DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

DE LOS PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA DE LA ICPP

DOC-ICPP-03

Versión 1.0

Firmado digitalmente por PEDRO BENJAMIN MANCUELLO PEREZ

CONTROL DOCUMENTAL

Documento	
Título: DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LOS PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA DE LA ICPP	**Nombre Archivo:** DOC-ICPP-03 Vers 1.0
Código: DOC-ICPP-03	**Soporte Lógico:** https://www.acraiz.gov.py/
Fecha: 04/08/2022	**Versión:** 1.0

Registro de cambios		
Versión	**Fecha**	**Motivo de cambio**
1.0	04/08/2022	Versión inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)

Autoridad Certificadora (AC)	Prestadores Cualificados de Servicios de Confianza (PCSC)
Documento Público	https://www.acraiz.gov.py/

Control del documento	
Elaborado por: ***JENNY RUÍZ DÍAZ***	Firmado digitalmente por JENNY ELIZABETH RUIZ DIAZ LEZCANO Fecha: 2022.08.04 15:58:18 -04'00'
Verificado por: ***LUJAN OJEDA***	MARIA LUJAN OJEDA CHAMORRO Digitally signed by MARIA LUJAN OJEDA CHAMORRO Date: 2022.08.04 15:25:21 -04'00'
Aprobado por: ***LUCAS SOTOMAYOR***	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2022.08.04 17:09:13 -03'00'

Contenido

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que deben ser obligatoriamente cumplidos por los Prestadores Cualificados de Servicios de Confianza (PCSC) en su carácter de Autoridad Certificación Intermedia (ACI), miembros la Infraestructura de Clave Pública del Paraguay (ICPP) en la elaboración de sus Declaraciones de Prácticas de Certificación (DPC).

La DPC es un documento que describe los procedimientos empleados por una autoridad de certificación (AC) para la correcta ejecución de sus servicios.

Toda DPC elaborada en el ámbito de la ICPP debe obligatoriamente adoptar la misma estructura de este documento, la cual se basa en el RFC 3647.

El PCSC responsable mantendrá actualizada toda la información de su DPC.

Este documento compone el conjunto normativo de la ICPP y en él se referencian otras reglamentaciones previstas en las demás normas del ICPP.

La firma electrónica cualificada basada en certificados cualificados conforme a la legislación vigente tiene un efecto jurídico equivalente a una firma manuscrita.

Un sello electrónico cualificado garantiza y da certeza de la integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté

vinculado.

Los certificados cualificados de firma electrónica y los certificados cualificados tributarios solo podrán emitirse a personas físicas, los certificados de sello electrónico están reservados para personas jurídicas. Los certificados citados deben ser emitidos por PCSC.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

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

1.3. PARTICIPANTES DE LA ICPP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

En este ítem deben ser identificadas las ACs integrantes de la ICPP a la que se refiere la DPC. Estas pueden ser:

I. AC Raíz-Py: En la cúspide de la Jerarquía de la Infraestructura de Clave Pública del Paraguay (ICPP), se ubica la AC Raíz-Py, la misma cuenta con un certificado auto emitido y aceptado por los terceros que confían en la ICPP. Emite certificados a los PCSC y a partir de allí, comienza la cadena de confianza. Los certificados electrónicos emitidos por la AC Raíz-Py se rigen y ajustan a su Declaración de Prácticas de Certificación (DPC), cuyo cumplimiento es de carácter obligatorio.

II. ACI; Es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, debe contar con un certificado digital emitido por la AC Raíz-Py y solo podrá emitir certificados a personas físicas y jurídicas. En el ámbito de la ICPP un PCSC es considerado una ACI.

Un PCSC presta servicios de **creación, verificación y validación de firmas electrónicas cualificadas y/o sello electrónico cualificado y certificados relativos a estos servicios.**

El PCSC además podrá ser habilitado para prestar servicios de **generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello** en los términos establecidos en el documento *DOC-ICPP-04 [1]* y *DOC-ICPP-07 [2].*

Un PCSC habilitado para brindar servicios **de generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello**, debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Las claves privadas de los firmantes y/o de los creadores de sellos almacenadas en dispositivos estandarizados conforme lo establecido en el documento *DOC-ICPP-04 [1]*, y las firmas electrónicas cualificadas o los sellos electrónicos cualificados realizadas con la clave privada del firmante y/o creador del sello son válidas de conformidad a la Ley N° 6822/2021.

1.3.2. AUTORIDADES DE REGISTRO (AR)

En este ítem debe identificarse la dirección de la página web (URL), donde se publican los datos referentes a las autoridades de registro (AR) habilitadas por el PCSC para los procesos de recepción, identificación y remisión de solicitudes de emisión o revocación de certificados electrónicos y de identificación de sus solicitantes:

El PCSC deberá mantener las informaciones siempre actualizadas.

La AR puede ser propia del PCSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente.

Las ARs delegadas son autoridades de registro vinculadas a un PCSC mediante un acuerdo operacional.

El PCSC deberá igualmente publicar información referente a:

- Lista de todas las ARs habilitadas
- Lista de las ARs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

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

La AV puede ser una entidad del PCSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente. Su función es suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por el PCSC.

Las AVs delegadas son autoridades de validación vinculadas a un PCSC mediante un acuerdo operacional.

El PCSC deberá igualmente publicar información referente a:

- Lista de todas las AVs habilitadas
- Lista de las AVs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación

1.3.4. TITULARES DEL CERTIFICADO

En este ítem se especifican las personas físicas o jurídicas que podrán ser titulares de los certificados emitidos por el PCSC según corresponda a un certificado cualificado de firma electrónica, tributario o de sello electrónico cualificado respectivamente conforme a esta DPC.

1.3.5. PARTE USUARIA

Se entenderá por parte usuaria, toda persona física o jurídica que confía en el servicio de confianza. Es decir confía en el contenido, validez y aplicabilidad del certificado electrónico y claves emitidas en el marco de la ICPP.

1.3.6. OTROS PARTICIPANTES

1.3.6.1. 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 PCSC, sea directamente o sea por intermedio de sus ARs.

Los PSS son entidades externas a las que recurre el PCSC o la AR para desempeñar actividades descritas en esta DPC o en una PC 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 PCSC deberá mantener las informaciones arriba citadas siempre actualizadas.

El funcionamiento de un PSS vinculado a un PCSC mediante un acuerdo operacional deberá ser autorizado por la AC Raíz-Py.

El PCSC deberá igualmente publicar información referente a:

- Lista de todos los PSSs habilitados
- Lista de los PSSs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

En este ítem, la DPC debe relacionar e identificar las PC implementadas por el PCSC, que definen cómo deberán ser utilizados los certificados emitidos. En estas PC estarán especificadas las aplicaciones para las cuales sean adecuadas, el uso de los certificados emitidos por un PCSC.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

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

1.5 ADMINISTRACIÓN DE LA POLÍTICA

En este ítem se debe incluir el nombre, la dirección y otra información del PCSC responsable de la DPC, el nombre, números de teléfono y la dirección de correo electrónico de una persona de contacto.

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PCSC:

1.5.2. PERSONA DE CONTACTO

Nombre:

Teléfono:

Dirección:

Fax:

Página web:

E-mail:

Otros:

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA PC

Nombre:

Teléfono:

Dirección

E-mail:

Otros:

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

Los procedimientos para la aprobación de DPC del PCSC son establecidos a criterio de AC Raíz-Py de la ICPP.

1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1. **Agente de registro:** persona responsable de la realización de las actividades inherentes a la AR. Realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.
2. **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
3. **Autenticación electrónica:** un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
4. **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
5. **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.
6. **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC 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 AC Raíz-Py son ejercidas por la AA.

7. **Autoridad de Certificación Intermedia**: entidad cuyo certificado ha sido emitido por la AC Raíz-Py, es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador cualificado de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.
8. **Autoridad de Registro:** entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.
9. **Autoridad de Validación:** entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por la AC. La AV puede ser propia del PCSC o delegada a un tercero.
10. **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
11. **Cadena de certificación:** lista ordenada de certificados que contiene un certificado del firmante o creador de sello y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante o creador de sello es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El firmante, creador de sello o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.
12. **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley Nº 6822/2021.

13. **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley Nº 6822/2021.
14. **Certificado cualificado tributario:** certificado expedido por un Prestador Cualificado de Servicios de Confianza, el cual podrá ser utilizado para todos los fines convencionales ante el Sistema Marangatú, Sistema Integrado de Facturación Electrónica Nacional, otros Sistemas de Información administrados por la Subsecretaría de Estado de Tributación (SET) así como otros usos afines autorizados por la Autoridad de Aplicación.
15. **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.
16. **Cifrado asimétrico:** tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
17. **Contrato de prestación de servicio de confianza:** Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado que contiene información relativa al solicitante del certificado y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.
18. **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
19. **Clave pública y privada:** la criptografía en la que se basa la ICPP, es la criptografía asimétrica. En ella, se emplean 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 electrónico, mientras

que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.

20. **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
21. **Data center (Centro de Datos):** infraestructura compuesta por espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una AC, 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 electrónicos emitidos por la AC.
22. **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.
23. **Declaración de Prácticas de Certificación:** documento en el cual se determina la declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
24. **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión, suspensión o revocación del certificado cualificado electrónico será considerada la cédula de identidad civil o el pasaporte del solicitante.
25. **Dossier del titular del certificado:** conjunto formado por la verificación de los documentos de identificación utilizados para la emisión, suspensión o revocación del certificado, solicitud de certificado, contrato de prestación de servicios, 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 contrato de prestación de servicios 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 electrónicamente con un certificado cualificado después de la generación de las claves y anterior a la instalación del certificado correspondiente.

26. **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
27. **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
28. **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
29. **Firmante:** una persona física que crea una firma electrónica.
30. **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 AC, 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.

31. **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
32. **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.
33. **Identificación del Solicitante 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 o mediante otros medios que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, conforme a los supuestos establecidos en la Ley y en base a los documentos de identificación previstos en la presente DPC.
34. **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 electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.
35. **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.

36. **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
37. **Lista de Confianza**: Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley Nº 6822/21.
38. **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
39. **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
40. **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
41. **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley Nº 6822/2021.
42. **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley Nº 6822/2021.
43. **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
44. **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

45. **Política de Certificación:** documento en el cual la AC 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.
46. **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
47. **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
48. **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada por la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.
49. **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.
50. **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
51. **Rol de confianza:** función crítica que desempeña personal de la AC, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la AC.
52. **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.

