POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DE LA ICPP

Ministerio de Industria y Comercio
Dirección General de Comercio Electrónico

DOC-ICPP-01
Versión 2.0

CONTROL DE CAMBIOS

Versión	Fecha	Descripción
1.0	04/08/2022	Versión inicial alineada a la Ley N.º 6822/2021.
2.0	02/07/2026	Versión consolidada de la PC/DPC que actualiza el alcance, la estructura y el contenido, controles armonizados con la Ley N.º 6822/2021, referencias RFC/ETSI/NIST/FIPS/ISO/IEC y anexos.

CONTENIDO

1. INTRODUCCIÓN

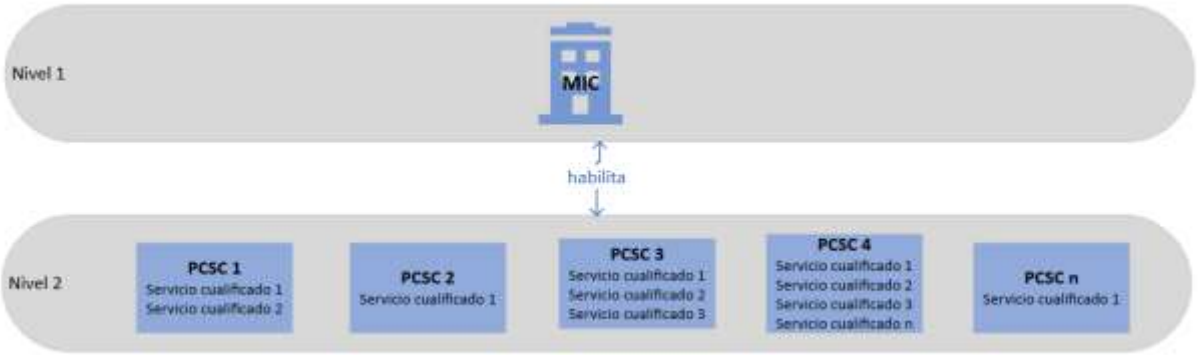
1.1. Visión general

La Infraestructura de Clave Pública del Paraguay (ICPP) constituye el conjunto organizado de políticas, normas, procedimientos, controles técnicos, medidas de seguridad y mecanismos de supervisión destinados a sustentar la confianza en la emisión, gestión, validación, revocación y publicación de certificados electrónicos, en el marco de los servicios cualificados de confianza regulados por la Ley N.º 6822/2021, su reglamentación y la normativa técnica dictada por el Ministerio de Industria y Comercio (MIC), por intermedio de la Dirección General de Comercio Electrónico (DGCE), en su carácter de Autoridad de Aplicación (AA).

Esta Política y Declaración de Prácticas de Certificación - PC/DPC describe las prácticas y procedimientos empleados por la ACR-Py de la ICPP en la ejecución de sus funciones.

La operación de la ACR-Py se realiza a través de la Dirección General de Comercio Electrónico (DGCE), conforme a la normativa aplicable.

La ACR-Py posee certificados de nivel superior dentro de la ICPP. Dichos certificados contienen las claves públicas correspondientes a las claves privadas utilizadas para firmar sus propios certificados, los certificados de los PCSC de nivel inmediatamente subsecuente y las Listas de Certificados Revocados - CRL/LCR. En consecuencia, la cadena de certificación tiene como máximo dos niveles; en el primer nivel se encuentra la ACR-Py, en el segundo nivel, se ubican los PCSC habilitados, y éstos a su vez solo podrán emitir certificados a personas físicas y/o jurídicas, generando de esta manera una estructura jerárquica como se muestra en la siguiente figura:



La estructura de esta PC/DPC está basada en el RFC 3647 – Certificate Policy and Certification Practices Framework.

1.2. Nombre e identificación del documento

Este documento se denomina “POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DE LA ICPP” y es identificado como DOC-ICPP-01.

El presente documento consolida, en un único instrumento, la Política de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC) de la ACR-Py de la ICPP.
A los efectos de identificación dentro de la jerarquía de certificación y de su vinculación con los objetos asociados, la ACR-Py utiliza el siguiente arco institucional de identificadores de objeto (OID):

a. Arco institucional base: 1.3.6.1.4.1.64751;
b. OID de la PC/DPC de la ACR-Py: 1.3.6.1.4.1.64751.1.1;

1.3. Participantes de la ICPP

A los efectos de este documento, los participantes de la ICPP se clasifican en las siguientes categorías:

a. Autoridades Certificadoras o de Certificación;
b. Autoridades de Registro;
c. Titulares del certificado;
d. Parte Usuaria;
e. Otros participantes.

1.3.1 Autoridades Certificadoras o de Certificación

Las autoridades de certificación o autoridades certificadoras (AC) son las entidades responsables de emitir, firmar, gestionar, revocar y publicar certificados electrónicos dentro de la ICPP.
Esta PC/DPC se refiere exclusivamente a la ACR-Py.

1.3.2 Autoridades de Registro

No aplica en la operativa de la ACR-Py.

1.3.3 Titulares de certificado

Los certificados electrónicos emitidos por la ACR-Py tienen como titulares a la propia ACR-Py (certificado autofirmado) o a los PCSC habilitados por la AA.

1.3.4 Parte Usuaria

Se considera Parte Usuaria (PU) a la persona física o jurídica que confía en un certificado electrónico emitido dentro de la ICPP, incluyendo la información contenida, su estado de validez y su aplicabilidad.

1.3.5 Otros participantes

El ecosistema de la ICPP integra participantes auxiliares que incluyen:

a. Los Organismos de Evaluación de la Conformidad (OEC) encargados de auditorías técnicas,
b. Los Prestadores de Servicios de Soporte (PSS) que asisten operativamente bajo documentación formal y controles estrictos, y
c. Otras entidades necesarias para el funcionamiento seguro de la infraestructura.

1.4. Uso del certificado

1.4.1 Usos apropiados del certificado

Los certificados electrónicos emitidos por la ACR-Py tienen como objetivo identificar a la propia ACR-Py o a los PCSC habilitados dentro de la ICPP y poner a disposición sus claves públicas de forma segura.

1.4.2 Usos prohibidos del certificado

Los certificados electrónicos emitidos por la ACR-Py no podrán utilizarse para:

a) la emisión directa de certificados electrónicos a usuarios finales;

b) la firma directa de documentos electrónicos, transacciones o actuaciones de usuarios finales;

c) la identificación o autenticación de personas físicas o jurídicas ajenas a su función de certificación raíz;

d) la prestación directa de servicios cualificados de confianza distintos del rol que corresponde a la ACR-Py como Autoridad Certificadora Raíz; y

e) cualquier otro uso que exceda su función de establecer y preservar la confianza superior de la infraestructura.

1.5. Administración de la política y del documento

La AA y la ACR-Py constituyen funciones diferenciadas dentro del MIC, con segregación de competencias y responsabilidades documentadas conforme a los actos administrativos internos vigentes. La AA ejerce las facultades regulatorias y de supervisión previstas en el Art. 98 de la Ley N.° 6822/2021; la ACR-Py opera la jerarquía técnica de certificación bajo la presente PC/DPC. Toda referencia a actos de una u otra debe entenderse en el marco de dicha distinción funcional, sin perjuicio de su unidad institucional.

1.5.1 Organización que administra el documento

Nombre: Ministerio de Industria y Comercio (MIC) - Dirección General de Comercio Electrónico (DGCE).

1.5.2 Persona o punto de contacto

El punto de contacto institucional para todas las consultas, comunicaciones y solicitudes relacionadas con este documento es el Director General de la DGCE del MIC, en su carácter de autoridad responsable dentro de la AA de la ICPP.

Dirección DGCE: Cap. Pedro Villamayor esquina Cap. Nicolás Blinoff (Edif. Ventanilla Única de Exportación, 1er. piso), Barrio Villa Aurelia, Asunción, Paraguay.

Teléfono: +595-(987)-333340/42 o +595-(987)-333360/62

Correo electrónico: info-dgfdce@mic.gov.py

Página web: https://www.acraiz.gov.py/

1.5.3 Persona que determina la adecuación de la DPC con la PC.

La DGCE es responsable de determinar la adecuación de la presente PC/DPC, en su carácter de órgano técnico competente de la AA.

1.5.4 Procedimientos de aprobación de la DPC

Este documento es aprobado mediante Resolución por el MIC a través de la DGCE, en su carácter de AA de la Ley N.º 6822/2021 para identificar las políticas, prácticas y procedimientos de la ACR-Py. Sus modificaciones o enmiendas se rigen por el ítem 9.12.

1.6. Definiciones y acrónimos

1.6.1 Definiciones

A los efectos de este documento, las expresiones utilizadas se interpretan conforme a la Ley N.º 6822/2021, a su reglamentación y, supletoriamente, conforme a los estándares técnicos y perfiles de referencia aplicables a la ICPP. El marco jurídico paraguayo prevalece sobre tales estándares conforme a la regla de interpretación establecida en el ítem 9.15.

a. **Autoridad de Aplicación (AA):** el Ministerio de Industria y Comercio, por intermedio de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios, en el ámbito de las competencias previstas en la Ley N.º 6822/2021 y en su reglamentación.

b. **Autoridad Certificadora Raíz del Paraguay (ACR-Py):** órgano técnico de la Infraestructura de Clave Pública del Paraguay, encargado de preservar la confianza raíz de la ICPP, emitir y gestionar su certificado raíz autofirmado, emitir certificados a los Prestadores Cualificados de Servicios de Confianza habilitados. Las funciones de la ACR-Py son ejercidas por la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios del Ministerio de Industria y Comercio.

c. **Cambio de clave:** la sustitución de un par de claves por un nuevo par de claves y la emisión del certificado correspondiente, conforme a este documento.

d. **Ceremonia criptográfica:** el acto formal, controlado, documentado y auditable mediante el cual se ejecutan operaciones críticas sobre material criptográfico, incluyendo, entre otras, generación, activación, respaldo, recuperación, sustitución o destrucción.

e. **Certificado electrónico**: el conjunto de datos electrónicos vinculados a una persona física, jurídica, servicio, sitio web, sello o autoridad de certificación, emitido conforme a la normativa aplicable y destinado a probar una vinculación de identidad, función, atributo o confianza.

f. **Certificado electrónico raíz:** el certificado electrónico autofirmado de la ACR-Py que constituye el ancla superior de confianza de la ICPP.

g. **CRL/LCR:** lista de certificados revocados emitida por la ACR-Py conforme al perfil técnico aplicable y publicada en el repositorio público oficial de la ICPP.

h. **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.

i. **Infraestructura de Claves Públicas del Paraguay (ICPP):** 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.

j. **Material criptográfico:** las claves privadas, componentes de activación, módulos criptográficos, dispositivos de creación de firmas o sellos electrónicos, respaldos, evidencias y demás elementos cuya afectación comprometería o podría comprometer la seguridad o continuidad de la certificación raíz.

k. **Organismo de Evaluación de la Conformidad (OEC):** 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 N.º 6822/2021.

l. **Parte Usuaria (PU):** la persona física o jurídica que confía en la validez de un certificado electrónico emitido dentro de la ICPP y que utiliza la información contenida en dicho certificado para verificar su autenticidad, integridad, procedencia, vigencia o estado de revocación.

m. **Política criptográfica:** el conjunto de criterios, parámetros, algoritmos, tamaños de clave, funciones hash, restricciones y reglas de transición criptográfica aplicables a la ACR-Py y, en lo pertinente, a los certificados emitidos a PCSC.

n. **Política de Certificación (PC):** 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.

o. **Prestador Cualificado de Servicios de Confianza (PCSC):** 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.

p. **Prestador de servicios de confianza:** una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.

q. **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 autorizado por el MIC para desempeñar actividades descritas en la DPC o en una PC.

r. **Repositorio público oficial:** el sitio y conjunto de recursos administrados por la ACR-Py para la publicación oficial de la información de certificación de la ICPP.

s. **Rol de confianza:** función crítica dentro de la ACR-Py, desempeñada por su personal o por terceros autorizados, independientemente de su vínculo laboral, cuyo desempeño

puede influir directamente en la seguridad, integridad y confiabilidad de la ICPP y de los servicios de confianza, de modo que su ejecución inadecuada podría comprometer la confianza en la Autoridad de Certificación.

t. **Servicio de confianza cualificado:** el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas cualificadas, sellos electrónicos cualificados, sellos cualificados de tiempo electrónicos, servicios cualificados de entrega electrónica certificada y certificados relativos a estos servicios, y/o b) la creación, verificación y validación de certificados cualificados para la autenticación de sitios web, y/o c) la preservación de firmas, sellos o certificados cualificados electrónicos relativos a estos servicios, d) servicio de expedición de medios de identificación en virtud a sistemas de identificación electrónica con nivel de seguridad alto.

u. **Titular de certificado:** la persona física, jurídica o entidad a cuyo nombre se emite un certificado electrónico y que acepta las condiciones aplicables a su emisión, uso, renovación, cambio de clave o revocación.

1.6.2 Acrónimos

Sigla	Descripción
AA	Autoridad de Aplicación
AC	Autoridad Certificadora
ACR-Py	Autoridad Certificadora Raíz del Paraguay
AIA	Authority Information Access
AR	Autoridad de Registro
CRL/LCR	Certificate Revocation List / Lista de Certificados Revocados
CSR	Certificate Signing Request
DGCE	Dirección General de Comercio Electrónico
DN	Distinguished Name
DPC	Declaración de Prácticas de Certificación
HSM	Hardware Security Module
ICPP	Infraestructura de Clave Pública del Paraguay
MIC	Ministerio de Industria y Comercio
OCSP	Online Certificate Status Protocol
OEC	Organismo de Evaluación de la Conformidad
OID	Object Identifier
PC	Política de Certificados
PC/DPC	Política y Declaración de Prácticas de Certificación
PCSC	Prestador Cualificado de Servicios de Confianza
PCN	Plan de Continuidad de Negocio

PKI	Public Key Infrastructure
PSS	Prestador de Servicios de Soporte
PU	Parte Usuaria
RFC	Request for Comments
RPO	Recovery Point Objective
RTO	Recovery Time Objective

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

La ACR-Py publica en su repositorio oficial los certificados electrónicos por ella emitidos, sus CRL/LCR y la documentación aplicable a la certificación raíz de la ICPP.

2.1. Repositorios

El repositorio oficial de la ACR-Py está disponible para consulta pública en https://www.acraiz.gov.py durante las veinticuatro (24) horas del día, los siete (7) días de la semana.

2.2. Publicación de información de certificación

La ACR-Py publica, como mínimo:

a. el certificado electrónico raíz vigente de la ACR-Py y, cuando corresponda, los certificados electrónicos raíz anteriores;

b. los certificados electrónicos emitidos por la ACR-Py a los PCSC, incluyendo los certificados vigentes y, cuando corresponda, los históricos necesarios para la validación de la cadena de certificación;

c. la Lista de Confianza de la ICPP, con la identificación de los PCSC habilitados;

d. las CRL/LCR emitidas por la ACR-Py;

e. la presente PC/DPC y sus versiones vigentes o históricas, cuando su conservación pública resulte aplicable;

f. los documentos técnicos, anexos, perfiles, parámetros operativos y demás instrumentos normativos o informativos;

g. la información de contacto institucional aplicable a la operación de la ACR-Py;

2.3. Tiempo o frecuencia de publicación

Los certificados electrónicos de la ACR-Py y de los PCSC se publican inmediatamente después de su emisión y se mantienen disponibles para validación y auditoría, conservando un registro histórico claramente diferenciado de las versiones vigentes. Por su parte, la frecuencia de emisión y publicación de las CRL/LCR se rige por los ítems 4.9.7, 4.9.8 y 4.10. Además, la ACR-Py publica y actualiza de inmediato las normativas, la información institucional y la Lista de Confianza ante cualquier modificación.

2.4. Controles de acceso a los repositorios

No existen restricciones para la consulta de la información disponible en el repositorio oficial. La modificación, actualización o publicación de información se restringe al personal autorizado por la ACR-Py.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

La ACR-Py verifica la autenticidad de la identidad y, cuando corresponda, de los atributos de los participantes de la ICPP antes de la emisión de certificados electrónicos.

3.1. Nombres

3.1.1 Tipos de nombres

Los titulares de certificados emitidos por la ACR-Py deberán poseer nombres que los identifiquen unívocamente dentro de la ICPP. La identificación se realizará mediante *Distinguished Names* (DN), conforme a la Recomendación ITU-T X.501, con atributos seleccionados según la Recomendación ITU-T X.520, codificados en ASN.1 (ITU-T X.680 y X.690 — DER) e incorporados a los certificados conforme a la Recomendación ITU-T X.509 v3 y al perfil RFC 5280.´

3.1.2 Necesidad de que los nombres sean significativos

Todos los certificados emitidos por la ACR-Py deberán incluir un nombre que identifique suficientemente al titular del certificado, conforme al perfil aplicable. Ver Anexos I - PERFIL DEL CERTIFICADO ELECTRÓNICO RAÍZ y Anexo II - PERFIL DE CERTIFICADOS ELECTRÓNICOS EMITIDOS A PCSC.

3.1.3 Anonimato o seudónimo de los titulares de certificado

No aplica.

3.1.4 Reglas para interpretar distintas formas de nombres

Los *Distinguished Names* (DN) presentes en los certificados emitidos bajo la ICPP se interpretarán conforme a:

a. las reglas de denominación y de comparación (*matching rules*) establecidas en la Recomendación ITU-T X.501;

b. las sintaxis y reglas de igualdad por atributo definidas en la Recomendación ITU-T X.520;

c. las disposiciones sobre tipos de cadenas, codificación y comparación de nombres establecidas en el RFC 5280 (en particular, ítems 4.1.2.4, 4.1.2.6 y 7);

d. la codificación ASN.1 DER conforme a las Recomendaciones ITU-T X.680 y X.690; y

e. los perfiles específicos de nombres definidos en los Anexos I y II del presente instrumento.

3.1.5 Unicidad de nombres

Los *Distinguished Names* (DN) deberán ser únicos para cada PCSC inmediatamente jerárquico a la ACR-Py dentro de la ICPP.

Para asegurar dicha unicidad, podrán incorporarse números, letras u otros atributos diferenciadores al DN, conforme a las Recomendaciones ITU-T X.501 y X.520 y al perfil del RFC 5280.

No se admitirá el uso de los campos subjectUniqueID ni issuerUniqueID (extensión "*Unique Identifiers*" del estándar ITU-T X.509) para diferenciar PCSC con nombres idénticos, en consonancia con los ítems 4.1.2.7 y 4.1.2.8 del RFC 5280.

3.1.6 Procedimiento para resolver disputas de nombres

La ACR-Py se reserva el derecho de decidir, de forma fundada y motivada, sobre toda disputa relacionada con los nombres utilizados en los certificados emitidos a los PCSC inmediatamente jerárquicos a su nivel dentro de la ICPP.

Durante el proceso de autenticación previsto en el ítem 3.2, el PCSC solicitante deberá acreditar fehacientemente su derecho o legitimación para el uso del nombre propuesto (DN), conforme a la legislación nacional aplicable.

3.1.7 Reconocimiento, autenticación y rol de las marcas registradas

Los PCSC no podrán solicitar certificados cuyo contenido vulnere derechos de propiedad intelectual, marcas registradas, nombres comerciales, denominaciones de origen u otros signos distintivos de terceros, conforme a la legislación nacional aplicable.

