS.

Este ítem debe incluir las obligaciones de los titulares de certificados emitidos por el PSC responsable de la CPS, contenidas en los **FORMATOS DE SOLICITUD Y ACUERDO DE SUSCRIPTORES** referidos en el ítem 4.1, y debe incluir al menos los ítems que se enumeran a continuación:

a) proporcionar, de manera completa y veraz, toda la información necesaria para su identificación;
b) garantizar la protección y confidencialidad de sus claves privadas, contraseñas y dispositivos criptográficos;
c) utilizar sus certificados y claves privadas de forma adecuada, según lo previsto en la CP correspondiente;
d) conocer sus derechos y obligaciones, contemplados en la CPS y la CP correspondiente y demás documentos aplicables de la PKI-Paraguay; y
e) informar al PSC emisor de cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

En el caso de un certificado emitido a una persona jurídica, máquina o aplicación, estas obligaciones se aplican a la persona responsable del certificado.

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

Conforme a lo estipulado en el ítem 9.6.4 de esta CPS.

## 4.6 RENOVACIÓN DEL CERTIFICADO

Conforme a lo estipulado en el ítem 3.3 de esta CPS.

### 4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

Conforme a lo estipulado en el ítem 3. 3 de esta CPS.

### 4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

Conforme a lo estipulado en el ítem 4.1.1 de esta CPS.

### 4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Conforme a lo estipulado en el ítem 4.2 de esta CPS.

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

Conforme a lo estipulado en el ítem 4.3.2 de esta CPS.

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

Conforme a lo estipulado en el ítem 4.4.1 de esta CPS.

### 4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO RENOVADO

Conforme a lo estipulado en el ítem 4.4.2 de esta CPS.

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

Conforme a lo estipulado en el ítem 4.4.3 de esta CPS.

## 4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY)

Este ítem no aplica.

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

Este ítem no aplica.

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

Este ítem no aplica.

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

Este ítem no aplica.

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

Este ítem no aplica.

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

Este ítem no aplica.

### 4.7.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS RE-EMITIDOS

Este ítem no aplica.

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

Este Ítem no aplica.

## 4.8 MODIFICACIÓN DE CERTIFICADOS

Este ítem no aplica.

### 4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

### 4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

### 4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

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

Este ítem no aplica.

### 4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Este ítem no aplica.

### 4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS

Este ítem no aplica.

### 4.8.7 NOTIFICACIÓN POR EL PSC DE UNA EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

Este ítem no aplica.

## 4.9 REVOCACIÓN Y SUSPENSIÓN

### 4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

En este ítem de la CPS, deben ser consignadas, las circunstancias en la cual un certificado podrá ser revocado.

Este ítem también debe establecer que un certificado deberá obligatoriamente ser revocado en las siguientes circunstancias:

a) que afecten la información contenida en el certificado:

i. modificación de alguno de los datos contenidos en el certificado;
ii. descubrimiento que algunos de los datos aportados en la solicitud de certificado sean incorrectos, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado; y
iii. descubrimiento que algunos de los datos contenidos en el certificado son incorrectos.

b) que afectan la seguridad de la clave o del certificado:
   i. compromiso de la clave privada o de la infraestructura o sistemas de la CA que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente;
   ii. infracción, por el PSC, de los requisitos previstos en los procedimientos de gestión de los certificados, establecidos en su propia CP y CPS;
   iii. compromiso o sospecha de compromiso de la seguridad de la clave, del certificado del titular del certificado o de su medio de almacenamiento;
   iv. acceso o utilización no autorizada, por un tercero, de la clave privada del titular; y
   v. el uso irregular por el titular, o falta de diligencia en la custodia de la clave privada;

c) circunstancias que afectan la seguridad del dispositivo criptográfico:
   i. compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico;
   ii. pérdida o inutilización por daños del dispositivo criptográfico; y
   iii. acceso no autorizado, por un tercero, a los datos de activación de la clave privada del titular del certificado;

d) circunstancias que afectan al suscriptor:
   i. infracción del titular del certificado en sus obligaciones, responsabilidad y garantías, establecidas en la CP y CPS del PSC que emitió el certificado;
   ii. la incapacidad de hecho sobrevenida o la muerte del titular del certificado; y
   iii. la extinción de la persona jurídica titular del certificado;
   iv. solicitud de revocación del certificado por su titular de acuerdo con lo establecido en la CP y en la CPS.

e) otras causales especificadas en la normativa y reglamentación vigente.

La CPS deberá indicar que el PSC emisor revocará, dentro del plazo definido en el ítem 4.9.3, el certificado del titular del certificado que incumpla con las políticas, estándares y reglas establecidas en el marco de la PKI-Paraguay.

La CPS también deberá indicar que la CA Raíz-Py podrá determinar la revocación del certificado del PSC que incumpla con la legislación vigente o las políticas, estándares, prácticas y reglas establecidas en el marco de la PKI-Paraguay.

### 4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

En este ítem de la CPS, debe establecer que la revocación de un certificado sólo podrá realizarse:

a) por solicitud del titular del certificado;
b) por solicitud del responsable del certificado, en el caso de un certificado de persona jurídica o un certificado de máquina o aplicación;
c) por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado o funcionario;
d) por el PSC emitente;
e) por una RA vinculada al PSC emitente;
f) por determinación de la CA Raíz-Py; y
g) por una autoridad judicial competente.

### 4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

En este apartado, la CPS debe describir los procedimientos establecidos por el PSC para la solicitud de revocación de certificados. El PSC deberá garantizar que quienes están autorizados a solicitar la revocación, conforme al ítem 4.9.2, puedan, fácilmente y en cualquier momento, solicitar la revocación de sus respectivos certificados.

Como directrices generales, la CPS debe establecer que:

a) el solicitante de revocación de un certificado será identificado;
b) las solicitudes de revocación, así como las acciones resultantes de ellas serán registradas y almacenadas;

c) se documentarán las razones de la revocación de un certificado; y
d) la revocación de un certificado terminará con la generación y publicación de una CRL que contenga los datos del certificado revocado y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PSC.

El plazo máximo admitido para la conclusión del proceso de revocación del certificado después de la recepción de la respectiva solicitud, para todos los tipos de certificados previstos en la PKI-Paraguay, será de 12 (doce) horas.

La CPS debe garantizar de que el PSC responsable responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su revocación y la emisión de la CRL correspondiente.

En caso de que sean requeridos procedimientos de revocación específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

### 4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

En este ítem, el CPS deberá observar que la solicitud de revocación debe ser inmediata cuando se configuren las circunstancias definidas en el ítem 4.9.1 y deberá establecer el plazo para la aceptación del certificado por su titular, dentro del cual la revocación de dicho certificado podrá ser solicitada sin que se aplique alguna tarifa por el PSC.

Si se requieren plazos específicos para las CPs implementadas, estos deberán estar descriptos en dichas CPs, en el ítem correspondiente.

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

En el caso de una solicitud formalmente constituida, de acuerdo con las reglas de la PKI-Paraguay, el PSC debe procesar la revocación inmediatamente después de analizar la solicitud.

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

En este apartado, la CPS debe referir la necesidad de que las partes que confían evalúen el estado del certificado y el estado de todos los certificados de la CA en la cadena a la que pertenece el mismo, 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 el PSC.

Antes de confiar en un certificado, la parte que confía debe confirmar la validez de cada certificado en la cadena de certificación de acuerdo con los estándares IETF PKIX, incluida la verificación de la validez del certificado, encadenando el nombre del emisor y el titular, restricciones de uso de claves y políticas de certificación y estado de revocación por medio de la CRL o respuestas OCSP identificadas en cada certificado en la cadena de certificación.

### 4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

En esta sección, se debe establecer la frecuencia de emisión de la CRL referente a los certificados de los usuarios finales.

La CRL debe actualizarse y publicarse inmediatamente cuando surja una revocación o con una frecuencia máxima para certificados de usuario final de 12 (doce) horas.

En caso que sean utilizadas frecuencias de emisión específicas de CRL para las CPs implementadas, deben ser descriptos en estas CPs, en el ítem correspondiente.

### 4.9.8 LATENCIA MÁXIMA PARA CRL

En este ítem se debe establecer la latencia máxima para la CRL. Este plazo será como máximo de 1 (hora) hora posterior a su generación.

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

En este ítem, la CPS debe informar, según sea el caso, las disponibilidades de recursos del PSC responsable para la revocación en línea del certificado o para la verificación en línea del estado de los certificados. El PSC o una VA vinculada, mediante el protocolo OCSP (On-line Certificate Status Protocol), permiten verificar en lìnea el estado de los certificados.

La CPS debe observar que todo certificado debe tener su validez verificada, en la respectiva CRL o OCSP, antes de ser utilizado.

La CPS también debe observar que la autenticidad de la CRL/OCSP además debe confirmarse mediante la verificación de la firma del PSC emisor y del período de validez de la CRL/OCSP.

### 4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

En este ítem, la CPS debe definir, cuando corresponda, los requisitos para la verificación en línea de la información de revocación de certificados por las partes que confían. Si se requieren procedimientos específicos para las CPs implementadas, se deben describir en dichas CPs, en el ítem correspondiente.

### 4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

En este ítem, la CPS informará, cuando existieren, otras formas utilizadas por el PSC responsable para la divulgación de informaciones de revocación de certificados.

La CPS definirá, en su caso, los requisitos para la verificación de las formas de divulgación señaladas en el ítem anterior y de las informaciones de revocación de certificados, por la parte que confía (*relying parties*).

### 4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

En este ítem de la CPS deben ser definidos los requisitos aplicables para la revocación del certificado provocado por el compromiso de la clave privada correspondiente. La CPS debe tener en cuenta que, en esta circunstancia, el titular del certificado deberá comunicar el hecho inmediatamente al PSC emitente. En el caso que haya requisitos específicos para las CPs implementadas, los mismos deben ser descriptos en esas CPs, en el ítem correspondiente.

La CPS debe contener también determinaciones que definan los medios utilizados para comunicar un compromiso o sospecha de compromiso de la clave privada.

### 4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

Este Ítem no aplica.

### 4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Este Ítem no aplica.

### 4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Este Ítem no aplica.

### 4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

Este Ítem no aplica.

## 4.10 SERVICIOS DE ESTADO DEL CERTIFICADO

### 4.10.1 CARACTERÍSTICAS OPERACIONALES

El PSC debe proporcionar un servicio de estado de certificado en forma de un punto de distribución de CRL en los certificados y OCSP, conforme al ítem 4.9.

### 4.10.2 DISPONIBILIDAD DEL SERVICIO

En este ítem, se debe establecer el tiempo de disponibilidad del servicio de publicación de la CRL, certificados emitidos en el repositorio público y el servicio de consulta en línea por medio del protocolo OCSP. Estos servicios deben estar disponibles durante las veinticuatro horas, los siete días de la semana. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0.5% anual.

### 4.10.3 CARACTERÍSTICAS OPCIONALES

El servicio OCSP, que permite consultar el estado de certificados es una característica opcional para la CA Raíz, sin embargo, para el PSC constituye una característica obligatoria.