53. **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una AC.
54. **Solicitud de Firma de Certificado:** petición de certificado electrónico que se envía a la AC, mediante la información contenida en el CSR, la AC, puede emitir el certificado electrónico una vez realizadas las comprobaciones que correspondan.
55. **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte de documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados de sello electrónico para persona jurídica.
56. **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
57. **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado 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 creación.
58. **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.
59. **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
AGD	Autoridad de Gestión de Datos
AGR	Agente de Registro
P	País (C por su sigla en inglés, Country)
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
ACI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad civil

NC	Nombre Común (CN por sus siglas en inglés, Common Name)
PC	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, Certification Practice Statement)
LCR	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)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
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
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Clave Pública del Paraguay
OEC	Organismo de Evaluación de la Conformidad
PCSC	Prestador cualificado de servicios de confianza
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte
Py	Paraguay
AR	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).

RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RUC	Registro único del Contribuyente
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).
AV	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 PCSC y su LCR/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 2 (dos) repositorios, en infraestructuras de red segregada, para la distribución del LCR/OCSP.

e) garantizar que en su sitio web exista un enlace a la lista de confianza pertinente al utilizar la etiqueta de confianza «PY» para los servicios de confianza cualificados.

En este ítem deben ser descriptos, los requisitos aplicables a los repositorios utilizados por el PCSC responsable de la DPC, 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 PCSC responsable de la DPC. El servicio de publicación de información de un PCSC 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 (24) 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 PCSC en su servicio de repositorio:

a) PC y DPC que implementan;
b) el certificado de la AC Raíz-Py;

c) su propio certificado;
d) la LCR;
e) certificados emitidos;
f) proforma del contrato de prestación de servicios de confianza;
g) las resoluciones que habilitan o revocan al PCSC:
h) leyes, decretos, reglamentos y resoluciones que rigen la actividad de la ICPP;
i) identificación, domicilio y medios de contacto;
j) una lista, actualizada periódicamente, que contiene las ARs propias y delegadas con las respectivas direcciones de sus instalaciones técnicas de operación, autorizadas por la AC Raíz-Py para funcionar;
k) acuerdos operacionales celebrados entre un PCSC y una AR delegada;
l) la lista actualizada de todas las ARs cuya habilitación fue revocada, con la indicación de la fecha de revocación.
m) la lista de todas las AVs habilitadas;
n) para cada AV, las direcciones de todas las instalaciones técnicas, autorizadas por la AC Raíz-Py para funcionar;
o) acuerdos operacionales celebrados entre un PCSC y una AV delegada;
p) la lista de todas las AVs cuya habilitación fue revocada, con la indicación de la fecha de revocación.
q) una lista, actualizada periódicamente de los PSS vinculados a un PCSC;

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 PCSC, de acuerdo a lo establecido en las normas, criterios, prácticas y procedimientos de la ICPP.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

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 PCSC responsable de la DPC. Entre los tipos de nombres considerados podrán estar el *distinguished name* según lo establecido en la ITU X.500, direcciones de correos electrónicos o direcciones de página web (URL).

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

En este apartado, la DPC 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 PCSC responsable.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS TITULARES DE CERTIFICADOS

Se admitirá el uso de seudónimos en los certificados cualificados firma electrónica emitidos por un PCSC y autorizados por la AC Raíz. El PCSC que consigne un seudónimo en un certificado electrónico cualificado deberá constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite, en el dossier de titular del certificado.

El PCSC estará obligado a revelar la identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

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 DPC.

Está prohibido el uso de nombres en certificados que violen los derechos de propiedad intelectual de terceros.

3.1.4.1 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO

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

Tabla Nº 2 - RUC Certificado Cualificado de Sello Electrónico

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

3.1.4.2 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA O CERTIFICADO CUALIFICADO TRIBUTARIO

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 Cualificado de Firma Electrónica o Certificado Cualificado Tributario

Tipo de Documento	Prefijo	Formato	Descripción
Cédula de identidad	CI	CI999999	Siglas CI seguido del número de cédula de identidad civil, 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 Cualificado de Firma Electrónica o Certificado Cualificado Tributario

Tipo de Documento	Prefijo	Formato	Descripción
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 DPC debe establecer, qué identificadores del tipo "Distinguished Name" (DN), deberán ser únicos para cada titular del certificado, en el ámbito del PCSC 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 DPC debe reservar al PCSC, 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 DPC 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

Se debe detallar la forma, los procedimientos y los requisitos para la primera identificación y registro ante la ICPP de los titulares o responsables de certificados electrónicos, comprendiendo los siguientes procesos:

a) **Identificación y registro 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, observando lo siguiente:

   i. para certificados cualificados de firma electrónica cualificada: prueba de que la persona física 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 cualificados de sello electrónico: 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 autorizado 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 cualificados tributarios: se procederá conforme a lo establecido en el ítem i. en el caso que el titular del certificado corresponda a una empresa unipersonal y conforme al ítem ii. en el caso de que el titular del certificado preste servicios en una organización.

b) **Emisión del certificado**: luego de cotejar los datos de la solicitud del certificado con los contenidos en los documentos presentados, en la etapa de identificación, se procede a la emisión del certificado en el sistema del PCSC. Se considera que la extensión ***Nombre Alternativo del Sujeto (Subject Alternative Name)*** está fuertemente relacionada con la clave pública contenida en el certificado, por lo que todas las partes de esta extensión deben verificarse y el solicitante del certificado debe demostrar que tiene los derechos sobre esta información ante la autoridad competente, o que está autorizado por el titular de la información para utilizarlos.

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

La DPC deberá indicar los procedimientos realizados por el PCSC responsable o las ARs vinculadas a ella para confirmar que la persona física o jurídica solicitante controla la clave privada correspondiente a la clave pública para la que se solicita el certificado, pudiendo utilizar las referencias contenidas en el RFC 4210 y 6712. Si se

requieren procedimientos específicos para las PCs implementadas, deben estar descritos en estas PCs, en el ítem correspondiente.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

3.2.2.1 DISPOSICIONES GENERALES

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

Se designará como responsable del certificado al representante autorizado de la persona jurídica que solicita el certificado conforme al numeral 3.2, inciso 'a', inciso (ii), quien tendrá el control de la clave privada.

La confirmación de la identidad de la persona jurídica y de la persona física responsable del certificado será verificada por el PCSC bien directamente o bien por medio de un tercero en los siguientes términos:

a) presentación de la lista de documentos enumerados en el punto 3.2.2.2;
b) presentación de la lista de documentos del responsable del certificado, enumerados en el ítem 3.2.3.1;
c) firma electrónica cualificada del *contrato de prestación de servicio de confianza* mencionado en el ítem 4.1 por el responsable del certificado. En caso de no ser factible, la AR solicitará que el contrato sea firmado manuscritamente por el responsable del certificado para su comparación con el documento de identidad. En este caso, se adjuntará al dossier de titular del certificado, el documento manuscrito digitalizado y firmado con firma electrónica cualificada por el AGR, debiendo mantenerse el original en papel para fines de auditoría.

Se prescinde lo dispuesto en el ítem "b" si el responsable del certificado posee un certificado cualificado de firma electrónica de la ICPP vigente, o cuando utilice un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto. En estos casos la verificación de los documentos enumerados en el punto 3.2.2.2 se puede realizar electrónicamente, siempre que se realice a través de fuentes oficiales de organismos competentes.

3.2.2.2 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA.

La confirmación de la identidad de una persona jurídica debe hacerse mediante la presentación de al 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 podrá realizarse por vía electrónica, siempre que se realice a través 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 AR delegada o AR propia del PCSC; 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.

3.2.2.3 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO

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 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 civil 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 *contrato de prestación de servicio de confianza* 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) cargo 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 en el dossier de titular del certificado.

Respecto a la responsabilidad derivada del uso del certificado de una persona jurídica, los actos realizados con el certificado 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 este ítem, se deben definir los procedimientos utilizados por las ARs vinculadas a un PCSC para la identificación y el registro de una persona física en la ICPP. Esta confirmación deberá realizarse:

La confirmación de la identidad de la persona física responsable del certificado será verificada por el PCSC bien directamente o por medio de un tercero en los siguientes términos:

a) en presencia de la persona física; o,

b) a distancia, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto, para los cuales se haya garantizado la presencia de la persona física previamente a la expedición del certificado cualificado; o,

c) por medio de un certificado de una firma electrónica cualificada expedido de conformidad con la letra a) o b); o,

d) mediante videoconferencia, de acuerdo con los procedimientos y requisitos técnicos definidos en la normativa de AC Raíz-Py, *DOC-ICPP-17 [3]*, que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, garantizando la validación de la misma identificación, mediante el uso de tecnologías electrónicas seguras de comunicación, interacción y documentación. La seguridad equivalente será confirmada por un OEC.

3.2.3.1 PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE UNA PERSONA

La identificación de la persona física solicitante del certificado debe realizarse de la siguiente manera:

a) presentación de la siguiente documentación, en su versión oficial original, física o electrónica:
   i) cédula de Identidad civil o pasaporte, si es paraguayo;
   ii) cédula de Identidad de extranjero, si es extranjero domiciliado en Paraguay; o
   iii) pasaporte, si es extranjero no domiciliado en Paraguay.

Se considera documento de identidad al documento oficial, físico o electrónico, según la legislación específica, emitido por el Ministerio del Interior a través de la Policía Nacional.

Los documentos electrónicos deberán ser verificados a través de fuentes oficiales de organismos competentes. Dicha verificación formará parte del dossier del titular del certificado. En caso de una identificación positiva, se omite el requerimiento de verificación descritos en el siguiente párrafo:

Los documentos en papel, para los cuales no existan formas de verificación a través de fuentes oficiales competentes, deberán ser verificados:

a) por un agente de registro distinto del que realizó el paso de identificación;

b) por la AR vinculada o AR propia del PCSC; 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.

La emisión de certificados a favor de los absolutamente incapaces y de los relativamente incapaces deberá observar las disposiciones de la ley vigente y las normas emitidas por la ICPP.

3.2.3.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

La información obligatoria contenida en los campos del certificado cualificado de firma electrónica 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 civil 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 contrato de prestación de servicios de confianza, puede solicitar llenar los campos con las siguientes informaciones:

c) el correo del titular del certificado;
d) el nombre de la organización en el que presta servicio el titular del certificado;
e) el nombre de la unidad de la organización en el que presta servicio el titular del certificado;
f) el número de RUC de la organización en el que presta servicio el titular del certificado
g) el número de RUC del titular del certificado;
h) posición o función asignada al titular del certificado en la organización en el que presta servicio; y
i) 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 en el dossier de titular del certificado.