No corresponde a la ACR-Py verificar la titularidad ni el derecho de uso del solicitante respecto de marcas registradas, nombres comerciales o signos distintivos. La ACR-Py no asume función constitutiva ni declarativa respecto de tales derechos, los que se rigen por la legislación específica y por la competencia de la Dirección Nacional de Propiedad Intelectual (DINAPI).

La ACR-Py se reserva el derecho de rechazar la emisión o de revocar cualquier certificado cuando el nombre utilizado resulte improcedente, engañoso o falaz, o cuando se encuentre controvertido de forma fundada, exista resolución de autoridad competente o controversia judicial o administrativa pendiente respecto del mismo.

3.2. Validación inicial de identidad

Dado que la ACR-Py actúa como Autoridad Certificadora Raíz, este proceso se aplica exclusivamente a PCSC que operen como AC subordinadas.

De conformidad con la Ley N.º 6822/2021, el PCSC podrá ser una Persona Física o una Persona Jurídica. En consecuencia, los procesos de validación de identidad se adecuarán a la naturaleza del solicitante.

La ACR-Py realiza la identificación del solicitante a través de medios legales, administrativos, documentales o técnicos suficientes para identificar de forma fehaciente a la persona física o jurídica interviniente.

La validación inicial de identidad constituye un proceso previo e independiente de la solicitud técnica de certificación. En particular, no se limita al análisis del Certificate Signing Request (CSR), el cual contiene información declarativa y técnica (clave pública y datos del sujeto), pero no constituye por sí mismo prueba de identidad.

Este proceso tiene por finalidad garantizar la veracidad, exactitud y legitimidad de la información que será incorporada en el certificado electrónico.

3.2.1 Método para probar posesión de la clave privada

La ACR-Py verifica que el PCSC solicitante posee la clave privada correspondiente a la clave pública cuya certificación se solicita, como condición previa a la emisión del certificado electrónico.
Se exceptúa el certificado raíz autofirmado de la propia ACR-Py, respecto del cual la posesión resulta inherente al proceso de generación, custodia y autoemisión realizado durante la Ceremonia de Constitución o de Generación de claves de la Autoridad Certificadora Raíz del Paraguay conforme a los controles previstos en el ítem 5 del presente documento.

La prueba de posesión (*Proof-of-Possession* – POP) se realiza mediante mecanismos criptográficos auditables y consistentes con el perfil del certificado, el algoritmo utilizado y el procedimiento de solicitud aplicable, adoptando como referencias técnicas el RFC 4211 para solicitudes en Formato de Mensaje de Solicitud de Certificado (CRMF), el RFC 2986 para solicitudes en formato PKCS#10, el RFC 9810 para el Protocolo de Gestión de Certificados (CMP) y, cuando corresponda, el RFC 9811 para el transporte de CMP sobre HTTP, o las normas que los modifiquen o sustituyan.

La intervención de funcionarios de la DGCE en estos actos comprende, cuando corresponda:

a) la presencia en Ceremonia de Constitución o de Generación de Claves del PCSC;
b) la verificación de la correspondencia entre la solicitud y el material criptográfico presentado;
c) la constatación de la ejecución del mecanismo de prueba de posesión; y
d) la validación de las evidencias, actas o registros que documenten el proceso.

La documentación, registros, actas, evidencias técnicas y demás antecedentes generados durante el proceso de prueba de posesión de clave privada se conservarán conforme a las reglas de trazabilidad, conservación de registros y auditabilidad establecidas en la presente PC/DPC.

3.2.2 Autenticación de la identidad de la organización (Persona Jurídica u Organismos o Entidades del Estado)

Previo a la emisión de cualquier certificado, la ACR-Py ejecuta un proceso formal de validación de identidad del solicitante considerando su naturaleza como Persona Física o Persona Jurídica.

El proceso de validación incluye, según corresponda

a. Revisión de documentación legal que acredite la existencia de la entidad (estatutos, registros públicos, etc.).
b. Verificación de la identidad de los representantes legales mediante documentación oficial vigente.
c. Validación de las facultades de representación.
d. Evaluación del cumplimiento de los requisitos técnicos, organizativos y de seguridad exigidos por la normativa aplicable.
e. Verificación de la correspondencia entre la identidad de la entidad del solicitante y los datos consignados en la solicitud.

Este proceso se realiza independientemente de la generación del par de claves criptográficas y de la presentación del Certificate Signing Request (CSR), el cual constituye únicamente un insumo técnico para la emisión del certificado.

La ACR-Py conservará evidencia documental del proceso de validación realizado, conforme a las políticas de auditoría y archivo establecidas.

Ante inconsistencias, dudas razonables, omisiones relevantes o discrepancias sustanciales, la ACR-Py podrá requerir aclaraciones o documentación complementaria, suspender la tramitación o rechazar la solicitud mediante acto fundado y motivado, sin perjuicio de las acciones de supervisión que correspondan respecto de la habilitación del PCSC.

3.2.3 Autenticación de la identidad del individuo (Persona Física)

La ACR-Py asegura la validación y autenticación de la identidad de toda Persona Física que intervenga en el proceso de solicitud, emisión, renovación o revocación de certificados, conforme a los principios establecidos en ETSI EN 319 411.

A los fines del presente documento:

a) La validación de identidad comprende la verificación documental, legal y registral de la identidad declarada.
b) La autenticación de identidad comprende la confirmación de que la persona que interviene en el proceso es efectivamente quien afirma ser, mediante su comparecencia presencial.

A los efectos del presente documento, el término "Persona Física" se corresponde con el concepto de "natural person" definido en dicha norma.

El proceso de validación de la identidad de la persona física que actúe como solicitante, comprende:

a) La verificación de la identidad mediante documentación oficial válida y vigente.
b) La evaluación de la autenticidad y consistencia de la documentación oficial presentada.
c) La confirmación de la vinculación entre la Persona Física y la entidad a la que representa, cuando corresponda.
d) La verificación de las facultades o autorizaciones para actuar en nombre de la entidad, mediante documentación habilitante.
e) La comprobación de que la información a ser incorporada en el certificado es exacta y corresponde a la identidad verificada.

La ACR-Py podrá utilizar fuentes internas y externas confiables e independientes para complementar el proceso de validación, garantizando un nivel de aseguramiento adecuado respecto a la identidad de la Persona Física.

Toda la evidencia asociada al proceso de autenticación será registrada y conservada.

3.2.4 Información no verificada del titular de certificado

No aplica. La ACR-Py no incorpora información sustancial no verificada en los certificados emitidos dentro de su ámbito.

3.2.5 Validación de autoridad

Cuando la solicitud de emisión, aceptación, renovación o revocación de un certificado electrónico sea presentada por una persona física que actúe en nombre de un PCSC, la ACR-Py validará la autoridad, facultad y legitimación con la que dicha persona interviene.

Esta validación complementa la autenticación prevista en el ítem 3.2.2 y tiene por objeto verificar que la persona interviniente se encuentra habilitada para realizar la actuación solicitada en representación del titular del certificado, en consistencia con la naturaleza del acto, la condición jurídica del PCSC y el alcance de la actuación pretendida.

A tales efectos, la ACR-Py podrá verificar, según corresponda:

a. estatuto social vigente del PCSC inscripto en la Dirección General de los Registros Públicos (DGRP), actas del órgano competente que designen al representante, o poderes otorgados ante escribano público, vigentes y debidamente inscriptos cuando la ley lo exija;
b. resoluciones, actos administrativos o autorizaciones del PCSC que confieran facultades específicas para la actuación pretendida;

c. correspondencia entre la persona interviniente, el PCSC representado y la actuación solicitada;

d. cualquier otro instrumento idóneo, que permita establecer la autoridad invocada de manera suficiente y auditable.

La representación invocada deberá encontrarse vigente al momento de la presentación de la solicitud y al momento de la actuación de la ACR-Py. La documentación reunida integra el expediente respectivo y se conserva conforme a los plazos previstos en el ítem 5 del presente instrumento.

Cuando la legitimación invocada no se encuentre suficientemente acreditada, la ACR-Py no emitirá ni procesará la solicitud, mediante acto fundado y motivado, hasta tanto se subsanen las deficiencias detectadas o se aporte evidencia suficiente.

3.2.6 Criterios para interoperabilidad

El presente ítem regula los criterios para interoperación, jerarquía cruzada o reconocimiento de autoridades y prestadores ajenos a la estructura jerárquica de la ICPP que requiera articulación con la ACR-Py.

En tales supuestos, la validación inicial de identidad considerará, además de los requisitos generales del presente documento:

a. coherencia técnica entre la identidad validada y el perfil del certificado (certificate policies, key usage, extended key usage);

b. compatibilidad con los identificadores, políticas y restricciones de la jerarquía ICPP (name constraints, path length, policy constraints);

c. uniformidad en la representación de nombres y atributos institucionales conforme al ítem 3.1;

d. consistencia con los requisitos de la AA, incluida la eventual incorporación a la Trusted Service List (TSL) nacional; y

e. cualquier otro criterio técnico o regulatorio aplicable.

Cuando la interoperación involucre servicios de confianza prestados fuera de la República del Paraguay, se aplicará el artículo 7° de la Ley N.º 6822/2021 y su Decreto Reglamentario N.º 7576/2022, exigiendo acuerdos de reconocimiento mutuo entre autoridades normativas u organismos internacionales y la verificación de equivalencia de requisitos.

3.3. Identificación y autenticación para solicitudes de nueva clave

Las "solicitudes de nueva clave" del RFC 3647 corresponden a la renovación del certificado electrónico, en el marco de la ICPP, toda renovación implica un nuevo par de claves.

La ACR-Py aplica procedimientos diferenciados conforme a los ítems 3.3.1 y 3.3.2. La renovación del certificado raíz autofirmado de la propia ACR-Py se tramita conforme el documento Ceremonia de Constitución de la Autoridad Certificadora Raíz de Paraguay o su equivalente y autoemisión, conforme al ítem 6 del presente instrumento.

3.3.1 Identificación y autenticación para emisión de nueva clave

El PCSC titular podrá renovar su certificado antes de la expiración del vigente mediante:

a. presentación del formulario correspondiente suscripto por él o los representantes legales del PCSC;
b. revalidación de los datos institucionales, confirmando vigencia y ausencia de modificaciones sustanciales (cambio de representante legal, de domicilio, entre otros) respecto del ítem 3.2;
c. prueba de posesión de la nueva clave privada conforme al ítem 3.2.1; y
d. verificación de la vigencia de la habilitación del PCSC ante la AA.

Acreditados estos extremos, la ACR-Py emite el nuevo certificado sin repetir íntegramente la validación inicial.

3.3.2 Identificación y autenticación para nueva clave después de revocación

La solicitud de un nuevo certificado electrónico por parte de un PCSC cuyo certificado anterior hubiera sido revocado o expirado se tramitará conforme al procedimiento de emisión inicial previsto en el ítem 3.2 en su integridad, sin acceso al procedimiento simplificado del ítem 3.3.1.

A tal efecto, él o los representantes legales del PCSC presentarán el formulario correspondiente, acompañado de la documentación que acredite la subsistencia o actualización de los antecedentes institucionales registrados.

Cuando la revocación se hubiera fundado en compromiso de clave privada, pérdida de confiabilidad documental, alteración de identidad o representación del PCSC, o causales equivalentes, la ACR-Py exigirá la revalidación íntegra conforme a los ítems 3.2.1, 3.2.2 y 3.2.5, con acreditación específica de la subsanación de las circunstancias que originaron la revocación.

3.4. Identificación y autenticación para solicitudes de revocación

El solicitante de la revocación de un certificado deberá ser identificado y autenticado. Solo los sujetos legitimados conforme al ítem 4.9.2 podrán solicitar la revocación de certificados emitidos por la ACR-Py.

La autenticación se realiza, según el sujeto solicitante y el nivel de riesgo, mediante uno o más de los siguientes mecanismos: solicitud firmada con certificado electrónico cualificado vigente; comunicación formal por los canales institucionales oficialmente establecidos, previamente registrados o reconocidos; verificación documental o procedimental de la identidad y representación invocada; validación mediante contacto directo con persona autorizada registrada; cotejo de autenticidad e integridad del acto administrativo o de la resolución judicial; u otros mecanismos equivalentes con evidencia fehaciente y trazable.

El procedimiento para la solicitud de revocación se encuentra descrito en el ítem 4.9.3. Todas las solicitudes de revocación deberán ser registradas.

No se considerarán válidas las solicitudes que no permitan establecer suficientemente la identidad, legitimación o correspondencia con el certificado afectado. Toda verificación de autenticidad se documenta y conserva conforme a los plazos del ítem 5.

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1. Solicitud del certificado

La ACR-Py tramita internamente la generación y autoemisión de su certificado raíz y recibe solicitudes para la emisión de certificados destinados a PCSC habilitados, autorizados o reconocidos conforme al acto administrativo aplicable. La ACR-Py no recibe solicitudes de certificados para usuarios finales.

4.1.1. Quién puede presentar una solicitud de certificado

La generación o sustitución del certificado raíz de la ACR-Py corresponde al MIC a través de la DGCE conforme al procedimiento institucional aplicable.

La solicitud de certificado de PCSC deberá ser presentada por su titular, representante legal o apoderado, según la naturaleza jurídica del prestador.

4.1.2. Proceso de registro y responsabilidades

El proceso de registro comprende el conjunto de actuaciones mediante las cuales la ACR-Py recibe, registra, documenta, identifica y verifica preliminarmente una solicitud de emisión de certificado, a fin de someterla al proceso de evaluación, aprobación o rechazo previsto en el ítem 4.2.

En el caso de certificados emitidos a PCSC, el proceso comprende, como mínimo:

a) recepción formal de la solicitud mediante el formulario correspondiente, a través del mecanismo admitido por la ACR-Py;
b) verificación de la habilitación vigente y firme del PCSC ante la AA;
c) identificación y autenticación del solicitante y de la persona interviniente, conforme al ítem 3;
d) validación de la autoridad o representación conforme al ítem 3.2.5;
e) recepción del Certificate Signing Request (CSR) en formato PKCS#10 conforme al RFC 2986 o solicitud firmada equivalente, el cual forma parte de la solicitud de certificado;
f) verificación preliminar de la correspondencia entre la solicitud, el perfil técnico requerido y el alcance del certificado solicitado;
g) verificación de la prueba de posesión de la clave privada conforme al ítem 3.2.1;
h) registro de la solicitud, antecedentes, documentación y evidencias generadas; e
i) apertura o incorporación al expediente técnico-documental correspondiente.

Cuando la solicitud se refiera al certificado raíz de la ACR-Py, el proceso se sustentará en el procedimiento institucional aplicable a la generación de la clave raíz, la Ceremonia de Constitución de la Autoridad Certificadora Raíz de Paraguay o Ceremonia de Generación de Claves, el acto de autoemisión y la documentación formal de las decisiones, autorizaciones y evidencias correspondientes, conforme al ítem 6.

En los casos de emisión de certificados a PCSC, la AA participa, en su rol de supervisión y cuando corresponda por la naturaleza del acto, en ceremonias, actos controlados o verificaciones institucionales vinculadas a la solicitud, en particular cuando resulte necesario reforzar la trazabilidad, la fehaciencia del procedimiento o la validación institucional de los antecedentes presentados.

Responsabilidades del PCSC solicitante:
a) presentar información veraz, completa, exacta y actualizada;
b) acompañar la documentación, antecedentes y evidencias requeridos;
c) actuar por medio de su titular, representante legal o apoderado;
d) generar el par de claves en dispositivo criptográfico seguro, conforme a los algoritmos, longitudes mínimas, perfiles, estándares y requerimientos de certificación establecidos en el DOC-ICPP-06 [3] y demás reglamentación ICPP que resulte aplicable, y custodiar la clave privada bajo control exclusivo; y
e) colaborar con la ACR-Py en las verificaciones necesarias para la tramitación.

Responsabilidades de la ACR-Py:
a) recibir y registrar adecuadamente la solicitud;
b) aplicar los procedimientos de identificación y autenticación establecidos;
c) verificar la consistencia técnica, jurídica y operativa;
d) preservar la trazabilidad del proceso;
e) proteger la documentación, registros y evidencias generadas; y
f) someter la solicitud al proceso de evaluación previsto en el ítem 4.2.
La sola recepción o registro de una solicitud no genera derecho a la emisión del certificado electrónico. Toda solicitud queda sujeta a la verificación integral del cumplimiento de los requisitos técnicos, jurídicos, operativos y documentales aplicables.

4.2. Procesamiento de la solicitud de certificado

Admitida formalmente una solicitud de certificado, la ACR-Py procederá a su procesamiento mediante la ejecución de las funciones de identificación, autenticación, verificación técnica, evaluación documental y decisión de aprobación, observación o rechazo, conforme a la presente PC/DPC y a los documentos ICPP aplicables.
El certificado raíz autofirmado de la ACR-Py se regirá por el procedimiento institucional de generación de claves, ceremonia y autoemisión previsto en el ítem 6, y no por el circuito ordinario aplicable a solicitudes externas.

4.2.1. Ejecución de las funciones de identificación y autenticación

La ACR-Py ejecuta las funciones de identificación y autenticación conforme a lo descrito en el ítem 3 de esta PC/DPC.

4.2.2. Aprobación o rechazo de solicitudes de certificado

La ACR-Py podrá aprobar o rechazar una solicitud de certificado de PCSC conforme al resultado de las verificaciones efectuadas y al cumplimiento de los requisitos técnicos, jurídicos, documentales y operativos aplicables.

4.2.3. Tiempo para procesar la solicitud de certificado

El plazo de procesamiento de la solicitud de certificado, computado desde la notificación de admisión formal hasta la notificación de la decisión prevista en el ítem 4.2.2, será de 5 (cinco) días hábiles. Las observaciones que requieran subsanación por parte del PCSC suspenderán el cómputo del plazo hasta su atención completa.

Aprobada la solicitud, la ACR-Py garantiza que la ceremonia de emisión del certificado se realizará en un plazo máximo de 30 (treinta) días hábiles, computados desde la notificación de aprobación de dicha solicitud al PCSC, salvo causa justificada debidamente documentada.

4.3. Emisión del certificado

4.3.1. Acciones de la ACR-Py durante la emisión de un certificado

La emisión de un certificado por la ACR-Py se realiza en ceremonia específica, con la presencia del titular del PCSC solicitante, cuando sea persona física, o de su representante legal o apoderado, cuando se trate de persona jurídica, organismo o entidad del Estado; funcionarios de la DGCE, auditores designados e invitados institucionales cuando corresponda, registrándose en acta todos los procedimientos ejecutados.

Las claves públicas de los certificados autofirmados de la ACR-Py se publican en el repositorio público de la ICPP previsto en el ítem 2.

El certificado se considera válido desde el momento de su emisión, conforme conste en el atributo **notBefore** del certificado.

La emisión de los certificados de la ACR-Py y de los certificados destinados a PCSC se realiza en equipos operando off-line, conforme a los requerimientos técnicos del DOC-ICPP-06 [3] y a los controles físicos y lógicos previstos en el ítem 6.