Para hacer uso del servicio de validación en línea es responsabilidad de la parte que confía disponer de un *cliente OCSP* que cumpla el RFC 6960.

## 4.11 FIN DE ACTIVIDADES

Este ítem de la CPS deberá describir los requisitos y procedimientos que deberán adoptarse en caso de extinción o cese de los servicios del PSC responsable, de una RA, VA o PSS vinculada a ella.

Deben ser detallados los procedimientos para notificar a los usuarios y transferir la custodia de sus datos y registros de archivo.

## 4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

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

En este ítem, la CPS debe informar sobre la imposibilidad que tiene el PSC de copiar o almacenar los datos de creación de firma de su suscriptor. Sin embargo, el usuario final podrá optar por el Servicio de Almacenamiento de claves, el cual será exclusivamente prestado por un PSA. El PSA es una entidad autorizada por la CA Raíz-Py y vinculada a un PSC, con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.

Este ítem la CPS también debe describir los procedimientos, las prácticas y las políticas de custodia para recuperar las claves de cifrado utilizadas por el PSC.

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

En este ítem, se debe identificar el documento o lista que contiene las políticas y prácticas para el encapsulado y recuperación de la clave de sesión de un PSC.

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

En los ítems siguientes, deben ser descriptos los controles de seguridad implementados por el PSC responsable de la CPS y por las RAs a ella vinculadas, para ejecutar de modo seguro sus funciones de generación de claves, identificación, certificación, auditoría y archivo de los registros.

## 5.1 CONTROLES FÍSICOS

En las secciones siguientes, la CPS debe describir los controles físicos referentes a las instalaciones que albergan los sistemas del PSC responsable y de las RA vinculadas.

### 5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La CPS debe establecer que la localización de las instalaciones donde se albergan los sistemas de certificación del PSC responsable, no deberá ser públicamente identificada. No deberá haber identificación pública externa de las instalaciones e internamente, no deberá ser admitido ambientes compartidos que permitan la visibilidad de las operaciones de emisión y revocación de los certificados. Esas operaciones deberán ser segregadas en compartimientos cerrados y físicamente protegidos.

En este ítem, la CPS debe también describir los aspectos de la construcción de las Instalaciones del PSC responsable, relevantes para los controles de seguridad física, comprendiendo entre otros:

a) instalaciones para equipamientos de apoyo, tales como: máquinas de aire acondicionado, grupos de generadores, UPS, baterías, tableros de distribución de energía y de telefonía;
b) instalaciones para sistemas de telecomunicaciones;
c) los sistemas de puesta a tierra y protección contra rayos; e

d) iluminación de emergencia;

### 5.1.2 ACCESO FÍSICO

Todo PSC integrante de la PKI-Paraguay deberá implementar un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme a al ítem 9 “control de accesos” de la norma ISO 27002:2013 y los siguientes puntos:

#### *5.1.2.1 NIVELES DE ACCESO FÍSICO*

La CPS debe definir por los menos 4 (cuatro) niveles de acceso físico a los diversos ambientes del PSC responsable, más 2 (dos) niveles relativos a la protección de la clave privada del PSC.

En el primer nivel deberá situarse la primera barrera de acceso a las instalaciones del PSC. Para acceder al área del nivel 1, cada persona deberá ser identificada y registrada por el personal de seguridad, a partir de ese nivel personas extrañas a la operativa del PSC deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PSC deberá ser ejecutado en ese nivel.

Excepto en los casos previstos por la ley, la posesión de armas no será admitida en las instalaciones del PSC, desde el nivel 1. A partir de ese nivel, equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles, será controlado su ingreso y sólo pueden ser utilizados mediante la autorización formal y supervisada.

El segundo nivel será interno al primero y deberá requerir, de la misma forma que el primero, una identificación individual de las personas que en él, accedan. Ese será el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso operacional o administrativo del PSC. El paso del primer al segundo nivel deberá exigir por lo menos 1 (uno) factor de autenticación electrónica y tarjeta de identificación visible.

En el tercer nivel deberá situarse dentro del segundo nivel y será el primer nivel en albergar material y actividades sensibles de la operativa del PSC. Cualquier actividad relativa al ciclo de vida de los certificados digitales deberá estar localizada a partir de este nivel. Personas que no están involucradas con esas actividades no deberán tener permiso para acceder a este

nivel. Las personas que no poseen permiso de acceso no podrán permanecer en ese nivel si no estuviesen acompañadas por alguien que tenga permiso de acceso.

En este nivel deberán ser controladas tanto las entradas como las salidas de cada persona autorizada. Los mecanismos de control que deberán ser requeridos para acceder a ese nivel como mínimo requerirán de 2 (dos) factores de autenticación electrónica y tarjeta de identificación visible.

Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PSC, no serán aceptadas desde el nivel 3.

En el cuarto nivel, interno al tercero, donde han de desplegarse, actividades especialmente sensibles a la operación del PSC, tales como la emisión y revocación de los certificados y la emisión de la CRL. Todos los sistemas y equipamientos necesarios a estas actividades deberán estar localizados a partir de este nivel. El nivel 4 deberá poseer 2 (dos) factores de autenticación como mínimo (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, deberá exigir, en cada acceso a su ambiente, la identificación de, como mínimo, 2 (dos) personas autorizadas. En este nivel, la permanencia de esas personas deberá ser exigida mientras el ambiente estuviera ocupado.

En el cuarto nivel, todas las barreras físicas (paredes y barrotes) deben ser sólidas, extendiéndose desde el piso real al techo real. Las paredes, piso y techo deberán ser realizadas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de comunicación no deberán permitir la penetración física en las áreas de cuarto nivel. Adicionalmente, debe tener una protección contra las interferencias electromagnéticas externas.

Este ambiente deberá ser construido según las normas internacionales aplicables.

Podrá existir, en el PSC, varios ambientes del cuarto nivel para albergar y segregar, cuando fuera el caso:

a) equipamientos de producción on-line y cofre de almacenamiento;
b) equipamientos de producción off-line y cofre de almacenamiento; y
c) equipamientos de redes e infraestructura (firewall, ruteadores, switches y servidores).

En el quinto nivel, interno al ambiente del nivel 4, deberá disponerse de un cofre o un gabinete reforzado, donde estarán almacenados: materiales criptográficos, tales como, claves, datos de activación, sus copias y equipamientos criptográficos

Para garantizar la seguridad del material almacenado, el cofre o el gabinete deberán obedecer las siguientes especificaciones mínimas:

a) estar hecho de acero o con material de resistencia equivalente; y
b) poseer cerraduras antirrobo.

En el sexto nivel, interno al ambiente del nivel 4, deberá comprender un cofre o un gabinete reforzado. Los datos de activación de la clave privada del PSC deberán ser almacenados en ese ambiente.

Para garantizar la seguridad del material almacenado, el cofre o el gabinete deberán obedecer las siguientes especificaciones mínimas:

a) estar hecho de acero o con material de resistencia equivalente; y
b) poseer cerraduras antirrobo.

#### *5.1.2.2 SISTEMAS FÍSICOS DE DETECCIÓN*

Toda transición entre los diferentes niveles de acceso, así como la sala de operaciones del nivel 4, deberán ser monitoreadas por cámaras de video ligadas a un sistema de grabación 24x7. El posicionamiento y la capacidad de esas cámaras no deberán permitir recuperar las contraseñas digitadas en los controles de acceso.

Las cintas de vídeo resultantes de grabación 24x7 deberán ser almacenadas, como mínimo, 2 (dos) años. Ellas deberán ser testeadas (verificación de estrechos aleatorios en el inicio, medio y final de la cinta) por lo menos cada 3 (tres) meses, con la elección, como mínimo, de 1 (una) cinta referente a cada semana. Esas cintas deberán ser almacenadas en el ambiente del nivel 3.

Todas las puertas de transición entre los ambientes de niveles 3 y 4 deberán ser monitoreadas por un sistema de notificación de alarmas. Donde hubiere, a partir del nivel 2, vidrios separando niveles de acceso, deberá ser implementado un mecanismo de alarma de quiebra de vidrios, que deberá estar funcionando ininterrumpidamente.

En todos los ambientes del cuarto nivel, una alarma de detección de movimientos deberá permanecer activa hasta que se satisfaga el criterio de acceso al ambiente. Así que si, debido a la salida de uno o más empleados, trae como consecuencia que el criterio mínimo de ocupación deje de ser satisfecha, deberán activarse automáticamente los sensores de presencia.

Los sistemas de notificación de alarmas deberán utilizar por lo menos 2 (dos) medios de notificación: sonoro y visual.

El sistema de monitoreo de las cámaras de video, así como el sistema de notificación de alarma, deberán ser permanentemente monitoreados por el personal autorizado en el ambiente de nivel 3 deben estar localizados en el nivel 3. Las instalaciones del sistema de monitoreo, a su vez, deben ser monitoreados por cámaras de vídeo cuyo posicionamiento debería permitir el seguimiento de las acciones del personal autorizado.

#### *5.1.2.3 SISTEMAS DE CONTROL DE ACCESO*

El sistema de control de acceso deberá estar en el ambiente de nivel 4.

#### *5.1.2.4 MECANISMOS DE EMERGENCIA*

Mecanismos específicos deberán ser implementados por el PSC para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia. Esos mecanismos deberán permitir el desbloqueo de las puertas por medio de accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada por medio de estos mecanismos debe accionar inmediatamente las alarmas de apertura de puertas.

El PSC podrá especificar e implementar otros mecanismos de emergencia, específicos necesarios para cada tipo de instalación. Todos los procedimientos referentes a esos mecanismos de emergencia deberán ser documentados. Los mecanismos y procedimientos de emergencia deberán ser verificados semestralmente, por medio de simulación de situaciones de emergencia.

### 5.1.3 ENERGÍA Y AIRE ACONDICIONADO

La infraestructura del ambiente de certificación del PSC deberá ser dimensionada con sistemas y dispositivos que garanticen el funcionamiento ininterrumpido de energía eléctrica en

las instalaciones. Las condiciones de funcionamiento ininterrumpido de energía deben ser mantenidas de forma de atender los requisitos disponibilidad de los sistemas del PSC y de sus respectivos servicios. Un sistema puesta a tierra deberá ser implantado.

Todos los cables eléctricos deben estar protegidos por tuberías y conductos apropiados.

Deberán ser utilizados tuberías, conductos, canaletas, paneles y cajas (de paso, distribución y terminación) diseñadas y construidas de forma a facilitar la inspección y detección de intentos de manipulación. Deberán ser utilizados conductos separados para los cables de energía, de telefonía y de datos.

Todos los cables deben ser catalogados, identificados e inspeccionados periódicamente, al menos cada seis (6) meses, en busca de evidencia de violación u otras anomalías.

Deberán ser mantenidos actualizados los registros sobre la topología de la red de cables, de acuerdo a los requisitos de confidencialidad establecidos en el ítem 13 “seguridad en las telecomunicaciones” de la norma ISO 27002/2013. Cualquier modificación en esa red deberá ser previamente documentada.

No deberán ser admitidas instalaciones provisorias, cableados expuestas o directamente conectadas a tomas sin la utilización de conectores adecuados.