3.2.3.3 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO TRIBUTARIO

La información obligatoria contenida en los campos del certificado cualificado tributario 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;
b) número de cédula de identidad civil o número de pasaporte de la persona física, según documento de identidad;
c) nombre de la organización en el que presta servicio el titular del certificado o razón social del titular del certificado en caso de tratarse de una organización unipersonal, según cédula tributaria; y
d) número de RUC correspondiente a la organización en el que presta servicio el titular del certificado o el número de RUC del titular del certificado en caso de tratarse de una organización unipersonal, según cédula tributaria.

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 contrato de prestación de servicios de confianza, puede solicitar llenar los campos con las siguientes informaciones:

e) el correo del titular del certificado;
f) el nombre de la unidad de la organización en el que presta servicio el titular del certificado;
g) posición o función asignada al titular del certificado en la organización en el que presta servicio; y
h) 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 en el dossier de titular del certificado.

3.2.4. INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

No aplica.

3.2.5. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

La AR, debe validar la capacidad del solicitante de un certificado y que no posea impedimentos legales. En el caso de certificados cualificados para firma electrónica, debe validar que el solicitante sea mayor de edad y en el caso de certificados cualificados para sello electrónico debe además validar la autoridad invocada por el representante con facultades suficientes para solicitar el certificado.

3.2.6. CRITERIOS PARA INTEROPERABILIDAD

Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos fuera del país serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados por los PCSC establecidos en la República del Paraguay si los servicios de confianza son reconocidos en virtud de acuerdos de reconocimiento mutuo celebrado entre autoridades oficiales de cada país o con organizaciones internacionales de conformidad a la reglamentación correspondiente.

Los acuerdos a que se refiere el párrafo anterior deben garantizar, en particular, que:

a) Los prestadores de servicios de confianza establecidos fuera del país u organizaciones internacionales y los servicios de confianza que prestan, cumplen los requisitos aplicables a los PCSC establecidos en el Paraguay y a los servicios de confianza cualificados que prestan.

b) Los servicios de confianza cualificados prestados por PCSC establecidos en Paraguay son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios establecidos fuera del país u organizaciones internacionales con los que se celebran acuerdos.

3.2.7 PROCEDIMIENTOS COMPLEMENTARIOS

El PCSC comprobará la identidad y/o atributos de las personas físicas y jurídicas antes de incluir estos atributos en un certificado en el marco de la ICPP. Se prohíbe a las personas físicas y jurídicas utilizar en sus certificados nombres que violen los derechos

de propiedad intelectual de terceros. El PCSC se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

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

Se debe mantener un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física o jurídica. Tales copias podrán ser conservadas en papel o en formato electrónico, sujetas a las condiciones definidas en el documento *DOC-ICPP-05 [4]*.

3.2.8 PROCEDIMIENTOS ESPECÍFICOS

En el caso de certificado emitido a Empleados del Servicio Exterior Paraguayo, en misión permanente en el exterior, si existen impedimentos para identificación conforme previsto en el ítem 3.2, es posible enviar la documentación por vía diplomática y realizar la identificación por otros medios seguros, a ser definidos y aprobados por la AC Raíz-Py.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

En este punto, la DPC deberá establecer los procesos de identificación y confirmación del registro del solicitante, utilizados por el PCSC responsable de generar un nuevo par de claves y su correspondiente nuevo certificado.

Este proceso puede realizarse de acuerdo con una de las siguientes posibilidades:

a) adopción de los mismos requisitos y procedimientos requeridos en los puntos 3.2.2 o 3.2.3;

b) solicitud, por medio electrónico, firmada electrónicamente utilizando un certificado cualificado de la ICPP válido del solicitante, que sea del mismo nivel de seguridad o superior, admitiéndose esta hipótesis únicamente para los certificados cualificados de firma electrónica y a los certificados cualificados tributarios;

c) solicitud, por medio electrónico, sellada electrónicamente utilizando un certificado cualificado de sello electrónico de la ICPP válido de una persona jurídica, que sea del mismo nivel de seguridad o superior, siempre que, mantenido en esta condición, presente un documento electrónico comprobable mediante fuente oficial de organismos competentes, que acredite el poder de representación legal en relación con la organización, siendo admitida esta hipótesis únicamente para los certificados cualificados de sello electrónico;

d) solicitud, por medio electrónico, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto.

e) mediante videoconferencia, de acuerdo con el procedimiento y requisitos técnicos definidos en la normativa de AC Raíz-Py, *DOC-ICPP-17 [3]*, que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, garantizando la validación de la misma identificación, mediante el uso de tecnologías electrónicas seguras de comunicación, interacción y documentación. La seguridad equivalente será confirmada por un OEC.

Si se requieren procedimientos específicos para las CPs implementadas, estos deben estar descritos en estas CPs, en el ítem correspondiente.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

El solicitante de la revocación de un certificado cualificado de la ICPP debe estar identificado. Únicamente los agentes descriptos en el ítem 4.9.2 pueden solicitar la revocación de dicho certificado.

El procedimiento para solicitar la revocación de un certificado cualificado por parte PCSC se describe en el ítem 4.9.3.

Las solicitudes de revocación de certificados deben registrarse.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

En este ítem de la DPC, deben ser descritos todos los requisitos y procedimientos operacionales establecidos por el PCSC responsable y las ARs, 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 PCSC y la AR en el proceso de solicitud del certificado electrónico. La descripción también debe contemplar:

a) la comprobación de los atributos de identificación que constan en el certificado, conforme al ítem 3.2;
b) el uso de un certificado cualificado de firma electrónica del del AGR responsable de gestionar las solicitudes de emisión, suspensión y revocación de certificados;.
c) un *contrato de prestación de servicio de confianza* firmado con firma electrónica cualificada por el titular del certificado o por la persona responsable del certificado, en el caso de un certificado cualificado de sello electrónico.

En caso de imposibilidad técnica de firmar electrónicamente el *contrato de prestación de servicio de confianza* será aceptada la firma manuscrita del contrato por parte del titular o responsable en el caso de un certificado cualificado de sello electrónico. En este caso será necesaria la verificación de la firma contra el documento de identificación y se adjuntará al dossier de titular del certificado, el documento manuscrito digitalizado y firmado con firma electrónica cualificada por el AGR, conforme al *DOC-ICPP-05 [4]*.

El formato del documento *contrato de prestación de servicio de confianza***,** según sea el tipo de certificado a ser emitido, será establecido por la AC Raíz-Py.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

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

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

a) para el caso de certificado cualificado de firma electrónica o tributario, puede ser solicitado por toda persona mayor de edad, sin distinción, con un documento de identidad válido y vigente, que será el sujeto a cuyo nombre se emita el certificado;
b) para el caso de certificado cualificado sello electrónico, el representante de la persona jurídica;

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 PCs implementadas, se deben describir en dichas PCs, en el ítem correspondiente.

4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PCSC

Responsabilidades:

a) los PCSC deben responder por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone la normativa vigente;
b) los PCSC deben asumir toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna/s de las funciones necesarias para prestación de servicios de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Obligaciones

En este ítem se deben incluir las obligaciones del PCSC responsable de la DPC, conteniendo al menos lo siguiente:

a) publicar información veraz y acorde con las reglamentaciones vigentes, en su sitio principal Internet:
   i) su DPC, y las PC aprobadas que implementa;
   ii) las informaciones definidas en el ítem 2.2. de este documento y
   iii) las informaciones sobre la desvinculación de una AR.
   iv) no almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, de sello de la persona física o jurídica a la que hayan emitido certificados, salvo en caso de su gestión en nombre del firmante o del creador del sello. En este caso, el PCSC tiene la obligación de:
   v) utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros;

vi) aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado;

vii) custodiar y proteger los datos de creación de firma, de sello frente a cualquier alteración, destrucción o acceso no autorizado; y

viii) garantizar su continua disponibilidad.

b) disponer de un servicio de consulta sobre el estado de validez y revocación de los certificados emitidos accesible al público;

c) conservar la información relativa a los servicios prestados por el término de diez años;

d) constituir un seguro de responsabilidad civil por importe mínimo de quinientos salarios mínimos previstos para actividades diversas no especificadas, excepto si el prestador pertenece al sector público. Si presta más de un servicio de los previstos en la normativa, se añadirán ciento cincuenta salarios mínimos más por cada servicio. La citada garantía puede ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior;

e) informar a la parte usuaria y los titulares de certificados sobre las garantías, cobertura, condiciones y limitaciones establecidas en la póliza de seguro de responsabilidad civil contraída en los términos indicado en el inciso e);

f) en el caso de cese de sus operaciones, comunicar a los que preste sus servicios y al organismo de supervisión con una antelación mínima de dos meses el cese efectivo de la actividad. El plan de cese del PCSC puede incluir la transferencia de clientes a otro prestador cualificado, una vez acreditada la ausencia de oposición de los mismos;

g) comunicar al organismo de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, debe comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él;

h) asegurarse de que el titular del certificado puede controlar el acceso y uso de los datos de creación de firma o sello correspondientes a los de verificación que consten en el certificado, antes de la expedición de un certificado cualificado;

i) enviar el informe de evaluación de la conformidad a la AC Raíz-Py en el plazo de tres días hábiles tras su recepción. El incumplimiento de esta obligación conlleva la suspensión de la cualificación al prestador y al servicio que éste presta, y su eliminación de la lista de confianza;

j) notificar, en un plazo de veinticuatro horas tras tener conocimiento de ellas, a la AC Raíz-Py de las violaciones de seguridad que sufran, entendiéndose como violación de seguridad a un evento que afecta de manera crítica la confidencialidad, integridad y/o disponibilidad de los activos de información y tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes;

k) gestionar los incidentes de seguridad que les afecten, debiendo prever los mecanismos adecuados para su prevención, detección, análisis y resolución;

l) ampliar tras la resolución del incidente, la información suministrada en la notificación inicial con arreglo a las directrices que pueda establecer AC Raíz-Py;

m) facilitar a la AC Raíz-Py toda la información y colaboración precisas para el ejercicio de sus funciones. En particular, deben permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate conforme al servicio que se preste. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas;

n) adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizan un nivel de seguridad proporcional al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes.

o) notificar al *organismo de supervisión* y al *centro de respuestas a incidentes Cibernéticos* del Ministerio de Tecnologías de la Información y Comunicación (MITIC), sin demoras indebidas, pero en cualquier caso en un plazo de veinticuatro horas tras tener conocimiento sobre cualquier violación de la seguridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes. Cuando la violación de seguridad pueda atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, se deberá notificar también a la persona física o jurídica, sin demora indebida, la violación de seguridad. El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad reviste interés público.

p) informar al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades.

q) contar con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas internacionales.

r) con respecto al riesgo de la responsabilidad por daños, mantener recursos financieros suficientes u obtener pólizas de seguros de responsabilidad adecuadas.

s) antes de entrar en una relación contractual, informar, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización.

t) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan.

u) utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

   i) estén a disposición del público para su recuperación sólo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos.

   ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados.

   iii) pueda comprobarse la autenticidad de los datos.

v) tomar medidas adecuadas contra la falsificación y el robo de datos.

w) registrar y mantener accesible durante un período de tiempo definido por la AC Raíz-Py, incluso cuando hayan cesado las actividades del PCSC, toda la información pertinente referente a los datos expedidos y recibidos por el PCSC, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos.

x) Contar con un plan de cese actualizado para garantizar la continuidad del servicio,

y) garantizar un tratamiento lícito de los datos personales.

z) mantener actualizada una base de datos de certificados.

aa) cuando los PCSC revocan un certificado, deberán registrar su revocación en su base de datos de certificados y publicar el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de veinticuatro horas después de la recepción de la solicitud.

bb) recolectar los datos personales directamente de la persona a quien esos datos se refieran. La recolección y procesamiento en general de los datos personales se realizarán solo en la medida en que los mismos sean necesarios para la prestación del servicio de confianza. Los datos personales no pueden ser procesados para otro fin distinto al acordado, sin el consentimiento expreso del titular de los datos.

cc) constatar la verdadera identidad del firmante o titular del certificado y conservar la documentación que la acredite en caso de expedir certificados que consignen seudónimos.

dd) revelar la verdadera identidad del firmante o titular del certificado en caso de expedir certificados que consignen seudónimos, cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

ee) proporcionar a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información debe estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente.

ff) operar de acuerdo a su DPC y PC que implementan;

gg) generar y gestionar sus pares de claves criptográficas;

hh) asegurar la protección de sus claves privadas;

ii) distribuir su propio certificado;

jj) emitir, expedir y distribuir los certificados de los usuarios finales;

kk) informar la emisión del certificado al respectivo solicitante;

ll) revocar o suspender los certificados por él emitidos, de acuerdo con lo establecido en la PC correspondiente y en la DPC;

mm) emitir, gestionar y publicar sus CRLs y disponibilizar la consulta online del estado de los certificados emitidos (OCSP-On-line Certificate Status Protocol);

nn) utilizar un protocolo de comunicación seguro cuando se preste servicios a través de la web a los solicitantes o usuarios de certificados electrónicos;

oo) identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por AC Raíz-Py;

pp) adoptar las medidas de seguridad y de control previstas en la DPC, PC y PS que se implementan, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.

qq) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por AC Raíz-Py, y la normativa vigente;

rr) mantener y garantizar la integridad, confidencialidad y seguridad de la información por él tratado;

ss) mantener y anualmente realizar prueba de su PCN;

tt) informar a la AC Raíz-Py, mensualmente, la cantidad de certificados electrónicos emitidos y revocados;

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

vv) someterse a una auditoría al menos una vez cada veinte y cuatro meses, corriendo con los gastos que ello genere, por un OEC debidamente acreditado, y remitir el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción;

ww) someterse a auditoría o evaluación de conformidad, corriendo con los gastos que ello genere,en cualquier momento, solicitada por el organismo de supervisión; y

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

yy) cumplir con las demás disposiciones reglamentadas por la AC Raíz-Py para asegurar que el PCSC se ajusta a la normativa vigente.

4.1.2.2 RESPONSABILIDADES Y OBLIGACIONES DE LA AR

Responsabilidades

La AR será responsable por los daños y perjuicios que ocasione.

Obligaciones

En este apartado de la DPC, deben ser incluidas las obligaciones de las ARs vinculadas al PCSC responsable de la DPC, conteniendo, como mínimo, las consideraciones mencionadas a continuación:

a) recibir las solicitudes de emisión, suspensión revocación de certificados;

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

c) remitir la solicitud de emisión, suspensión revocación del certificado al PCSC responsable, por medio de acceso remoto al ambiente de la AR alojado en las instalaciones del PCSC, utilizando un protocolo de comunicación seguro, conforme al patrón definido en el documento *DOC-ICPP-05 [4]*;

d) informar a los respectivos titulares la emisión, suspensión 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 PCSC vinculado, la AC Raíz-Py y en especial con lo contenido en el documento *DOC-ICPP-05 [4]*;

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 y 3.2.3.; y
h) divulgar sus prácticas, relacionadas con la cadena del PCSC a la que se vincula, de acuerdo a los principios y criterios establecidas por la AC Raiz-Py para las AR.

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

El PCSC y la AR realizan las funciones de identificación y autenticación según el ítem 3 de esta DPC.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

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

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

El PCSC debe cumplir con los procedimientos determinados por la AC Raíz-Py. No habrá tiempo máximo para procesar solicitudes en el marco de la ICPP.

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

En este punto de la DPC deben ser descriptos los requisitos operacionales establecidos por el PCSC para la emisión de un certificado y para la notificación de la emisión al solicitante. En caso de que sean requeridos procedimientos específicos para cada PC implementada, los mismos deben ser descriptos, en el ítem correspondiente.

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

4.3.2 NOTIFICACIONES AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISIÓN DEL CERTIFICADO

En este ítem de la DPC, deben ser descriptos los requisitos operacionales establecidos por el PCSC responsable para la notificación al solicitante sobre la emisión de su certificado..

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 PC implementadas, los mismos deben ser descriptos en esas PC, en el ítem correspondiente.

La DPC debe garantizar que la aceptación de todo certificado emitido sea declarada expresamente por el respectivo titular. En caso de los certificados emitidos para sello electrónico, 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 DPC.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

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

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

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

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

El titular o responsable de un certificado debe usar el par de claves y el certificado correspondiente de acuerdo a la DPC y las PCs que implementa el PCSC emisor de su certificado, establecidas de acuerdo con este documento y con el documento *DOC-ICPP-04 [1]*.

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR O RESPONSABLE

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

Obligaciones del Titular del Certificado

Este ítem debe incluir las obligaciones de los titulares de certificados emitidos por el PCSC responsable de la DPC, contenidas del *contrato de prestación de servicio de confianza* referidos en el ítem 4.1, y debe incluir al menos los ítems que se enumeran a continuación:

a) proporcionar al PCSC información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia;

b) comunicar sin demora al PCSC de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico;

c) conservar adecuadamente sus datos de creación de firma o sello, asegurar su confidencialidad y proteger de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos;

d) solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma o sello o, en su caso, de los medios que den acceso a ellos.

e) no utilizar los datos de creación de firma o sello cuando haya expirado el período de validez del certificado electrónico o el PCSC le notifique la extinción o suspensión de su vigencia.

f) utilizar sus certificados y claves privadas de forma adecuada, según lo previsto en la PC correspondiente;

g) conocer sus derechos y obligaciones, contemplados en la DPC y la PC correspondiente y demás documentos aplicables de la ICPP; y

h) informar al PCSC emisor de cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA

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

4.6 RENOVACIÓN DEL CERTIFICADO

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

4.6.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DE CERTIFICADO

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

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

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

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

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

4.6.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

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

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

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

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

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

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

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

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 TITULAR DEL CERTIFICADO 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 PCSC DE LOS CERTIFICADOS RE-EMITIDOS

Este ítem no aplica.

4.7.7 NOTIFICACIÓN POR EL PCSC 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 TITULAR DEL CERTIFICADO 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 PCSC DE LOS CERTIFICADOS MODIFICADOS

Este ítem no aplica.

4.8.7 NOTIFICACIÓN POR EL PCSC 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 DPC, deben ser consignadas, las circunstancias en la cual un certificado podrá ser revocado.

Igualmente se debe establecer que los PCSC extinguirán la vigencia de los certificados mediante revocación en los siguientes supuestos:

a) solicitud formulada por el firmante, la persona física titular o jurídica representada por un tercero autorizado, el creador del sello.

b) violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del PCSC, o utilización indebida de dichos datos por un tercero.

c) resolución judicial o administrativa competente que lo ordene.

d) fallecimiento del firmante; incapacidad sobrevenida, total o parcial, del firmante y extinción de la personalidad jurídica o disolución del creador del sello,

e) cese en la actividad del PCSC salvo que la gestión de los certificados electrónicos expedidos por aquél sea transferida a otro prestador de servicios de confianza.

f) descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado.

Además los PCSC podrán establecer en su DPC cualquier otra causa lícita de revocación.

En su caso, y de manera previa o simultánea a la indicación de revocación de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, el PCSC informará al firmante acerca de esta circunstancia, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto.

La DPC deberá indicar que el PCSC 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 ICPP.

La DPC también deberá indicar que la AC Raíz-Py podrá determinar la revocación del certificado del PCSC que incumpla con la legislación vigente o las políticas, estándares, prácticas y reglas establecidas en el marco de la ICPP.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

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

a) por solicitud formulada del firmante, la persona física o jurídica representada por éste, un tercero autorizado o el creador del sello;
b) resolución judicial o administrativa competente que lo ordene.
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 PCSC emitente;
e) por una AR vinculada al PCSC emitente;

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

En este apartado, la DPC debe describir los procedimientos establecidos por el PCSC para la solicitud de revocación de certificados. El PCSC 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 DPC 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 LCR 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 PCSC.

Los PCSC que revoquen un certificado electrónico cualificado, deben registrar su revocación en su base de datos de certificados y publicar el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

La DPC debe garantizar de que el PCSC 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 LCR correspondiente.

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

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

En este ítem, el DPC 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 PCSC.

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

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

En el caso de una solicitud formalmente constituida, de acuerdo con las reglas de la ICPP, el PCSC debe procesar la revocación inmediatamente después de analizar la solicitud.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTES USUARIA

En este apartado, la DPC debe referir la necesidad de que las partes usuarias verifiquen el estado del certificado y el estado de todos los certificados de la AC en la cadena a la que pertenece el mismo, antes de confiar en él. Para ello, las partes usuarias pueden verificar el estado del certificado mediante el servicio de: OCSP o LCR más reciente, proveído por el PCSC.