La emisión de certificados por la ACR-Py a los PCSC estará condicionada a la presentación de póliza de seguro de responsabilidad civil vigente, con cobertura suficiente y compatible con el riesgo de las actividades de servicios de confianza, conforme a los requisitos de habilitación establecidos por la AA en la normativa aplicable;

La ACR-Py entrega el certificado emitido, en el formato definido en el DOC-ICPP-06 [3], al titular del certificado o a quien ejerza válidamente su representación presente en la ceremonia, dejando constancia en acta de la recepción.

4.3.2. Notificación al titular de certificado por la ACR-Py

Posterior a la emisión del certificado, la ACR-Py notificará al titular, representante legal o apoderado mediante el canal de comunicación oficialmente establecido.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye aceptación del certificado

Al emitir un certificado a un PCSC, la ACR-Py garantiza que la información contenida en dicho certificado fue verificada conforme a la presente PC/DPC.

Al momento de la entrega del certificado, durante la ceremonia de su emisión por la ACR-Py, el titular o representante legal del PCSC deja constancia de su recepción mediante la suscripción de los siguientes instrumentos:
a) Acta de Ceremonia de Emisión del Certificado;
b) Acta de Ceremonia de Entrega de Clave Pública; o
c) Acuerdo de Términos y Responsabilidades.

La aceptación del certificado se producirá cuando el PCSC verifique los datos contenidos en el certificado y manifieste su conformidad, o con la primera utilización de la clave privada correspondiente al certificado emitido, lo que ocurra primero.

La verificación de los datos del certificado deberá ser realizada por el PCSC titular en el plazo de 2 (dos) días hábiles contados desde su recepción. Vencido dicho plazo sin objeción formal, el certificado se considerará aceptado tácitamente.

Al aceptar el certificado, el PCSC titular:
a) acepta las responsabilidades, obligaciones y deberes establecidos en el Acuerdo de Términos y Responsabilidades y la presente PC/DPC;
b) declara que ninguna persona no autorizada ha tenido acceso a la clave privada asociada al certificado;
c) confirma que la información proporcionada durante el proceso de habilitación, registro y solicitud es verdadera, completa, exacta y se encuentra reproducida correctamente en el certificado emitido.

La objeción o rechazo del certificado formulado dentro del plazo previsto, fundada en errores u observaciones del PCSC, implicará la realización de una nueva ceremonia, en la cual se procederá a la revocación del certificado no aceptado y a la emisión de un nuevo certificado debidamente subsanado.

4.4.2. Publicación del certificado por la ACR-Py

El certificado raíz y los certificados emitidos a PCSC se publican conforme al ítem 2.2 de esta PC/DPC.

4.4.3. Notificación de emisión del certificado a otras entidades

La notificación a otras entidades se realizará conforme al ítem 2.2 de esta PC/DPC.

La publicación del certificado en el repositorio de la ICPP constituirá notificación suficiente frente a terceros, salvo que una disposición normativa, acto administrativo o procedimiento específico exija una notificación adicional.

4.5. Uso del par de claves y del certificado

El PCSC titular de un certificado emitido por la ACR-Py deberá operar conforme a la propia Declaración de Prácticas de Certificación (DPC) y a las Políticas de Certificación (PC) que implemente, las cuales se establecerán en conformidad con los requisitos mínimos previstos en los documentos normativos DOC-ICPP-03 [1] y DOC-ICPP-04 [2].

El uso del par de claves y del certificado emitido por la ACR-Py deberá limitarse estrictamente a los fines, alcances, políticas, extensiones y restricciones establecidos en el certificado, en la presente PC/DPC y en el acto de habilitación correspondiente.

4.5.1. Uso de la clave privada y del certificado por el titular

El PCSC titular deberá utilizar la clave privada asociada al certificado emitido por la ACR-Py exclusivamente para las operaciones autorizadas por el perfil del certificado, su DPC, sus PC, la presente PC/DPC y el alcance de su habilitación.

El PCSC deberá proteger la clave privada bajo su exclusivo control, conforme a su DPC y a los requisitos técnicos, físicos, lógicos y procedimentales aplicables. No podrá utilizar el certificado para fines distintos de los autorizados, ni continuar utilizando la clave privada cuando exista revocación, expiración, compromiso o sospecha de compromiso.

4.5.2. Uso de la clave pública y del certificado por la Parte Usuaria

La PU deberá aceptar los términos establecidos en la presente PC/DPC como condición para confiar en los certificados emitidos por la ACR-Py.

La PU verificará la validez y fiabilidad de los certificados emitidos por la ACR-Py conforme al procedimiento previsto en el ítem 9.6.4 de la presente PC/DPC.

4.6. Renovación del certificado

4.6.1. Circunstancias para la renovación del certificado

La ACR-Py no permite la renovación de certificados con el mismo par de claves; toda renovación requerirá la generación de un nuevo par de claves y la emisión de un nuevo certificado, conforme a los ítems 3.3 y 4.7 de la presente PC/DPC.

4.6.2. Quién puede solicitar la renovación

Podrá solicitar la renovación, entendida como emisión de nuevo certificado con nuevo par de claves, el PCSC titular del certificado vigente, por intermedio de su representante legal o apoderado de acuerdo

con el ítem 4.1.1, siempre que mantenga vigente su habilitación ante la AA y no registre causal pendiente de suspensión, revocación, cese o pérdida de confianza.

4.6.3. Procesamiento de solicitudes de renovación

No aplica. Toda renovación requerirá la generación de un nuevo par de claves y la emisión de un nuevo certificado, conforme a los ítems 3.3 y 4.7 de la presente PC/DPC.

4.6.4. Notificación de nueva emisión al titular

No aplica. Toda renovación requerirá la generación de un nuevo par de claves y la emisión de un nuevo certificado, conforme a los ítems 3.3 y 4.7 de la presente PC/DPC.

4.6.5. Conducta que constituye aceptación de un certificado renovado

No aplica. Toda renovación requerirá la generación de un nuevo par de claves y la emisión de un nuevo certificado, conforme a los ítems 3.3 y 4.7 de la presente PC/DPC.

4.6.6. Publicación del certificado renovado

No aplica. Toda renovación requerirá la generación de un nuevo par de claves y la emisión de un nuevo certificado, conforme a los ítems 3.3 y 4.7 de la presente PC/DPC.

4.6.7. Notificación de emisión a otras entidades

No aplica. Toda renovación requerirá la generación de un nuevo par de claves y la emisión de un nuevo certificado, conforme a los ítems 3.3 y 4.7 de la presente PC/DPC.

4.7. Nueva clave de certificado

4.7.1. Circunstancias para la generación de un nuevo par de claves y la emisión de un nuevo certificado

La generación de un nuevo par de claves y la emisión de un nuevo certificado proceden cuando:
a) el PCSC solicite la emisión de un nuevo certificado antes de la expiración del vigente, a fin de asegurar la continuidad operativa del servicio de confianza y evitar interrupciones en la validez de los certificados utilizados para su prestación.
b) el certificado anterior haya expirado;
c) el certificado anterior haya sido revocado;
d) exista un requerimiento de sustitución, actualización criptográfica o migración de algoritmo aprobado por la AA;
e) exista compromiso real o sospechado de clave privada; o
f) exista decisión fundada de la ACR-Py o de la AA.

4.7.2. Quién puede solicitar certificación de una nueva clave pública

Podrá solicitar la certificación de una nueva clave pública el titular del certificado o quien o quienes ejerzan válidamente su representación, según corresponda.

La ACR-Py o la AA podrá ordenar la generación de nueva clave cuando resulte necesario para preservar la confianza, seguridad, interoperabilidad o continuidad de la ICPP.

4.7.3. Procesamiento de solicitudes de nueva clave

Cuando el certificado anterior se encuentre vigente y no exista causal de revocación, la solicitud podrá tramitarse por el procedimiento simplificado del ítem 3.3.1.

Cuando el certificado anterior haya expirado, haya sido revocado o exista compromiso de clave privada, pérdida de confiabilidad documental, alteración de identidad o representación, la solicitud se tramitará conforme al procedimiento de validación inicial previsto en el ítem 3.2.

4.7.4. Notificación de nueva emisión al titular

Posterior a la emisión del certificado, la ACR-Py notificará al titular, representante legal o apoderado mediante el canal de comunicación oficialmente establecido.

4.7.5. Conducta que constituye aceptación de un certificado con nueva clave

La aceptación se regirá por el ítem 4.4.

4.7.6. Publicación del certificado con nueva clave

El certificado con nueva clave será publicado conforme al ítem 2.2. La ACR-Py conservará la trazabilidad entre el certificado anterior y el nuevo certificado, sin reutilización de números de serie ni de pares de claves.

4.7.7. Notificación de emisión a otras entidades

La emisión será notificada o publicada conforme al ítem 2.2 de esta PC/DPC.

4.8. Modificación del certificado

4.8.1. Circunstancias para modificación

No aplica.

4.8.2. Quién puede solicitar modificación

No aplica.

4.8.3. Procesamiento de solicitudes de modificación

No aplica.

4.8.4. Notificación de nueva emisión al titular

No aplica.

4.8.5. Conducta que constituye aceptación de certificado modificado

No aplica.

4.8.6. Publicación del certificado modificado

No aplica.

4.8.7. Notificación de emisión a otras entidades

No aplica.

4.9. Revocación y suspensión del certificado

4.9.1. Circunstancias para revocación

El certificado emitido por la ACR-Py a un PCSC podrá ser revocado en cualquier momento, a solicitud del titular del certificado, a solicitud de quien o quienes ejerzan válidamente su representación o por decisión motivada de la ACR-Py en ejercicio de sus facultades conforme a la Ley N.º 6822/2021 y su Decreto Reglamentario N.º 7576/2022, garantizando el debido proceso administrativo.

La ACR-Py procederá a la revocación del certificado cuando se verifique cualquiera de las siguientes circunstancias:
a) se constate emisión impropia o defectuosa del mismo, es decir se emitió y no correspondía emitirlo, o se emitió con errores o incumplimientos;
b) resulte necesaria la alteración de cualquier información consignada en el mismo;
c) pérdida de la habilitación como prestador cualificado de servicios de confianza.
d) se produzca el cese de la actividad del PCSC titular del certificado, incluyendo su disolución, liquidación, extinción o cualquier otra circunstancia que implique la imposibilidad de continuar prestando el servicio de confianza cualificado; o
e) se verifique el compromiso de la clave privada del PCSC o de su soporte de almacenamiento.

La ACR-Py podrá revocar o disponer la revocación del certificado, según corresponda, del PCSC que deje de cumplir con la legislación vigente o con las políticas, normas, prácticas y reglas establecidas para la ICPP.

Las claves públicas correspondientes a certificados emitidos por un PCSC que haya cesado en su actividad, cualquiera sea la causa, serán almacenadas por otro PCSC, previa aprobación de la ACR-Py Cuando exista más de un PCSC interesado, asumirá la responsabilidad de la custodia de las claves públicas el indicado por el PCSC que cesa sus actividades.

El PCSC que cesa sus actividades deberá transferir obligatoriamente la totalidad de la información relativa a certificados emitidos, incluyendo certificados, claves públicas, registros, evidencias y documentación necesaria para la validación histórica, garantizando su integridad, autenticidad, disponibilidad y trazabilidad.

En ausencia de un PCSC receptor, la información será transferida a la ACR-Py o a la entidad que esta determine.

4.9.2. Quién puede solicitar revocación

La revocación del certificado de un PCSC solamente podrá efectuarse:
a) por determinación de la ACR-Py, sea de oficio o por instrucción de la AA en ejercicio de sus competencias regulatorias o de supervisión;
b) por solicitud del PCSC titular del certificado; o
c) por resolución judicial que lo ordene.

4.9.3. Procedimiento para la solicitud de revocación

La solicitud de revocación del certificado de un PCSC deberá presentarse mediante el formulario correspondiente, firmado por el titular cuando se trate de una persona física, o quien o quienes ejerzan válidamente su representación, cuando se trate de una persona jurídica. En caso de utilizarse una versión electrónica del formulario, deberá estar firmado con certificado electrónico cualificado vigente.

Recibida la solicitud, la ACR-Py procederá a verificar la identidad y legitimación del solicitante, así como la correspondencia de la solicitud con el certificado cuya revocación se requiere. Asimismo, evaluará la causal invocada y la suficiencia de la información aportada.
Cuando la solicitud se encuentre completa y la causal de revocación haya sido debidamente constatada, la ACR-Py procederá a ejecutar la revocación del certificado, finalizando el proceso con la publicación efectiva de su estado de revocado en la correspondiente CRL/LCR, dentro de un plazo máximo de veinticuatro (24) horas.

Sin perjuicio de lo anterior, en casos de compromiso real o sospechado de la clave privada, emisión impropia o defectuosa, orden judicial, pérdida de habilitación, incidente de seguridad grave o riesgo sistémico para la ICPP, la ACR-Py podrá disponer la revocación de oficio mediante decisión fundada, garantizando las notificaciones y el debido proceso administrativo que correspondan.

Un certificado de PCSC que haya sido revocado solo podrá utilizarse para la verificación de firmas o sellos generados durante el período en que dicho certificado se encontraba vigente.

4.9.4. Período de gracia para la solicitud de revocación

La solicitud de revocación deberá ser inmediata cuando se configuren las circunstancias definidas en el ítem 4.9.1 de la presente PC/DPC.

4.9.5. Tiempo dentro del cual la ACR-Py debe procesar la solicitud de revocación

La ACR-Py deberá concluir con la publicación efectiva del estado de revocación dentro del plazo máximo de veinticuatro (24) horas contado desde:
a) la recepción de una solicitud completa y debidamente constatada; o
b) la determinación de revocación emitida por la ACR-Py.

Cuando el riesgo afecte la clave privada de la ACR-Py, la integridad de la ICPP, la confianza de la jerarquía o la seguridad de la PU, la ACR-Py aplicará el procedimiento de emergencia previsto en el Plan de Respuesta a Incidentes y en el Plan de Continuidad de Negocio.

4.9.6. Requisito de verificación de revocación para la Parte Usuaria

El estado de los certificados (incluidos los certificados revocados) estará disponible a la PU conforme al ítem 2.1.

4.9.7. Frecuencia de emisión de CRL/LCR

La ACR-Py emite la CRL/LCR conforme a la siguiente frecuencia operativa:
a) CRL/LCR ordinaria: cada noventa (90) días; y
b) CRL/LCR extraordinaria: cuando una revocación, incidente o circunstancia relevante haga necesaria una actualización anticipada será realizada en el plazo previsto en el ítem 4.9.3 y la nueva CRL/LCR se notificará a todos los PCSC.

Cuando se revoque el certificado de la propia ACR-Py, deberá emitirse una CRL/LCR con período de validez igual al del certificado, cerrando la emisión de la CRL/LCR por parte de dicha AC.

4.9.8. Latencia máxima para CRL/LCR

La CRL/LCR se publica en el repositorio oficial dentro del plazo máximo de una (1) hora desde su generación.

4.9.9. Disponibilidad de verificación en línea de revocación o estado

La ACR-Py no dispone de servicio OCSP para la consulta del estado de certificados. La verificación del estado de revocación se realizará mediante la CRL/LCR publicada en el repositorio oficial.

4.9.10. Requisitos para verificación en línea de revocación

No aplica.

4.9.11. Otras formas disponibles de publicación de la revocación

La información de revocación de certificados de PCSC y de los certificados autofirmados de la ACR-Py también podrá divulgarse en el sitio web de la ACR-Py, sin sustituir la CRL/LCR como fuente técnica de estado.

4.9.12. Requerimientos especiales por compromiso de clave privada

El PCSC deberá notificar inmediatamente a la ACR-Py todo compromiso real o sospechado de su clave privada, de los datos de activación, del soporte criptográfico o de los sistemas que puedan afectar la confiabilidad del certificado.

La ACR-Py deberá comunicar a la AA todo incidente de seguridad que afecte o pueda afectar la confidencialidad, integridad, disponibilidad, autenticidad, continuidad o confiabilidad de la ACR-Py,

de los certificados emitidos, de las CRL/LCR, de la Lista de Confianza, de la clave privada raíz o de los sistemas de certificación, dentro del plazo máximo de veinticuatro (24) horas contado desde su conocimiento.

La comunicación incluirá, como mínimo, descripción del incidente, fecha y hora de detección, activos afectados, impacto preliminar, medidas adoptadas, necesidad de revocación, necesidad de actualización de la Lista de Confianza, medidas de contención, responsable del seguimiento y evidencias disponibles.

4.9.13. Circunstancias para suspensión

No aplica. La suspensión no constituye operación reconocida del ciclo de vida de los certificados emitidos por la ACR-Py. Toda interrupción de la vigencia del certificado se resuelve mediante revocación.

4.9.14. Quién puede solicitar suspensión

No aplica.

4.9.15. Procedimiento para solicitud de suspensión

No aplica.

4.9.16. Límite del período de suspensión

No aplica.

4.10. Servicios de estado del certificado

4.10.1. Características operacionales

La ACR-Py presta el servicio de estado mediante puntos de distribución de CRL/LCR incorporados en los certificados y publicados en el repositorio oficial.

4.10.2. Disponibilidad del servicio

La CRL/LCR estará disponible para consulta pública a través del repositorio oficial de la ACR-Py previsto en el ítem 2.1 y será publicada conforme al ítem 2.2.

La ACR-Py garantizará una disponibilidad mínima anual del servicio de estado de certificados y del repositorio oficial del noventa y nueve coma cinco por ciento (99,5%), salvo interrupciones justificadas por mantenimiento programado, caso fortuito, fuerza mayor, incidente de seguridad o razones técnicas debidamente documentadas.

La ACR-Py adoptará medidas técnicas y organizativas adecuadas para asegurar la disponibilidad, integridad y autenticidad de la CRL/LCR publicada.

4.10.3. Funcionalidades opcionales

No aplica. La ACR-Py no presta servicios opcionales de estado de certificado, tales como OCSP u otros mecanismos de consulta en línea distintos de la CRL/LCR publicada en el repositorio oficial.

4.11. Fin de la suscripción

El fin de la suscripción se produce por expiración, revocación, sustitución, pérdida de habilitación, cese del titular o decisión fundada de la ACR-Py. La terminación no extingue las obligaciones de conservación de registros, certificados, CRL/LCR y evidencias.

La DPC del PCSC deberá describir los requisitos y procedimientos a ser adoptados en los casos de extinción de los servicios del PCSC responsable.

4.12. Custodia y recuperación de claves

No está permitida la custodia o depósito de claves privadas de terceros (key escrow) por parte de la ACR-Py. La recuperación de la clave privada raíz solo podrá realizarse mediante copias de seguridad cifradas, encapsuladas o wrapped, bajo control multiparte y conforme al ítem 6.2.4.

4.12.1. Política y prácticas de custodia y recuperación de claves

No aplica para claves privadas de PCSC ni para claves de usuarios finales (persona físicas o jurídicas titulares de certificados). Para la clave privada raíz de la ACR-Py, aplican exclusivamente los procedimientos de respaldo y recuperación previstos en el ítem 6.2.4.

4.12.2. Política y prácticas de encapsulamiento y recuperación de claves de sesión

No aplica a la ACR-Py.

5. CONTROLES DE INSTALACIONES, DE GESTIÓN Y OPERACIONALES

El proceso de gestión de certificados de la ACR-Py incluye controles físicos, ambientales, procedimentales, de personal, auditoría, archivo, continuidad, gestión de incidentes y seguridad organizativa.