El sistema climatización deberá cumplir con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente y disponer de filtros de polvo. En los ambientes de nivel 4, el sistema de climatización deberá ser independiente y tolerable a fallas.

La temperatura de los ambientes atendidos por el sistema de climatización deberá ser permanentemente monitoreada por el sistema de notificación de alarmas.

Los sistemas de aire acondicionados de los ambientes de nivel 4 deberán ser internos, con cambio de aire realizado apenas por la abertura de la puerta.

La capacidad de redundancia de toda la estructura de energía y aire acondicionado deberá ser garantizada, por medio de:

a) generadores de un tamaño compatible;
b) generadores de reserva;

c) sistemas de UPS redundantes; y

d) sistemas redundantes de aire acondicionado.

### 5.1.4 EXPOSICIÓN AL AGUA

La estructura interna al ambiente de nivel 4, deberá proveer protección física contra exposición a agua, filtraciones e inundaciones provenientes de cualquier fuente externa.

### 5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

El sistema de prevención contra incendios, internos a los ambientes deberán posibilitar alarmas preventivas antes que el humo sea visible, activados solamente con la presencia de partículas que caracterizan el sobrecalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

En las instalaciones del PSC no está permitido fumar o portar objetos que produzcan fuego o chispa.

El nivel 4 deberá poseer un sistema para detección precoz de humo y un sistema de extinción de incendio por gas.

En caso de incendio de las instalaciones del PSC, o el aumento de la temperatura interna del ambiente del nivel 4, no deberá exceder 50 grados Celsius, y el ambiente deberá soportar esta condición, como mínimo, 1 (una) hora.

### 5.1.6 ALMACENAMIENTO DE MEDIOS

El PSC deberá asegurar el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y deberá impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

La información relacionada a la infraestructura del PSC debe almacenarse de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida.

### 5.1.7 ELIMINACIÓN DE RESIDUOS

Todos los documentos en papel que contengan información clasificada como sensible deberán ser triturados antes de ir como residuo.

Todos los dispositivos electrónicos que ya no son utilizables y que se han utilizado previamente para el almacenamiento de información sensible, deberán ser destruidos físicamente.

### 5.1.8 RESPALDO FUERA DE SITIO

Las instalaciones de respaldo deberán cumplir con los requisitos mínimos establecidos por este documento. Su localización deberá ser tal que, en caso de siniestro que torne inoperante la instalación principal del PSC, las instalaciones de respaldo no se vean afectadas y tomen totalmente las operaciones del PSC en condiciones idénticas en, un máximo, de 48 (cuarenta y ocho) horas.

## 5.2 CONTROLES PROCEDIMENTALES

En los siguientes ítems de la CPS deben ser descriptos los requisitos para la caracterización y el reconocimiento de los Roles de Confianza en el PSC responsable y las RAs vinculadas a ella, junto con las responsabilidades definidas para cada perfil. Para cada tarea asociada a los perfiles definidos, también se debe establecer el número de personas necesarias para su ejecución.

### 5.2.1 ROLES DE CONFIANZA

El PSC responsable de la CPS deberá garantizar la segregación de tareas para las funciones críticas, con el fin de evitar que un empleado o funcionario que asume un rol de confianza utilice incorrectamente su sistema de certificación sin ser detectado. Las acciones de cada uno de los empleados o funcionarios se limitarán de acuerdo a su perfil.

Los Roles de un PSC, deben contemplar, al menos las siguientes responsabilidades que a continuación serán descriptos:

a) responsables de seguridad: deberán llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido

aprobadas por el PSC, controlar la formalización de los convenios entre el personal y el PSC, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, deberá cumplir y hacer cumplir las políticas de seguridad del PSC y deberá encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Será el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls. Deberá comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a éstos, asimismo deberá resolver o hacer que resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. y es el encargado de la gestión y control de seguridad física, y de los movimientos de material fuera de las instalaciones del PSC;

b) responsables de sistemas: los responsables de este rol no deberán estar implicados en tareas de auditoría interna. Serán encargados de la instalación y configuración de sistemas operativos, del mantenimiento y actualización de los programas instalados; con capacidad para configurar, mantener los sistemas, pero sin acceso a los datos. Asimismo, deberán establecer y documentar los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Serán responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación del PSC y asumirán la gestión de los servicios de ruteamiento y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Serán encargados de la instalación de hardware criptográfico del PSC y de la eliminación del hardware criptográfico del PSC de producción. Serán responsables del mantenimiento o reparación de equipos criptográficos PSC (incluida la instalación de nuevo hardware, firmware o software), y la eliminación de desmontaje y permanente por el uso;

c) responsables de la operación diaria del PSC: será encargada de realizar las tareas de ejecución y revisión de las copias de seguridad del sistema. Asimismo, debe velar, para que se lleven a cabo las copias de seguridad local y del traslado de las mismas de acuerdo con lo establecido en la política de seguridad. Serán responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Serán encargados de la

gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios;

d) responsables de auditoría: serán los responsables de las tareas de ejecución y revisión de auditoría de los sistemas que conforman la infraestructura tecnológica del PSC. Esta auditoría deberá realizarse de acuerdo con las normas y criterios de auditoría establecidos la presente CPS. Además, deberá tener acceso a todos los registros del sistema mencionados;
e) responsables del ciclo de vida de claves criptográficas: son los responsables de la gestión del ciclo de vida de las claves criptográficas (ejemplo: oficial criptográfico, oficial de activación, etc.);
f) responsables de desarrollo de sistemas del PSC: serán los encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones; y
g) agentes de registros: son los responsables de la realización de las actividades inherentes a una RA, realizan la identificación de los solicitantes en la solicitud de emisión/revocación de un certificado y autoriza en el sistema la emisión o revocación del mismo.

Todos los operadores del sistema de certificación del PSC deberán recibir entrenamiento específico antes de obtener cualquier tipo de acceso. El tipo o nivel de acceso serán determinados, en un documento formal, con base en las necesidades de cada perfil.

Cuando un empleado o funcionario se desvincula del PSC, sus permisos de acceso deberán ser revocados inmediatamente. Cuando hay un cambio en la posición o función que el empleado o funcionario ocupa dentro del PSC, deberán ser revisadas sus permisos de acceso. Deberá existir una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado o funcionario deberá devolver al PSC en el momento de su desvinculación.

### 5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

La CPS debe establecer el requisito de control multi-usuarios para la generación y la utilización de la clave privada del PSC responsable, de la forma definida en el ítem 6.2.2.

Todas las tareas ejecutadas en el ambiente donde está localizado el equipamiento de certificación del PSC deberá requerir, como mínimo, de 2 (dos) de sus empleados o funcionarios

con rol de confianza. Las demás tareas del PSC podrán ser ejecutadas por un único empleado o funcionario.

### 5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

La CPS debe garantizar que todo empleado o funcionario que asume un rol de confianza en el PSC responsable será identificado y su perfil será verificado antes de que:

a) sean incluido en una lista de acceso a las instalaciones del PSC;
b) sean incluido en una lista para acceso físico al sistema de certificación del PSC;
c) reciban un certificado electrónico para ejecutar sus actividades operacionales en el PSC; y
d) reciban una cuenta de usuario del sistema de certificación del PSC.

Los certificados, cuentas y contraseñas utilizados para la identificación y autenticación de los empleados o funcionarios deberán:

a) ser directamente asignados a un único empleado o funcionario;
b) no ser compartidos; y
c) restringirse a las acciones asociadas con el perfil para el que fueron creados.

### 5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

En este ítem la CPS debe describir aquellos roles que requieren separación de funciones. Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

a) los responsables del ciclo de vida de claves criptográficas no podrán cumplir funciones de los responsables de auditoría;
b) los responsables de sistemas no podrán cumplir funciones de los responsables de seguridad ni de los responsables de auditoría;
c) los responsables de seguridad no podrán cumplir funciones de los responsables de sistemas, de los responsables del ciclo de vida de claves criptográficas, de los agentes de registros ni de los responsables de auditoría; y
d) los responsables de auditoría no podrán cumplir otra función o rol.

Además, otras tareas que deben ser segregadas son:

a) la puesta en operación del PSC en producción;
b) la emisión o destrucción de los certificados del PSC; y
c) la validación de información en los sistemas de certificación del PSC y de solicitudes de emisión/revocación o información del suscriptor.

## 5.3 CONTROLES DE PERSONAL

En los siguientes ítems de la CPS deben ser descriptos los requisitos y procedimientos, implementados por el PSC responsable, por las RAs y PSSs vinculadas a todo su personal, refiriéndose a aspectos como: verificación de antecedentes e idoneidad, capacitación, rotación de puestos, sanciones por acciones no autorizadas, controles para contratación y documentación a ser proporcionada.

La CPS debe garantizar de que todos los empleados o funcionarios del PSC responsable, de las RAs y de los PSSs vinculados, a cargo de las tareas operativas, se hayan registrado en un contrato o término de responsabilidad:

a) los términos y condiciones del perfil que ocuparán;
b) el compromiso de observar las reglas, políticas y normas aplicables a la PKI-Paraguay; y
c) el compromiso de no divulgar información confidencial a la que tenga acceso.

### 5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Todo el personal del PSC responsable y de las RA vinculadas e involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser seleccionado y admitido, conforme a lo establecido en el ítem 7 “seguridad ligada a los recursos humanos” de la norma ISO 27002/2013 y además deberán:

a) haber demostrado capacidad para ejecutar sus deberes;
b) haber suscripto un acuerdo de confidencialidad y disponibilidad;
c) no poseer otros antecedentes que puedan interferir o causar conflicto con los del PSC;
d) no tener antecedentes de negligencia o incumplimiento de labores; y
e) no tener antecedentes judiciales ni policiales.

El PSC responsable podrá definir requisitos adicionales para la admisión.

### 5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PSC responsable y de las RA vinculadas involucradas en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser sometido a:

a) confirmación de empleos anteriores;
b) verificación de referencias profesionales;
c) título académico obtenido; y
d) verificación de antecedentes judiciales y policiales.

El PSC responsable puede definir requisitos adicionales para la verificación de antecedentes.

### 5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PSC responsable y de las RA vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá recibir entrenamiento documentado suficiente para el dominio de los siguientes temas:

a) principios y mecanismos de seguridad del PSC y de las RA vinculadas;
b) sistema de certificación en uso del PSC;
c) procedimientos de recuperación de desastres y continuidad del negocio;
d) reconocimiento de firmas y validación de documentos presentados en los ítems 3.2.2., 3.2.3. y 3.2.4.;
e) normativa vigente que rige la materia; y
f) otros asuntos relacionados con las actividades bajo su responsabilidad.

### 5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PSC responsable y de las RAs vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución,

revocación y gerenciamiento de certificados deberá ser mantenido y actualizado sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PSC o de las RAs.

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

En este ítem, la CPS podrá definir una política a ser adoptada por el PSC responsable y por las RA vinculadas, para la rotación del personal en los diversos cargos y perfiles por ellas establecidas. Esa política no deberá contrariar los propósitos establecidos en el ítem 5.2.1.