Antes de confiar en un certificado, las partes usuarias deben 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 del certificado, restricciones de uso de claves y políticas de certificación y estado de revocación por medio de la LCR o respuestas OCSP identificadas en cada certificado en la cadena de certificación.

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

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

La LCR debe actualizarse y publicarse inmediatamente cuando surja una revocación o suspensión o con una frecuencia máxima para certificados de los usuarios finales de doce (12) horas.

La LCR mantiene publicado obligatoriamente:

- el certificado revocado hasta que expire, y
- el certificado suspendido, mientras permanezca tal condición.

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

4.9.8 LATENCIA MÁXIMA PARA LCR

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

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

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

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

La DPC también debe observar que la autenticidad de la LCR/OCSP además debe confirmarse mediante la verificación de la firma del PCSC emisor y del período de validez de la LCR/OCSP.

4.9.10 REQUISITOS PARA LA VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

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

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

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

La DPC 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 las partes usuarias.

4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

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

La DPC 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

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

Siempre que la DPC del PCSC prevea la posibilidad de suspender los certificados, se debe proceder a la suspensión del certificado conforme a los siguientes supuestos:

a) solicitud formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado, el creador del sello.

b) sospecha o duda de violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del PCSC, o utilización indebida de dichos datos por un tercero.

c) resolución judicial o administrativa competente que lo ordene.

d) sospecha o duda de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado.

Además los PCSC podrán establecer en su DPC cualquier otra causa lícita de suspensión.

De manera previa o simultánea a la indicación de la suspensión de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez de los certificados por él expedidos, el PCSC informará al titular de certificado o al responsable del mismo acerca de esta circunstancia, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto. La vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

En este ítem de la DPC, debe establecer que la suspensión de un certificado sólo podrá realizarse:

a) por solicitud formulada a través del firmante, la persona física o jurídica representada por éste, un tercero autorizado o el creador del sello;

b) resolución judicial o administrativa competente que lo ordene.

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 PCSC emitente;

e) por una AR vinculada al PCSC emitente;

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

En este apartado, la DPC debe describir los procedimientos establecidos por el PCSC para la solicitud de suspensión de certificados. El PCSC deberá garantizar que quienes están autorizados a solicitar la suspensión conforme al ítem 4.9.14, puedan, fácilmente y en cualquier momento, solicitar la suspensión de sus respectivos certificados.

Como directrices generales, la DPC debe establecer que:

a) el solicitante de suspensión de un certificado será identificado;

b) las solicitudes de suspensión, así como las acciones resultantes de ellas serán registradas y almacenadas;
c) se documentarán las razones de la suspensión de un certificado; y
d) la suspensión de un certificado terminará con la generación y publicación de una LCR que contenga los datos del certificado suspendido y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PCSC.

Los PCSC que suspendan un certificado electrónico cualificado, deben registrar su suspensión en su base de datos de certificados y publicar el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La suspensión será efectiva inmediatamente después de su publicación.

La DPC debe garantizar de que el PCSC responsable responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su suspensión y la emisión de la LCR correspondiente.

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

4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

El límite del periodo de suspensión será establecido por el titular del certificado. La vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el PCSC no la hubiera levantado.

4.10 SERVICIOS DE ESTADO DEL CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

El PCSC debe proporcionar un servicio de estado de certificado en forma de un punto de distribución de LCR en los certificados y OCSP, conforme al ítem 4.9.9

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 (24/7). En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro (24) 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 los certificados es una característica opcional para la AC Raíz-Py, sin embargo, para el PCSC constituye una característica obligatoria.

Para hacer uso del servicio de validación en línea es responsabilidad de las partes usuarias disponer de un cliente OCSP que cumpla el RFC 6960.

4.11 FIN DE ACTIVIDADES

En este ítem, el PCSC debe describir las condiciones en las cuales se daría por finalizado el servicio conforme a lo establecido en el ítem 5.8 de esta DPC.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

En este ítem, la DPC debe estipular que el PCSC no podrá almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma o sello de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante o del creador del sello. En este caso, se debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma o de sello, frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

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 PCSC.

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

En los ítems siguientes, deben ser descriptos los controles de seguridad implementados por el PCSC responsable de la DPC y por las ARs 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 DPC debe describir los controles físicos referentes a las instalaciones que albergan los sistemas del PCSC responsable y de las ARs vinculadas.

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La DPC debe establecer que la localización de las instalaciones donde se albergan los sistemas de certificación del PCSC 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 DPC debe también describir los aspectos de la construcción de las Instalaciones del PCSC 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, subestaciones, rectificadores, estabilizadores y similares;
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 PCSC integrante de la ICPP deberá implementar un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme al ítem 9 "control de accesos" de la norma ISO 27002:2022 y los siguientes puntos:

5.1.2.1 NIVELES DE ACCESO FÍSICO

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

En el primer nivel deberá situarse la primera barrera de acceso a las instalaciones del PCSC. 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 PCSC deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PCSC 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 PCSC, desde el nivel 1. A partir de ese nivel, el ingreso de equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles,

será controlado 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 PCSC. El paso del primer al segundo nivel deberá exigir 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 PCSC. Cualquier actividad relativa al ciclo de vida de los certificados electrónicos 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 cuenten con permiso de acceso no podrán permanecer en ese nivel salvo que 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 son dos: algún tipo de identificación individual, como una tarjeta electrónica, y la identificación biométrica.Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PCSC, 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 PCSC, 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 PCSC, 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 PCSC 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 vídeo 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, 4 (cuatro) 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 y estar localizados en el ambiente de 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 PCSC 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 PCSC 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 PCSC 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 a atender los requisitos de disponibilidad de los sistemas del PCSC 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 27002/2022. Cualquier modificación en esa red deberá ser previamente documentada.

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

El sistema de 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 PCSC 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 incendios por gas.

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

5.1.6 ALMACENAMIENTO DE MEDIOS

El PCSC 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 PCSC 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 residuos.

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 PCSC, las instalaciones de respaldo no

se vean afectadas y tomen totalmente las operaciones del PCSC en condiciones idénticas en, un máximo, de 48 (cuarenta y ocho) horas.

5.2 CONTROLES PROCEDIMENTALES

En los siguientes ítems de la DPC deben ser descriptos los requisitos para la caracterización y el reconocimiento de los Roles de Confianza en el PCSC responsable y las ARs 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 PCSC responsable de la DPC 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 PCSC, 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 aprobados por el PCSC, controlar la formalización de los convenios entre el personal y el PCSC, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, deberá cumplir y hacer cumplir las

políticas de seguridad del PCSC 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 PCSC;

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 PCSC 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 PCSC y de la eliminación del hardware criptográfico del PCSC de producción. Serán responsables del mantenimiento o reparación de equipos en general así como de dispositivos criptográficos del PCSC (incluida la instalación de nuevo hardware, firmware o software), Igualmente serán responsables de los desmontajes y la eliminación permanente por el uso;

c) **responsables de la operación diaria del PCSC**: 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 auditorías**: serán los responsables de las tareas de ejecución y revisión de auditoría de los sistemas que conforman la infraestructura tecnológica del PCSC. Esta auditoría deberá realizarse de acuerdo con las normas y criterios de auditoría establecidos en la presente DPC. 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 PCSC**: 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 AR, 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 PCSC 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 PCSC, 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 PCSC, deberán ser revisados y actualizados en su caso, sus permisos de acceso. Deberá existir una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado o funcionario deberá devolver al PCSC en el momento de su desvinculación.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

La DPC debe establecer el requisito de control multi-usuario para la generación y la utilización de la clave privada del PCSC 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 PCSC deberá requerir, como mínimo, de 2 (dos) de sus empleados o funcionarios con rol de confianza. Las demás tareas del PCSC podrán ser ejecutadas por un único empleado o funcionario.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

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

a) sean incluido en una lista de acceso a las instalaciones del PCSC;

b) sean incluido en una lista para acceso físico al sistema de certificación del PCSC;

c) reciban un certificado cualificado de firma electrónica para ejecutar sus actividades operacionales en el PCSC; y

d) reciban una cuenta de usuario del sistema de certificación del PCSC.

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) ser restringidas las acciones asociadas con el perfil para los cuales fueron creados.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

En este ítem la DPC 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 PCSC en producción;
b) la emisión o destrucción de los certificados del PCSC; y
c) la validación de información en los sistemas de certificación del PCSC y de solicitudes de emisión/revocación/suspensión o información del titular o responsable del certificado.

5.3 CONTROLES DE PERSONAL

En los siguientes ítems de la DPC deben ser descriptos los requisitos y procedimientos, implementados por el PCSC responsable, por las ARs y PSSs vinculados 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 DPC debe garantizar de que todos los empleados o funcionarios del PCSC responsable, de las ARs 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 ICPP; 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 PCSC responsable y de las ARs 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 27002/2022 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 PCSC;
d) no tener antecedentes de negligencia o incumplimiento de labores; y
e) no tener antecedentes judiciales ni policiales.

El PCSC 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 PCSC responsable y de las ARs 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 PCSC responsable puede definir requisitos adicionales para la verificación de antecedentes.

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC responsable y de las ARs 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 PCSC y de las ARs vinculadas;
b) sistema de certificación en uso del PCSC;
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 PCSC 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 PCSC o de las ARs.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

En este ítem, la DPC podrá definir una política a ser adoptada por el PCSC responsable y por las ARs 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 PCSC responsable y las ARs 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 DPC 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 PCSC responsable o de una AR vinculada, el PCSC 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 PCSC responsable deberá comunicar sus conclusiones a la AC 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 PCSC responsable y de las ARs 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 27002/2022 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 PCSC responsable o AR 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 DPC debe asegurar que el PCSC responsable pone a disposición de todo el personal del PCSC y para todo el personal de las ARs vinculados al menos:

a) su DPC;
b) las PCs que implementan;
c) la política de seguridad que implementa el PCSC;
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 DPC deben describirse los aspectos de los sistemas de auditoría y registro de eventos implementados por el PCSC con el fin de mantener un entorno o ambiente seguro.

5.4.1. TIPOS DE EVENTOS REGISTRADOS

El PCSC responsable de la DPC, 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 PCSC;
c) los cambios en la configuración del PCSC 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 PCSC 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 PCSC responsable de la DPC 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 DPC debe especificar todas las informaciones que deberán ser registradas por el PCSC responsable.

La DPC 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 PCSC 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 27002/2022.