5.1. Controles físicos

La ACR-Py mantiene políticas de seguridad para los activos y sistemas utilizados en los procesos de gestión de certificados. Estas políticas cubren controles de acceso físico, protección contra desastres naturales, seguridad contra incendios, fallas de servicios de soporte (como energía, telecomunicaciones, enlaces de datos, entre otros), colapso estructural, inundación, protección contra robo, accesos indebidos y recuperación ante desastres. Estos controles deberán implementarse para evitar pérdida, daños o compromiso de los activos, interrupción de las actividades operativas relacionadas con los procesos de gestión de certificados, robo de información y compromiso de las instalaciones de procesamiento de información.

5.1.1. Localización y construcción del sitio

La ACR-Py opera en instalaciones bajo control institucional, cuya selección, construcción y acondicionamiento responden a criterios de seguridad física, controles ambientales, restricción de acceso y protección del material criptográfico, compatibles con la criticidad de los procesos de certificación raíz y orientados a minimizar riesgos físicos, ambientales y operativos.

Las áreas destinadas a la operación raíz, custodia del material criptográfico y ejecución de ceremonias criptográficas se mantienen física y operacionalmente diferenciadas de otros entornos. Las instalaciones se organizan por perímetros de seguridad con restricciones crecientes según la criticidad de los activos contenidos en cada área.

5.1.2. Acceso físico

El acceso físico a las dependencias de la ACR-Py donde se realizan las actividades relacionadas con los procesos de gestión de certificados es gestionado y controlado internamente conforme a los requisitos definidos en la Política de Seguridad de la ICPP.

El control de acceso se realiza mediante tarjetas criptográficas, identificaciones biométricas u otros dispositivos, de manera que solamente personas autorizadas participen de las actividades pertinentes. Adicionalmente, el acceso físico y todos los ambientes son monitoreados mediante Circuito Cerrado de Televisión (CCTV), con grabación digital 24x7.

El sistema de certificación de la ACR-Py se sitúa en ambientes seguros redundantes, tipo rack cofre, localizados en instalaciones geográficamente segregadas. La seguridad física y los controles de acceso mediante identificación biométrica restringen el acceso a los equipos y sistemas relativos a los procesos de gestión de certificados.

Se definen al menos 4 (cuatro) niveles de acceso físico a los diversos ambientes de la ACR-Py, y 2 (dos) niveles adicionales relativos a la protección de las claves privadas:

El primer nivel o nivel 1 constituye la primera barrera de acceso a las instalaciones de la ACR-Py. A partir de este nivel, las personas ajenas a la operación de la ACR-Py circulan debidamente identificadas y acompañadas. Ningún tipo de proceso operativo o administrativo relacionado con la gestión de certificados deberá ser ejecutado en este nivel.

Exceptuados los casos previstos en la ley, el porte de armas no será admitido en las instalaciones de la ACR-Py a partir del nivel 1. A partir de este nivel, los equipos de grabación, fotografía, video, sonido o similares, así como los computadores portátiles, tendrán su ingreso controlado y solamente podrán ser utilizados mediante autorización formal y supervisión.

El segundo nivel o nivel 2, es interno al primero y requiere la identificación individual de las personas que ingresan a él. Este es el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso

operativo o administrativo de la ACR-Py. El paso del primer al segundo nivel deberá exigir factor de autenticación electrónica y tarjeta de identificación visible.

El tercer nivel o nivel 3, se sitúa dentro del segundo y será el primer nivel en albergar material y actividades sensibles relacionadas con los procesos de gestión de certificados de la ACR-Py.

Las personas que no estén involucradas con dichas actividades no deberán tener permiso de acceso a este nivel. Las personas que no posean permiso de acceso no podrán permanecer en este nivel si no se encuentran acompañadas por un personal de la AC.

En el tercer nivel se controlan tanto las entradas como las salidas de cada persona autorizada. Se requieren dos tipos de mecanismos de control para el ingreso a este nivel: algún tipo de identificación individual (como tarjeta electrónica) e identificación biométrica.

Los teléfonos celulares, así como otros equipos portátiles de comunicación y almacenamiento de datos, exceptuados aquellos requeridos para la operación de la ACR-Py, no son admitidos a partir del nivel 3.

El cuarto nivel o nivel 4, interior al tercero, es donde ocurren actividades especialmente sensibles de la operación de la ACR-Py, tales como la emisión y revocación de certificados y la emisión de la CRL/LCR. Todos los sistemas y equipos necesarios para dichas actividades se localizan a partir de este nivel.

El nivel 4 posee los mismos controles de acceso del nivel 3 y, adicionalmente, exige en cada acceso a su ambiente la identificación de, como mínimo, 2 (dos) personas de la AC. En este nivel, la permanencia de dichas personas deberá ser exigida mientras el ambiente esté ocupado.

En el cuarto nivel 4, todas las paredes, piso y techo están revestidos de acero y hormigón o de otro material de resistencia equivalente. Las paredes, piso y techo son macizos, constituyendo una célula estanca contra amenazas de acceso indebido, agua, vapor, gases y fuego. Los ductos de refrigeración y de energía, así como los ductos de comunicación, no permiten la invasión física de las áreas del cuarto nivel. Adicionalmente, estos ambientes de nivel 4 poseen protección contra interferencia electromagnética externa, o disponen de equipos tipo rack que posean dicha característica.

Podrán existir, en la ACR-Py, varios ambientes de cuarto nivel para albergar y segregar, según corresponda:
a) equipos de producción on-line y cofre de almacenamiento;
b) equipos de producción off-line y cofre de almacenamiento; y
c) equipos de red e infraestructura (firewall, routers, switches y servidores).
El quinto nivel o nivel 5, interior al ambiente de nivel 4, comprende un cofre o gabinete reforzado con cerradura. Los materiales criptográficos — tales como claves, datos de activación, sus copias y equipos criptográficos — son almacenados en ambientes de nivel 5 o superior.

Para garantizar la seguridad del material almacenado, el cofre o gabinete cumple con las siguientes especificaciones mínimas:
a) ser fabricado en acero o material de resistencia equivalente; y
b) poseer cerradura con llave.

El sexto nivel o nivel 6 consiste en pequeños depósitos localizados en el interior del cofre o gabinete del quinto nivel. Cada uno de dichos depósitos dispone de acceso individual a su contenido. Los datos de activación de la clave privada de la ACR-Py son almacenados en estos depósitos.

5.1.2.1. Sistemas de detección física

Todos los puntos de paso entre los distintos niveles de acceso, así como las salas operativas de Nivel 4, cuentan con un sistema de videovigilancia por cámaras con grabación continua las veinticuatro horas del día, los siete días de la semana (24/7), destinado exclusivamente a fines de seguridad física, control de acceso, prevención de incidentes, protección de activos críticos y preservación de evidencia vinculada a la operación de la ACR.

La ubicación, el ángulo y la resolución de las cámaras se configuran de manera proporcional a dichos fines, procurando evitar la captura innecesaria de imágenes, datos personales o información sensible no vinculada a la seguridad física. Las cámaras no deberán permitir la captura o visualización de contraseñas, PIN o credenciales ingresadas por el personal en los lectores de control de acceso o sistemas operativos.

Las grabaciones continuas de video vigilancia (CCTV) se conservarán por un plazo ordinario mínimo de noventa (90) días corridos y un máximo de ciento ochenta (180) días corridos. Transcurrido este plazo sin que se reporten incidentes, anomalías, requerimientos de auditoría o solicitudes de autoridad competente, las grabaciones serán eliminadas mediante mecanismos de borrado seguro o sobreescritura automática.

En caso de detectarse alarmas de intrusión, anomalías operativas, accesos no autorizados, incidentes de seguridad, eventos bajo investigación, requerimientos de auditoría o actuaciones administrativas, judiciales o de control vinculadas a la operación de la ACR-Py, el fragmento de video correspondiente ser identificado, protegido contra alteraciones y conservado como evidencia por un plazo mínimo de cinco (5) años, o por el plazo mayor que resulte necesario mientras subsista el procedimiento, investigación, auditoría o requerimiento de autoridad competente.

Los registros de auditoría asociados al sistema de videovigilancia, incluyendo constancias de acceso, extracción, copia, transferencia, verificación de integridad, hash, actas de revisión, reportes de auditoría y demás metadatos de control, podrán conservarse por un plazo de siete (7) años, sin que ello implique la conservación generalizada de la totalidad de las grabaciones de video por dicho período.

El acceso a las grabaciones y a los registros asociados estará restringido exclusivamente al personal autorizado, conforme a perfiles de acceso. Toda visualización, extracción, copia, o eliminación de grabaciones deberá quedar registrada mediante mecanismos que permitan identificar, como mínimo, la persona interviniente, fecha, hora, motivo, archivo afectado y acción realizada.

Se realizarán verificaciones periódicas de integridad y calidad sobre los archivos multimedia mediante muestreo aleatorio de tramos, incluyendo el inicio, medio y fin de los archivos seleccionados. Esta verificación se ejecutará con frecuencia trimestral, garantizando al menos una muestra por semana, con el objeto de validar la continuidad de las grabaciones, la legibilidad de las imágenes y la adecuada conservación de las evidencias necesarias para la seguridad física de la ACR-Py.

Los ambientes de nivel 4 disponen de sensores de detección de movimiento que se mantienen activos hasta tanto se cumpla el procedimiento autorizado de ingreso. Una vez que el ambiente queda por debajo del mínimo de personas autorizadas exigido, los sensores se reactivan automáticamente.

El sistema de alarmas emplea al menos dos medios de aviso: sonoro y visual.

Los sistemas de monitoreo por video y de alarmas operan bajo supervisión permanente de personal calificado ubicado en ambiente de nivel 3. La sala de monitoreo cuenta, a su vez, con cámaras propias que registran las acciones del personal a cargo.

5.1.2.2 Mecanismos de emergencia

La ACR-Py implementa mecanismos específicos para preservar la seguridad de su personal y de sus equipos ante situaciones de emergencia. Estos mecanismos permiten la apertura manual de las puertas para la evacuación de los ambientes con control de acceso. La utilización de dichas salidas activa de inmediato las alarmas correspondientes de apertura.

La ACR-Py podrá incorporar mecanismos de emergencia adicionales conforme a las particularidades de cada instalación. Todos los procedimientos asociados se encuentran documentados y se someten a verificación periódica mediante simulacros de situaciones de emergencia.

5.1.3. Energía y aire acondicionado

La infraestructura de la ACR-Py cuenta con sistemas y dispositivos que garantizan el suministro ininterrumpido de energía eléctrica.

Además de la conexión a la red eléctrica pública, las instalaciones disponen de redundancia integral de los sistemas de energía y climatización, a fin de asegurar la operación continua aun ante interrupciones del suministro externo, mediante:

a) generador eléctrico de capacidad compatible con la carga operativa;
b) generador eléctrico de reserva en configuración redundante;

c) sistemas de alimentación ininterrumpida (UPS) redundantes;
d) sistema de puesta a tierra y protección contra descargas atmosféricas; e
e) iluminación de emergencia.

Todos los cables eléctricos se encuentran protegidos por tuberías o ductos apropiados. Se utilizan canalizaciones, ductos, bandejas, tableros y cajas de paso, distribución y terminación diseñados para facilitar las inspecciones y la detección de intentos de manipulación. Los cables de energía, telefonía y datos circulan por ductos separados.

Todo el cableado se encuentra catalogado, identificado y se somete a inspección periódica al menos cada 6 (seis) meses, en búsqueda de evidencias de violación u otras anomalías.

El sistema de climatización satisface los requisitos de temperatura y humedad exigidos por los equipos del ambiente, dispone de filtros de polvo y opera de manera independiente del sistema de climatización del edificio que lo aloja.

En los ambientes de nivel 4, el sistema de climatización es independiente, tolerante a fallas y redundante, integrado por equipos de aire acondicionado de precisión y de refrigeración de confort para el área administrativa y demás ambientes. El sistema correspondiente al nivel 4 es interno, con renovación de aire únicamente mediante apertura de puerta, y la temperatura de los ambientes así climatizados se monitorea permanentemente a través del sistema de alarmas.

5.1.4. Exposición al agua

La estructura integral del nivel 4, provee protección física contra exposición a agua, filtraciones e inundaciones provenientes de cualquier fuente externa. Asimismo, cuenta con mecanismos de detección de humedad integrados a los sistemas de monitoreo y alarma.

5.1.5. Prevención y protección contra incendios

En las instalaciones de la ACR-Py no está permitido fumar ni portar objetos que generen fuego o chispas.

Las instalaciones cuentan con sistema de detección de humo, sistema de detección temprana de incendios mediante análisis de partículas iónicas, y sistema de extinción por gas inerte, no corrosivo, no combustible y no reactivo con la mayoría de las sustancias.

Los sistemas de prevención contra incendios internos permiten alarmas preventivas antes de la aparición de humo visible, activándose únicamente ante la detección de partículas que evidencien sobrecalentamiento de materiales eléctricos u otros materiales combustibles.

En caso de incendio, el aumento de la temperatura interna dentro del rack cofre no deberá superar los 50 (cincuenta) grados Celsius, debiendo la sala soportar dicha condición por al menos 1 (una) hora.

5.1.7. Eliminación de residuos

Todos los documentos en papel que contengan información sensible son destruidos mediante trituración antes de ir como residuos. Todos los dispositivos electrónicos en desuso que hayan sido utilizados para el almacenamiento de información sensible son borrados de manera irreversible o destruidos físicamente.

5.1.8. Respaldo fuera de sitio

La ACR-Py dispone de una instalación de respaldo (off-site) que cumple con los mismos requisitos de seguridad que la instalación principal. Su ubicación se encuentra geográficamente separada, de modo que ante un siniestro que torne inoperante a la instalación principal, la instalación de contingencia no resulte afectada y pueda alcanzar plena operación en condiciones idénticas dentro de un plazo máximo de 48 (cuarenta y ocho) horas.

5.2. Controles procedimentales

5.2.1. Roles de confianza

La ACR-Py garantiza la segregación de tareas para las funciones críticas, con el objetivo de evitar conflictos de interés y proveer la seguridad adecuada de las operaciones. Las acciones de cada persona se encuentran limitadas conforme al perfil que tiene asignado.

La ACR-Py establece los siguientes perfiles confiables diferenciados: coordinación de infraestructura, coordinación de seguridad, operación de la ACR-Py, auditoría, y depositarios de la clave de activación de las cadenas de certificación. La distribución de responsabilidades es la siguiente:

a) Coordinación de infraestructura: planificar, coordinar y supervisar los procesos de gestión de los recursos tecnológicos de infraestructura, especialmente los relacionados con software, sistemas de información, bases de datos y redes de comunicación; mantener la disponibilidad de la infraestructura para la publicación de la información; coordinar las actividades de implantación y mantenimiento de los sistemas de información y criptográficos de la ACR-Py; realizar la instalación, personalización e integración de los sistemas adquiridos o desarrollados en el ámbito de la ACR-Py; responsable de la gestión de cambios y del control de configuraciones.

b) Coordinación de seguridad: planificar, coordinar y supervisar la gestión de continuidad de la ACR-Py, del repositorio de Políticas de Firma, certificados y CRL/LCR; coordinar las actividades de política de acceso y gestión del entorno de TI; mantener la integridad, confidencialidad y seguridad de la información tratada por la ACR-Py; dar seguimiento a las investigaciones y evaluaciones de daños derivados de brechas de seguridad; responsabilizarse de la implementación de las prácticas y políticas de seguridad y de la gestión de los operadores de la ACR-Py; identificar, mapear y analizar los riesgos;

elaborar planes de acción para los riesgos identificados; y elaborar el plan de contingencia tecnológico de la infraestructura de la ACR-Py.

c) Operación de la ACR-Py: gestionar la implantación, mantenimiento y operación de los sistemas criptográficos de la ACR-Py; gestionar el ciclo de vida de los certificados; coordinar la emisión, publicación y revocación de los certificados; administrar los contenidos de los repositorios de la ACR-Py y coordinar los procesos de gestión del personal involucrado en sus actividades.

d) Auditoría: responsable de supervisar y fiscalizar el cumplimiento de las actividades de certificación conforme a las normas y orientaciones de la ACR-Py; responsable de verificar el cumplimiento de la presente PC/DPC y de la Política de Seguridad en el ámbito de la ACR-Py.

e) Depositarios de la clave de activación de las cadenas de certificación: personas designadas, en representación del MIC, que custodian las claves para la activación de las cadenas de certificación, necesarias para la operación del módulo de seguridad criptográfico (HSM) de la ACR-Py.

5.2.2. Número de personas requerido por tarea

El acceso al sistema de gestión de certificados — utilizado para la generación y revocación de certificados y la generación de la CRL/LCR — se realiza mediante control multiusuario con secreto compartido (*split-secret*), por personal con roles de confianza.

Las claves privadas de las cadenas de certificación de la ACR-Py se almacenan en hardware criptográfico (HSM) ubicado dentro del ambiente seguro del rack cofre. Se establece la exigencia de control múltiple para la utilización de las claves privadas de la ACR-Py, de modo que se requiere la concurrencia de al menos 3 (tres) de los 5 (cinco) personas con roles de confianza para activar las claves privadas.

Todas las tareas ejecutadas en el ambiente donde se encuentran los equipos de certificación de la ACR-Py requieren la presencia de al menos 2 (dos) operadores funcionarios o personal con roles de confianza con perfiles habilitados. Las demás tareas de la ACR-Py podrán ser ejecutadas por un único operador con perfil habilitado.

5.2.3. Identificación y autenticación para cada rol

Para la designación de la persona que asume un rol de confianza, la ACR-Py ejecuta una verificación de antecedentes. Cada función descrita en el ítem 5.2.1 es identificada y autenticada de modo que la persona designada se encuentre asignada a la función correcta y pueda apoyar adecuadamente las actividades de la ACR-Py.

Toda persona con rol de confianza en la ACR-Py tiene su identidad y perfil verificado antes de:
a) ser incorporados a la lista de acceso a las instalaciones de la ACR-Py;
b) ser incorporados a la lista de acceso físico al sistema de certificación de la ACR-Py;

c) recibir credenciales para ejecutar sus actividades operativas en la ACR-Py; y
d) recibir una cuenta de usuario en el sistema de certificación de la ACR-Py.

Los certificados, cuentas y contraseñas utilizados para la identificación y autenticación de los funcionarios o personal deben:
a) ser atribuidos directamente a una única persona;
b) no permitir compartición; y
c) encontrarse restringidos a las acciones asociadas al perfil para el cual fueron designados.

5.2.4. Roles que requieren separación de funciones

La ACR-Py impone la segregación de actividades para el personal específicamente asignado a las funciones definidas en el ítem 5.2.1
No se permite, en ningún caso, ejercer simultáneamente las siguientes funciones:
a) Coordinación de Infraestructura y Operación de la ACR-Py;
b) Coordinación de Seguridad y Operación de la ACR-Py;
c) Auditoría y Coordinación de Infraestructura o de Seguridad;
d) Auditoría y Operación de la ACR-Py.

5.3. Controles sobre el personal

5.3.1. Requerimientos de experiencia, capacidades y autorización

Todo personal de la ACR-Py que desempeñe actividades directamente relacionadas con el ciclo de vida de los certificados — emisión, expedición, distribución, revocación y gestión — es admitido conforme a lo establecido en la Política de Seguridad de la ICPP.