El PSC responsable y las RA vinculadas deberán efectuar una rotación de sus roles de confianza como mínimo una vez cada 5 años.

### 5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

La CPS deberá prever así como en su política de RRHH que, en la eventualidad de una acción no autorizada, real o sospechada, realizada por una persona encargada del proceso operacional del PSC responsable o de una RA vinculada, el PSC deberá de inmediato, suspender el acceso de esa persona a su sistema de certificación, iniciar un procedimiento administrativo para determinar los hechos y, si es necesario, tomar las medidas legales pertinentes.

El proceso administrativo referido en el párrafo anterior deberá contener, como mínimo, los siguientes puntos:

a) relato de lo ocurrido con el modo de operación;
b) identificación de los involucrados;
c) eventuales perjuicios causados;
d) las sanciones aplicadas, si fuere el caso; y
e) conclusiones.

Concluido el proceso administrativo, el PSC responsable deberá comunicar sus conclusiones a la CA Raíz-Py.

Las sanciones que podrían aplicarse como resultado de un procedimiento administrativo son:

a) advertencia;
b) suspensión por un plazo determinado; o

c) cese de sus funciones

### 5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Todo el personal del PSC responsable y de las RA vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, deberá ser contratado conforme a lo establecido en los ítems 7 “seguridad ligada a los recursos humanos” y 15 “relaciones con suministradores” norma ISO 27002/2013 y bajo las siguientes condiciones mínimas:

a) que exista un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas;
b) que el PSC responsable o RA vinculada no posea personal disponible para llenar los roles de confianza;
c) que el personal a contratar cumpla con los mismos requisitos del ítem 5.3.1; y
d) que una vez finalizado el servicio contratado se revoquen los derechos de acceso.

### 5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

La CPS debe asegurar que el PSC responsable pone a disposición de todo el personal del PSC y para todo el personal de las RA vinculados al menos:

a) su CPS;
b) las CP que implementa;
c) la política de seguridad que implementa el PSC;
d) documentación operacional relativa a sus actividades; y
e) contratos, normas y políticas relevantes para sus actividades.

Toda documentación entregada o disponibilizada al personal deberá estar clasificada y deberá ser mantenida actualizada.

## 5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems de la presente CPS deben describirse los aspectos de los sistemas de auditoría y registro de eventos implementados por el PSC con el fin de mantener un entorno o ambiente seguro.

### 5.4.1. TIPOS DE EVENTOS REGISTRADOS

El PSC responsable de la CPS, deberá registrar en archivos de auditoría, todos los eventos relacionados a la seguridad de su sistema de certificación. Entre otros, los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoría:

a) iniciación y terminación del sistema de certificación;
b) los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del sistema de los operadores del PSC;
c) los cambios en la configuración del PSC o en sus claves;
d) los cambios en las políticas de creación de certificados;
e) los intentos de acceso (*login*) y de salida del sistema (*logoff*);
f) los intentos no autorizados de acceso a los archivos del sistema;
g) la generación de claves propias del PSC o de claves de sus usuarios finales;
h) la emisión y revocación de certificados;
i) la generación de la CRL;
j) los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;
k) las operaciones fallidas de escritura o lectura en el repositorio de los certificados y de la CRL, en su caso; y
l) las operaciones de escritura en ese repositorio, en su caso.

El PSC responsable de la CPS deberá también registrar, electrónicamente o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

a) registros de accesos físicos;
b) el mantenimiento y los cambios en la configuración de sus sistemas;
c) los cambios de personal y los cambios de su rol de confianza;
d) los informes de discrepancia y de compromiso; y
e) el registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados o de la información personal de los usuarios.

En este ítem, la CPS debe especificar todas las informaciones que deberán ser registradas por el PSC responsable.

La CPS debe prever que todos los registros de auditoría, electrónicos o manuales, deberán contener la fecha y hora del evento registrado y la identidad del agente que lo causó.

Para facilitar los procesos de auditoría, toda documentación relacionada a los servicios del PSC deberá ser almacenada, electrónicamente o manualmente, en un local único, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

El PSC responsable de la CPS, deberá registrar electrónicamente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los certificados. Los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoría:

a) los AGR que realizan las operaciones;
b) fecha y hora de las operaciones;
c) la asociación entre los agentes que realizan la validación, aprobación y el certificado generado; y
d) la firma digital del ejecutante.

El PSC a la que está vinculada la RA, debe establecer, en un documento que esté disponible en las auditorías de cumplimiento, el local de archivo de las copias de los documentos utilizados para la identificación del suscriptor, presentados en el momento de la solicitud y revocación de certificados. El formulario de solicitud y el acuerdo de suscriptores.

### 5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (*LOGS*)

La CPS debe establecer el periodo, no superior a 1 (un) mes, con que los registros de auditoría del PSC responsable serán analizados por el personal operacional. Todos los eventos significativos deberán ser explicados en un informe de auditoría de registros. Tal análisis deberá involucrar una inspección breve de todos los registros, con la verificación de que no fueron alterados, seguida de una investigación más detallada de cualquier alerta o irregularidades en esos registros. Todas las medidas adoptadas como resultado de este análisis deberán ser documentadas.

### 5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (*LOGS*) DE AUDITORÍA

En este ítem, la CPS debe establecer que el PSC responsable, mantendrá localmente sus registros de auditoría por los menos 2 (dos) meses y, consecuentemente, deberá almacenarlos de la manera descrita en el ítem 5.5.2.

Además de las revisiones oficiales, los registros de auditoría deben ser revisados en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas del PSC.

### 5.4.4 PROTECCIÓN DEL REGISTRO (*LOGS*) DE AUDITORÍA

En este ítem, la CPS debe describir los mecanismos obligatorios incluidos en el sistema de registro de eventos del PSC responsable para proteger sus registros de auditoría contra lectura no autorizada, modificación y eliminación.

También deben ser descriptos, los mecanismos obligatorios de protección de información manual de auditoria contra la lectura no autorizada, modificación y eliminación.

Los mecanismos de protección descriptos en este ítem deben obedecer a lo dispuesto en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

### 5.4.5. PROCEDIMIENTOS DE RESPALDO (*BACKUP*) DE REGISTRO (*LOGS*) DE AUDITORÍA

En este ítem de la CPS deben ser descriptos los procedimientos adoptados por el PSC responsable para generar copias de seguridad de sus registros de auditorías y su frecuencia, que no debe ser superior a 1 (un) mes.

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

En este ítem las CPS deben ser descritas y localizadas los recursos utilizados por el PSC responsable para la recolección de datos de auditoría.

### 5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

La CPS debe tener en cuenta que cuando un evento fuera registrado por el conjunto de sistemas de auditoría del PSC responsable, no se requerirá notificar a ninguna persona, organización, dispositivo o aplicación que causó el evento.

### 5.4.8. EVALUACIÓN DE VULNERABILIDADES

La CPS debe asegurar que los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoría del PSC responsable, serán analizados detalladamente y, dependiendo de su gravedad, registrados por separado. Acciones correctivas que surjan deberán ser implementadas por el PSC y registradas con fines de auditoría.

## 5.5. ARCHIVOS DE REGISTROS

En los ítems siguientes de la CPS debe ser descrita la política general de archivo de registros, para uso futuro, implementada por el PSC responsable y por las RA a ella vinculada.

### 5.5.1. TIPOS DE REGISTROS ARCHIVADOS

En este ítem de la CPS deben ser especificados los tipos de registros archivados, que deberá comprender, entre otros:

a) solicitudes de certificados;
b) solicitudes de revocación de certificados;
c) notificaciones de compromiso de claves privadas;
d) emisiones y revocaciones de certificados;
e) emisiones de CRL;
f) cambio de claves criptográficas del PSC responsable;
g) Información de auditoría prevista en el ítem 5.4.1.

### 5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS

En este ítem, la CPS debe establecer los periodos de retención para cada registro archivado, teniendo en cuenta que:

a) las CRLs y los certificados emitidos de firma digital deberán ser conservados permanentemente para fines de consulta histórica;
b) los dossiers de los titulares de certificado como mínimo, por 10 (diez) años, a contar desde la fecha de expiración o revocación del certificado; y
c) Las demás informaciones, inclusive los archivos de auditoría deberán ser almacenadas, como mínimo, 10 (diez) años.

### 5.5.3 PROTECCIÓN DE ARCHIVOS

La CPS debe establecer que todos los registros archivados deberán ser clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

### 5.5.4 PROCEDIMIENTOS DE RESPALDO (*BACKUP*) DE ARCHIVO

La CPS debe establecer que una segunda copia de todo el material archivado deberá ser almacenada en un local externo al PSC responsable, recibiendo el mínimo tipo de protección utilizada para el archivo principal.

Las copias de seguridad deberán seguir los periodos de retención definidos para los registros de las cuales son copias.

El PSC responsable de la CPS deberá verificar la integridad de esas copias de seguridad, como mínimo, cada 6 (seis) meses.

### 5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Este ítem no aplica.

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

En este ítem de la CPS, deben ser descriptos y localizados los recursos utilizados por el PSC responsable para la recolección de datos de auditoría.

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

En esta sección de la CPS, deben ser detalladamente descriptos los procedimientos definidos por el PSC responsable y por las RA vinculada para la obtención y verificación de sus informaciones de archivo.

## 5.6 CAMBIO DE CLAVE

En este ítem, la CPS debe describir los procedimientos para el suministro, por el PSC responsable, de un nuevo certificado, antes de la expiración del certificado a pedido del titular del certificado.

El PSC debe cambiar su clave de acuerdo con el *tiempo de uso* y *tiempo operacional* de los certificados emitidos dentro de la PKI-Paraguay, este cambio técnicamente implica la emisión de un nuevo certificado. *El tiempo operacional* de un certificado coincide con el descripto en los campos de ‘’Válido desde’’ y ‘’Válido hasta’’ del mismo. El *tiempo de uso* refiere al establecido para los certificados emitidos en el marco de la PKI-Paraguay para determinados usos, como se aprecia a continuación:

Tabla Nº 6 – Certificados emitidos en el marco de la PKI-Paraguay

| Tipo de Certificado | Tiempo de uso en años | Tiempo operacional en años | Descripción |
|---|---|---|---|
| Certificado de Suscriptores (F2, F3, C2 y C3) | 2 | 2 | El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez. |
| Certificado de Suscriptores | 1 | 1 | El certificado emitido al usuario final es otorgado por un tiempo máximo de un año, al finalizar ese período pierde su validez. |

| | | | |
|---|---|---|---|
| (F1 y C1) | | | |
| Certificado de PSC | 8 | 10 | El Certificado emitido al PSC tendrá un tiempo operacional de 10 años, que resulta de la suma del tiempo de uso de su certificado (8 años) más el tiempo de validez máximo del certificado de su suscriptor (2 años).<br><br>Solamente durante el tiempo de uso de su certificado, el PSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional sólo podrá firmar el CRL de usuarios o suscriptores. |
| Certificado CA Raíz-Py | 10 | 20 | El Certificado emitido a la CA Raíz-Py tendrá un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado (10 años) más el tiempo de validez máximo del certificado de su suscriptor (10 años).<br><br>Solamente durante el tiempo de uso de su certificado, la CA Raíz-Py podrá emitir certificados a un PSC. En los años restantes del tiempo operacional sólo podrá firmar el CRL de PSC. |

Del cuadro anterior, se deduce que, en determinado momento, puede haber dos certificados del mismo nivel y tipo activos, donde el tiempo de vigencia simultánea de los certificados debe ser de al menos el tiempo operacional del certificador.