El PCSC responsable de la DPC, 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 electrónica cualificada del ejecutante.

El PCSC a la que está vinculada la AR, debe establecer, en un documento que esté disponible en las auditorías de cumplimiento, el lugar de archivo de los expedientes de los titulares de certificados.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

La DPC debe establecer el periodo, no superior a 1 (un) mes, con que los registros de auditoría del PCSC 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 DPC debe establecer que el PCSC 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 PCSC.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

En este ítem, la DPC debe describir los mecanismos obligatorios incluidos en el sistema de registro de eventos del PCSC 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 auditoría 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 27002/2022.

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

En este ítem de la DPC deben ser descriptos los procedimientos adoptados por el PCSC 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 DPC deben ser descritas y localizadas los recursos utilizados por el PCSC responsable para la recolección de datos de auditoría.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

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

5.4.8. EVALUACIÓN DE VULNERABILIDADES

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

5.5. ARCHIVOS DE REGISTROS

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

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

En este ítem de la DPC 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 PCSC responsable;
g) Información de auditoría prevista en el ítem 5.4.1.

5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS

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

a) las LCR y los certificados emitidos por el PCSC 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 DPC 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 27002/2022.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

La DPC debe establecer que una segunda copia de todo el material archivado deberá ser almacenada en un local externo al PCSC 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 PCSC responsable de la DPC 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 DPC, deben ser descriptos y localizados los recursos utilizados por el PCSC responsable para la recolección de datos de auditoría.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

En esta sección de la DPC, deben ser detalladamente descriptos los procedimientos definidos por el PCSC responsable y por las ARs vinculadas para la obtención y verificación de sus informaciones de archivo.

5.6 CAMBIO DE CLAVE

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

El PCSC debe cambiar su clave de acuerdo con el *tiempo de uso* y *tiempo operacional* de los certificados emitidos dentro de la ICPP, 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 ICPP para determinados usos, como se aprecia a continuación:

Tabla Nº 6 – Certificados emitidos en el marco de la ICPP

Tipo de Certificado	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado cualificado de firma, tributario y sello (F2, F3, S2 y S3)	4	4	El certificado emitido al titular o responsable del certificado es otorgado por un tiempo máximo de 4 (cuatro) años, al finalizar ese período pierde su validez.
Certificado cualificad	1	1	El certificado emitido al titular o responsable del certificado es otorgado por un tiempo máximo de 1 (un) año, al finalizar ese período pierde su validez.

o tributario (F1, S1)			
Certificado del PCSC	6	10	El Certificado emitido al PCSC tendrá un tiempo operacional de 10 (diez) años, que resulta de la suma del tiempo de uso de su certificado [6 (seis) años] más el tiempo de validez máximo del certificado emitido al usuario final [4 (cuatro) años]. Solamente durante el tiempo de uso de su certificado, el PCSC podrá emitir certificados a usuarios finales. En los años restantes del tiempo operacional, sólo podrá firmar o sellar la LCR de usuarios finales.

Certificado AC Raíz-Py	10	20	El certificado emitido a la AC Raíz-Py tendrá un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado [10 (diez) años] más el tiempo de validez máximo del certificado de un PCSC [10 (diez) años]. Solamente durante el tiempo de uso de su certificado, la AC Raíz-Py podrá emitir certificados a un PCSC. En los años restantes del tiempo operacional sólo podrá firmar o sellar la LCR de los PCSC.

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 LCR correspondiente y validar la cadena de confianza de la ICPP; el nuevo certificado emitido, será utilizado para emitir nuevos certificados y firmar la nueva lista de LCR.

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

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

En los siguientes ítems de la DPC deben ser descriptos los requisitos relacionados con los procedimientos de notificación y recuperación de desastres, previstos en la PCN del PCSC 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 27002/2022, para garantizar la continuidad de sus servicios críticos.

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

El PCSC 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 DPC deberá describir los procedimientos previstos en el PCN de las ARs vinculadas para la recuperación total o parcial de las actividades de las ARs, 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 DPC, deben ser descriptos los procedimientos de recuperación utilizados por el PCSC 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 DPC, deben ser descriptos los procedimientos de recuperación utilizados en caso de revocación del certificado del PCSC responsable.

5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

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

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

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

5.8 EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

En este ítem la DPC, debe describir los requisitos y los procedimientos que deberán ser adoptados en el caso de la extinción de servicios del PCSC responsable o de una AR, AV 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 PCSC responsable, deje de operar deberá cumplir, como mínimo, con lo siguiente:

a) solicitar a la AC Raíz-Py, con al menos un mes de anticipación la cancelación de sus suscripción en el registro público de PCSCs, 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 titulares o responsables de certificados por él emitidos, 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 DPC 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 PCSC, 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 PCSC.

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 PCSC, además publicará el cese de actividades o finalización del servicio del PCSC responsable en su sitio principal de Internet

6. CONTROLES TÉCNICOS DE SEGURIDAD

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

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

En los siguientes ítems, la DPC deberá definir las medidas de seguridad implementadas por el PCSC responsable para proteger su clave criptográfica y sus datos de activación, así como las claves criptográficas de los titulares de certificados emitidos por él. También se deben definir otros controles técnicos de seguridad utilizados por el PCSC y las ARs relacionadas en la ejecución de sus funciones operativas.

6.1.1. GENERACIÓN DEL PAR DE CLAVES

En este ítem, la DPC debe describir los requisitos y procedimientos referentes a los procesos de generación de las claves criptográficas del PCSC responsable. El par de claves criptográficas del PCSC responsable de la DPC deberá ser generado por el propio PCSC, posterior a la habilitación otorgada por la AC Raíz-Py vía resolución ministerial.

La DPC 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 un certificado. La DPC debe indicar como regla general que el PCSC no genera ni almacena las claves privadas asociadas a los certificados expedidos por él, que son generadas bajo el exclusivo control del titular o responsable del certificado, salvo en caso de su gestión en nombre del firmante o del creador del sello, en donde las claves privadas asociadas a los certificados son generadas y custodiadas por el módulo de activación de firma o sello del PCSC, de forma que el acceso a dichas claves se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante o creador del sello. Los procedimientos específicos deben ser descritos en cada PC implementada.

Cada PC implementado por la PCSC responsable debe definir el medio utilizado para almacenar la clave privada, en base a los requisitos aplicables establecidos por el documento *DOC-ICPP-04 [1]*.

La DPC debe indicar que el proceso de generación del par de claves del PCSC se realiza mediante hardware.

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

La DPC describirá los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada del PCSC responsable, en base a los requerimientos establecidos en el documento *DOC-ICPP-06 [5]*.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL TITULAR

La DPC debe indicar que la generación y guarda de la clave privada del PCSC será responsabilidad exclusiva del mismo.

El método de entrega de la clave privada al titular de certificado será establecido de acuerdo a cada tipo de certificado emitido por el PCSC y descripto en la PC correspondiente.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

En este ítem, la DPC debe describir los procedimientos utilizados por el PCSC responsable para la entrega de su clave pública a la AC Raíz-Py encargada de la emisión de su certificado. Para la generación del CSR por el PCSC, deberá adoptarse el formato definido en el documento**,** *DOC-ICPP-06 [5]*.

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

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA

En este ítem, la DPC debe definir las formas para la disponibilización del certificado del PCSC responsable, y de todos los certificados de la cadena de certificación, para los usuarios y las partes usuarias, 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-ICPP-06 [5]*;
b) un directorio;
c) una página WEB del PCSC; y
d) otros medios seguros aprobados por la AC Raíz-Py.

6.1.5. TAMAÑO DE LA CLAVE

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

Además, la DPC debe indicar que cada PC implementada por el PCSC responsable definirá el tamaño de las claves criptográficas asociadas a los certificados emitidos, en base a los requerimientos aplicables establecidos en el documento *DOC-ICPP-06 [5]*.

6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

La DPC debe prever que los parámetros para la generación de claves asimétricas del PCSC responsable adoptarán el estándar definido en el documento *DOC-ICPP-06 [5]*.

Los parámetros de verificación de calidad, deberán ser verificados de acuerdo con las normas establecidas en el documento *DOC-ICPP-06 [5]***.**

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

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

La clave privada del PCSC responsable deberá ser utilizada solamente para la firma o sello de los certificados por ella emitidos y de sus LCR.

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

En los ítems siguientes, la DPC debe definir los requisitos para la protección de las claves privadas del PCSC responsable. Las claves privadas deberán ser cifradas en el envío del módulo que lo generó al medio utilizado para su almacenamiento. Cuando aplique, la DPC debe también definir los requisitos para proteger las claves privadas de los titulares de certificados emitidos por el PCSC. Cada CP implementada debe describir los requisitos específicos aplicables.

6.2.1. ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

La DPC debe prever que el módulo criptográfico de generación de claves asimétricas del PCSC responsable adoptará las normas definidas en el documento *DOC-ICPP-06 [5]*.

La DPC debe también, cuando sea el caso, especificar las normas como, por ejemplo, aquellas definidas en el documento *DOC-ICPP-06 [5]*, requeridos para los módulos de generación de claves criptográficas de los titulares de certificados. Cada PC implementada debe especificar los requisitos adicionales aplicables.

6.2.2. CONTROL MULTIPERSONA DE LA 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 DPC debe establecer la exigencia de control multipersona para la utilización de la clave privada del PCSC responsable. Como mínimo serán requeridos 2 (dos) de "M" titulares de partición de clave, formalmente designada por el PCSC.

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

En este ítem, la DPC 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 DPC debe observar que, como directriz general, cualquier persona física o jurídica, titular de certificado, podrá, a su criterio, mantener una copia de seguridad de su propia clave privada.

El PCSC responsable de la DPC deberá mantener una copia de seguridad de su propia clave privada.

El PCSC responsable de la DPC no podrá almacenar, ni mantener una copia de seguridad, por sí o a través de un tercero, la clave privada del titular de un certificado emitido, salvo en caso de su gestión en nombre del firmante o del creador del sello. Cada PC deberá 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-ICPP-06 [5]* 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 DPC, debe indicarse que no podrán ser archivadas las claves privadas de las personas físicas o jurídicas titulares de certificados emitidos por el PCSC.

En este ítem también debe indicarse que las claves privadas del PCSC responsable deben ser archivadas por un periodo de 10 (diez) años después de la emisión del último certificado.