El personal de la ACR-Py que ejerce roles de confianza o ejecuta funciones críticas formalizará mediante contrato o acta de responsabilidad:
a) los términos y condiciones del perfil que ocupan; y
b) el compromiso de no divulgar la información confidencial a la que tienen acceso.

Antes de la incorporación de cualquier persona al proceso de gestión de certificados, la ACR-Py verifica la identidad y la confiabilidad de dicha persona.

La ACR-Py mantiene una dotación suficiente de personal que posee el conocimiento especializado, la experiencia y las calificaciones necesarias para las actividades que desempeña.

El personal de la ACR-Py cumple los requisitos del cargo mediante conocimiento especializado, experiencia y calificaciones, acreditados a través de capacitación y educación formales y de experiencia efectiva.

El personal de la ACR-Py tiene atribuciones definidas en función de su nivel de responsabilidad, considerando la sensibilidad de la posición, los deberes asignados, los niveles de acceso, los antecedentes verificados, la capacitación recibida y la idoneidad acreditada.

5.3.2. Procedimientos de verificación de antecedentes

Todo el personal de la ACR-Py con rol de confianza debe encontrarse libre de conflictos de interés que puedan comprometer la imparcialidad de las operaciones de la ACR-Py. No será designada para cumplir con un rol de confianza ninguna persona cuyos antecedentes resulten incompatibles con el cargo.

Las personas designadas a roles de confianza son seleccionadas en base a lealtad, confiabilidad e integridad, y se encuentran sujetas a investigación de antecedentes.

Todo el personal de la ACR-Py en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de certificados es anualmente sometido a:
a) verificación de antecedentes penales;
b) verificación de antecedentes judiciales;
c) verificación de empleos anteriores;
d) verificación de antecedentes académicos; y
e) suscripción de actas o su equivalente de confidencialidad y de responsabilidad específicas.
El personal no accede a las funciones de confianza hasta tanto se hayan concluido las verificaciones necesarias y analizado sus resultados.

5.3.3. Requisitos de capacitación

Todo el personal de la ACR-Py en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de certificados recibe capacitación suficiente para el dominio de los siguientes temas:
a) política y procedimientos de seguridad de la ACR-Py;
b) software de certificación y hardware en uso en la ACR-Py;
c) procedimientos de recuperación ante desastres y de continuidad de negocio; y
d) actividades bajo su responsabilidad.
e) normativa vigente que rige la materia
La ACR-Py mantiene registros de las capacitaciones realizadas y asegura que el personal mantenga el nivel de habilidades que les permita desempeñar sus tareas satisfactoriamente.

5.3.4. Frecuencia y requisitos de actualización de conocimientos

Todo el personal de la ACR-Py en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de certificados se mantiene actualizado sobre los eventuales cambios tecnológicos en el sistema de certificación.

La ACR-Py provee capacitación en seguridad de la información y gestión del entorno seguro a las personas directamente relacionadas con los procesos de certificación. Las capacitaciones de actualización se realizan siempre que sea necesario.

5.3.5. Frecuencia y secuencia de rotación de puestos

No se encuentra definida una frecuencia específica para la rotación de cargos. No obstante, la ACR-Py garantiza que toda modificación en la composición de su personal no afectará la eficacia operativa ni la seguridad de sus servicios.

5.3.6. Sanciones por acciones no autorizadas

Todo personal de la ACR-Py que ejerza roles de confianza o ejecute funciones críticas quedará sujeto de manera uniforme a los procesos de evaluación, control de seguridad, capacitación, así como a las disposiciones establecidas en la Política de Seguridad de la ICPP para el desarrollo de sus actividades.

Ante la eventualidad de una violación de las políticas o de una acción no autorizada realizada por una persona involucrada en los procesos de emisión, expedición, distribución, revocación o gestión de certificados, la ACR-Py suspende de inmediato su acceso y privilegios hasta tanto se concluya la investigación, adoptando las medidas administrativas y legales pertinentes y aplicando las sanciones que correspondan al caso.

5.3.7. Requisitos de contratación de terceros independientes

Los terceros independientes, contratistas, consultores, proveedores de servicios o personal externo que intervengan en actividades vinculadas a la operación de la ACR-Py deberán cumplir, en lo que resulte aplicable, con la Política de Seguridad de la ICPP, la presente PC/DPC y los procedimientos internos correspondientes.

5.3.8. Documentación suministrada al personal

La ACR-Py pone a disposición de todo su personal:
a) la PC/DPC de la ACR-Py;
b) la Política de Seguridad de la ICPP;
c) la documentación operacional relativa a sus actividades; y
d) los contratos, normas, políticas y demás información que resulten relevantes para sus actividades.

5.4. Procedimientos de auditoría de registros

5.4.1. Tipos de eventos registrados

Los registros de auditoría se generan para todos los eventos relacionados con la operación, la seguridad y demás servicios de la ACR-Py. Siempre que sea posible, los registros se generan automáticamente; cuando ello no resulte factible, se utiliza un libro de registro, formulario en papel u otro mecanismo físico. Todos los registros de auditoría de seguridad — electrónicos o no — son mantenidos.

La ACR-Py garantiza que todos los eventos relacionados con los procesos de gestión de certificados se registran de manera que permitan su trazabilidad. Todas las acciones ejecutadas por el personal de la ACR-Py en el desempeño de sus atribuciones se registran de modo que cada acción quede asociada a la persona que la realizó.

La ACR-Py registra en archivos de auditoría todos los eventos relacionados con la seguridad del sistema de certificación. Entre otros, deben incluirse obligatoriamente:
a) inicio y apagado del sistema de certificación;
b) intentos de crear, eliminar, definir contraseñas o modificar los privilegios de sistema de los operadores de la ACR-Py;
c) cambios en la configuración de la ACR-Py y/o en sus claves;
d) cambios en las políticas de creación de certificados;
e) intentos de acceso (login) y de salida del sistema (logoff);
f) intentos no autorizados de acceso a los archivos del sistema;
g) generación de claves propias de la ACR-Py;
h) emisión y revocación de certificados;
i) generación de LCR;
j) intentos de crear, eliminar, habilitar y deshabilitar usuarios, y de actualizar y recuperar sus credenciales; y
k) operaciones fallidas de escritura y lectura en el directorio de certificados y de las LCR.

Todos los registros — electrónicos o manuales — deben contener la fecha y hora del evento y la identificación del usuario que lo realizó. La ACR-Py también recopila y consolida, de manera electrónica o manual, información de seguridad no generada directamente por el sistema de certificación, tal como:
a) registros de accesos físicos;
b) mantenimiento y cambios en la configuración de los sistemas;
c) cambios de funcionario/personal y de su rol de confianza;
d) reportes de discrepancia y de compromiso; y
e) registros de destrucción de medios que contengan claves criptográficas, datos de activación de certificados o información personal de usuarios.

A fin de facilitar el proceso de auditoría, todos los registros se recopilan y consolidan, de manera electrónica o manual, en un lugar único, conforme a la Política de Seguridad de la ICPP.

5.4.2. Frecuencia de procesamiento del registro

La ACR-Py garantiza que sus registros de auditoría son analizados dependiendo de su criticidad o ante caso de sospecha de compromiso de seguridad.

Todos los eventos significativos se describen en un informe de auditoría. Dicho análisis comprende una inspección breve de todos los registros, verificando que no hayan sido alterados, seguida de una

investigación más detallada de las alertas o irregularidades observadas. Todas las acciones adoptadas como resultado de este análisis se documentan.

5.4.3. Período de conservación del registro de auditoría

La ACR-Py mantiene en sus propias instalaciones — principal y de respaldo — sus registros de auditoría por un período mínimo de 10 (diez) años, o mayor cuando así lo exija la ley. La ACR-Py pone dichos registros a disposición del auditor, previa solicitud.

5.4.4. Protección del registro de auditoría

El sistema de registro de eventos de auditoría incluye mecanismos de protección de los archivos de auditoría contra lectura no autorizada, modificación y eliminación. A su vez, la información manual de auditoría se protege igualmente contra lectura no autorizada, modificación y eliminación.

Los eventos se registran de manera que se encuentren protegidos contra eliminación o destrucción (con excepción de su transferencia a soporte de largo plazo).

Los registros de eventos se protegen para evitar alteraciones y detectar adulteración, garantizando que únicamente las personas con acceso autorizado puedan realizar operaciones, preservando la integridad, autenticidad y, cuando sea necesario, la confidencialidad de los datos.

5.4.5. Procedimientos de respaldo del registro de auditoría

Los registros de eventos y los resúmenes de auditoría del sistema de gestión de certificados, las plataformas criptográficas y demás componentes de la infraestructura cuentan con copias de seguridad semanales, mensuales y anuales, o siempre que se utilicen tales equipos cuando se encuentren en ambiente off-line.

Los registros de auditoría se almacenan en un lugar seguro (rack cofre o caja fuerte) a prueba de incendio, bajo el control de personas autorizadas en función de confianza, y en un lugar distinto de los componentes que los originaron. Las copias de seguridad se protegen con el mismo grado de seguridad que los originales.

5.4.6. Sistema de recolección de auditoría

El sistema de recolección de datos de auditoría interno de la ACR-Py es una combinación de procesos automatizados y manuales, ejecutados por su personal operativo o por sus sistemas.

Los procesos de auditoría comienzan con el inicio de los sistemas y finalizan únicamente con su apagado. El sistema garantiza la integridad y disponibilidad de los datos recopilados y, cuando sea necesario, protege su confidencialidad.

5.4.7. Notificación al sujeto causante del evento

Cuando un evento es registrado por el conjunto de sistemas de auditoría, no se envía notificación a la persona, organización, dispositivo o aplicación que lo causó. No obstante, los eventos considerados como posibles violaciones de seguridad que involucren el ciclo de vida de los certificados o la infraestructura son escalados al equipo de seguridad a fin de adoptar las medidas correspondientes de corrección o mitigación.

5.4.8. Evaluaciones de vulnerabilidad

Los eventos que representen posibles vulnerabilidades detectadas en el análisis de los registros de auditoría son analizados en detalle y, dependiendo de su gravedad, son registrados de manera separada. Como consecuencia, se implementan y registran acciones correctivas a efectos de auditoría.

La ACR-Py realiza también evaluaciones regulares de vulnerabilidad que abarcan los principales activos relacionados con la emisión, divulgación y gestión de certificados.

5.5. Archivo de registros

5.5.1. Tipos de registros archivados

La ACR-Py almacena registros con el detalle suficiente para establecer la validez de una firma y la operación adecuada del sistema de la ACR-Py.

Se almacenan tanto la información de auditoría detallada en el numeral 5.4.1 como los procesos de habilitación de PCSC.

5.5.2. Período de retención del archivo

La documentación relativa a los eventos referidos en el numeral anterior se retiene por los siguientes períodos:

a) los certificados emitidos por la ACR-Py y sus respectivas LCR deberán retenerse permanentemente, para fines de consulta histórica;

b) las copias de los procesos de habilitación de PCSC, por un mínimo de 30 (treinta) años a contar desde la fecha de expiración o revocación del certificado; y

c) las demás informaciones, incluidos los archivos de auditoría, deberán retenerse por un mínimo de 10 (diez) años.

5.5.3. Protección del archivo

Todos los archivos son protegidos y almacenados físicamente con los mismos requisitos de seguridad que los de su instalación. Las copias de seguridad se mantienen en un lugar distinto y separado del que las originó, con requisitos equivalentes de seguridad y disponibilidad.

Los archivos se crean de modo que no puedan ser eliminados ni destruidos (con excepción de su transferencia a soporte de largo plazo) durante el período de retención obligatorio. Las protecciones de

archivado aseguran que únicamente el acceso confiable autorizado pueda realizar operaciones, preservando la integridad, autenticidad y confidencialidad de los datos. Si el soporte original no pudiera retener los datos por el período requerido, se define un mecanismo de transferencia periódica de los datos archivados a nuevos soportes.

5.5.4. Procedimientos de respaldo de archivo

Una segunda copia de todo el material descrito en el numeral 5.4.1 se almacena en un lugar externo a la ACR-Py, recibiendo el mismo tipo de protección utilizado por la ACR-Py. Estas copias respetan los períodos de retención definidos para los registros originales. La ACR-Py verifica la integridad de las copias de seguridad como mínimo una (1) vez al año.
Se realizan copias de seguridad para el archivado de los sistemas de la ACR-Py — en línea y off-line. Las copias se almacenan en un cofre de medios con clasificación contra fuego. La copia de seguridad de la información del ambiente off-line se realiza al finalizar cada ceremonia y se almacena en un lugar fuera del ambiente, siguiendo los mismos criterios de seguridad.

5.5.5. Requisitos de fecha y hora de los registros

La información de fecha y hora asociada a los registros archivados por la ACR-Py se basará en el Tiempo Universal Coordinado —Coordinated Universal Time, UTC— o en una fuente de tiempo confiable.
La fecha y hora deberán registrarse, cuando corresponda, en el formato YYYYMMDDHHMMSSZ, incluyendo los segundos aun cuando su valor sea cero.
Los sistemas automatizados deberán mantener mecanismos de sincronización horaria y control de cambios de fecha y hora. En los procedimientos manuales o ejecutados en ambientes fuera de línea, deberán consignarse la fecha y hora oficial, preservando la trazabilidad del evento registrado.

5.5.6. Sistema de recolección de archivo

Todos los sistemas de recopilación de datos de archivo utilizados por la ACR-Py en sus procedimientos operativos son internos. El sistema de recopilación cumple con los requisitos de seguridad establecidos en el ítem 5.

5.5.7. Procedimientos para obtener y verificar información archivada

Los soportes de almacenamiento de la información en la medida posible son verificados en su creación. Periódicamente se prueban muestras de la información archivada para verificar la integridad y legibilidad continuas de los datos, mediante procedimientos de restauración.
Solamente los equipos autorizados de la ACR-Py, el personal con rol de confianza y otras personas autorizadas pueden acceder a los archivos. Las solicitudes de obtención de información son coordinadas por los administradores del ambiente seguro conforme sus roles de confianza (Auditoría, Coordinación de Infraestructura y Coordinación de Seguridad).

La verificación de información del archivo debe ser solicitada formalmente a la ACR-Py, identificando con precisión el tipo y el período de la información a verificar. El solicitante debe encontrarse debidamente identificado.

5.6. Cambio de clave

El PCSC deberá iniciar, hasta 3 (tres) meses antes de la fecha de expiración de su certificado, el proceso de generación del nuevo par de claves y de emisión del nuevo certificado.

Revocado o expirado el certificado de un PCSC, la ACR-Py remueve de inmediato dicho certificado del directorio y de su sitio web oficial, manteniéndolo almacenado permanentemente para fines de consulta histórica.

Las claves privadas utilizadas para firmar los certificados de los PCSC deben mantenerse hasta el momento en que todos los certificados de los PCSC firmados con ellas hayan expirado.

5.7. Compromiso y recuperación ante desastres

5.7.1. Procedimientos de gestión de incidentes y compromisos

La ACR-Py cuenta con un Plan de Continuidad de Negocio (PCN) de acceso restringido, para garantizar la continuidad de sus servicios críticos. Cuenta asimismo con un Plan de Respuesta a Incidentes y un Plan de Recuperación ante Desastres.

La ACR-Py revisa y actualiza si es requerido estos procedimientos bienalmente (cada dos años) El Plan de Continuidad de Negocio incluye, como mínimo:
a) las condiciones para activar el plan;
b) procedimientos de emergencia;
c) procedimientos de respaldo o fallback;
d) procedimientos de restauración;
e) cronograma de mantenimiento del plan;
f) requisitos de concientización y formación;
g) responsabilidades individuales;
h) Objetivo de Tiempo de Recuperación (RTO);
i) pruebas regulares de los planes de contingencia;
j) plan para mantener o restaurar las operaciones de la ACR-Py de manera oportuna tras la interrupción o falla de procesos críticos;
k) definición de requisitos para almacenar material criptográfico crítico en una ubicación alternativa;
l) definición de interrupciones aceptables del sistema y del tiempo de recuperación correspondiente;
m) frecuencia de realización de copias de respaldo;
n) distancia entre las instalaciones de recuperación y el sitio principal de la ACR-Py; y
o) procedimientos para proteger las instalaciones tras un desastre y antes de restaurar el ambiente seguro en el sitio original o remoto.

Todo incidente de seguridad que afecte o pueda afectar la confidencialidad, integridad, disponibilidad, autenticidad, continuidad, trazabilidad o confiabilidad de la ACR-Py, de los certificados, de las CRL/LCR, de la Lista de Confianza, de la clave privada raíz, de los HSM, de los repositorios, de los sistemas de publicación o de los servicios de confianza deberá ser comunicado a la AA dentro del plazo máximo de veinticuatro (24) horas contado desde su conocimiento.

Cuando el incidente pueda afectar a PCSC, PU, datos personales, servicios cualificados, reconocimiento mutuo, interoperabilidad o confianza pública, la comunicación deberá incluir alcance, impacto, medidas de contención, necesidad de revocación, necesidad de actualización de la Lista de Confianza, medidas correctivas y responsable de seguimiento.

La ACR-Py conservará evidencia de detección, clasificación, comunicación, contención, erradicación, recuperación, cierre y lecciones aprendidas.

5.7.2. Procedimientos de recuperación ante corrupción de recursos informáticos, software o datos

La ACR-Py mantiene un sitio de contingencia geográficamente separado que replica su instalación principal, de modo que, ante la corrupción de software o datos, la operación pueda restaurarse desde el sitio de respaldo mediante una conexión segura.

Si algún equipo resulta dañado o inoperante pero las claves privadas no se hubieran destruido, la operación se restablecerá a la mayor brevedad posible, priorizando la capacidad de generar información de estado de certificados (LCR), conforme al Plan de Recuperación ante Desastres de la ACR-Py. Los demás procedimientos se detallan en el PCN de la ACR-Py.

5.7.3. Procedimientos en caso de compromiso de clave privada de entidad

Ante el compromiso, sospecha de compromiso, pérdida, destrucción o imposibilidad de uso seguro de una clave privada de la ACR-Py o de un PCSC, se activarán los procedimientos de respuesta a incidentes, continuidad, recuperación, revocación y comunicación previstos en la presente PC/DPC y en los planes aplicables.

Cuando el incidente afecte la clave privada de la ACR-Py, se notificará inmediatamente a la AA, a los PCSC, a las PU y a las demás entidades que correspondan, adoptándose las medidas necesarias para preservar la confianza de la ICPP.

Cuando el incidente afecte la clave privada de un PCSC, dicho prestador deberá comunicarlo inmediatamente a la AA, a fin de que se adopten las medidas de revocación, actualización de estado, notificación y sustitución de claves que correspondan.

Los demás procedimientos se detallan en el PCN de la ACR-Py.

5.7.4. Capacidades de continuidad del negocio después de desastre

El equipo de infraestructura y seguridad empleará todos los medios razonables para monitorear las instalaciones de la ACR-Py luego de un desastre natural o de otra naturaleza, a fin de proteger contra pérdidas, daños adicionales y robo de materiales e información confidencial.
El Plan de Recuperación ante Desastres, junto con el PCN descritos en el ítem 5.7.1, establecen procedimientos para que la información de estado de certificados se encuentre disponible.