Por lo tanto, el certificado anterior podrá ser utilizado únicamente para firmar la CRL correspondiente y validar la cadena de confianza de la PKI-Paraguay; el nuevo certificado emitido, será utilizado para emitir nuevos certificados y firmar la nueva lista de CRL.

Los responsables del PSC tendrán la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

## 5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

En los siguientes ítems de la CPS deben ser descriptos los requisitos relacionados con los procedimientos de notificación y recuperación de desastres, previstos en la PCN del PSC responsable, establecido de acuerdo con el ítem 17 “aspectos de seguridad de la información en la gestión de la continuidad del negocio” de la norma ISO 27002/2013, para garantizar la continuidad de sus servicios críticos.

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

El PSC debe contar con un PCN, con acceso restringido, probado al menos una vez al año, para garantizar la continuidad de sus servicios críticos. También debe contar con un Plan de Respuesta a Incidentes y un Plan de Recuperación ante Desastres.

En este ítem la CPS deberá describir los procedimientos previstos en el PCN de las RAs vinculadas para la recuperación total o parcial de las actividades de las RA, conteniendo al menos la siguiente información:

a) identificación de eventos que pueden causar interrupciones en los procesos del negocio, por ejemplo, fallas de equipos, inundaciones e incendios, si fuera el caso;
b) identificación y concordancia de todas las responsabilidades y procedimientos de emergencia;
c) implementación de procedimientos de emergencia que permitan la recuperación y restauración dentro de los plazos necesarios;
d) documentación de procesos y procedimientos conforme a lo establecido;
e) capacitación adecuada del personal en procedimientos y procesos de emergencia definidos, incluida la gestión de crisis; y
f) prueba y actualización de planes.

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

En este apartado de la CPS, deben ser descriptos los procedimientos de recuperación utilizados por el PSC responsable cuando los recursos computacionales, software y/o corrupción de datos estuvieren comprometidos o en sospecha de corrupción.

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

#### *5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO*

En este ítem de la CPS, deben ser descriptos los procedimientos de recuperación utilizados en caso de revocación del certificado del PSC responsable.

#### *5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA*

En este ítem de la CPS, deben ser descriptos los procedimientos de recuperación utilizados en caso de compromiso de la clave privada del PSC responsable.

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

En este ítem de la CPS, deben ser descriptos los procedimientos de recuperación utilizados por el PSC después de la ocurrencia de un desastre natural o de otra naturaleza, antes del restablecimiento de un ambiente seguro.

## 5.8 EXTINCIÓN DE UN PSC O ENTIDADES VINCULADAS

En este ítem la CPS, debe describir los requisitos y los procedimientos que deberán ser adoptados en el caso de la extinción de servicios del PSC responsable o de una RA, VA o PSS a ella vinculada.

Deben ser detallados, los procedimientos para notificación de usuarios y para transferencia de guarda de sus datos de registros y de archivo.

En caso que un PSC responsable, deje de operar deberá cumplir, como mínimo, con lo siguiente:

a) solicitar a AA, con al menos un mes de anticipación la cancelación de sus suscripción en el registro público de PSCs, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda;
b) notificar a sus suscriptores con al menos un mes de anticipación antes de la suspensión efectiva o cese de sus operaciones;
c) publicar en su sitio principal de Internet la fecha de suspensión de los servicios con al menos un mes de anticipación;
d) publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese de las operaciones;
e) preservar toda la información en concordancia con esta CPS y la normativa aplicable; y
f) proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

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

El titular del certificado podrá seguir utilizando el certificado emitido hasta que se extinga el plazo de vigencia o hasta que fuera revocado. En caso de que el certificado llegue a su fecha de expiración no se podrá confiar en dicho certificado.

El MIC custodiará toda la información referida al cese de operación del PSC, además publicará el cese de actividades o finalización del servicio del PSC responsable en su sitio principal de Internet

# 6. CONTROLES TÉCNICOS DE SEGURIDAD

En los ítems siguientes, la CPS debe definir las medidas de seguridad implementadas por el PSC responsable para proteger sus claves criptográficas y sus datos de activación, así como las claves criptográficas de los titulares de certificado. Deben también ser definidos otros controles técnicos de seguridad utilizados por el PSC y por las RAs a ella vinculadas para la ejecución de sus funciones operacionales.

## 6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

### 6.1.1. GENERACIÓN DEL PAR DE CLAVES

En este ítem, la CPS debe describir los requisitos y procedimientos referentes a los procesos de generación de las claves criptográficas del PSC responsable. El par de claves criptográficas del PSC responsable para la CPS deberá ser generado por el propio PSC, posterior a la habilitación otorgada por el MIC vía resolución ministerial.

La CPS debe describir también los requisitos y procedimientos referentes al proceso de generación del par de claves criptográficas de las personas físicas o jurídicas solicitantes de certificado. El par de claves deberá ser generado solamente por el titular del certificado correspondiente. Los procedimientos específicos deben ser descriptos en cada CP implementada.

La CPS debe indicar que el proceso de generación del par de claves del PSC responsable se realiza mediante hardware.

Cada CP implementada por el PSC responsable debe definir el proceso utilizado para la generación de claves criptográficas de los titulares de los certificados, en base a los requerimientos establecidos en el documento DOC-PKI-04 [1].

### 6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ítem no aplicable. La CPS debe indicar que la generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

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

En este ítem, la CPS debe describir los procedimientos utilizados por el PSC responsable para la entrega de su clave pública a la CA Raíz-Py encargada de la emisión de su certificado. Para la generación del CSR por el PSC, deberá adoptarse el formato definido en el documento**,** DOC-PKI-06 [3].

La CPS debe también describir los procedimientos utilizados para la entrega de la clave pública de un solicitante de certificado al PSC responsable. Los procedimientos específicos aplicables deben ser detallados en cada CP implementada.

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

En este ítem, la CPS debe definir las formas para la disponibilización del certificado del PSC responsable, y de todos los certificados de la cadena de certificación, para los usuarios y las partes que confían de la PKI-Paraguay, la cual podrá comprender, entre otras:

a) en el momento de disponibilización de un certificado para su titular, usando el formato definido en el documento, DOC-PKI-06 [3];
b) un directorio;
c) una página WEB del PSC; y
d) otros medios seguros aprobados por la AA.

### 6.1.5. TAMAÑO DE LA CLAVE

En este ítem, la CPS definirá el tamaño de las claves criptográficas del PSC, en base a los requerimientos aplicables establecidos en el documento DOC-PKI-04 [1].

Además, la CPS debe indicar que cada CP implementada por el PSC responsable definirá el tamaño de las claves criptográficas asociadas a los certificados emitidos, en base a los requerimientos aplicables establecidos en el documento DOC-PKI-06 [3].

### 6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

Los parámetros de verificación de calidad, deberán ser verificados de acuerdo con las normas establecidas por el patrón definido en el documento DOC-PKI-06 [3].

### 6.1.7. PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X.509 V3)

En este ítem, la CPS debe especificar los propósitos para los cuales podrán ser utilizadas las claves criptográficas de los titulares de los certificados emitidos por el PSC responsable, así como las posibles restricciones aplicables, de conformidad con las aplicaciones definidas para los certificados correspondientes. Cada CP implementada debe especificar los propósitos específicos aplicables.

La clave privada del PSC responsable deberá ser utilizada solamente para la firma de los certificados por ella emitidos y de sus CRL.

## 6.2 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA

En los ítems siguientes, la CPS debe definir los requisitos para la protección de las claves privadas del PSC Responsable. Las claves privadas deberán ser cifradas en el envío del módulo que lo generó al medio utilizado para su almacenamiento. Cuando aplique, la CPS debe también definir los requisitos para proteger las claves privadas de los titulares de certificados emitidos por el PSC y almacenados en un dispositivo criptográfico custodiado por un PSA vinculada a ella. Cada CP implementada debe especificar los requisitos específicos aplicables.

### 6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

La CPS debe prever que el módulo criptográfico de generación de claves asimétricas del PSC responsable adoptará los patrones definidos en el documento DOC-PKI-06 [3].

La CPS debe también, cuando sea el caso, especificar los patrones como, por ejemplo, aquellas definidas en el documento DOC-PKI-06 [3] requeridos para los módulos de generación de claves criptográficas de los titulares de certificado. Cada CP implementada debe especificar los requisitos adicionales aplicables.

### 6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

En este ítem, cuando sea el caso, debe ser definida la forma de control múltiple, de tipo "N" personas de un grupo "M", requerido para la utilización de las claves privadas.

La CPS debe establecer la exigencia de control multi-persona para la utilización de la clave privada del PSC responsable. Como mínimo serán requeridos 2 (dos) de "M" titulares de partición de clave, formalmente designada por el PSC.

### 6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

En este ítem, la CPS debe identificar quién es el agente de custodia (escrow), de qué manera está la clave en custodia (por ejemplo, incluye el texto en claro, cifrado, por división de clave) y cuáles son los controles de seguridad del sistema de custodia.

### 6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

La CPS debe observar que, como directriz general, cualquier persona física o jurídica, titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

El PSC responsable de la CPS deberá mantener una copia de seguridad de su propia clave privada.

El PSC no podrá mantener copia de seguridad de la clave privada del titular de certificado de firma digital por ella emitida. Por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado/funcionario o cliente, el PSC podrá mantener una copia de seguridad de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada CP debe definir los requisitos específicos aplicables.

En cualquier caso, la copia de seguridad deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento DOC-PKI-06 [3] y protegida con un nivel de seguridad no inferior a aquel definido para la clave original.

### 6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

En este ítem de la CPS, deben ser definidos, cuando sea el caso, los requisitos para el archivado de las claves privadas de uso permitido para cifrado. Las claves deberán ser

archivadas en un nivel de seguridad no inferior a aquella definida para la clave original. No deben ser archivadas las claves privadas de uso permitido para firma digital.

Defínase archivado como el almacenamiento de la clave privada para su uso futuro, después del periodo de validez del certificado correspondiente.

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

En este ítem de la CPS, deben ser descriptos los requisitos de transferencia de la clave privada del PSC responsable de un módulo criptográfico a otro. La RFC 4210 o 6712 podrá ser utilizada para ese fin. Cada CP implementada debe definir, cuando sea aplicable, los requisitos de transferencia de la clave privada de los titulares del certificado de un módulo criptográfico a otro.

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

La CPS debe describir los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada del PSC responsable. Pueden indicarse estándares de referencia, como los definidos en el documento DOC-PKI-06 [3].

Cada CP implementada por el PSC responsable, debe definir el medio utilizado para el almacenamiento de la clave privada del usuario final, en base a los requerimientos establecidos en el documento DOC-PKI-04 [1].