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 DPC, deben ser descritos los requisitos de transferencia de la clave privada del PCSC responsable de un módulo criptográfico a otro. La RFC 4210 o 6712 podrá ser utilizada para ese fin. Cada PC 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

Conforme al ítem 6.1

6.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la DPC deben ser descritos los requisitos y procedimientos necesarios para la activación de la clave privada del PCSC 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 PC implementada debe describir los requisitos y procedimientos necesarios para la activación de la clave privada de la persona física o jurídica titular del certificado.

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la DPC, deben ser descritos los requisitos y procedimientos necesarios para la desactivación de la clave privada del PCSC 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 PC implementada debe describir los requisitos y procedimientos necesarios para la desactivación de la clave privada de la de la persona física o jurídica titular del certificado.

6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

En este ítem de la DPC, deben ser descritos los requisitos y procedimientos necesarios para la destrucción de la clave privada del PCSC 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 PC

implementada debe describir los requisitos y procedimientos necesarios para la destrucción de la clave privada de la persona física o jurídica titular del certificado.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La DPC debe prever que las claves públicas del PCSC responsable y de los titulares de los certificados, así como las LCRs emitidas y sistemas de OCSP, serán almacenadas y gestionadas por el PCSC emisor, después de la expiración de los certificados correspondientes por un periodo de 10 (diez) años desde su última emisión, para la verificación de firmas o sellos generados durante su periodo de validez.

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

La clave privada del PCSC responsable de la DPC y de los titulares de certificados de firma o sello, tendrán un periodo operacional y periodo de uso conforme a la tabla N° 6 – Certificados emitidos en el marco de la ICPP 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 o sellos generados durante el plazo de validez de los respectivos certificados.

Cada PC implementada por el PCSC responsable debe definir el periodo máximo de validez del certificado que define, con base a los requisitos aplicables establecidos en esta DPC y en el documento *DOC-ICPP-04 [1]*.

6.4 DATOS DE ACTIVACIÓN

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

6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

El PCSC 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 PCSC responsable serán únicos.

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

Cada PC 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 DPC, 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 DPC debe prever que la generación del par de claves del PCSC responsable será realizada offline para impedir el acceso remoto no autorizado.

En este ítem, la DPC 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 PCSC responsable. Los requisitos específicos aplicables deben ser descriptos en cada PC implementada.

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

a) control de acceso a los servicios y perfiles del PCSC;
b) clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PCSC;
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 PCSC;
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 PCSC, 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 PCSC. Todos estos eventos deberán ser registrados con fines de auditoría.

Cualquier equipo incorporado en el PCSC 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 DPC, debe ser informado, cuando esté disponible, la calificación atribuida a la seguridad computacional del PCSC 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 DPC debe describir los requisitos de seguridad computacional de las estaciones de trabajo y de los computadores portátiles utilizados por la AR para los procesos de validación y aprobación de certificados.

Deben ser incluidos, por lo menos, los requisitos especificados en el documento *DOC-ICPP-05 [4]*.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

En los ítems siguientes de la DPC, deben ser descritos, cuando sea aplicable, los controles implementados por el PCSC responsable y por las AR 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 DPC, 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 PCSC responsable o cualquier otro software desarrollado o utilizado por el PCSC responsable.

Los procesos de proyecto y desarrollo llevados a cabo por el PCSC, deberán proveer documentación suficiente para soportar evaluaciones de seguridad externas de los componentes del PCSC.

6.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD

En este ítem de la DPC deben ser descriptos, las herramientas y los procedimientos empleados por el PCSC responsable y por las ARs 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 PCSC.

6.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

En este ítem, la DPC 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 LCR

Antes de su publicación, todas las LCR generadas por el PCSC, deben ser comprobadas en cuanto a la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de LCR, 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 DPC, deben ser descriptos los controles relativos a la seguridad de red del PCSC responsable, incluidos firewalls y recursos similares.

En los servidores del sistema de certificación del PCSC, 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 PCSC, 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 desarrollo o 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 PCSC.

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, LCR Y OCSP

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PCSC 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 PCSC responsable deberán implementar la versión 3 (tres).

7.1.2. EXTENSIONES DEL CERTIFICADO

La ICPP define como obligatorias las siguientes extensiones para los certificados del PCSC:

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 AC Raíz-Py que emite el certificado;

b) **Identificador de la clave del la persona física o jurídica titular del certificado** "***Subject Key Identifier*", no crítica:** debe contener el hash SHA-1 de la clave pública del PCSC titular del certificado;

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

d) **Directivas del Certificado "*Certificate Policies*", no crítica:**

d.1.1) el campo ***policyIdentifier*** debe contener los OIDs de las PCs implementadas por el PCSC titular del certificado, para la emisión de certificados de personas físicas o jurídicas;

d.1.2) el campo **policyQualifiers**

d.1.2.1 el campo ***CPS Pointer*** debe contener la dirección web de la DPC del PCSC que emite el certificado.

d.1.2.2 el campo User Notice debe decir: "Sujeta a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de [*nombre del PCSC*]"

e) **Restricciones Básicas** "***Basic Constraints*", crítica:**

e.1 el campo ***Subject Type*** debe contener CA=True

e.2 el campo ***PathLenConstraint*** debe tener valor cero;

f) **Puntos de distribución de las LCR** "**CRL Distribution Points", no crítica:**

f.1 el campo ***Distribution Point 1*** debe contener la dirección web donde se obtiene la LCR correspondiente al certificado.

g) **Acceso a la Información de la Autoridad Certificadora "Authority Information Access", no crítica:**

g.1.1 en el campo ***Access Method 1*** debe contener el identificador de método de acceso a la información de revocación (OCSP)

g.1.2 en el campo ***Access Location 1*** debe contener la dirección Web del servicio del OCSP

g.2.1 en el campo ***Access Method 2*** debe contener el identificador de método de acceso del certificado de la ACRaiz-Py

g.2.2 en el campo ***Access Location 2*** debe contener la dirección web donde se encuentra alojado el certificado de la ACRaiz-Py

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS

Los certificados del PCSC deberán ser firmados o sellados utilizando el algoritmo definido en el documento *DOC-ICPP-06 [5]*.

7.1.4. FORMAS DEL NOMBRE

7.1.4.1. El nombre del PCSC 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:

h) **OID=2.5.4.6 C= PY**;

i) **OID=2.5.4.10 O= Prestador Cualificado de Servicios de Confianza**;

j) **OID=2.5.4.11 OU= [***denominación o razón social de la persona física o jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación***]**;

k) **OID: 2.5.4.3 CN= [***siglas CA - seguido de la denominación o razón social de la física o persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación***]**; y

l) **OID: 2.5.4.5 Serial Number=[** *conforme al formato descripto en el ítem 3.1.4.1 de este documento***]**.

7.1.4.2. Excepcionalmente, para aquellos Prestadores de Servicios de Certificación habilitados por Leyes anteriores cuyo certificado se encuentre válido y vigente, deberán 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) **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].**

En caso de revocación o emisión de un nuevo certificado de PSC, esta excepción no podrá aplicarse por lo que el Prestador de Servicios de Certificación deberá indefectiblemente adoptar lo dispuesto en el ítem 7.1.4.1.

7.1.5. RESTRICCIONES DEL NOMBRE

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

7.1.6. OID (OBJECT IDENTIFIER) DE LA DPC

En este ítem se debe informar el OID de la DPC del PCSC responsable.

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 los certificados del PCSC, el campo ***policyQualifiers*** de la extensión "***Certificate Policies***" debe contener la dirección web (URL) de la DPC de la CA Raíz-Py que emite el certificado.

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 LCR

Las Listas de Certificados Revocados LCRs deberán ser firmadas o selladas utilizando el algoritmo definido en el documento *DOC-ICPP-06 [5]*.

7.2.1 NÚMERO (S) DE VERSIÓN

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

7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE LCR

En este ítem, la DPC debe describir todas las extensiones de LCR utilizadas por el PCSC responsable y su criticidad.

La AC Raíz-Py define las siguientes extensiones de LCR como obligatorias:

a) **Identificador de la clave de la Autoridad Certificadora *"Authority Key Identifier" no crítico:*** debe contener el hash SHA-1 de la clave pública del PCSC que firma o sella la LCR;
b) ***Número de LCR "CRL Number" no crítico:*** debe contener un número secuencial para cada LCR emitida por el PCSC; y
c) **Puntos de Distribución del Emisor "Issuing Distribution Point" crítico:** debe contener la dirección Web donde se obtiene la LCR correspondiente al certificado.

7.3 PERFIL DE OCSP

Los servicios de respuestas OCSP deberán implementar la versión 1 de la norma ITU X.509 de acuerdo con el perfil establecido en el RFC 6960. Los mismos deben ser firmados o sellados utilizando el algoritmo definido en el documento *DOC-ICPP-06 [5]*.

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 el RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

En este ítem la DPC debe indicar que los PCSC serán auditados, al menos cada veinticuatro (24) meses, corriendo con los gastos que ello genere, por un OEC. La finalidad de la auditoría es confirmar que tanto los PCSC, como los servicios de confianza cualificados que prestan cumplen con los requisitos establecidos en esta DPC y en la normativa vigente. Los PCSC enviarán el informe de evaluación de la conformidad correspondiente a la AC Raíz-Py en el plazo de 3 (tres) días hábiles tras su recepción.

Sin perjuicio de lo dispuesto en el párrafo anterior, la AC Raíz-Py podrá en cualquier momento auditar o solicitar a un OEC que realice una evaluación de conformidad de los PCSC, corriendo con los gastos dichos PCSC, para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos de esta DPC y de la normativa vigente.

Además cada PCSC, deberá implementar un programa de auditorías internas conforme a lo estipulado en el ítem 18 "cumplimiento" de la norma ISO 27002/2022 para la verificación de su sistema de gestión.

Cuando la AC Raíz-Py requiera a un PCSC que corrija el incumplimiento de requisitos de esta DPC o de la normativa vigente, y este prestador no actúe en consecuencia, en su caso, en el plazo fijado por la AC Raíz-Py, la AC Raíz-Py, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, puede retirar la cualificación al prestador o al servicio que este presta y actualizar la lista de confianza. La AC Raíz-Py comunicará al PCSC la retirada de su cualificación o de la cualificación del servicio de que se trate.

Tales supervisiones deberán ser efectuadas conforme a las disposiciones en materia de auditoría, reglamentadas por la AC Raíz-Py.

Todo PCSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la ICPP.

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

8.2 IDENTIDAD / CALIDAD DEL EVALUADOR

En este ítem, la DPC 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 DPC 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.