5.8. Terminación, cese o sucesión de la ACR-Py

La ACR-Py mantendrá un Plan de Cese, Terminación o Sucesión aprobado formalmente, actualizado y probado periódicamente, destinado a preservar la confianza, continuidad, verificabilidad histórica y seguridad de la ICPP.

Cuando resulte necesario cesar, sustituir, reorganizar o transferir la operación de la ACR-Py, deberán adoptarse, como mínimo, las siguientes medidas:
a) decisión formal y fundada de la AA;
b) designación de autoridad sucesora, mecanismo de transición o esquema de cierre ordenado;
c) comunicación a todos los PCSC, OEC, PSS, PU y entidades afectadas;
d) publicación de aviso oficial en el repositorio y en la Lista de Confianza;
e) conservación de certificados, CRL/LCR, registros, evidencias, actas, auditorías y documentación durante el período legal aplicable y necesario para la validación;
f) mantenimiento de servicios de estado, repositorio y validación histórica durante el período necesario;
g) emisión de CRL/LCR final o extraordinaria cuando corresponda;
h) revocación, sustitución o migración de certificados emitidos por la ACR-Py, conforme al plan aprobado;
i) destrucción, resguardo o transferencia controlada del material criptográfico conforme a ceremonia documentada;
j) auditoría extraordinaria del proceso de cese o sucesión;
k) preservación de la cadena de confianza histórica; y
l) publicación de constancia de cierre, sucesión o migración.

La ACR-Py deberá mantener operación mínima de soporte y validación histórica por un período no inferior a un (1) año desde la notificación de cese, salvo que exista sucesor plenamente operativo que asuma tales funciones, sin perjuicio de la conservación permanente de certificados y CRL/LCR para fines de validación histórica.

6. CONTROLES TÉCNICOS DE SEGURIDAD

Es competencia de la ACR-Py acompañar la evolución tecnológica y, cuando resulte necesario, actualizar los estándares y algoritmos criptográficos utilizados en la ICPP conforme a lo establecido en el DOC-ICPP-06 [3].

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves criptográficas de la ACR-Py se genera por la propia ACR-Py en un módulo criptográfico seguro, conforme a los estándares y algoritmos definidos en el DOC-ICPP-06 [3].

El par de claves criptográficas de un PCSC se genera por el propio PCSC, tras el otorgamiento de su habilitación y la consecuente autorización de funcionamiento en el ámbito de la ICPP.

Los algoritmos y dispositivos criptográficos a utilizar para las claves criptográficas de la ACR-Py se encuentran definidos en el DOC-ICPP-06 [3].

6.1.2. Entrega de la clave privada al titular de certificado

No aplica.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública generada bajo el exclusivo control del PCSC es entregada a la ACR-Py mediante una solicitud de certificado —CSR— que contenga la clave pública cuya certificación se solicita, en el formato y bajo los parámetros definidos en el DOC-ICPP-06 [3] y demás documentos ICPP aplicables. Los eventos correspondientes serán registrados a efectos de trazabilidad y auditoría.

6.1.4. Entrega de la clave pública de la ACR-Py a la Parte Usuaria

La entrega del certificado de la ACR-Py a la PU y demás participantes de la ICPP se realiza mediante alguna de las siguientes vías:
a) en el momento de la disponibilización del certificado a su titular;
b) en directorio;
c) en la página web de la ACR-Py o de los PCSC integrantes de la ICPP; o
d) por otros medios seguros definidos por la AA.
La clave pública de la ACR-Py será puesta a disposición de la PU mediante la publicación del certificado raíz correspondiente en su repositorio oficial.

6.1.5. Tamaños de clave

El tamaño de las claves criptográficas asimétricas de la ACR-Py y de los PCSC se encuentra definido en el DOC-ICPP-06 [3].

6.1.6. Generación de parámetros de clave pública y verificación de calidad

Los parámetros de generación de claves asimétricas de la ACR-Py adoptan los estándares definidos en el DOC-ICPP-06 [3].
Los parámetros se verifican conforme a las normas referenciadas en el DOC-ICPP-06 [3].

6.1.7. Propósitos de uso de clave

La clave privada de la ACR-Py se utiliza únicamente para la firma de su propio certificado, de los certificados de los PCSC y de su CRL/LCR.

6.2. Protección de la clave privada y controles de ingeniería del módulo criptográfico

La clave privada de la ACR-Py deberá ser generada, almacenada, activada, utilizada, respaldada, restaurada y destruida exclusivamente bajo controles criptográficos, físicos, lógicos y procedimentales compatibles con la criticidad de una Autoridad de Certificación Raíz nacional.

La clave privada de la ACR-Py no podrá existir ni ser expuesta en texto claro fuera del módulo criptográfico. Toda operación sobre la clave privada raíz requerirá ceremonia criptográfica documentada, control multiparte, segregación de funciones, registro de auditoría y evidencia verificable.

6.2.1. Estándares y controles del módulo criptográfico

El módulo criptográfico utilizado para la generación, custodia y uso de la clave privada de la ACR-Py deberá estar conforme a los estándares, niveles y parámetros definidos en el DOC-ICPP-06 [3].

6.2.2. Control multiparte 3 de 5 sobre la clave privada

La clave criptográfica de activación del componente seguro de hardware que almacena la clave privada de la ACR-Py se divide en cinco (5) partes y se distribuye entre cinco (5) personas designadas por la ACR-Py. Se requiere la concurrencia de al menos tres (3) de esas cinco (5) personas para la activación del componente y la utilización de la clave privada de la ACR-Py.

6.2.3. Custodia de la clave privada

No se permite la custodia (escrow) de la clave privada de la ACR-Py ni de las claves privadas de los PCSC. La ACR-Py mantiene bajo su exclusiva custodia su clave privada raíz, la cual es protegida conforme a los controles técnicos, físicos y procedimentales establecidos en la presente PC/DPC.

6.2.4. Respaldo de la clave privada

La ACR-Py podrá mantener copias de seguridad de su clave privada raíz únicamente en forma cifrada, utilizando mecanismos de envoltura de claves (key wrapping / wrapped) soportados por el módulo criptográfico seguro, bajo esquemas de control multiparte, segregación de funciones y ceremonia formalmente documentada.

Las copias de seguridad deberán conservarse con un nivel de protección físico, lógico, criptográfico y procedimental no inferior al de la clave original, en instalaciones seguras y geográficamente separadas. La ACR-Py no mantendrá copia de seguridad, custodia ni mecanismos de custodia (escrow) de las claves privadas de los PCSC.

6.2.5. Archivo de la clave privada

No aplica.

6.2.6. Transferencia de la clave privada hacia o desde un módulo criptográfico

La clave privada de la ACR-Py será generada dentro del módulo criptográfico seguro y no podrá ser exportada, transferida, almacenada ni tratada en texto claro fuera de dicho módulo.

Toda restauración, migración o transferencia lógica de material criptográfico deberá realizarse exclusivamente en forma cifrada, utilizando mecanismos de envoltura de claves (key wrapping / wrapped), entre módulos criptográficos seguros, bajo ceremonia documentada, control multiparte, doble control operativo, verificación de integridad, registro de auditoría y aprobación previa conforme al DOC-ICPP-06 [3].

Queda prohibido todo procedimiento que implique exposición, copia, impresión, almacenamiento temporal o manipulación de la clave privada raíz en texto claro.

6.2.7. Almacenamiento de la clave privada en módulo criptográfico

La clave privada de la ACR-Py deberá mantenerse dentro del módulo criptográfico seguro, protegida por los mecanismos criptográficos, físicos y lógicos establecidos en el DOC-ICPP-06 [3] y en esta PC/DPC.

6.2.8. Método de activación de la clave privada

La activación de la clave privada de la ACR-Py requerirá la concurrencia de al menos tres (3) de cinco (5) depositarios autorizados, conforme al esquema de control multiparte establecido en esta PC/DPC.

La activación deberá realizarse mediante dispositivos criptográficos o tokens asignados individualmente, datos de activación protegidos, autenticación individual, presencia física en entorno seguro, registro de auditoría y procedimiento ceremo nial u operativo correspondiente.

Ningún depositario podrá compartir, transferir, copiar, delegar o revelar sus datos de activación. La ACR-Py documentará la emisión, reposición, revocación, sustitución y destrucción de dispositivos y datos de activación.

6.2.9. Método de desactivación de la clave privada

Al finalizar toda operación autorizada, la clave privada de la ACR-Py deberá ser desactivada conforme al procedimiento del módulo criptográfico, eliminándose de la memoria operativa todo dato sensible asociado a la sesión. La desactivación deberá quedar registrada y verificada por los operadores presentes.

6.2.10. Método de destrucción de la clave privada

La destrucción de la clave privada de la ACR-Py, de sus copias de seguridad, de los datos de activación y de todo soporte que los haya alojado deberá ser documentado mediante acta firmada, bajo control multiparte, con identificación de medios, números de serie, método de destrucción, testigos, evidencias, y verificación de inutilización.

La destrucción deberá impedir la recuperación técnica del material criptográfico.

6.2.11. Calificación del módulo criptográfico

La calificación del módulo criptográfico adopta los estándares y niveles definidos por el DOC-ICPP-06 [3] y por la reglamentación aplicable aprobada por la AA.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Las claves públicas de la ACR-Py y de los PCSC se almacenan permanentemente, posteriormente a la expiración de los certificados correspondientes, para la verificación de firmas generadas durante su plazo de validez.

6.3.2. Períodos operacionales del certificado y períodos de uso del par de claves

La clave privada de la ACR-Py se utiliza únicamente durante el período de validez del certificado correspondiente. La clave pública de la ACR-Py podrá utilizarse durante todo el período determinado por la legislación aplicable para la verificación de firmas generadas durante el plazo de validez del certificado correspondiente.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de la clave privada de la ACR-Py serán generados mediante mecanismos criptográficamente seguros, con entropía suficiente, durante ceremonia documentada o procedimiento equivalente aprobado. Cada dato de activación será único, individual, no compartido y asignado a un depositario específico.

Los datos de activación se instalarán en dispositivos de control de acceso en hardware o tokens criptográficos, bajo evidencia de entrega, aceptación, custodia y responsabilidad individual.

6.4.2. Protección de datos de activación

Los datos de activación deberán conservarse bajo custodia individual, en dispositivos o medios protegidos, almacenados en nivel físico 6 o equivalente cuando no estén en uso. Queda prohibida su

copia, revelación, almacenamiento no autorizado, transmisión por canales no aprobados o uso por persona distinta al depositario asignado.

La pérdida, sospecha de compromiso, sustitución, cambio de depositario o daño del dispositivo de activación deberá notificarse de inmediato y dará lugar a revocación, sustitución o regeneración conforme al procedimiento aprobado.

6.4.3. Otros aspectos de los datos de activación

La ACR-Py mantendrá inventario actualizado de dispositivos, depositarios, entregas, reposiciones, revocaciones, destrucciones y eventos relacionados con datos de activación.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

La generación del par de claves de la ACR-Py y la emisión de certificados de los PCSC deberán realizarse en un ambiente off-line, a fin de impedir el acceso remoto no autorizado. La información utilizada en estos procedimientos debe mantenerse en el ambiente off-line, con acceso restringido.

Cada servidor de la ACR-Py directamente relacionado con los procesos de emisión, expedición, distribución, revocación y gestión de certificados deberá contar, como mínimo, con las siguientes características:
a) control de acceso a los servicios y perfiles de la ACR-Py;
b) clara separación de tareas y atribuciones relacionadas con cada perfil de la ACR-Py;
c) uso de criptografía para la seguridad de la base de datos;
d) generación y almacenamiento de registros de auditoría de la ACR-Py;
e) mecanismos internos de seguridad para garantía de la integridad de datos y procesos críticos; y
f) mecanismos para copias de seguridad (backup).

6.5.2. Calificación de seguridad informática

No aplica.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo del sistema

La ACR-Py utiliza software diseñado y desarrollado mediante una metodología formal rigurosa, específica para entornos de seguridad crítica.

6.6.2. Controles de gestión de seguridad

Se utiliza una metodología formal de gestión de configuración para la instalación y mantenimiento continuo del sistema de certificación de la ACR-Py. Las nuevas versiones del software solo se instalan tras comunicación del fabricante y pruebas en ambiente de homologación de la ACR-Py.

6.6.3. Controles de seguridad del ciclo de vida

Los sistemas y componentes críticos de la ACR-Py estarán sujetos a controles de seguridad durante todo su ciclo de vida, incluyendo adquisición, desarrollo, instalación, configuración, operación, mantenimiento, actualización, reemplazo y retiro seguro.

El retiro, sustitución o baja de sistemas, componentes, medios o soportes deberá realizarse mediante procedimientos documentados.

6.7. Controles de seguridad de red y aislamiento operacional

El servidor de la ACR-Py que aloja el sistema de certificación opera offline, físicamente desconectado de cualquier red.

6.8. Sello de tiempo

No aplica.

7. PERFILES DE CERTIFICADO, CRL/LCR Y OCSP

7.1. Perfil de certificado

El formato de todos los certificados emitidos por la ACR-Py cumple con el estándar ITU-T X.509 / ISO/IEC 9594, el perfil RFC 5280 y el DOC-ICPP-06 [3] observando que:
a) el certificado de la ACR-Py es el único certificado autofirmado de la ICPP, con validez máxima de veinte (20) años, salvo decisión fundada de la AA conforme al perfil establecido en el Anexo I;
b) el certificado del PCSC es firmado por la ACR-Py y posee validez limitada hasta diez (10) años, sin exceder la vigencia admitida por la AA. Ver Anexo II.

7.1.1. Número(s) de versión

El certificado raíz y los certificados emitidos a PCSC implementan la versión 3 de X.509.

7.1.2. Extensiones de certificado

Las extensiones obligatorias, criticidad y restricciones se establecen en los Anexos I y II.

7.1.3. Identificadores de objeto de algoritmo

El certificado de la ACR-Py y los certificados emitidos a PCSC se firman utilizando los algoritmos definidos en el DOC-ICPP-06 [3].

7.1.4. Formas de nombre

Los nombres del titular y del emisor del certificado de la ACR-Py, contenidos en el campo Distinguished Name (DN), son los mismos y siguen el estándar ITU-T X.501 (define el modelo y estructura de nombres) / ISO/IEC 9594-2 (referencia para la estructura de nombres en certificados), al

estándar X.509 (define el uso de esos nombres en certificados) y al perfil RFC 5280 (define el perfil obligatorio para PKI en Internet). Ver Anexos I y II.

7.1.5. Restricciones de nombre

Los campos del DN deberán codificarse conforme a RFC 5280, X.509 y los perfiles aplicables. Se admitirá el uso de cadenas UTF8String para nombres oficiales en idioma español; cuando la AA lo determine por razones de interoperabilidad, podrá requerirse una forma normalizada sin acentos o caracteres especiales.

7.1.6. Identificador de objeto de la política de certificado

El OID de la presente PC/DPC es 1.3.6.1.4.1.64751.1.1.

A efectos de la extensión Certificate Policies de los certificados emitidos por la ACR-Py a los PCSC, el OID 1.3.6.1.4.1.64751.1.1 identifica la política de certificado aplicable bajo el presente DOC-ICPP-01, salvo que la AA apruebe un OID específico para una política o tipo de servicio determinado.
Todo OID utilizado en certificados, CRL/LCR, políticas, perfiles o documentos normativos de la ICPP deberá encontrarse registrado, documentado y aprobado por la AA. La ACR-Py mantendrá un registro actualizado de OID asignados, su objeto, alcance, versión, estado y documento normativo asociado.

7.1.7. Uso de Name Constraints, Policy Constraints y pathLenConstraint

Los certificados emitidos por la ACR-Py que tengan la condición de autoridad de certificación deberán incorporar la extensión **Basic Constraints** conforme al RFC 5280 y a los perfiles establecidos en los Anexos I y II.

El certificado raíz de la ACR-Py incluirá **cA=TRUE** y **pathLenConstraint=1**, salvo decisión fundada de la AA conforme al perfil aplicable.

Los certificados emitidos por la ACR-Py a PCSC incluirán **cA=TRUE** y **pathLenConstraint=0**, a fin de impedir la emisión de certificados de AC subordinada por debajo del PCSC.
Las extensiones **Name Constraints** y **Policy Constraints** no se incorporarán como requisito general, salvo decisión expresa y fundada de la AA o cuando resulte necesario por razones de interoperabilidad, reconocimiento externo, certificación cruzada, restricción de nombres, políticas o alcance de confianza.

7.1.8. Sintaxis y semántica de calificadores de política

Cuando la extensión Certificate Policies incluya calificadores de política, éstos deberán ajustarse a la sintaxis y semántica admitidas por el RFC 5280.

7.1.9. Semántica de procesamiento para la extensión crítica Certificate Policies

No aplica, salvo que una política específica aprobada por la AA determine lo contrario.

7.2. Perfil de CRL/LCR

Las CRL/LCR emitidas por la ACR-Py deberán ajustarse al perfil X.509 v2 CRL previsto en el RFC 5280, al DOC-ICPP-06 [3] y al Anexo III de esta PC/DPC.

La CRL/LCR de la ACR-Py constituye la fuente técnica oficial para determinar el estado de revocación de los certificados emitidos por la ACR-Py.

La Lista de Confianza constituye la fuente oficial para determinar la habilitación, estado y alcance de los PCSC y servicios cualificados que prestan.

La emisión ordinaria de CRL/LCR no impedirá la emisión extraordinaria inmediata cuando exista revocación, compromiso de clave, incidente de seguridad, orden de autoridad competente o circunstancia que afecte la confianza en la ICPP.

7.2.1. Número(s) de versión

La ACR-Py implementa su CRL/LCR conforme a la versión 2 del estándar ITU-T X.509, de acuerdo con el perfil definido en el RFC 5280.

7.2.2. Extensiones de CRL/LCR y de sus entradas

Las extensiones obligatorias, criticidad y restricciones se establecen en el Anexo III.

7.3. Perfil de OCSP

OCSP no aplica como servicio operativo de verificación de estado en el nivel de la ACR-Py. El estado se verificará exclusivamente mediante CRL/LCR publicadas en el repositorio oficial.

La no aplicabilidad de OCSP en la ACR-Py no impide que los PCSC implementen OCSP para certificados finales, cuando así lo exijan sus políticas, la normativa de la ICPP, los estándares ETSI u otros estándares aplicables.

7.3.1. Número(s) de versión

No aplica.

7.3.2. Extensiones de OCSP

No aplica.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Las fiscalizaciones y auditorías realizadas en el ámbito de la ICPP tienen por objeto verificar que los procesos, procedimientos y actividades de los participantes de la ICPP se encuentren en conformidad con sus respectivas DPC, PC, PS, la Ley N.º 6822/2021, su reglamentación y demás normas y procedimientos establecidos para la ICPP.

8.1. Frecuencia o circunstancias de evaluación

La ACR-Py estará sujeta a evaluaciones de cumplimiento, auditorías o verificaciones específicas, con periodicidad no superior a veinticuatro (24) meses, o cuando lo disponga la AA por razones de seguridad, continuidad, incidente, cambio significativo, modificación de la PC/DPC, compromiso de clave, migración criptográfica, cese, sucesión o cualquier circunstancia que pueda afectar la confianza de la ICPP.