### 6.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la CPS deben ser descriptos los requisitos y procedimientos necesarios para la activación de la clave privada del PSC responsable. Deben ser definidos los agentes autorizados para activar esa clave, el método de confirmación de identidad de esos agentes (por ejemplo, contraseñas, tokens, biometría, etc.) y las acciones necesarias para la activación. Cada CP implementada debe describir los requisitos y procedimientos necesarios para la activación de la clave privada de la persona física o jurídica titular de certificado.

### 6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la CPS, deben ser descriptos los requisitos y procedimientos necesarios para la desactivación de la clave privada del PSC responsable. Deben ser definidos los agentes autorizados para desactivar esa clave, el método de confirmación de identidad de esos agentes y las acciones necesarias para la desactivación. Cada CP implementada debe describir los requisitos y procedimientos necesarios para la desactivación de la clave privada de la de la persona física o jurídica titular de certificado.

### 6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

En este ítem de la CPS, deben ser descriptos los requisitos y procedimientos necesarios para la destrucción de la clave privada del PSC responsable y de sus copias de seguridad. Deben ser definidos los agentes autorizados, el método de confirmación de identidad de esos agentes y las acciones necesarias, tales como la destrucción física, la sobre-escritura o la eliminación de los medios de almacenamiento. Cada CP implementada debe describir los requisitos y procedimientos necesarios para la destrucción de la clave privada de la persona física o jurídica titular de certificado.

## 6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

### 6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La CPS debe prever que las claves públicas del PSC responsable y de los titulares de los certificados de firma digital, así como las CRL emitidas y sistemas de OCSP, serán almacenadas y gestionadas por el PSC emisor, después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

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

La clave privada del PSC responsable de la CPS y de los titulares de certificados de firma digital, tendrán un periodo operacional y periodo de uso conforme a la tabla N° 6 – Certificados emitidos en el marco de la PKI-Paraguay del ítem 5.6 de este documento. Las correspondientes claves públicas podrán ser utilizadas durante todo el periodo de tiempo

determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

Los periodos de uso de las claves correspondientes a los certificados de cifrado emitidos por el PSC responsable de la CPS deben ser definidos en las respectivas CPs.

Cada CP implementada por el PSC responsable debe definir el periodo máximo de validez del certificado que define, con base a los requisitos aplicables establecidos en esta CPS y en el documento DOC-PKI-04 [1].

## 6.4 DATOS DE ACTIVACIÓN

En los siguientes ítems de la CPS, deben ser descriptos los requerimientos generales de seguridad referentes a los datos de activación. Los datos de activación son distintos a las claves criptográficas y se definen como aquellas claves requeridas para la operación de algunos módulos criptográficos. Cada CP implementada debe describir los requisitos específicos aplicables.

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

El PSC debe mantener estrictos controles de sus datos de activación para operar los módulos criptográficos conforme a lo establecido en el ítem 6.2.2. Además, debe garantizar que los datos de activación de la clave privada del PSC responsable serán únicos.

Cada CP implementada debe garantizar que los datos de activación de la clave privada del titular del certificado serán únicos.

### 6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

La CPS debe garantizar que los datos de activación de la clave privada del PSC responsable serán protegidos contra el uso no autorizado, por medio de mecanismos de criptografía y de control de acceso físico.

Cada CP implementada debe garantizar que los datos de activación de la clave privada de la persona física o jurídica titular del certificado, si se utiliza, serán protegidos contra el uso no autorizado.

### 6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

En este ítem de la CPS, deben ser definidos, otros aspectos referentes a los datos de activación. Entre esos otros aspectos pueden ser considerados algunos de aquellos tratados, en relación de las claves, en los ítems 6.1 al 6.3.

## 6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

### 6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La CPS debe prever que la generación del par de claves del PSC responsable será realizada offline para impedir el acceso remoto no autorizado.

En este ítem, la CPS debe también describir los requisitos generales de seguridad computacional del equipamiento donde será generado el par de claves criptográficas de los titulares de certificados emitidos por el PSC responsable. Los requisitos específicos aplicables deben ser descriptos en cada CP implementada.

Cada computador del PSC responsable, relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, deberá implementar, entre otras, las siguientes características:

a) control de acceso a los servicios y perfiles del PSC;
b) clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PSC;
c) uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;
d) generación y almacenamiento de registros de auditoría del PSC;
e) mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y
f) mecanismos para copias de seguridad (*backup*).

Estas características deberán ser implementadas por el sistema operativo o por medio de combinación de este con el sistema de certificación y con mecanismos de seguridad física.

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento deberán haber borrado la información confidencial que contenga y controlar su número de serie y las fechas de envío y recepción. Al regresar a las instalaciones del PSC, el equipo que fue sometido a mantenimiento debe ser inspeccionado. Cualquier equipo que ya no se utilice de forma permanente, deberán ser destruidas de él, de manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad del PSC. Todos estos eventos deberán ser registrados con fines de auditoría.

Cualquier equipo incorporado en el PSC será preparado y configurado según lo previsto en la política de seguridad implementada u otro documento aplicable con el fin de mostrar el nivel de seguridad requerido para su propósito.

### 6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

En este apartado de la CPS, debe ser informado, cuando esté disponible, la calificación atribuida a la seguridad computacional del PSC responsable, de acuerdo con criterios tales como: *Trusted System Evaluation Criteria* (TCSEC), *Canadian Trusted Products Evaluation Criteria*, *European Information Technology Security Evaluation Criteria* (ITSEC) o *Common Criteria*.

### 6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

En este ítem, la CPS debe describir los requisitos de seguridad computacional de las estaciones de trabajo y de los computadores portátiles utilizados por la RA para los procesos de validación y aprobación de certificados.

Deben ser incluidos, por lo menos, los requisitos especificados en el documento DOC-PKI-05 [2]**.**

## 6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

En los ítems siguientes de la CPS, deben ser descriptos, cuando sea aplicable, los controles implementados por el PSC responsable y por las RAs a ella vinculada en el desarrollo de sistemas y en la gestión de la seguridad.

### 6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

En esta sección de la CPS, deben ser abordados aspectos tales como: seguridad del ambiente y del personal de desarrollo, prácticas de ingeniería del software adoptadas, metodología de desarrollo de software, entre otros, aplicados al software del sistema de certificación del PSC responsable o cualquier otro software desarrollado o utilizado por el PSC responsable.

Los procesos de proyecto y desarrollo conducidos por el PSC, deberán proveer documentación suficiente para soportar evaluaciones de seguridad externas de los componentes del PSC.

### 6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

En este ítem de la CPS deben ser descriptos, las herramientas y los procedimientos empleados por el PSC responsable y por las RAs vinculadas, para garantizar que sus sistemas y redes operacionales, implementen los niveles de configuración de seguridad.

Una metodología formal de gerenciamiento de configuración deberá ser usada para la instalación y el continuo mantenimiento del sistema de certificación del PSC.

### 6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

En este ítem, la CPS debe informar, cuando esté disponible, el nivel de madurez asignado al ciclo de vida de cada sistema, basado en criterios tales como: *Trusted Software Development Methodology* (TSDM) o el *Capability Maturity Model* do *Software Engineering Institute* (CMM-SEI).

### 6.6.4. CONTROLES EN LA GENERACIÓN DE CRL

Antes de su publicación, todas las CRLs generadas por el PSC, deben ser comprobadas en cuanto a la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de CRL, la fecha / hora de emisión y otras informaciones relevantes.

## 6.7 CONTROLES DE SEGURIDAD DE RED

### 6.7.1. DIRECTRICES GENERALES

En este ítem de la CPS, deben ser descriptos los controles relativos a la seguridad de red del PSC responsable, incluidos firewalls y recursos similares.

En los servidores del sistema de certificación del PSC, sólo los servicios estrictamente necesarios para el funcionamiento de la aplicación deben estar habilitados.

Todos los servidores y elementos de la infraestructura y protección de redes, tales como ruteadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red en que se hospeda el sistema de certificación del PSC, deberán estar localizados y operar en un ambiente de nivel, como mínimo, 4 (cuatro).

Las últimas versiones de los sistemas operativos y servidores de aplicaciones, así como las eventuales correcciones (patches), disponibilizadas por los respectivos fabricantes deberán ser implementadas inmediatamente después del testeo en el ambiente de homologación.

El acceso lógico a los elementos de la infraestructura y protección de la red deberán restringirse por medio de un sistema de autenticación y autorización de acceso. Los ruteadores (routers) conectados a redes externas deberán implementar filtros de paquetes de datos, que sólo permitan conexiones a los servicios y servidores previamente definidos como objeto de acceso externo.

### 6.7.2. FIREWALL

Mecanismos de firewall se deberán implementar en equipos de uso específico, configurados exclusivamente para esa función. Un firewall deberá promover el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona desmilitarizada" (DMZ) - en relación a los equipos con acceso exclusivamente interno al PSC.

El software de firewall, entre otras características, deberá implementar registros de auditoría.

### 6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El sistema de detección de intrusos deberá tener la capacidad de ser configurado para reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar traps SNMP, ejecutar programas definidos por la administración de la red, enviar e-mail a los administradores, enviar mensajes de alerta al firewall o al terminal de gerenciamiento, promover la desconexión automática de conexiones sospechosas, o incluso la reconfiguración del firewall.

El IDS deberá ser capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de actualizar su base de reconocimiento.

El IDS deberá proveer un registro de los eventos en logs, recuperables en archivos de tipo texto, e implementar una gestión de la configuración.

### 6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Las tentativas de acceso no autorizado en ruteadores, Firewall o IDS, deberán ser registradas en archivos para posterior análisis, que podrá ser automatizada. La frecuencia de examen de los archivos de registro deberá ser, como mínimo, diario y todas las acciones tomadas como resultado de este examen deben ser documentadas.

## 6.8. FUENTES DE TIEMPO

Todos los sistemas deben estar sincronizados en fecha y hora utilizando una fuente confiable de tiempo ajustados a la fecha y hora oficial paraguaya.

# 7. PERFILES DE CERTIFICADOS, CRL Y OCSP

## 7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PSC responsable deben ajustarse al formato definido por la norma ITU X.509 o ISO/IEC 9594-8, según el perfil establecido en RFC 5280.

### 7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PSC responsable deberán implementar la versión 3 (tres) del estándar ITU X.509.

### 7.1.2. EXTENSIONES DEL CERTIFICADO

La PKI-Paraguay define como obligatorias las siguientes extensiones para los certificados del PSC:

a) **Identificador de la clave de la Autoridad Certificadora** "***Authority Key Identifier*", no crítica:** el campo key Identifier debe contener el hash SHA-1 de la clave pública de la CA Raíz que emite el certificado;

b) **Identificador de la clave del suscriptor** "***Subject Key Identifier*", no crítica:** debe contener el hash SHA-1 de la clave pública del PSC titular del certificado;

c) **Uso de Claves** "***Key Usage*", crítica:** solamente los bits *keyCertSign* y *CRLSign* deben estar activados;

d) **Políticas de Certificación"*Certificate Policies*", no crítica:**

d.1.1) el campo ***policyIdentifier*** debe contener el OID de la CP aplicable.

d.1.2) el campo **policyQualifiers** debe contener la dirección Web de la CP aplicable.

d.2.1) el campo ***policyIdentifier*** debe contener el OID de la CPS aplicable.

d.2.2) el campo **policyQualifiers** debe contener la dirección Web de la CPS aplicable.

e) **Restricciones Básicas** "***Basic Constraints*", crítica:** debe contener el campo SubjectType CA=True y el campo PathLenConstraint debe tener valor cero;

f) **Puntos de distribución de las CRL** "**CRL Distribution Points", no crítica:** debe contener la dirección Web donde se obtiene la CRL correspondiente al certificado; y

g) **Acceso a la Información de la Autoridad Certificadora "Authority Information Access", no crítica:** debe contener el método de *acceso id-ad-calssuer* al certificado de la CA Raíz, para recuperar la cadena de certificación.