La AC Raíz-Py, aplicará el procedimiento de acreditación de los OEC conforme al *DOC-ICPP-11 [6]* para la recepción del informe de evaluación de la conformidad y respecto a las disposiciones en materia de auditoría con arreglo a las cuales los OEC realizarán la evaluación de la conformidad de los PCSC se regirán conforme al *DOC-ICPP-12 [7]* Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP.

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Las inspecciones y auditorías realizadas en el ámbito de la ICPP tienen como objetivo verificar si los procesos, procedimientos y actividades de las entidades que componen la ICPP están en cumplimiento de sus respectivos DPC, PC, PSS y demás normas y procedimientos establecidos por ICPP.

En este punto de la DPC, el PCSC responsable debe informar que ha recibido una auditoría previa por parte del OEC para fines de habilitación por parte de la AC Raíz-Py y que es auditado al menos cada veinticuatro (24) meses, con el objetivo de mantener la habilitación con base en lo establecido en los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP *DOC-ICPP-12 [7]*. Este documento aborda el objetivo, la frecuencia y el alcance de las auditorías, la identidad y las calificaciones del auditor y otros temas relacionados.

En este ítem de la DPC, el PCSC responsable debe informar que las entidades del ICPP directamente vinculados él (AV, AR y PSS), también recibieron una auditoría previa, por parte del OEC para fines de habilitación por parte de la AC Raíz-Py, y que es auditado que es auditado conforme a lo establecido en el párrafo anterior.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

De acuerdo con los Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP (*DOC-ICPP-17 [3)]* y con los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP (*DOC-ICPP-12 [7]).*

8.6 COMUNICACIÓN DE RESULTADOS

De acuerdo con los Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP (*DOC-ICPP-14 [8])* y con los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP (*DOC-ICPP-12 [7]).*

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

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

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Las tarifas para la emisión y renovación de certificados por la AC Raíz-Py de la ICPP para los PCSC están definidas en el documento Directrices de la Política Tarifaria de la AC Raíz-Py de la ICPP (*DOC-ICPP-13 [9]*) .

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 DPC se debe informar sobre políticas de reembolso en el caso que las apliquen.

9.2 RESPONSABILIDAD FINANCIERA

En este ítem de la DPC 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 DPC debe describir los aspectos relativos a la cobertura de seguro que posee el PCSC 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 LAS PERSONAS FÍSICAS O JURÍDICAS TITULARES DE CERTIFICADOS

En este ítem de la DPC, en el caso que aplique, deben describirse los aspectos relativos a la cobertura de seguro o garantía disponible para los titulares de certificados emitidos por el PCSC. En el caso que sean aplicadas cobertura de seguro o garantía para titulares de certificados específicos para las PCs implementadas, las mismas deben ser descriptas en las PCs, 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 PCSC responsable de la DPC y de sus ARs y AVs vinculadas, de acuerdo con las normas, criterios, prácticas y procedimientos de la ICPP.

La DPC debe establecer, como principio general, que ningún documento, información o registro entregado al PCSC o a las ARs, y VAs 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 PCSC responsable de la DPC y por las AR, AV a ellas vinculadas, los cuales deberán comprender, entre otros:

a) los certificados y las LCRs/OCSPs emitidos por el PCSC;
b) las PCs implementadas por el PCSC;
c) la DPC del PCSC;y
d) la conclusión de los informes de auditoría.
e) Versión pública de la PS

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

El PCSC también podrá divulgar, de forma consolidada o segmentada por tipo de certificado, el número de certificados emitidos en el ámbito de ICPP.

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

La DPC deberá informar que los titulares de certificados de firma electrónica cualificada, tributario o a los responsables por el uso de certificados cualificados de sello electrónico, tendrán la tarea 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 que un PCSC habilitado brinde servicios de generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello, debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación de firma se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Si existen responsabilidades específicas para las PCPs implementadas, las mismas deben ser descriptas en dichas PCs, en el ítem correspondiente.

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

En este ítem de la DPC, el PCSC 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 DPC se debe indicar que cualquier información acerca de los titulares o responsables de certificados 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 DPC 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 LCR/OCSP.

9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

En este ítem de la DPC, se debe indicar que el PCSC y la AR vinculada son responsables de la divulgación indebida de información privada, por lo que deben 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 PCSC podrá ser utilizada o divulgada a terceros, previa notificación al titular o responsable del certificado y con su autorización expresa.

El titular o responsable del certificado 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 o sellos válidos garantizados por un certificado reconocido por la ICPP; o
b) mediante solicitud por escrito con firma autenticada.

9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

En este ítem de la DPC, 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 DPC.

9.5. DERECHO DE PROPIEDAD INTELECTUAL

Según legislación vigente.

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DEL PCSC

En este ítem de la DPC el PCSC debe indicar que el marco de prestación de servicios de creación, verificación y validación de firmas electrónicas cualificadas y/o sello electrónico cualificado y certificados relativos a estos servicios, 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 dichos servicios.

El PCSC declara y garantiza lo siguiente:

9.6.1.1. AUTORIZACIÓN PARA CERTIFICADO

En este ítem el PCSC debe indicar que implementa procedimientos para verificar la autorización de emisión de un certificado en el marco de la ICPP, contenido en los ítems 3 y 4 de esta DPC. El PCSC, dentro del alcance de la autorización de emisión de un certificado, analiza, audita e inspecciona los procesos de la AR conforme a sus DPC, PCs y normas complementarias.

9.6.1.2. PRECISIÓN DE LA INFORMACIÓN

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

9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO

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

9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO

En este ítem la DPC debe indicar que el PCSC implementa un *contrato de prestación de servicio de confianza* para la expresión del consentimiento del titular de certificado, de conformidad a lo establecido en los puntos 3 y 4 de esta DPC.

9.6.1.5. SERVICIO

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

9.6.1.6. REVOCACIÓN

En este ítem de la DPC, el PCSC debe indicar que revocará los certificados de la ICPP por cualquier motivo especificado en este documento.

9.6.1.7. EXISTENCIA LEGAL

En este ítem, el PCSC deberá indicar que la DPC se ajusta a las disposiciones de la Ley Nº 6822/2021 sus modificaciones y reglamentaciones.

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA AR

Aplícase conforme al ítem 4 de esta DPC.

9.6.3. REPRESENTACIONES Y GARANTÍAS DEL TITULAR DE CERTIFICADO

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

El PCSC debe informar a la AC 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 USUARIAS

Constituyen derechos de la parte usuaria:

a) negarse a utilizar el certificado para fines distintos de los previstos en esta DPC; y
b) verificar, en cualquier momento, la vigencia del certificado.

El certificado del PCSC se considera válido cuando:

a) ha sido emitido por la AC Raíz-Py;
b) no aparece como revocado por la AC Raíz-Py;
c) no ha expirado; y
d) puede ser verificado utilizando el certificado válido de la AC Raíz-Py.

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

9.6.5. 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 DPC, el PCSC deberá indicar que en el marco de su actividad como PCSC la limitación de su responsabilidad será conforme a las disposiciones de la Ley Nº 6822/2021, sus modificaciones y reglamentaciones.

9.9. INDEMNIZACIONES

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

9.10. PLAZO Y FINALIZACIÓN

9.10.1. PLAZO

En este ítem, se debe establecer que la DPC entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AC Raíz-Py.

9.10.2. FINALIZACIÓN

Esta DPC tendrá una vigencia indefinida, manteniéndose vigente y eficaz hasta que sea revocada o sustituida, expresa o tácitamente.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Los actos realizados durante la vigencia de esta DPC son válidos y eficaces a todos los efectos legales, produciendo efectos incluso después de su revocación o sustitución.

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Las notificaciones, citaciones, solicitudes o cualquier otra comunicación necesaria sujeta a las prácticas descritas en la presente DPC se realizarán, preferentemente, mediante sistema de información firmado o sellado electrónicamente, o, en su defecto, mediante oficio de la autoridad competente.

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

En este ítem de la DPC se debe indicar el procedimiento para enmiendas y que propuestas de modificación de la DPC deben ser revisadas y aprobadas por la AC Raíz-Py 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 DPC. Toda enmienda o modificación de la DPC, deberá ser publicada en el repositorio del PCSC.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

En este ítem de la DPC se debe indicar que los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OIDs 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, debe indicar que las controversias derivadas de la presente DPC se resolverán de conformidad con la legislación vigente. Debe también establecerse que la DPC del PCSC responsable no prevalecerá sobre las normas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.

9.14. NORMATIVA APLICABLE

Esta DPC se rige por la legislación de la República del Paraguay, en particular por la Ley Nº 6822/2021, 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 DPC se adecua a la legislación aplicable y que el PCSC 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 o responsables de certificados y las partes usuarias que confían en los certificados asumen en su totalidad el contenido de la presente DPC y PC.

Esta DPC representa las obligaciones y deberes aplicables al PCSC y autoridades vinculadas.

En caso de conflicto entre esta DPC y otras resoluciones de la AC Raíz-Py, prevalecerá siempre la última editada.

9.16.2. ASIGNACIÓN

Los derechos y obligaciones previstos en esta DPC son públicos e indisponibles, y no pueden ser cedidos o transferidos a terceros.

9.16.3. DIVISIBILIDAD

La invalidez, nulidad o ineficacia de cualquiera de las disposiciones de esta DPC no perjudicará las demás disposiciones, que seguirán siendo plenamente válidas y efectivas. En este caso, la disposición inválida, nula o ineficaz se tendrá por no escrita, por lo que la presente DPC se interpretará como si no la contuviera y, en la medida de lo posible, manteniendo la intención original de las restantes disposiciones.

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

De acuerdo con la legislación vigente.

9.16.5. FUERZA MAYOR

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

9.17. OTRAS DISPOSICIONES

Éste ítem no aplica.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIA EXTERNA

- Ley Nº 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos."
- 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 27002:2022:" - 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".

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

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 Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-04
[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación del PCSC que genera o gestiona datos de creación de firma electrónica y/o de sello electrónico.	DOC-ICPP-07
[3]	Procedimiento de identificación del solicitante de certificados por videoconferencia en la ICPP	DOC-ICPP-17
[4]	Características mínimas de seguridad para las autoridades de registro de la ICPP.	DOC-ICPP-05
[5]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[6]	Guía para la acreditación de los organismos de evaluación de la conformidad	DOC-ICPP-11

[7]	Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP	DOC-ICPP-12
[8]	Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP	DOC-ICPP-14
[9]	Directrices de la Política tarifaria de la AC Raíz-Py	DOC-ICPP-13