8.2. Identidad/calificaciones del evaluador

El evaluador o equipo evaluador deberá contar con competencia técnica y experiencia verificable en PKI, servicios de confianza, seguridad de la información, auditoría de sistemas, criptografía aplicada, gestión de riesgos y normas aplicables.
El proceso de evaluación deberá ser realizado por uno o más evaluadores que actúen con independencia, imparcialidad y objetividad asegurando:
a) separación de funciones,
b) ausencia de dependencia jerárquica directa con la DGCE,
c) ausencia de conflicto de interés real, potencial o aparente,
d) aplicación de mecanismos de revisión o supervisión adicionales, cuando sea necesario.

8.3. Relación del evaluador con la entidad evaluada

La auditoría de la ACR-Py deberá ser realizada por un evaluador o equipo evaluador independiente desde el punto de vista organizacional y funcional respecto de la DGCE.
El evaluador no podrá haber diseñado, implementado, operado, administrado y mantenido los controles que evalúa, salvo en supuestos expresamente permitidos por el esquema de evaluación aplicable y siempre que se preserve la independencia material.
Toda situación que pudiera constituir conflicto de interés deberá ser declarada y gestionada antes del inicio de la evaluación.

8.4. Temas cubiertos por la evaluación

Las auditorías y evaluaciones deberán cubrir, como mínimo y según el alcance aplicable, los siguientes ámbitos:
I. Cumplimiento normativo y documental

a) cumplimiento de la Ley N.º 6822/2021, Decreto N.º 7576/2022, resoluciones de la AA y documentos DOC-ICPP;
b) cumplimiento de la presente PC/DPC y demás documentos aplicables;

c) conformidad con la estructura documental definida en RFC 3647;

II. Cumplimiento técnico y criptográfico

d) perfiles de certificados conforme a RFC 5280 / ITU-T X.509;

e) CRL/LCR, OID, nombres, extensiones, algoritmos y validación de cadena (path validation);

f) ciclo de vida de claves: generación, custodia, uso, respaldo, restauración y destrucción;

g) dispositivos criptográficos (HSM), control multiparte, split-secret, datos de activación y ceremonias;

III. Controles de seguridad y operación

h) controles físicos, lógicos y de red;

i) operación offline, transferencia segura y repositorios;

j) identificación, autenticación, representación y validación de atributos;

IV. Operación del servicio de certificación

k) revocación, CRL/LCR, gestión de incidentes;

l) continuidad del negocio, recuperación ante desastres y cese;

m) gestión de riesgos, SGSI, vulnerabilidades y protección de datos;

V. Confianza e interoperabilidad

n) Lista de Confianza de la ICPP: publicación, estados y trazabilidad;

VI. Estándares y esquemas de evaluación (cuando corresponda)

o) WebTrust for CAs y Baseline Requirements del CA/Browser Forum;

p) ETSI EN 319 401, 319 411-1, 319 411-2, 319 412 y ETSI TS 119 612;

q) ISO/IEC 27001, 27002, 27005 e ISO 21188;

VII. Evidencia y trazabilidad

r) documentación, registros, evidencias, archivos, trazabilidad y conservación.

8.5. Acciones adoptadas como resultado de una deficiencia

Todo hallazgo deberá clasificarse, como mínimo, en Crítico, Alto, Medio o Bajo, considerando impacto en la confianza, seguridad, legalidad, continuidad, interoperabilidad y cumplimiento.

Los hallazgos críticos y altos deberán dar lugar a la definición e implementación de acciones correctivas inmediatas. En caso de hallazgos críticos, la AA podrá disponer medidas tales como la suspensión de emisión, revocación de certificados, activación de planes de contingencia, notificación de incidentes, actualización de la Lista de Confianza o medidas equivalentes cuando corresponda.

La ACR-Py mantendrá un registro de hallazgos, acciones correctivas, responsables, plazos, evidencias de cierre, verificación independiente y aceptación residual de riesgo, cuando esta última sea admisible.

8.6. Comunicación de resultados

Los resultados de auditoría o evaluación deberán documentarse y comunicarse a la AA. Cuando se trate de evaluación de conformidad de servicios cualificados, el informe deberá contener detalle suficiente para que la AA concluya fehacientemente el cumplimiento de los requisitos legales, técnicos y operativos aplicables.

La ACR-Py podrá publicar constancias, resúmenes ejecutivos o estados de conformidad sin divulgar información sensible, material criptográfico, configuraciones críticas, vulnerabilidades explotables o información que pueda comprometer la seguridad.
La ACR-Py publicará, cuando corresponda, una constancia o resumen de conformidad que indique el esquema evaluado, período cubierto, entidad evaluadora, alcance, resultado general y fecha de emisión, sin divulgar información sensible, vulnerabilidades explotables, detalles de configuración, material criptográfico ni información que comprometa la seguridad de la ICPP.
Cuando existan hallazgos críticos, la constancia deberá reflejar que la conformidad se encuentra condicionada, suspendida o no otorgada, según corresponda.
La matriz de conformidad, el plan de acciones correctivas y las evidencias de cierre deberán conservarse durante el período de retención aplicable.

9. OTROS ASUNTOS JURÍDICOS, ECONÓMICOS Y ADMINISTRATIVOS

9.1. Tarifas

9.1.1. Tarifas de emisión y renovación de certificados

Las tarifas de emisión y renovación de certificados por la ACR-Py se encuentran definidas en el documento Política Tarifaria (DOC-ICPP-13).

9.1.2. Tarifas de acceso al certificado

No aplica. La consulta del certificado raíz y de la información pública del repositorio es gratuita.

9.1.3. Tarifas de revocación o acceso a información de estado

No existe tarifa por consulta de CRL/LCR o información de estado publicada por la ACR-Py.

9.1.4. Tarifas por otros servicios

Las tarifas para otros servicios de la ACR-Py están definidas en el documento Política Tarifaria (DOC-ICPP-13).

9.1.5. Política de reembolso

No aplica.

9.2. Responsabilidad financiera

La responsabilidad financiera de la ACR-Py se rige por la normativa paraguaya y el régimen institucional aplicable a la AA.

9.2.1. Cobertura de seguro o garantía

No aplica para la ACR-Py.

Los PCSC deberán mantener vigente la póliza de seguro de responsabilidad civil, seguro de caución, aval bancario u otra garantía admitida conforme al artículo 10, numeral 3, inciso b), de la Ley N.° 6822/2021, el Decreto N.° 7576/2022 y las disposiciones complementarias dictadas por la AA conforme al alcance y riesgo de los servicios cualificados habilitados.
La ACR-Py podrá requerir evidencia de vigencia y cobertura de la garantía como condición para emitir, renovar, mantener o no revocar el certificado del PCSC.

9.2.2. Otros activos

No aplica.

9.2.3. Cobertura de seguro o garantía para entidades finales

No aplica en el ámbito de esta PC/DPC de la ACR-Py.
Las obligaciones de información a titulares, suscriptores o usuarios finales deberán regularse en las políticas y declaraciones de prácticas de los PCSC, cuando corresponda.

9.3. Confidencialidad de la información comercial

9.3.1. Alcance de la información confidencial

Se considerará información confidencial todo dato, documento, registro, antecedente o contenido , independientemente de su formato o medio de almacenamiento, perteneciente a la ACR-Py o a los participantes de la ICPP (incluyendo titulares de certificado, terceros relacionados, proveedores y auditores), que no esté clasificada como pública y cuyo acceso, uso, divulgación, modificación o destrucción no autorizada pueda comprometer la seguridad de la misma, la continuidad operativa, la confianza en los servicios, el cumplimiento normativo o los intereses legítimos de la ICPP.
Se consideran, a título enunciativo y no limitativo, como información confidencial:

a. Procedimientos y manuales internos no publicados;
b. Configuraciones de sistemas, arquitectura y controles de seguridad;
c. Información de seguridad de la información y gestión de riesgos;
d. Reportes técnicos no públicos y documentación de incidentes;
e. Informes de auditoría en su versión completa, incluyendo evidencias y hallazgos;
f. Registros internos, bitácoras y evidencias operativas;
g. Información de proveedores y contratos no públicos;
h. Datos de activación y material criptográfico, incluyendo claves privadas;
i. Planes de continuidad del negocio y recuperación ante desastres;
j. Planes y procedimientos de respuesta a incidentes;
k. Datos personales tratados en el marco de la ICPP que no sean de acceso público.
l. Otra información clasificada como confidencial.

El tratamiento de la información confidencial deberá realizarse de acuerdo con las políticas y controles de seguridad de la información establecidos por la ACR-Py, así como con las obligaciones legales y regulatorias aplicables.

9.3.2. Información excluida del alcance de la información confidencial

No se considerará información confidencial aquella que, por su naturaleza, finalidad o disposición normativa, deba ser de acceso público o se encuentre expresamente destinada a su publicación en el marco de la operación de la ICPP.

En particular, se consideran no confidenciales:

a. los certificados electrónicos emitidos, así como los datos contenidos en ellos, en la medida en que su publicación o disponibilidad sea requerida para el funcionamiento de los servicios de certificación;

b. las LCR/CRL y demás mecanismos de verificación de estado de certificados;

c. la información incorporada en repositorios públicos o directorios accesibles, limitada a aquella estrictamente necesaria conforme a los perfiles de certificados aplicables;

d. la información corporativa o personal que forme parte de certificados o publicaciones obligatorias, en el marco de la normativa vigente y con la finalidad de garantizar la interoperabilidad y confianza en la ICPP.

e. las Políticas de Certificación (PC) aplicables;

f. las Declaraciones de Prácticas de Certificación (DPC);

g. las políticas de seguridad (PS) en su versión pública;

h. los informes de auditoría en sus versiones resumidas o conclusiones, sin incluir evidencias, hallazgos detallados ni información sensible; y

i. información estadística agregada, ya sea en forma consolidada o segmentada por tipo de certificado o servicio, siempre que dicha información no permita la identificación de suscriptores, operaciones específicas ni la inferencia de información confidencial.

La determinación de la información no confidencial se realizará sin perjuicio del cumplimiento de las disposiciones legales aplicables en materia de protección de datos personales, seguridad de la información y demás normativa vigente.

9.3.3. Responsabilidad de proteger la información confidencial

La ACR-Py es responsable de implementar y mantener controles técnicos, organizativos y administrativos adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información confidencial, incluyendo los datos personales tratados en el marco de la ICPP, durante todo su ciclo de vida (recolección, acceso, uso, almacenamiento, transmisión y eliminación).

La ACR-Py define en el presente documento los principios y lineamientos aplicables a la protección de datos personales, asegurando su tratamiento conforme a la normativa vigente y a los principios de proporcionalidad, finalidad y seguridad de la información.

Los participantes de la ICPP que reciban, procesen o tengan acceso a información confidencial están obligados a:

a) Proteger dicha información mediante controles de seguridad adecuados;

b) Limitar su acceso exclusivamente a personal autorizado bajo el principio de necesidad de conocer;

c) Utilizar la información únicamente para los fines autorizados;

d) Evitar su divulgación a terceros no autorizados;

e) Implementar medidas para prevenir accesos, usos o divulgaciones no autorizadas.

Estas obligaciones deberán estar formalizadas mediante acuerdos contractuales, cláusulas de confidencialidad u otros instrumentos jurídicos equivalentes, cuando corresponda.

El incumplimiento de estas obligaciones dará lugar a las responsabilidades administrativas, civiles o penales previstas en la normativa aplicable, así como a las sanciones establecidas en los acuerdos correspondientes.

La ACR-Py podrá definir y mantener políticas, procedimientos y controles complementarios para reforzar la protección de la información confidencial y los datos personales.

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

La ACR-Py tratará los datos personales que resulten estrictamente necesarios para la emisión, administración, revocación, auditoría, control, trazabilidad, seguridad y continuidad de la certificación raíz, conforme a la normativa paraguaya vigente en materia de protección de datos personales, la Ley N.° 6822/2021, su reglamentación y la normativa técnica de la ICPP.

El tratamiento deberá observar los principios de licitud, finalidad determinada, proporcionalidad, minimización, exactitud, seguridad, confidencialidad, trazabilidad y limitación del plazo de conservación.

9.4.2. Información tratada como privada

Se considera información privada todo dato personal tratado por la ACR-Py que no esté destinado a su publicación, incluyendo los registros y documentación asociados a los servicios de certificación.

Dicha información será tratada como confidencial, salvo que exista obligación legal de divulgación o consentimiento expreso del titular.

9.4.3. Información no considerada privada

No se considera información privada aquella que deba ser publicada para el funcionamiento de la ICPP, incluyendo:

a) Datos contenidos en certificados electrónicos, en la medida en que su inclusión y divulgación resulte necesaria conforme a los perfiles de certificados aplicables y haya sido consentida por el titular;

b) Listas de certificados revocados (LCR/CRL);

c) Información disponible en repositorios o directorios públicos;

d) Documentación institucional en su versión pública.

9.4.4. Responsabilidad de proteger la información privada

La ACR-Py es responsable por la divulgación indebida de información confidencial, mediante la implementación de medidas de seguridad adecuadas, conforme a la legislación aplicable.

9.4.5. Aviso y consentimiento para usar información privada

Cuando el tratamiento de datos personales requiera información previa, aviso, consentimiento o cualquier otra base jurídica o documental suficiente, la ACR-Py dejará constancia de ello en la solicitud, expediente, acto, formulario, procedimiento o instrumento aplicable.
El titular del certificado, o su representante legal debidamente acreditado, podrá:

a) Acceder a sus datos personales;

b) Solicitar su corrección cuando corresponda;

c) Autorizar su divulgación a terceros.

Las autorizaciones podrán otorgarse a través de un canal de comunicación oficialmente establecido por la AA o de forma escrita, conforme a los mecanismos reconocidos por la ACR-Py.

9.4.6. Divulgación por proceso judicial o administrativo

La ACR-Py podrá divulgar información personal o confidencial cuando sea requerido por autoridad judicial o administrativa competente conforme a la normativa aplicable.
En tales casos, se adoptarán medidas para limitar la divulgación a la información estrictamente necesaria.

9.4.7. Otras circunstancias de divulgación de información

No aplica.

9.5. Derechos de propiedad intelectual

Los derechos de propiedad intelectual se rigen por la legislación vigente.

9.6. Declaraciones y garantías

9.6.1. Declaraciones y garantías de la ACR-Py

La ACR-Py declara y garantiza, dentro del alcance de su competencia como Autoridad Certificadora Raíz de la ICPP y conforme a la presente PC/DPC, que:
a) aplica procedimientos de identificación, autenticación, validación de autoridad, prueba de posesión de clave privada y verificación técnica antes de emitir certificados a PCSC, conforme a los ítems 3 y 4 de la presente PC/DPC;
b) emite certificados únicamente a PCSC habilitados conforme a la normativa aplicable, a los documentos ICPP y al acto administrativo correspondiente;
c) adopta medidas razonables para verificar que la información incorporada en los certificados emitidos por la ACR-Py sea consistente con las documentaciones verificadas al momento de la emisión;

d) emite certificados conforme a los perfiles técnicos aplicables, al RFC 5280, a la Recomendación ITU-T X.509, al DOC-ICPP-06 [3] y a los anexos técnicos de la presente PC/DPC;
e) mantiene disponible el repositorio oficial, los certificados publicados y las CRL/LCR emitidas por la ACR-Py, conforme a las condiciones de publicación, actualización y disponibilidad previstas en la presente PC/DPC;
f) revoca los certificados emitidos por la ACR-Py cuando se configuren las causales previstas en esta PC/DPC, en la normativa paraguaya aplicable, en los documentos ICPP o en decisión fundada de autoridad competente;
g) protege su clave privada raíz, material criptográfico, datos de activación, registros, evidencias y sistemas críticos conforme a los controles físicos, lógicos, criptográficos, procedimentales y de auditoría establecidos en esta PC/DPC; y
h) mantiene la presente PC/DPC en adecuación con la Ley N.º 6822/2021, el Decreto N.º 7576/2022, las resoluciones de la AA y los documentos ICPP aplicables.
Las declaraciones y garantías de la ACR-Py se limitan al alcance de sus funciones como Autoridad Certificadora Raíz de la ICPP. La ACR-Py no asume, por esta PC/DPC, las declaraciones, garantías u obligaciones propias de los PCSC respecto de los certificados finales, titulares, suscriptores, partes usuarias o servicios cualificados prestados bajo responsabilidad de dichos PCSC.

9.6.2. Declaraciones y garantías de la AR

No aplica.

9.6.3. Declaraciones y garantías del titular

El titular del certificado garantiza que:
a) La información proporcionada es completa y precisa;
b) Es responsable por los datos incluidos en su certificado;
c) Notificará sin demora cualquier compromiso de su clave privada y solicitará la revocación inmediata del certificado.

9.6.4. Declaraciones y garantías de la Parte Usuaria

La PU deberá:
a) negarse a utilizar el certificado para fines distintos a los previstos en la presente PC/DPC; y
b) verificar, en cualquier momento, la validez del certificado.
El certificado de la ACR-Py o de un PCSC se considera válido cuando:
a) haya sido emitido por la ACR-Py;
b) no figure en la última LCR/CRL de la ACR-Py;
c) no esté expirado; y
d) pueda ser verificado con el uso del certificado válido de la ACR-Py.
El uso o la aceptación de certificados sin observar las precauciones descritas corre por cuenta y riesgo del tercero que utilice o acepte el uso del certificado correspondiente.

9.6.5. Declaraciones y garantías de otros participantes

No aplica.

9.7. Exclusiones de garantía

No aplica.

9.8. Limitaciones de responsabilidad

La ACR-Py no responderá por los daños que no le sean imputables o a los que no haya dado causa, conforme a la legislación vigente.

9.9. Indemnizaciones

La ACR-Py será responsable por los daños directos que resulten de incumplimientos a la presente PC/DPC, a la normativa aplicable o a sus obligaciones como entidad de certificación, siempre que le sean imputables conforme a la legislación vigente.
Las responsabilidades de indemnización se determinarán conforme al marco legal aplicable y a los acuerdos contractuales que resulten de aplicación dentro de la ICPP.

9.10. Plazo y terminación

Este documento regula su propio plazo de vigencia y las condiciones de su terminación, así como los efectos de dicha terminación sobre la operación de la ACR-Py, la validez histórica de la información de certificación y la conservación de registros y evidencias.

9.10.1. Plazo

Este documento entra en vigencia conforme al acto administrativo aprobatorio correspondiente y se mantiene vigente hasta su modificación, sustitución, derogación o terminación formal dispuesta por la AA.

9.10.2. Terminación

La vigencia de este documento povdrá terminar por:

a) sustitución por una nueva versión aprobada por la AA;
b) derogación o reemplazo formal;
c) terminación, sustitución o reconfiguración institucional de la ACR-Py;
d) modificación del marco normativo que haga necesaria su sustitución integral; o
e) cualquier otra decisión válida adoptada por la AA conforme al marco jurídico aplicable.

9.10.3. Efectos de la terminación y supervivencia

La terminación de este documento no extingue, por sí sola, las obligaciones de:

a) conservación de registros, evidencias, certificados y CRL/LCR;
b) preservación de la validez histórica de la información de certificación;
c) tratamiento de incidentes, controversias o actuaciones pendientes;
d) control institucional, supervisión, evaluación de conformidad y auditoría; y
e) demás obligaciones cuya naturaleza exija subsistencia posterior.