### 7.1.3. IDENTIFICADORES DE OBJETO DE ALGORÍTMOS

Los certificados del PSC deberán ser firmados utilizando el algoritmo definido en el documento DOC-PKI-06 [3].

### 7.1.4. FORMAS DEL NOMBRE

El nombre del PSC titular del certificado, que consta el campo "*Subject*", deberá adoptar el "*Distinguished Name"* (DN) del estándar ITU X.500/ISO 9594 de la siguiente forma:

a) **OID=2.5.4.6** **C= PY**;
b) **OID=2.5.4.10** **O= [***denominación o razón social de la persona jurídica habilitada como PSC en mayúsculas y sin tildeS, según documento de identificación***]**;
c) **OID: 2.5.4.3** **CN= [***siglas* **CA-** *seguido de la denominación o razón social de la persona jurídica habilitada como PSC en mayúsculas y sin tildes, según documento de identificación***]**; y
d) **OID: 2.5.4.5** **Serial Number[** *conforme al formato descripto en el ítem 3.1.4.1 de este documento***]**.

### 7.1.5. RESTRICCIONES DEL NOMBRE

En este ítem de la CPS, deben ser descritas las restricciones aplicables para los nombres del PSC, titulares de certificados, de conformidad con las restricciones generales establecidas por la PKI-Paraguay en el documento DOC-PKI-04 [1].

### 7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

En este ítem se debe informar los OID asignado a la CP y el OID asignado a la CPS, aplicables. Todo certificado emitido bajo esta CPS debe contener, en la extensión "Políticas de Certificado" estas informaciones.

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

Este Ítem no aplica.

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

En este ítem se debe informar la dirección Web (URL) de la CP y la dirección Web (URL) de la CPS, aplicables. Todo certificado emitido bajo estos documentos deben contener, en el campo policyQualifiers de la extensión Políticas de certificado “Certificate Policies” estas informaciones.

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

Las extensiones críticas deben interpretarse de acuerdo con RFC 5280.

## 7.2. PERFIL DE LA CRL

Los Listas de Certificados Revocados CRL deberán ser firmados utilizando el algoritmo definido en el documento DOC-PKI-06 [3].

### 7.2.1 NÚMERO (S) DE VERSIÓN

Las CRL generadas por el PSC responsable deberán implementar la versión 2 del estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

### 7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

## 7.3 PERFIL DE OCSP

Las Respuestas OCSP deberán ser firmados utilizando el algoritmo definido en el documento DOC-PKI-06 [3].

### 7.3.1 NÚMERO (S) DE VERSIÓN

Los servicios de respuesta OCSP deben implementar la versión 1 del estándar ITU X.509, según el perfil establecido en RFC 6960.

### 7.3.2 EXTENSIONES DE OCSP

Si se implementa, debe cumplir con RFC 6960.

# 8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

El Art. 42 de la Ley Nro. 4017/2010 establece que los PSC, deben ser auditados periódicamente, de acuerdo con el sistema de auditoría que diseñe y apruebe el MIC.

Por Resolución Ministerial se establece el sistema de auditoría al cual será sometido el PSC.

Todo PSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la PKI-Paraguay.

El proceso de auditoría incluye entre otras: Revisión de seguridad y de prácticas, las cuales incluyen instalaciones, documentos de seguridad, declaración de prácticas de certificación, acuerdos entre las partes, política de privacidad y validación de los planes para asegurar el cumplimiento de estándares.

El MIC o terceros designados por él, serán responsables de ejecutar las auditorías, de acuerdo a lo estipulado en la normativa vigente.

Cada PSC, debe implementar un programa de auditorías internas conforme a lo estipulado en el sistema de auditoría que diseñe el MIC y lo establecido en el ítem 18 “cumplimiento” de la norma ISO 27002/2013 para la verificación de su sistema de gestión.

La disposición o resolución que ordena una Auditoría o evaluación no será recurrible.

## 8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

En este ítem, la CPS debe indicar que la auditoría externa al PSC responsable se deberá ejecutar al menos una vez al año y los costos deben ser asumidos por el PSC.

Además, la CPS debe indicar de conformidad al programa de auditoría interna de cada PSC, la frecuencia o circunstancias de su realización, que como mínimo, deberán ser ejecutadas al menos una vez al año.

## 8.2 IDENTIDAD/CALIDAD DEL EVALUADOR

En este ítem, la CPS debe describir las cualidades del equipo de Auditoría (Interna o externa), que de modo general debe estar conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de PKI y criptografía.

## 8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

En este ítem, la CPS debe indicar que, para el caso de las auditorías externas, los auditores deberán ser independientes e imparciales y que deberán ejecutar las evaluaciones acordes a los procedimientos establecidos.

En este ítem, la CPS también debe indicar que, para el caso de las auditorías internas, los auditores deberán ser independientes funcionalmente del área objeto de evaluación.

## 8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

En este ítem, la CPS debe también describir los aspectos cubiertos por la evaluación, que como mínimo, deberá contemplar:

a) controles de seguridad física y estándares técnicos de seguridad;
b) confidencialidad y calidad de los sistemas de control;
c) integridad y disponibilidad de los datos;
d) cumplimiento de los estándares tecnológicos;
e) seguridad del personal;
f) cumplimiento de la política y declaración de prácticas de certificación;
g) procesos de certificación de clave pública;
h) política de seguridad y privacidad;
i) controles administrativos del PSC;
j) administración de los servicios del PSC; y
k) revisión de contratos.

## 8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

En este ítem, la CPS debe describir los procedimientos que el PSC responsable, VA y RA vinculadas a ella, deben ejecutar para realizar acciones correctivas en base a las deficiencias detectadas tanto en las Auditorías externas como en las internas.

En caso de detectarse una irregularidad en la Auditoría externa realizada al PSC, podrán tomarse entre otras las siguientes acciones dependiendo de la gravedad de la misma:

a) indicar las irregularidades, pero permitir al PSC responsable o a las VA y RA vinculadas que continúen sus operaciones hasta la próxima auditoría programada;
b) permitir al PSC responsable o a las VA y RA vinculadas que continúen sus operaciones con un máximo de treinta días corridos, tiempo durante el cual deberá subsanar la irregularidad detectada;
c) recomendar suspender la operación del PSC responsable o a las VA y RA vinculadas.

En caso de que se resuelva la suspensión de actividades del PSC Responsable, este sólo podrá realizar servicios de soporte técnico y atención a los titulares de certificados ya existentes, en ningún caso podrá seguir brindando servicios de certificación.

### 8.6 COMUNICACIÓN DE RESULTADOS

En este ítem, la CPS debe indicar que el PSC responsable deberá publicar en su sitio principal de Internet los informes relevantes de las auditorías realizadas.

## 9. OTROS ASUNTOS LEGALES Y COMERCIALES

### 9.1 TARIFAS

En los siguientes ítems, deben ser especificados por el PSC responsable de la CPS, las políticas tarifarias y reembolso aplicables según la norma que rige la materia. En caso que sean aplicadas tarifas específicas para las CP implementadas, las mismas deben ser descriptas en las CP, en el ítem correspondiente.

#### 9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

#### 9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

Este ítem no aplica.

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

No hay tarifa de revocación ni de acceso a la información del estado del certificado.

#### 9.1.4 TARIFAS POR OTROS SERVICIOS

Este ítem no aplica.

#### 9.1.5 POLÍTICAS DE REEMBOLSO

En este ítem de la CPS se debe de informar sobre políticas de reembolso en el caso que las apliquen.

## 9.2 RESPONSABILIDAD FINANCIERA

En este ítem de la CPS se debe indicar sobre los recursos financieros suficientes para mantener las operaciones y cumplir con las obligaciones así como para afrontar riesgos de conformidad a la normativa vigente.

### 9.2.1 COBERTURA DE SEGURO

En este apartado, la CPS debe describir los aspectos relativos a la cobertura de seguro que posee el PSC responsable como un medio de garantía suficiente para cubrir las actividades inherentes a su gestión de conformidad con lo establecido en la normativa vigente.

### 9.2.2 OTROS ACTIVOS

Este ítem no aplica.

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

En este ítem de la CPS, en el caso que aplique, deben describirse los aspectos relativos a la cobertura de seguro o garantía disponible para los suscriptores.

En el caso que sean aplicadas cobertura de seguro o garantía para usuarios finales específicos para las CP implementadas, las mismas deben ser descriptas en las CP, en el ítem correspondiente.

## 9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

### 9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

En este ítem, deben ser identificados los tipos de informaciones consideradas confidenciales por el PSC responsable de la CPS y de sus RAs y VA vinculadas, de acuerdo con las normas, criterios, prácticas y procedimientos de la PKI-Paraguay.

La CPS debe establecer, como principio general, que ningún documento, información o registro entregado al PSC o a las RA vinculadas deberán ser divulgados.

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

En este ítem deben ser indicados los tipos de informaciones consideradas NO confidenciales por el PSC responsable de la CPS y por las RA y VA a ellas vinculadas, los cuales deberán comprender, entre otros:

a) los certificados y las CRL emitidas por la CA;
b) las CP implementadas por el PSC;
c) la CPS del PSC;y
d) la conclusión de los informes de auditoría.

Los Certificados, CRL/OCSP y la información corporativa o personal que necesariamente forme parte de ellos o de directorios públicos se consideran información no confidencial.

### 9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Los participantes que reciban o tengan acceso a información confidencial deberán contar con mecanismos que aseguren la protección y confidencialidad, evitando su uso o divulgación a terceros, bajo pena de responsabilidad, de acuerdo con la ley.

La clave privada de firma digital del PSC responsable de la CPS será generada y mantenida por el propio PSC, quien será responsable de su secreto. La divulgación o el uso indebido de la clave privada por parte del PSC será de su exclusiva responsabilidad.

La CPS deberá informar que los titulares de certificados emitidos a personas físicas o a los responsables del uso de certificados emitidos a personas jurídicas, máquina o aplicación, tendrán las tareas de generar y mantener la confidencialidad de sus respectivas claves privadas. Además, son responsables de la divulgación o uso indebido de estas mismas claves.

En el caso de certificados de cifrado emitidos por el PSC, la CPS debe definir las responsabilidades para mantener y garantizar la confidencialidad de las respectivas claves privadas. Si existen responsabilidades específicas para las CPs implementadas, las mismas deben ser descriptas en esas CPs, en el ítem correspondiente.