9.11. Notificaciones individuales y comunicaciones con los participantes

Las notificaciones, intimaciones, solicitudes o cualquier otra comunicación necesaria sujeta a las prácticas descritas en la presente PC/DPC se realizarán, preferentemente, por correo electrónico firmado con un certificado electrónico cualificado, o, en su imposibilidad, por oficio de la autoridad competente o por publicación en su repositorio público.

9.12. Enmiendas

9.12.1. Procedimiento para enmiendas

Toda modificación a la presente PC/DPC deberá ser aprobada por el MIC, conforme al procedimiento administrativo y documental aplicable.
La ACR-Py podrá proponer modificaciones a la presente PC/DPC cuando resulte necesario por cambios normativos, técnicos, criptográficos, operativos, de seguridad, interoperabilidad, auditoría, gestión de riesgos o mejora continua de la ICPP.

9.12.2. Mecanismo y período de notificación

Las modificaciones se notificarán mediante publicación en el repositorio oficial y, cuando corresponda, comunicación directa a los participantes afectados.

9.12.3. Circunstancias en las que debe cambiarse el OID

El OID de la PC/DPC o de una política de certificación deberá cambiarse cuando una modificación altere materialmente el nivel de garantía, alcance, uso permitido, comunidad de aplicación, requisitos de identificación, perfil de certificado, controles criptográficos, obligaciones de los participantes o condiciones de confianza.
No requerirán cambio de OID las modificaciones editoriales, aclaratorias o de mejora que no alteren el nivel de garantía ni el alcance de la política. Toda decisión de mantener o cambiar el OID deberá estar documentada y aprobada por la AA.

9.13. Disposiciones de resolución de controversias

Los litigios derivados de la presente PC/DPC se resolverán conforme a la **legislación vigente**.

9.14. Ley aplicable

La presente PC/DPC se rige por la legislación de la República del Paraguay, en particular la Ley N.° 6822/2021 y su Decreto Reglamentario N.° 7576/2022, la legislación que las modifique o sustituya, así como las demás leyes y normas vigentes en el Paraguay.

9.15. Cumplimiento de la ley aplicable

La ACR-Py se encuentra sujeta al marco jurídico paraguayo y deberá cumplir las obligaciones legales, regulatorias, técnicas y de seguridad que le resulten aplicables.

9.16. Disposiciones varias

9.16.1. Integridad normativa del documento

La presente PC/DPC representa las obligaciones y deberes aplicables a la ACR-Py. En caso de conflicto entre esta PC/DPC y otras resoluciones de la AA, prevalecerá siempre la última emitida.

9.16.2. Cesión

Los derechos y obligaciones vinculados a la certificación raíz no podrán cederse sin decisión válida de la Autoridad de Aplicación y preservación de la confianza de la ICPP.
Los derechos y obligaciones previstos en la presente PC/DPC son de orden público e intransferibles, no pudiendo ser cedidos ni transferidos a terceros.

9.16.3. Divisibilidad o independencia de disposiciones

La invalidez, nulidad o ineficacia de cualquiera de las disposiciones de la presente PC/DPC no afectará las demás disposiciones, las cuales permanecerán plenamente válidas y eficaces. En tal caso, la disposición inválida, nula o ineficaz se considerará como **no escrita**, de forma que esta PC/DPC se interpretará como si no contuviera dicha disposición, manteniendo, en la medida de lo posible, la intención original de las disposiciones remanentes.

9.16.4. Ejecución

Conforme a la legislación vigente.

9.16.5. Fuerza mayor

La ACR-Py no será responsable por eventos de fuerza mayor o caso fortuito ajenos a su control razonable, sin perjuicio de activar medidas de continuidad y comunicación.

9.17. Otras disposiciones

No aplica.

10. DOCUMENTOS REFERENCIADOS DE LA ICPP

Los documentos abajo enumerados son aprobados por Resolución Ministerial del MIC o por el acto administrativo que corresponda, pudiendo ser modificados mediante el mismo instrumento legal o por el mecanismo formal que establezca la AA.

Ref.	Documento	Código
[1]	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
[2]	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
[3]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[4]	Política Tarifaria	DOC-ICPP-13

11. REFERENCIAS JURÍDICAS, TÉCNICAS Y BIBLIOGRÁFICAS

11.1. Marco jurídico nacional

a. Constitución Nacional de la República del Paraguay.

b. Ley N.º 6822/2021, "De los Servicios de Confianza para las Transacciones Electrónicas, del Documento Electrónico y los Documentos Transmisibles Electrónicos".

c. Decreto N.º 7576/2022, reglamentario de la Ley N.º 6822/2021.

d. Ley N.º 6715/2021, "De Procedimientos Administrativos".

e. Ley N.º 1294/1998, "De Marcas".

f. Ley N.º 1328/1998, "De Derecho de Autor y Derechos Conexos".

g. Ley N.º 7593/2025, "De Protección de Datos Personales en la República del Paraguay".

h. Resoluciones y actos administrativos dictados por la AA en el ámbito de la ICPP.

11.2. Estándares técnicos PKI

a. RFC 3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

b. RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile, y sus actualizaciones aplicables.

c. RFC 2986 — PKCS #10: Certification Request Syntax Specification.

d. RFC 9810 — Certificate Management Protocol.

e. RFC 4211 — Certificate Request Message Format, actualizado por RFC 9045.

f. RFC 9811 — HTTP Transfer for CMP.

g. Recomendación ITU-T X.509 / ISO/IEC 9594-8 — The Directory: Public-key and attribute certificate frameworks.

h. Recomendación ITU-T X.501 / ISO/IEC 9594-2 — The Directory: Models.

i. Recomendación ITU-T X.520 / ISO/IEC 9594-6 — The Directory: Selected attribute types.

j. Recomendación ITU-T X.680 / ISO/IEC 8824-1 — Abstract Syntax Notation One (ASN.1): Specification of basic notation.

k. Recomendación ITU-T X.690 / ISO/IEC 8825-1 — ASN.1 encoding rules: BER, CER and DER.

11.3. Estándares ETSI/eIDAS

a. Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior — eIDAS.

b. Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, por el que se modifica el Reglamento (UE) N.º 910/2014 en lo relativo al establecimiento del Marco Europeo de Identidad Digital — comúnmente denominado eIDAS 2.0.

c. ETSI EN 319 401 — General Policy Requirements for Trust Service Providers.

d. ETSI EN 319 411-1 — Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

e. ETSI EN 319 411-2 — Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

f. Serie ETSI EN 319 412 — Certificate Profiles, partes aplicables.

g. ETSI TS 119 612 — Trusted Lists.

h. ETSI EN 319 403-1 — Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

11.4. Auditoría, seguridad y criptografías

a. WebTrust Principles and Criteria for Certification Authorities, versión vigente aplicable.

b. WebTrust for CA/Browser Forum Baseline Requirements, versión vigente aplicable.

c. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, versión vigente aplicable.

d. CA/Browser Forum Network and Certificate System Security Requirements, versión vigente aplicable.

e. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements.

f. ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls.

g. ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

h. ISO 21188:2018 — Public key infrastructure for financial services — Practices and policy framework.

i. FIPS 140-3 — Security Requirements for Cryptographic Modules.

j. Common Criteria / ISO/IEC 15408:2022 — Evaluation criteria for IT security, y perfiles de protección aplicables a dispositivos criptográficos, cuando corresponda.

11.5. Referencias comparadas

a. Documentos rectores de ICP-Brasil aplicables a la AC Raíz, especialmente DOC-ICP-01.

b. Repositorio público de la FNMT-RCM, incluyendo Declaraciones de Prácticas de Certificación, certificados raíz, declaración de conformidad y normativa publicada.

Las referencias técnicas no desplazan la prevalencia del marco jurídico paraguayo ni modifican automáticamente la presente PC/DPC o el DOC-ICPP-06 [3].

ANEXO I. PERFIL DEL CERTIFICADO ELECTRÓNICO RAÍZ

I.1. Características generales

El certificado electrónico raíz de la ACR-Py es un certificado autofirmado que constituye el ancla superior de confianza de la ICPP. Se ajusta al perfil X.509 v3, al RFC 5280, a esta PC/DPC y al DOC-ICPP-06 [3].

I.2. Campos y extensiones mínimas

Campo / extensión	Obligatorio	Criticidad	Valor / restricción
Versión	Sí	N/A	X.509 v3
Número de serie	Sí	N/A	Valor único, positivo y no reutilizable
Emisor	Sí	N/A	Debe identificar inequívocamente a la ACR-Py
Sujeto	Sí	N/A	Debe coincidir con el Emisor
Validez	Sí	N/A	Hasta veinte (20) años, salvo decisión fundada de la AA
Subject Public Key Info	Sí	N/A	Clave pública generada conforme al DOC-ICPP-06 [3]
Signature Algorithm	Sí	N/A	Conforme al DOC-ICPP-06 [3]
Basic Constraints	Sí	Crítico	cA=TRUE; pathLenConstraint=1
Key Usage	Sí	Crítico	keyCertSign, cRLSign
Subject Key Identifier	Sí	No crítico	Derivado de la clave pública del certificado raíz
Authority Key Identifier	Sí	No crítico	Consistente con el SKI del certificado raíz
Certificate Policies	Sí	No crítico	OID 1.3.6.1.4.1.64751.1.1, salvo OID específico aprobado por la AA
CRL Distribution Points	Sí	No crítico	URL=https://www.acraiz.gov.py/arl/arl_v2/ac_raiz_py_v2.crl
Authority Information Access	No	N/A	No se incorpora como requisito general
Extended Key Usage	No	N/A	No se incorpora
Name Constraints	No	N/A	No se incorpora salvo decisión expresa de la AA
QCStatements	No	N/A	No aplica

I.3. Composición del DN o nombre distinguido del certificado raíz

Identifica a la ACR-Py

C = PY

O = ICPP
OU = Ministerio de Industria y Comercio
CN = Autoridad Certificadora Raíz del Paraguay v2

Nota: v: versión y el valor numérico que debe corresponder a la última versión a emitir

I.4. Punto de distribución de CRL/LCR

El valor de referencia será: URL=https://www.acraiz.gov.py/arl/ac_raiz_pyv2.crl

I.5. Uso permitido

El certificado raíz solo podrá utilizarse como ancla superior de confianza de la ICPP y para verificar certificados y CRL/LCR emitidos por la ACR-Py.

I.6. Uso prohibido

El certificado raíz no podrá utilizarse para firma directa de documentos electrónicos, transacciones, actuaciones administrativas, certificados de usuarios finales ni servicios distintos de la certificación raíz.

ANEXO II. PERFIL DE CERTIFICADOS ELECTRÓNICOS EMITIDOS A PCSC

II.1. Características generales

Los certificados emitidos por la ACR-Py a los PCSC son certificados de autoridad de certificación subordinada dentro de la ICPP y se ajustan a X.509 v3, RFC 5280, al alcance de habilitación otorgado por la AA y al DOC-ICPP-06 [3].

II.2. Campos y extensiones mínimas

Campo / extensión	Obligatorio	Criticidad	Valor / restricción
Versión	Sí	N/A	X.509 v3
Número de serie	Sí	N/A	Valor único, positivo y no reutilizable
Emisor	Sí	N/A	Debe identificar a la ACR-Py conforme al Anexo I
Sujeto	Sí	N/A	Debe identificar al PCSC titular conforme a información validada
Validez	Sí	N/A	Hasta diez (10) años, sin exceder la vigencia admitida por la AA
Subject Public Key Info	Sí	N/A	Clave pública del PCSC conforme al DOC-ICPP-06 [3]
Signature Algorithm	Sí	N/A	Conforme al DOC-ICPP-06 [3]
Basic Constraints	Sí	Crítico	cA=TRUE; pathLenConstraint=0
Key Usage	Sí	Crítico	keyCertSign, cRLSign

Subject Key Identifier	Sí	No crítico	Derivado de la clave pública del PCSC
Authority Key Identifier	Sí	No crítico	Referencia a la clave pública de la ACR-Py
Certificate Policies	Sí	No crítico	OID 1.3.6.1.4.1.64751.1.1, salvo OID específico aprobado por la AA
CRL Distribution Points	Sí	No crítico	Al menos una URI HTTPS bajo dominio oficial de la ACR-Py. Valor de referencia: URL=https://www.acraiz.gov.py/arl/arl_v2/ac_raiz_py_v2.crl
Authority Information Access	Condicional	No crítico	Solo caIssuers; no incluirá id-ad-ocsp en el nivel de la ACR-Py
Extended Key Usage	No	N/A	No se incorpora salvo decisión expresa de la AA
Name Constraints	No	N/A	No se incorpora salvo decisión expresa de la AA

II.3. Composición del nombre distinguido del PCSC

Identifica al PCSC

C = PY

O = ICPP

OU = [denominación que debe coincidir con el Nombre o Razón Social del PCSC validado con cédula tributaria expedida por la DNIT]

SERIALNUMBER = RUC80080001-7 (**Nota:** número de RUC que debe coincidir con cédula tributaria expedida por la DNIT, incluyendo **-** dígito verificador)

CN = Autoridad Certificadora denominación autorizada del PCSC **v3** (**Nota**: v: versión y el valor numérico que debe corresponder a la última versión a emitir)

II.4. Aclaración sobre Certificate Policies

A efectos de la extensión Certificate Policies de certificados emitidos por la ACR-Py a PCSC, el OID 1.3.6.1.4.1.64751.1.1 identifica la política aplicable bajo el DOC-ICPP-01, salvo OID específico aprobado por la AA.

II.5. Uso permitido

El certificado emitido a un PCSC solo podrá utilizarse para la función de autoridad de certificación subordinada dentro de la ICPP y dentro del alcance de la habilitación otorgada por la AA.

II.6. Uso prohibido

El certificado emitido a un PCSC no podrá utilizarse para fines distintos de los autorizados, crear niveles adicionales de certificación ni emitir certificados fuera del alcance de su habilitación.

ANEXO III. PERFIL DE CRL/LCR Y NO APLICABILIDAD DE OCSP EN RAÍZ

III.1. Perfil de CRL/LCR

Las CRL/LCR emitidas por la ACR-Py se ajustan al perfil X.509 v2 CRL previsto en el RFC 5280 y al DOC-ICPP-06 [3].

III.1.1 Campos básicos de la CRL/LCR

Campo	Obligatorio	Criticidad	Valor / restricción
Versión	Sí	N/A	X.509 v2 CRL
Signature Algorithm	Sí	N/A	Conforme al DOC-ICPP-06 [3]
Issuer	Sí	N/A	Debe identificar a la ACR-Py
thisUpdate	Sí	N/A	Fecha y hora de emisión de la CRL/LCR
nextUpdate	Sí	N/A	No posterior a noventa (90) días desde thisUpdate
Entradas de certificados revocados	Condicional	N/A	Se incorporan cuando existan certificados revocados

III.1.2. Extensiones de la CRL/LCR

Extensión	Obligatorio	Criticidad	Valor / restricción
CRL Number	Sí	No crítico	Numeración creciente, única y no reutilizable
Authority Key Identifier	Sí	No crítico	Identifica la clave emisora de la ACR-Py
Delta CRL Indicator	No	N/A	No se utiliza
Freshest CRL	No	N/A	No se utiliza

III.1.3. Campos de entrada de certificados revocados

Cuando existan certificados revocados, cada entrada de la CRL/LCR deberá contener, como mínimo:

Campo de entrada	Obligatorio	Criticidad	Valor / restricción
Serial Number de certificado revocado	Si	N/A	Debe identificar el certificado revocado
Revocation Date	Si	N/A	Fecha efectiva de revocación

III.1.4. Extensiones de entrada de certificados revocados

Extensión de entrada	Obligatorio	Criticidad	Valor / restricción
Invalidity Date	Condicional	No crítico	Cuando corresponda

CRL Reason / Reason Code	Condicional	No crítico	Cuando corresponda según la causa de revocación

III.2. Frecuencia, latencia y publicación de CRL/LCR

La ACR-Py emite CRL/LCR ordinaria como máximo cada noventa (90) días y siempre antes de la expiración de la CRL/LCR vigente. La CRL/LCR extraordinaria se emite ante revocación, incidente o circunstancia relevante. La publicación se realiza conforme a los numerales 4.9.7, 4.9.8 y 4.10.

III.3. No aplicabilidad de OCSP en raíz

OCSP no aplica como servicio operativo de verificación de estado en el nivel de la ACR-Py. El estado se verifica exclusivamente mediante CRL/LCR publicadas en el repositorio oficial.

ANEXO IV. CEREMONIA DE GENERACIÓN DE CLAVE RAÍZ

IV.1. Regla general

Toda generación, activación, respaldo, recuperación, sustitución, cambio de clave, destrucción o intervención crítica sobre material criptográfico de la ACR-Py se realiza mediante ceremonia criptográfica formalmente documentada o procedimiento equivalente aprobado.

IV.2. Controles previos a la ceremonia

Antes de iniciar la ceremonia se verifican autorización institucional, objeto, versiones aplicables del DOC-ICPP-01 y DOC-ICPP-06 [3], perfil técnico, intervinientes, módulo criptográfico, entorno físico y documentación de respaldo.

IV.3. Controles mínimos durante la ceremonia

La ceremonia deberá contemplar roles de confianza, control multiparte 3 de 5, entorno offline o aislamiento equivalente, uso de módulo criptográfico conforme al DOC-ICPP-06 [3], controles físicos y lógicos reforzados y registro de eventos.

IV.4. Evidencia mínima de la ceremonia

La ACR-Py conservará actas que incluyan, al menos: fecha y hora, objeto, intervinientes, roles, versiones documentales aplicables, identificación del módulo criptográfico, resultado, incidencias y evidencias técnicas complementarias.

IV.5. Cierre, custodia y publicación posterior

Al cierre se verifica el resultado, se resguarda el material criptográfico y los datos de activación, se conservan evidencias, se actualizan registros y se publica la información de certificación que corresponda.

IV.6. Requisitos ampliados de evidencia de ceremonia

Toda ceremonia criptográfica de la ACR-Py deberá contar con guion aprobado, versión controlada, lista de intervinientes, roles, autorización (Aprobación del Responsable de Seguridad/Notificación o Resolución interna de aprobación previa u otros), identificación de HSM, identificación de medios, perfil de certificado o CRL/LCR aplicable, parámetros criptográficos, checklist (previo, de ejecución, de cierre) y acta final.

La evidencia mínima incluirá:
a) autorización correspondiente;
b) objeto y alcance de la ceremonia;
c) fecha, hora de inicio y fin;
d) lugar de realización y nivel físico de seguridad;
e) identificación de participantes, roles y verificación de documentos de identidad;
f) identificación de HSM, tokens, medios y componentes utilizados;
g) versiones de software, firmware, u otros componentes críticos utilizados como ser: scripts, perfiles, plantillas y parámetros;
h) resultado de la operación realizada (generación, emisión, respaldo, restauración, destrucción o publicación);
i) incidentes, desviaciones y acciones correctivas;
j) firmas de participantes y testigos;
k) evidencia audiovisual cuando la AA lo determine; y
l) custodia posterior de actas, medios, respaldos, tokens y registros.

Ninguna ceremonia podrá considerarse cerrada hasta que se haya verificado la integridad del resultado, la correspondencia con el perfil aplicable, la desactivación del material criptográfico, el resguardo de datos de activación y la conservación de evidencias.