## 9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

### 9.4.1 PLAN DE PRIVACIDAD

En este ítem de la CPS, el PSC debe garantizar la protección de los datos personales de acuerdo con su política de privacidad. Dicha política debe de contemplar aspectos y procedimientos de seguridad organizativos con el fin de garantizar que los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño y procesamiento no autorizado.

### 9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

En este ítem de la CPS se debe indicar que cualquier información acerca de los suscriptores que no esté públicamente disponible a través del contenido del certificado emitido y servicios de CRL/OCSP debe ser tratada como información privada.

### 9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

En este ítem de la CPS se debe de indicar que el tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa al efecto. Únicamente se considera pública la información contenida en el certificado y CRLs/OCSP.

### 9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

En este ítem de la CPS, se debe indicar que el PSC y la RA vinculada son responsables de la divulgación indebida de información privada, por lo que deben de asegurar que no pueda ser comprometida o divulgada a terceros.

### 9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

La información privada obtenida por el PSC podrá ser utilizada o divulgada a terceros, previa notificación al titular y con su autorización expresa.

El titular del certificado o su representante en el caso de un certificado de persona jurídica tendrán amplio acceso a cualquiera de sus propios datos e identificaciones, y podrán autorizar la divulgación de sus registros a otras personas.

La autorización formal se podrá formalizar:

a) por medios electrónicos, conteniendo una firma válida garantizada por un certificado reconocido por la PKI-Paraguay; o
b) mediante solicitud por escrito firmada.

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

En este ítem de la CPS, debe indicarse que la información privada solamente podrá divulgarse en el marco de un procedimiento judicial o administrativo cuya solicitud emane de una orden judicial o autoridad administrativa competente.

### 9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Este ítem no aplica.

### 9.4.8 INFORMACIÓN A TERCEROS

Aplícase lo dispuesto en el ítem 9.4.5 de la CPS.

## 9.5 DERECHO DE PROPIEDAD INTELECTUAL

Según legislación vigente.

## 9.6 REPRESENTACIONES Y GARANTÍAS

### 9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC

En este ítem de la CPS el PSC debe indicar que el marco de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en las Políticas, Declaración de Prácticas de certificación y en la normativa vigente. De igual manera asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

El PSC declara y garantiza lo siguiente:

#### *9.6.1.1 AUTORIZACIÓN PARA CERTIFICADO*

En este ítem el PSC debe indicar que implementa procedimientos para verificar la autorización de emisión de un certificado en el marco de la PKI-Paraguay, contenido en los ítems 3 y 4 de esta CPS. El PSC, dentro del alcance de la autorización de emisión de un certificado, analiza, audita e inspecciona los procesos de la RA conforme a sus CPSs, CPs y normas complementarias.

#### *9.6.1.2 PRECISIÓN DE LA INFORMACIÓN*

El PSC implementa procedimientos para verificar la veracidad de la información en los certificados, contenidos en los ítems 3 y 4 de esta CPS. A su vez, la CA Raíz-Py, la veracidad de la información contenida en los certificados que emite, analiza, audita e inspecciona los procesos del PSC y RA conforme a sus CPS, CPs y normas complementarias.

#### *9.6.1.3 IDENTIFICACIÓN DEL SOLICITANTE*

El PSC implementa procedimientos para verificar la identificación de los solicitantes de certificados, contenidos en los ítems 3 y 4 de esta CPS. El PSC, en el ámbito de la identificación del solicitante contenida en los certificados que emite, analiza, audita e inspecciona los procesos de la RA conforme sus CPS, CPs y normas complementarias.

#### *9.6.1.4 CONSENTIMIENTO DE LOS TITULARES*

En este ítem el PSC debe indicar que implementa el formulario de Solicitud y Acuerdo de Suscriptores para la expresión del consentimiento del titular de conformidad a los formatos de Solicitud y Acuerdo de Suscriptores establecidos por la CA Raíz, contenidos en los puntos 3 y 4 de esta CPS.

#### *9.6.1.5 SERVICIO*

En este ítem de la CPS, el PSC debe indicar que mantiene acceso 24x7 a su repositorio con información sobre sus propios certificados, consulta de certificados emitidos y CRL/OCSP.

#### *9.6.1.6 REVOCACIÓN*

En este ítem de la CPS, el PSC debe indicar que revocará los certificados de la PKI-Paraguay por cualquier motivo especificado en este documento.

#### *9.6.1.7 EXISTENCIA LEGAL*

En este ítem, el PSC deberá indicar que la CPS se ajusta a las disposiciones de la Ley Nro. 4017/2010 sus modificaciones y reglamentaciones.

### 9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Aplícase conforme al ítem 4 de esta CPS.

### 9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

Toda la información necesaria para la identificación del titular del certificado debe proporcionarse de manera completa y precisa. Al aceptar un certificado emitido por el PSC, el titular es responsable de toda la información proporcionada por el, contenida en ese certificado.

El PSC debe informar a la CA Raíz-Py de cualquier compromiso de su clave privada y solicitar la revocación inmediata de su certificado.

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

La parte que confía; es aquel que confía en el contenido, validez y aplicabilidad del certificado digital.

Constituyen derechos de la parte que confía:

a) negarse a utilizar el certificado para fines distintos de los previstos en esta CPS; y
b) verificar, en cualquier momento, la vigencia del certificado.
c) El certificado del PSC se considera válido cuando:
d) ha sido emitido por la CA Raíz-Py;
e) no aparece como revocado por la CA Raíz-Py;
f) no ha expirado; y
g) puede ser verificado utilizando el certificado válido de la CA Raíz-Py.

El uso o aceptación de certificados sin observar las medidas descriptas es por cuenta y riesgo de la parte que confía, que usa o acepta la utilización del certificado respectivo.

### 9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

El repositorio del PSC deberá:

a) disponibilizar, inmediatamente después de su emisión, los certificados emitidos por el PSC y su CRL;
b) estar disponible para consulta durante 24 (veinticuatro) horas al día, siete (7) días a la semana; y
c) aplicar los recursos necesarios para la seguridad de los datos almacenados en él.

### 9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Este ítem no aplica.

## 9.7 EXENCIÓN DE GARANTÍA

Este ítem no aplica.

## 9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

En este ítem de la CPS, el PSC deberá indicar que en el marco de su actividad como Prestador de Servicios de Certificación la limitación de su responsabilidad será conforme a las disposiciones de la Ley Nro. 4017/2010, sus modificaciones y reglamentaciones.

## 9.9 INDEMNIZACIONES

En este ítem, la CPS debe indicar las condiciones de aplicación y limitaciones considerando las responsabilidades del PSC establecidas en la normativa vigente.

## 9.10 PLAZO Y FINALIZACIÓN

### 9.10.1 PLAZO

En este ítem, se debe establecer que la CPS entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AA.

### 9.10.2 FINALIZACIÓN

Esta CPS permanecerá en vigencia indefinidamente, siendo válida y efectiva hasta que sea revocada.

### 9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Finalizada la vigencia de la CPS, por reemplazo o revocación, esta se mantendrá válida para todos los efectos legales.

## 9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

En este ítem de la CPS, deben ser descriptos los mecanismos de notificación y comunicación que serán utilizados, los cuales preferentemente se realizarán a través de sistemas de información electrónicos con un documento firmado digitalmente.

## 9.12. ENMIENDAS

### 9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

En este ítem de la CPS se debe indicar el procedimiento para enmiendas y que propuestas de modificación de la CPS deben ser revisadas y aprobadas por la AA antes de ser implementadas. Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

### 9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

En este ítem, deben ser descriptos los procedimientos utilizados para publicar y notificar las enmiendas o modificaciones realizadas a la CPS. Toda enmienda o modificación de la CPS, deberá ser publicada en el repositorio del PSC.

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

En este ítem de la CPS se debe indicar que los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OID adicionales. Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

## 9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

En este ítem, deben ser definidos los procedimientos a ser adoptados para resolución de disputas que se derive de la presente CPS. Debe también establecerse que la CPS del PSC responsable no prevalecerá sobre las normas, criterios, prácticas y procedimientos establecidos por el MIC.

## 9.14 NORMATIVA APLICABLE

Esta CPS se rige por la legislación de la República del Paraguay, en particular la Ley Nro. 4017/2010, su modificación y reglamentaciones, y la legislación que la sustituya o modifique, así como las demás leyes y normas vigentes en el Paraguay.

## 9.15 ADECUACIÓN A LA LEY APLICABLE

En este ítem se debe indicar que la CPS se adecua a la legislación aplicable y que el PSC responsable se compromete a cumplir y observar las disposiciones previstas en ella.

## 9.16 DISPOSICIONES VARIAS

### 9.16.1 ACUERDO COMPLETO

En este ítem debe indicarse que los titulares y partes que confían en los certificados asumen en su totalidad el contenido de la presente CPS y CP.

Esta CPS representa las obligaciones y deberes aplicables al PSC y autoridades vinculadas.

En caso de conflicto entre esta CPS y otras resoluciones del MIC, prevalecerá siempre la última editada.

### 9.16.2 ASIGNACIÓN

Los derechos y obligaciones previstos en esta CPS, no pueden ser cedidos ni transferidos a terceros.

### 9.16.3 DIVISIBILIDAD

La invalidez, nulidad o ineficacia de cualquiera de las disposiciones de esta CPS no perjudicará las demás disposiciones, que seguirán siendo plenamente válidas y efectivas.

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

Este ítem no aplica

### 9.16.5 FUERZA MAYOR

En este ítem de la CPS se debe indicar la limitación de responsabilidad en caso de fuerza mayor que pueda aplicar al servicio de certificación.

## 9.17 OTRAS DISPOSICIONES

Éste ítem no aplica.

# 10. DOCUMENTOS DE REFERENCIA

## 10.1 REFERENCIAS

- Ley N° 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Ley N° 4610/2012 "Que modifica y amplía la Ley Nº 4017/10 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Decreto N° 7369/2011 "Por el cual se aprueba el reglamento general de la Ley Nº 4017/2010 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- RFC 4210: "Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP)".
- RFC 5280: "Internet X.509 Public Key Infrastructure.Certificate and Certificate Revocation List (CRL) Profile".
- RFC 6712: "Internet X.509 Public Key Infrastructure.HTTP Transfer for the Certificate Management Protocol (CMP)".
- RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".
- ISO/IEC27002:" -Information technology - Security techniques - Code of practice for information security management".
- ITU X.500/ISO 9594: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".
- ITU X.509/ISO/IEC9594-8:"-Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".
- WebTrust Principles and Criteria for Certification Authorities.
- WebTrustSM/TM Principles and Criteria for Registration Authorities.

## 10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla Nº 7– Documentos Referenciados

| REF. | NOMBRE DEL DOCUMENTO | CÓDIGO |
|---|---|---|
| [1] | Directivas obligatorias para la formulación y elaboración de la política de certificación de los prestadores de servicios de certificación de la PKI-Paraguay. | DOC-PKI-04 |
| [2] | Características mínimas de seguridad para las autoridades de registro de la PKI-Paraguay. | DOC-PKI-05 |
| [3] | Normas de algoritmos criptográficos de la PKI-Paraguay. | DOC-PKI-06 |